Proceedings of
WInnComm- Europe 2014
Wireless Innovation European Conference on Wireless Communications Technologies and Software Defined Radio
4-6 November 2014, Rome, Italy

Edited by: Lee Pucker, Claudio Armani, Stephanie Hamill

Event host and Platinum Sponsor:

WInnComm-Europe 2014 Organization

Conference Chair:
Claudio Armani, *Selex ES*

Thank you to our Technical Program Committee:

Marc Adrat, *Fraunhofer-Institut*
Anwer Al-Dulaimi, *Ryerson University*
Onur Altintas, *Toyota*
Claudio Armani, *Selex ES*
Fabio Casalino, *Selex ES*
David Chester, *Harris Corporation*
Francois Delaveau, *Thales*
Antonio Di Rocco, *Selex ES*
Ismael Gomez, *CTVR*
Wolfgang Koenig, *Alcatel Lucent*
Vincent Kovarik, *PrismTech*
Ruediger Leschhorn, *Rohde & Schwarz*
Fa-Long Luo, *Element CXI*
Dania Marabissi, *Universita degli Studi di Firenze*
James Neel, *Cognitive Radio Technologies*
David Renaudeau, *Thales*
Charles Sheehe, *NASA*
Sarvpreet Singh, *Fraunhofer-Institut*
Rahul Sinha, *Tata Consultancy Services*
Chayil Timmerman, *MIT Lincoln Laboratory*
Manuel Uhm, *Coherent Logix, Inc*.
Gerald Ulbricht, *Fraunhofer-Institut*
Bill Xenakis, *Aviacomm Inc*

Table of Contents

NOVEL TRANSFORMATIONS OF EXTRINSIC INFORMATION APPLIED TO INNOVATIVE BICM-ID RECEIVERS: FUNDAMENTALS AND LIMITS

M. Adrat, T. Osten, M. Tschauner, M. Antweiler
Fraunhofer Institute for Communication,
Information Processing and Ergonomics FKIE
53343 Wachtberg, Germany
marc.adrat@fkie.fraunhofer.de

J. Lewandowsky
University of Federal Armed Forces Munich
85579 Neubiberg, Germany
j.lewandowsky@unibw.de

ABSTRACT

In this paper we propose a novel idea to increase the applicability of *Bit Interleaved Coded Modulation with Iterative Decoding* (BICM-ID) to legacy waveforms. One essential design parameter of BICM-ID receivers with respect to the error correcting capabilities is the symbol mapping of the digital modulation scheme. For instance, a so-called *Semi-Set Partitioning* (SSP) symbol mapping is well known to provide higher stepwise gains in robustness in every iteration than a *Gray encoded* symbol mapping.
The novel approach is based on the idea to make in a first step in BICM-ID the deliberately false assumption that a well performing symbol mapping has been used at the transmitter, even though in reality a less powerful symbol mapping was applied. In a second step, the mismatch in both symbol mappings is compensated by a novel innovative *transformation of extrinsic information*.
After having explained the novel idea in more detail, in this paper we will introduce the fundamentals of the required novel signal processing. In addition, we will present some first simulation results which demonstrate the best possible theoretically achievable performance gains.

1. INTRODUCTION

The key motivation for this research project is the assumption that in the future established legacy radios as well as modern *Software Defined Radios* (SDRs) will operate together in the same mission. Our objective is to provide the operator of an SDR an added value if compared to the operator of the legacy radio even if both are using the same waveform. This added value can be expressed in, e.g., an increased robustness of the waveform and thus, in an increased communication range. In order not to impair the interoperability on the air interface with the established legacy radios in mixed mode, the actions to be taken should be applied primarily on the receiver side.

It has already been analyzed in a preliminary study [1], whether a so-called *Bit Interleaved Coded Modulation with Iterative Decoding* (BICM-ID) [2] receiver structure alone can provide the desired profits. Such a receiver is characterized in that the decoding result of the error protection mechanism is fed back to the demodulator in the form of reliability information (so-called *extrinsic information*). The latter one can exploit this extra knowledge to improve its initial detection result. By multiple, iterative exchanges of reliability information between demodulation as well as error protection significant gains can be achieved in case of an appropriate parameterization of the error protection as well as the modulation schemes.
The preliminary studies [1] showed that it is not possible to achieve any gain by means of BICM-ID [2] when a *Gray encoded* symbol mapping is used in modulation. Around the turn of the millennium X. Li *et. al.* [3] have already shown that when using a so-called *Semi Set Partitioning* (SSP) symbol mapping significant gains in *Bit Error Rate* (BER) performance can be realized. But, this assumes that the SSP symbol mapping is used on both ends of the communication scheme, the transmitting and receiving end. However, the established legacy radios, to which interoperability is to be maintained, usually use a *Gray encoded* symbol mapping which is optimal for non-iterative receiver structures.
As part of the research project it was now investigated whether it is possible to realize gains in robustness by an innovative BICM-ID receiver structure even for still applying a *Gray encoded* symbol mapping at the transmitter. The basic idea is to make the deliberately false assumption in the demodulation that at the transmitting end a (modified) SSP symbol mapping was used. This deliberately false assumption is corrected again in a subsequent novel *transformation of extrinsic information*.
In this paper, it will be shown by using a representative example that a round-trip transformation between a *Gray encoded* symbol mapping as well as a (modified) SSP

symbol mapping exists. A particular challenge is that these transformations are not at the bit level (i.e., in GF (2), *Galois Field*), but work with reliability information (i.e., so-called *Log-Likelihood Ratios* (LLRs or *L*-values) in the set of real numbers $\mathbb{R}$). It will then be demonstrated in the context of a boundary experiment that in case of *Error-Free Feedback* (EFF) from the error protection mechanism to demodulation significant gains can theoretically be realized. However, so far these gains could not be obtained by simulation with the first practical implementation.

3. TRANSMISSION SYSTEM WITH BICM-ID

Figure 1 shows the block diagram of a transmission system employing *Bit Interleaved Coded Modulation with Iterative Decoding* (BICM-ID).

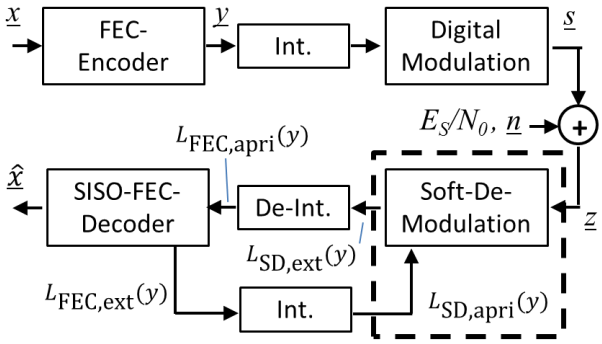


Figure 1: Block Diagram of a Transmission System with *Bit Interleaved Coded Modulation with Iterative Decoding* (BICM-ID)

Let us assume that a binary random source generates a sequence $\underline{x}$ of N bits $x \in \{0,1\}$. A channel encoder (*forward error correction*, FEC) of rate r adds redundancy which can be exploited at the receiving end of the communication scheme for error correction. The channel encoded sequence $\underline{y}$ is then bit-interleaved. Digital modulation of order M maps $ld\ M$ consecutive bits of the bit-interleaved sequence into a sequence $\underline{s}$ of symbols s.

After transmission of the individual symbols s over an *Additive White Gaussian Noise* (AWGN) channel with known channel quality E_S/N_0, a sequence $\underline{z}$ of noisy elements $z \in \mathbb{R}$ is received. E_S is the mean energy per symbol s and $N_0/2$ the single-sided noise power spectral density of the AWGN.

The aim of the BICM-ID receiver is to recover the originally sent bits x as good as possible from the received sequence $\underline{z}$. For this purpose, the inner component of the iterative process, i.e. *Soft-Demodulation* (SD), determines so-called *extrinsic information* in terms of L-values $L_{SD,ext}(y)$ individually for each coded bit y. Please notice, that the sign of these L-values indicates the binary *hard-decision* in bi-polar format (i.e. a logical *0* becomes a bi-polar *+1* and a logical *1* becomes a bi-polar *-1*) while the magnitude represents the reliability. Thus, the L-values can take any real value $L(y) \in \mathbb{R}$.

After de-interleaving the L-values $L_{SD,ext}(y)$ of soft-demodulation become *a priori* input knowledge $L_{FEC,apri}(y)$ for the *Soft-Input/Soft-Output* (SISO) FEC-Decoder. On the one hand, the SISO-FEC-Decoder can provide the hard decoded estimate x for the possibly send data bit x. On the other hand, the SISO-FEC-Decoder can provide its decoding gain in terms of $L_{FEC,ext}(y)$, or the interleaved counterpart $L_{SD,apri}(y)$, as *a priori* knowledge to *soft-demodulation*. This new extra information helps *soft-demodulation* to refine the original L-values $L_{SD,ext}(y)$. In case of a proper configuration of the system parameters, several iterations can provide reliability gains such that the number of residual bit errors in $\underline{x}$ decreases steadily.

The comparison of the originally sent sequence $\underline{x}$ and its estimated reconstruction $\underline{\hat{x}}$ allows to determine the *Bit Error Rate* (BER) as a function of the channel quality E_S/N_0.

3.1. Simulation Examples

Figure 3 shows the simulation examples for two different configurations of system parameters. In both examples, a terminated convolution code of rate $r=3/4$ with generator polynomial $G(133,171)_8$ and puncturing pattern (1,1,0; 1,0,1) is used to encode a sequence $\underline{x}$ of $N=894$ bits (plus *6* bits for termination). In addition, in both examples 8-PSK (*Phase Shift Keying*) is used for *digital modulation*. The key difference between both examples is the *symbol mapping* which is used in *digital modulation*.

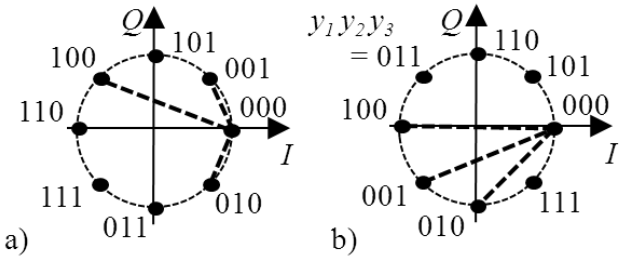


Figure 2: 8-PSK Signal Constellation Sets with
a) Gray encoded Symbol mapping
b) (modified)[1] SSP symbol mapping

On the one hand, a *Gray encoded* symbol mapping is used (see Fig. 2a). On the other hand, a (modified)[1] SSP symbol mapping is applied (see Fig. 2b). It can clearly be seen in the simulation results that both system configurations provide different BER-over-E_S/N_0 behavior. A system design with a *Gray encoded* symbol mapping works best if no iterations are carried out, i.e. if soft-demodulation and

[1] The SSP symbol mapping used here is not identical to the one proposed in [3], but offers the same *Harmonic Mean* $d_h^{SSP} = 2.877$.

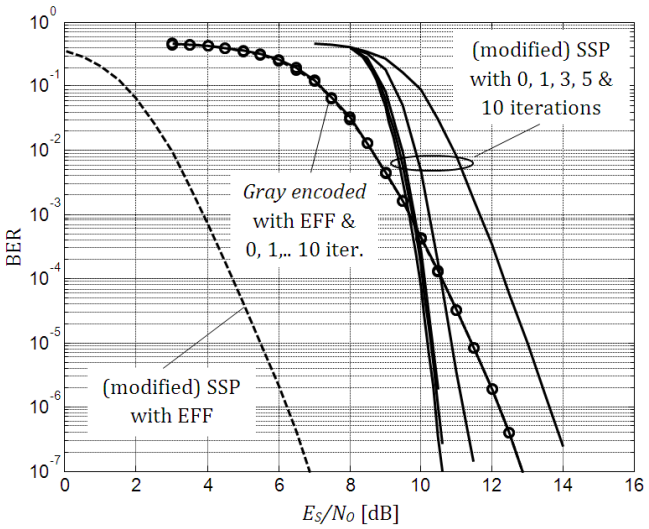


Figure 3: Bit Error Rate (BER) curves for BICM-ID receivers with different symbol mappings

SISO-FEC-decoding are realized only once. However, with a *Gray encoded* symbol mapping no noteworthy gains in BER can be realized by higher numbers of iteration. The BER performance remains the same for different numbers of iteration. In contrast, significant gains in BER can be realized by several iterations if a (modified) SSP symbol mapping is applied. The dashed-curve illustrates the best possible performance in case of *Error-Free Feedback* (EFF) of reliability information from the SISO-FEC-decoder to the *soft-demodulator*.

4. NOVEL IDEA WITH TRANSFORMATION OF EXTRINSIC INFORMATION

Obviously, a BICM-ID receiver with a (modified) SSP symbol mapping provides a much better BER behavior than a receiver with a *Gray encoded* symbol mapping. One of the reasons is a higher so-called *Harmonic Mean* d_h [3]. The *Harmonic Mean* is a measure which is related to the EFF case. It determines a measure for the average *Euclidean Distance* between those signal constellation points which differ in exactly one bit position. The dashed lines in Fig. 2 illustrate an example for the symbol mapping *000*. It can be seen that on average the distances are higher for the (modified) SSP symbol mapping if compared to the *Gray encoded* symbol mapping. Thus, the question arises if we can exploit the higher *Harmonic Mean* of a BICM-ID receiver with a (modified) SSP symbol mapping even if a *Gray encoded* symbol mapping is used at the transmitter ($d_h^{\mathrm{SSP}} = 2.877$ is greater than $d_h^{\mathrm{GRAY}} = 0.809$).

Our novel innovative idea tries to exploit the higher *Harmonic Mean* d_h of a (modified) SSP symbol mapping on communication links where actually *Gray encoded* symbol mappings are used. For that purpose, we make the deliberately false assumption in the *soft-demodulation* that at the transmitting end a (modified) SSP symbol mapping was used. This deliberately false assumption is corrected again in a subsequent novel *transformation of the extrinsic information* from $L_{\mathrm{SD,ext}}^{\mathrm{SSP}}\ y$ to $L_{\mathrm{SD,ext}}^{\mathrm{GRAY}}\ y$. The respective *inverse transformation* needs to be applied to the reliability information $L_{\mathrm{SD,apri}}^{\mathrm{GRAY}}(y)$ (becomes $L_{\mathrm{SD,apri}}^{\mathrm{SSP}}(y)$), which is fed back from the SISO-FEC-decoder.

Figure 3 illustrates the signal processing blocks which need to be replaced in the overall block diagram shown in Fig. 1.

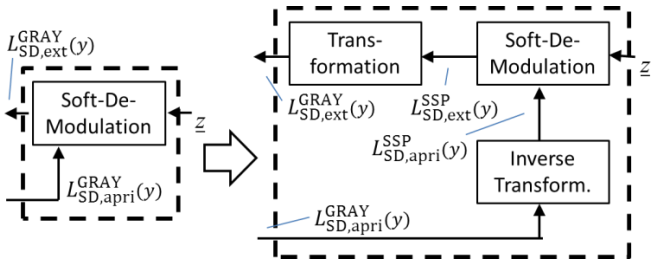


Figure 4: Soft-Demodulation with additional Transformations at Input and Output

4.1. Transformations in case of Hard-Decision Decoding

In order to simplify matters and to improve comprehensibility of the new proposed scheme with *Transformations of Extrinsic Information*, let us start with the extreme case of *Hard-Decision* decoding. In that case we can focus on the coded bits $y \in \{0,1\}$ instead of considering the reliability values $L\ y \in \mathbb{R}$. The transfer of our considerations to these *L*-values will follow in Section 4.2.

If we want to use a (modified) SSP symbol mapping in *soft-demodulation* even though a *Gray encoded* symbol mapping was used at the transmitter, the *Transformation* block in Fig. 3 needs to realize the mapping between both domains. In case of *hard-decision* decoding this can simply be done by matrix operations in GF(2), e.g.,

$$y_{GRAY} = y_{SSP} \cdot \begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{matrix} . \qquad (1)$$

For instance, the symbol mapping $y_{SSP} = (101)$ (see Fig. 2b) becomes $y_{GRAY} = 001$ (see Fig. 2a). Thus, the matrix on the right hand side of Eq. (1) can be used to transform symbol labels from the SSP domain in the *Gray encoded* domain. It is easy to prove that the inverse is given by

$$y_{SSP} = y_{GRAY} \cdot \begin{matrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{matrix} . \qquad (2)$$

Thus, as a first important intermediate result we can conclude that a transformation between both domains exists in case of *hard-decision* decoding.

4.2. Transformations in case of Soft-Decision Decoding

However, BICM-ID receivers are based on *Soft-Decision* Decoding. That means reliability information in terms of *L*-values is exchanged between the soft-demodulation and SISO-FEC-decoding components. In conclusion, simple matrix computations like in Eqs. (1) and (2) cannot be used to transform from the SSP domain into the *Gray encoded* domain and vice versa.

4.2.1 The box-plus Operator $\boxplus$

However, techniques which are well known from Turbo-decoding of linear block codes can be applied. In [4] J. Hagenauer *et al.* have introduced the so-called *box-plus* operation $\boxplus$. The *box-plus* operation $\boxplus$ is defined as

$$L\ x_A \otimes x_B\ = L\ x_A\ \boxplus L\ x_B\ = \log\frac{1+e^{L\ x_A\ +L(x_B)}}{e^{L\ x_A\ }+e^{L\ x_B}} \quad (3)$$

and determines the reliability value for the combination of two *L*-values. Simply speaking, applying the *box-plus* operation "$\boxplus$" to *L*-values corresponds to the XOR-combination "$\otimes$"of binary values. Thus, Eq. (1) becomes (the lower index "SD,ext" is skipped to enhance readability)

$$\begin{aligned} L^{\mathrm{GRAY}}\ y_1\ &= L^{\mathrm{SSP}}\ y_1\ \boxplus L^{\mathrm{SSP}}\ y_3 \\ L^{\mathrm{GRAY}}\ y_2\ &= L^{\mathrm{SSP}}\ y_1\ \boxplus L^{\mathrm{SSP}}\ y_2\ \boxplus L^{\mathrm{SSP}}\ y_3 \\ L^{\mathrm{GRAY}}\ y_3\ &= L^{\mathrm{SSP}}\ y_2\ \boxplus L^{\mathrm{SSP}}\ y_3 \end{aligned} \quad (4)$$

in case of soft-decision decoding. Eq. (4) determines the set of equations which need to be applied to the *L*-values in order to perform the transformation from the SSP domain into the *Gray encoded* domain.

4.2.2 The box-minus Operator $\boxminus$

For the inverse transformation we need another operator which was at first introduced by T. Clevorn *et al.* [5] as *box-minus* operator $\boxminus$. This *box-minus* operator $\boxminus$ is defined as

$$L\ x_A\ \boxminus L\ x_B\ = \log\frac{1-e^{L\ x_A\ +L\ x_B}}{e^{L\ x_A\ }-e^{L\ x_B}} \quad (5)$$

and can be considered as the inverse operator to $\boxplus$. With the *box-minus* operator $\boxminus$ we can ensure that

$$L\ x_A\ \boxplus L\ x_B\ \boxminus L\ x_B\ = L\ x_A\ . \quad (6)$$

Hence, it is easy to prove that Eq. (2) must be re-written as (the lower index "SD,apri" is skipped to enhance readability)

$$\begin{aligned} L^{\mathrm{SSP}}\ y_1\ &= L^{\mathrm{GRAY}}\ y_2\ \boxminus L^{\mathrm{GRAY}}\ y_3 \\ L^{\mathrm{SSP}}\ y_2\ &= L^{\mathrm{GRAY}}\ y_2\ \boxminus L^{\mathrm{GRAY}}\ y_1 \\ L^{\mathrm{SSP}}\ y_3\ &= L^{\mathrm{GRAY}}\ y_1\ \boxminus\ L^{\mathrm{GRAY}}\ y_2\ \boxminus L^{\mathrm{GRAY}}\ y_3 \end{aligned} \quad (7)$$

in order to make sure that Eq. (7) is the inverse of (4). It is important to note that the *box-minus* operation, as it is defined in Eq. (5), provides a real numbered output value $L\ x_A\ \boxminus L\ x_B\ \in \mathbb{R}$ only if $L(x_A) < L(x_B)$.

Thus, as a second important intermediate result we can conclude that also in case of *soft-decision* decoding transformations between both domains, the SSP domain as well as the *Gray encoded* domain, exist. However, in order to make sure that both transformations are exactly inverse to each other the *box-minus* operator $\boxminus$ becomes necessary. Introducing the *box-minus* operator $\boxminus$ reveals some new challenges for a practical implementation because it provides real-valued outputs only for specific relations of the inputs (i.e. $L(x_A) < L(x_B)$). Unfortunately, this cannot be guaranteed in the BICM-ID receiver because of the *soft-demodulation* block which is located between both transformations (see Figure 3).

4.2.3 The Box-Minus Operation Issue in the EFF Case

Before proposing a first attempt to solve the *box-minus* operation issue, let us consider the extreme case of *Error-Free Feedback* (EFF). On one hand, the EFF case will give us some idea about the best possible theoretically attainable performance of the BICM-ID receiver. On the other hand, it allows us avoiding the *box-minus* operation issue. In the EFF case the *L*-values $L^{GRAY}_{SD,apri}(y)$ take the values $\pm\infty$ (i.e. $+\infty$ for $y = 0$ and $-\infty$ for $y = 1$). Table 1 summarizes the results of the *box-minus* operation according to Eq. (5) for all combinations of $L\ x_A$ and $L\ x_B$ in the EFF case.

Table 1: Results of the $\boxminus$ Operation in the EFF case

$L\ x_A$	$L\ x_B$	$L\ x_A\ \boxminus L\ x_B$
$+\infty$	$+\infty$	$+\infty$
$+\infty$	$-\infty$	$-\infty$
$-\infty$	$+\infty$	$-\infty$
$-\infty$	$-\infty$	$+\infty$

Thus, in the EFF case we can use a lookup table instead of implementing the *box-minus* operation as defined in Eq. (5).

4.2.4 First Attempt to solve the Box-Minus Operation Issue

The EFF case is an extreme case that gives insights in the best possible theoretically attainable performance of the BICM-ID receiver. For a practical implementation under regular conditions it remains to be a challenging task to provide solutions for situations in which $L(x_A) \not< L(x_B)$. As a first attempt, we propose to replace all these *box-minus* operations of Eq. (7) by *box-plus* operations whenever $L(x_A) \not< L(x_B)$. For instance, Eq. (7) becomes

$$\begin{aligned} L^{\mathrm{SSP}}\ y_1\ &= L^{\mathrm{GRAY}}\ y_2\ \boxplus L^{\mathrm{GRAY}}\ y_3 \\ L^{\mathrm{SSP}}\ y_2\ &= L^{\mathrm{GRAY}}\ y_2\ \boxminus L^{\mathrm{GRAY}}\ y_1 \\ L^{\mathrm{SSP}}\ y_3\ &= L^{\mathrm{GRAY}}\ y_1\ \boxminus\ L^{\mathrm{GRAY}}\ y_2\ \boxplus L^{\mathrm{GRAY}}\ y_3 \end{aligned} \quad (8)$$

if $L^{\mathrm{GRAY}}\ y_2\ > L^{\mathrm{GRAY}}\ y_3$. Note, on a case-by-case decision we only replace the operation and not the entire line in which $L(x_A) \not< L(x_B)$ (see, e.g., last line of Eq. (8)).

Thus, instead of using the *box-minus* operation we propose to use the *box-plus* operation. Of course, this also means

$$L\ x_A \boxplus L\ x_B \boxplus L\ x_B \neq L\ x_A \ . \qquad (9)$$

Anyways, the main purpose of this paper is to provide the basic idea of an innovative BICM-ID receiver with a novel *transformation of extrinsic information*. For this we introduce the fundamental math in Section 4.1 and Sections 4.2.1 and 4.2.2 as well as an approach to determine the best possible theoretically attainable performance in Section 4.2.3. The solution for the *box-minus* operation issue proposed in Section 4.2.4 may just be considered as a first attempt allowing a first implementation for simulation purposes. Better approaches might exist. This is a matter of ongoing research work at our institutes.

5. SIMULATION RESULTS

Figure 5 shows the simulation results for the novel BICM-ID receiver with a *Transformation of Extrinsic Information* (TEI, see right part of Fig. 4). The simulation settings are the same as in Section 3 (see Fig. 3) for the classic BICM-ID schemes with a standard *soft-demodulation* block (see left part of Fig. 4).

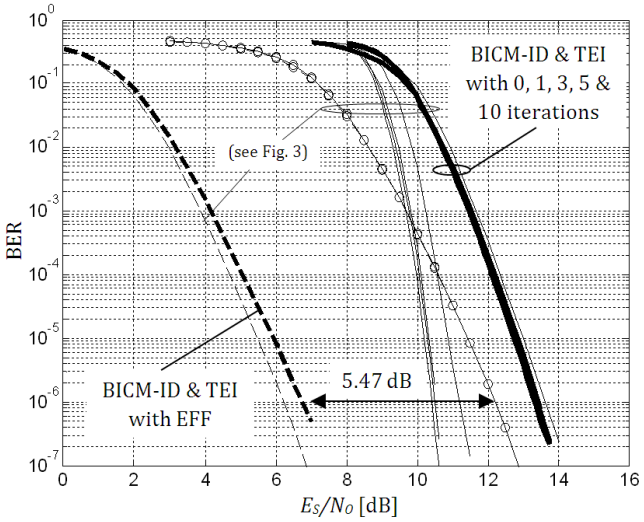


Figure 5: BER curves for a BICM-ID receiver with *transformation of extrinsic information* (TEI)

Obviously, the BER curve for the EFF case of the new BICM-ID receiver with *transformation of extrinsic information* (TEI) outperforms the BICM-ID receiver with a classic *soft-demodulator* for a *Gray-encoded* symbol mapping considerably. For instance, for a BER of 10^{-6} gains in E_S/N_0 of up to 5.47 dB are theoretically achievable.
However, we are not able to realize these theoretical gains with the first attempt to solve the *box-minus* operation issue as introduced in Section 4.2.4. Like the simulation results for the (modified) SSP symbol mapping shown in Fig. 3 there is an expected loss in BER-over-E_S/N_0 performance if we realize *soft-demodulation* and SISO-FEC decoding only once. But, unlike the simulation results for the (modified) SSP symbol mapping the performance does not improve for higher numbers of iteration. Unfortunately, the BER behavior remains the same for different numbers of iteration. Further research work (like an EXIT-chart analysis) is necessary to find a better solution for the challenging *box-minus* operation issue.

6. CONCLUSIONS

In this paper we have proposed a novel innovative idea for BICM-ID receivers. The key motivation for introducing the new signal processing was to provide an added value (higher robustness, longer communication ranges) to operators of modern SDRs while preserving interoperability to legacy equipment. For this purpose, in a first step, the deliberately false assumption is made that a well performing symbol mapping has been used at the transmitter, even though in reality a less powerful symbol mapping was applied. In a second step, the mismatch in the symbol mappings at the transmitter and receiver is compensated by a novel *transformation of extrinsic information*.
After having introduced the fundamentals of the required novel signal processing, we have demonstrated by simulation the theoretically achievable performance gains in the *error-free feedback* case are considerable. However, for a practical implementation under regular conditions the *box-minus* operation turned out to be a critical element. Finding a proper solution for the *box-minus* operation issue is still a matter of ongoing research work.

7. REFERENCES

[1] J. Leduc, M. Adrat, M. Antweiler, and H. Elders-Boll, „*Legacy Waveforms on Software Defines Radios: Benefits of Advanced Digital Signal Processing*“, in Proc. of NATO Information Systems Technology (IST) Panel Symposium, Breslau (Poland), Sept. 2010

[2] X. Li and J. A. Ritcey, „*Bit Interleaved Coded Modulation with Iterative Decoding*“, in IEEE Communication Letters, Vol. 1, No. 6, pp. 169–171, Nov. 1997

[3] X. Li, A. Chindapol, and J. A. Ritcey, „*Bit-Interleaved Coded Modulation with Iterative Decoding and 8-PSK Signaling*“, in IEEE Transactions on Communications, Vol. 50, No. 8, pp. 1250-1257, August 2002.

[4] J. Hagenauer, E. Offer, and L. Papke. „*Iterative Decoding of Binary Block and Convolutional Codes*“, in IEEE Transactions on Information Theory, pp. 429-445, March 1996.

[5] T. Clevorn and P. Vary, „*The Box-minus Operator and its Application to Low-Complexity Belief Propagation Decoding*“, in Proc. of IEEE Vehicular Technology Conference (VTC Spring), Vol. 1, pp. 687 – 691, May 2005

LOW-COST FULLY-SOFTWARE WAVEFORMS FOR TACTICAL COMMUNICATIONS

Carmine Vitiello
(University of Pisa, Pisa, Italy, and CNIT, Parma Italy; carmine.vitiello@for.unipi.it);
Giacomo Bacci
(University of Pisa, Pisa, Italy, and CNIT, Parma Italy; giacomo.bacci@iet.unipi.it);
Fulvio Arreghini
(CSSN-ITE Vallauri Institute, Italian Navy, Italy, fulvio.arreghini@marina.difesa.it);
Marco Luise
(University of Pisa, Pisa, Italy, and CNIT, Parma Italy; marco.luise@unipi.it);

ABSTRACT

In this paper we show an overview of development, implementation and improvement of waveform for tactical communications. Our philosophy is based on the utilization of low-cost software-defined radio (SDR) platforms in low-rate communications. We choose a fully-software approach to minimize development times and costs, and to exploit the technological progress in terms of general purpose processors. For this reason, Ettus universal serial radio peripheral (USRP) platforms have been chosen. The waveforms implementation has been done thanks to an open-source SCA (software communication architecture) compliant framework, called OSSIE (Open Source SCA Implementation Embedded), which provides useful tools that allow correct and easy implementation. This work is the result of collaboration between CNIT-University of Pisa and CSSN-ITE Vallauri Institute of Italian Navy.

1. INTRODUCTION

The evolution of tactical radio has always been in contrast with money saving, both for the technical requirements of radio military standards and for the cost of new technological solutions. Until now, hundreds of radio standards are developed to satisfy the need to communicate in several ways and to operate in different scenarios and frequency ranges, and hundreds of hardware are made to handle this kind of communications. From this point of view, software defined radios (SDRs) represent the present and the future of telecommunications and could be a promising solution in terms of costs and compactness. Their huge versatility, combined with new fast wideband components, allows several waveforms to be managed, exploiting the same platform hardware, covering large portions of frequencies and reducing costs to buy and employ different hardware radios. Working on low-cost SDR platforms, some fully-software approaches have appeared in the last few years [1], thanks to the fact that all signal processing blocks can be run on general purpose processor (GPP), thus significantly reducing development costs and times. The paradigm has already been the winning choice for the diffusion of SDRs in the commercial field, also thanks to several open-source development tools. This methodology can also be applied in the military context, in which most research is orienting in developing waveforms jointly, based on a common software communication architecture (SCA). Following this trend of research, this paper presents our recent results in which we focused on building several digital waveforms, such as STANAG 4285, STANAG 4539, MIL-STD-188-110A and MIL-STD-188-110B [2-5], to mention a few. In order to follow our low-cost philosophy, we implemented our codes on Ettus USRP B100 and USRP 1, two of the cheapest SDR platforms available on the SDR market, exploiting an open-source SCA-compliant development tool. In particular, we made use of Open-Source SCA Implementation - Embedded (OSSIE) [6] in its last version, which guarantees the code portability. This set of codes provides a suite of baseline waveforms which are useful to test the interoperability of different waveforms on several platforms, and to prove the potential of the fully-software approach on the SCA environment. Thanks to several complexity-saving architectural choices, these waveforms require few resources in terms of occupied memory and central processing unit (CPU) consumption, and they can also be run also in limited-resource equipment, always maintaining good communication performance.

2. WAVEFORM

The waveforms used in this work are a suite of digital high frequency (HF) / very high frequency (VHF) waveforms for tactical and strategic communication. To the best of our knowledge, these waveforms are rarely used with SDR technology. These standards are characterized by low data rates, no need for infrastructure, and unclassified documentation in most parts. The PHY (Physical) and MAC (Medi-

um Access Control) layers can represent the starting point for a common upper layer.

2.1 STANAG 4285

The STANAG 4285 standard [2] is the simplest waveform implemented in this work. More in detail, it provides six data rates, from 75 bits/s up to 2400 bits/s, with different feature in terms of forward error correction (FEC), interleaver dimension, and modulation.
This waveform is composed by a digital source that generates information bits and other data necessary for the communications, such as SOM (start-of-message) and EOM (end-of-message) words, expedient to understand when source transmission begins and ends, and flush bits, useful to reset memories of the interleaver and the encoder.
FEC is a function of the data rate, and it is based on convolutional encoding with rate 1/2, constraint length 7, polynomial generator $(91,121)_{10}$ and repetition encoding. For the highest data rate, a code rate of 2/3 is achieved when applying convolutional coding and puncturing. After that, the encoded and punctured bits are forwarded to the interleaver. For data rates 1200 and 600 bits/s, only the convolutional code is used. For the other cases, FEC is composed by a concatenation of repetition encoding and convolutional encoding.
A convolutional interleaver with pseudorandom access to delay lines that compose the component follows the FEC phase, shuffling encoded bits in order to avoid burst errors. The interleaver dimension ranges from 0.853 s (short) to 10.24 s (long). Puncturing, when applied, is used to modify the data rate after interleaving operation.
After this operation, the interleaved bits are mapped into PSK modulated symbol by using BPSK (binary phase shift keying), QPSK (quaternary phase shift keying) or 8-PSK (8-ary phase shift keying), according to employed data rate. These symbols are scrambled and included in a frame composed by 80 synchronization symbols, and four slots of data symbols separated by 16 reference symbols set to zero. Finally, the frames are sent to a transmission filter shaped as a square-root-raised-cosine filter with roll-off factor $\alpha = 0.2$.

2.2 STANAG 4539

The STANAG 4539 standard was introduced by NATO to support interoperability with U.S. MIL-STD-188-110B. In this work, we have developed the high data rate traffic waveform, described in [3, Annex B], supporting data rate from 3200 bits/s up to 12800 bits/s.
This waveform is composed by a digital source that produces information bits or EOM to close data transmission or flush bits set to zero to reset memory of the components. Information bits are encoded, where foreseen, by convolution code with rate 1/2, constraint length 7, polynomial generator $(91,121)_{10}$, punctured to produce a rate 3/4 block code that shows the same length as the interleaver one. The latter is a block interleaver with variable dimension, followed by a PSK mapper (QPSK or 8PSK), or QAM (16, 32, 64) according with data rate.
Mapped symbols are scrambled and are included in a frame composed by synchronization preamble, data and reference symbols called mini-probe.
Then, the frame are filtered by a root raised cosine (RRC) filter with roll-off factor $\alpha = 0.35$.

2.3 MIL-STD-188-110A

The MIL-STD-188-110A standard [4] is a low rate HF waveform, comparable with HF NATO version STANAG 4285. Its data rate ranges from 75 bits/s to 4800 bits/s. Two transmission options are provided: fixed frequency and frequency hopping.
Similarly to the prior waveform, this digital source produces information bits or EOM message to close data transmission or flush bits set to zero to reset memory of the components.
FEC is given by convolutional code with rate 1/2, constraint length 7 and polynomial generator $(91,121)_{10}$, with possible puncturing, or concatenation of repetition code with a convolutional code.
Block interleaving follows the FEC component, and a modified Gray decoder maps the input data into a Gray map. Frames are composed from these binary digits, including synchronization preamble and reference symbols, mapped into PSK maps. Complex symbols are scrambled and sent to the transmission filter.

2.4 MIL-STD-188-110B

The MIL-STD-188-110B, Appendix C standard is considered in this work [5]. The waveform features are the same as STANAG 4539. For this reason, we omit its description for the sake of brevity.

3. FRAMEWORK

There are several frameworks that can be used for the design and the development of SDR waveforms. Among these, GNUradio [7] is probably one of the most widely known and appreciated by community of developers, as it is user friendly, requires a light implementation, and supports the major low-cost development platforms, such as USRPs [8] (through UHD driver) and RTL-SDR [9] receivers (through Osmocom driver).
Another good example is provided by Mathworks MATLAB [10], that recently released functionalities to integrate low cost hardware platforms (such as USRPs, and RTL-SDR) to go beyond simulation.

However, when dealing with tactical waveforms, a different perspective shall be taken into account. Although there is not an official and universally accepted standard for tactical waveforms, the SCA [11] is a *de facto standard*.

In brief, SCA represents the open implementation-independent framework, introduced from U.S. Defence with JTRS (Joint Tactical Radio System) program, to create a common interface between any hardware and waveform components.

This simplifies the waveform development on many SDR platforms, irrespectively of the internal architecture, in order to maximize portability, interoperability, and configurability.

SCA and SCA-based development tools allow components and logical devices to be easily designed. The first one provides for the management and execution of the software that manipulates input data and determines the output of the system. The latter represents the software that provides the capabilities for waveforms to execute and access to the systems hardware resources. The presence of a middleware called CORBA (Common Object Request Broker Architecture) enables communications between components and between components and device [12]. SCA, currently published in version 4, is adopted in the U. S. under the control of Joint Tactical Network Center (JTNC). Moreover, the version 2.2.2 of the SCA standard is the basis of the major reference architecture for SDR in Europe, in particular European Secure SOftware defined Radio (ESSOR).

These are the reasons that led us to select a SCA-compliant framework. In particular, OSSIE [6] has been chosen as the SCA-based development tool. It is an open-source tool, based on a Linux operational environment that facilitates the component and waveform construction, device allocation and connection between themselves. The software package includes: an SDR core framework based on the JTRS SCA v2.2.2; the Waveform Workshop, a set of tools for rapid development of SDR components and waveforms applications; and an evolving library of pre-built components and waveform applications. Furthermore, OSSIE supports the employment of low cost SDR platform such as Ettus USRP and its libraries.

OSSIE has been developed by Virginia tech. Since its support has been discontinued, the latest available version is 0.8.2. In this work, we worked on this version of OSSIE in which we installed UHD (Universal Hardware Driver) to control each kind of USRP platform. Given that last release of OSSIE was on 2010, we modified some files of UHD in order to be able to use newer platforms.

This modification focuses on definition of the USRP port, both for reception and transmission, and other syntax components.

We have also customized an Ubuntu operational environment in which we can find a well-functioning OSSIE version with external updates libraries, such as liquid-dsp [13], modified UHD driver and device and component suite.

The REDHAWK project [14] is the follow-up of the OSSIE project. REDHAWK is freely available, although it is not open source as it is copyrighted by a group comprising the U. S. Government, research institutions and Industries. REDHAWK is partly based on the code developed within OSSIE project, and allows the development and testing of waveforms with a graphic interface based on block diagrams, similar to well-known products such as Simulink and LabView.

REDHAWK is designed to run on Linux CentOs, although a porting for Ubuntu Linux is available. We have started experimenting development with REDHAWK framework even though we found that integrating USRPs is not trivial, as some issues with the UHD driver are still to be resolved.

4. PLATFORM

To test implemented waveforms on development platforms, we chose USRPs, manufactured by Ettus research [7]. In a nutshell, the USRP is a low-cost development platform widely adopted by research community, at the point that it has nearly become the *de facto* standard platform in the research community.

The USRP offers all the functionalities of a radio frequency (RF) front-end, intermediate frequency (IF) conversion, and baseband conversion. It gives high flexibility in the choice of hardware as it is based on a motherboard-daughterboards paradigm: core functionalities are performed on a motherboard where several types of daughterboards can be plugged, depending on the operational requirements.

For example, on the motherboard side of USRP 1, we find an analog-to-digital converter (ADC) section composed by four ADCs, that are in charge of the digital conversion with a sample rate of 64 MS/s and a digital-to-analog converter (DAC) section composed of four DACs working with a resolution of 14 bits. The heart of the motherboard is a field programmable gate array (FPGA), which is mainly in charge of baseband conversion of digital signal and of the sample rate adaptation between USRP and universal serial bus (USB), which represents the interface with the GPP.

On the RF side, the daughterboards can be chosen among different models, according to the operating band in TX and RX. Each daughterboard can access two out of four ADCs (in RX) and DACs (in TX) of the motherboard. The daughterboard is connected with the FPGA, so that it can receive commands from the motherboard. Daughterboards manage the path from IF conversion till RF front-end.

The USRP is designed so that baseband processing required by the waveform is carried out on the GPP of the host personal computer (PC). This means that most signal processing burden, such as filtering, modulation, and coding, is performed by the GPP. On the TX side, the processed digi-

tal I/Q samples are processed on the GPP and then transferred via the USB link to the USRP motherboard. Here, digital samples are interpolated in order to increase the sample rate from 32 MB/S allowed by USB 2.0 link to 64 MS/s. As each digital sample is represented by 16 bits (for the I and Q branches) on the USB link, we need 4 bytes of data to be transferred in order to obtain a complex sample. Then, since the USB link allows a 32 MB/s rate, this is equal to an 8 MS/s rate. This means that on the USRP motherboard we need to interpolate the received samples by a factor of (at least) 8, in order to obtain a 64 MB/s rate.

After interpolation, samples are digitally converted to IF. Finally, digital samples are converted to analog I and Q by the DACs and passed to the RF frontend of the daughterboard. On the RX side, the same operations are performed in the opposite order.

The main drawback of the USRP is the bottleneck caused by the USB link that represents a limit for high-rate communications. However, USRPs have evolved from the first series, and now several types of platforms are available, with different characteristics and performance:

- X series: for high-performance applications, with multiple connection options;
- N series: with Gigabit Ethernet connection;
- B series: with USB 3.0 connection;
- E series (embedded) with an embedded processor.

In this works USRP B100 and USRP 1 have been used.

5. IMPLEMENTATION

The implementation phase has been divided in two phases: the first one focused on developing components, and the second one on building, simulating and improving the waveforms.

Using OSSIE, we can implement components and nodes in a guided way. Nodes are groups of logical devices that represent hardware items in which we allocate components and running them. To build logical devices, drivers prove to be necessary, whereas for components we just select few option, such as the number and the type of input/output ports, properties, etc. to generate some files which define the component, for example, XML files, that describe component, package and properties, and component class header and implementation definition files, responsible of the internal processing.

The latter two files are C++ codes, and they have been modified to customize the executed procedure. These represent the core of our work, and inside theirs we can use external libraries, such as dsp-liquid [14] or fftw [15].

Talking about parameters, it is important to underline that OSSIE does not properly manage the properties that could be changed real-time. Indeed through Wavedash, a tool offered by OSSIE suite, we can modify these parameters while the code is being executed, although in some cases these modifications are not processed by OSSIE. To avoid this problem, we defined some global variables directly on the header file, although it cannot be modified while the component is running.

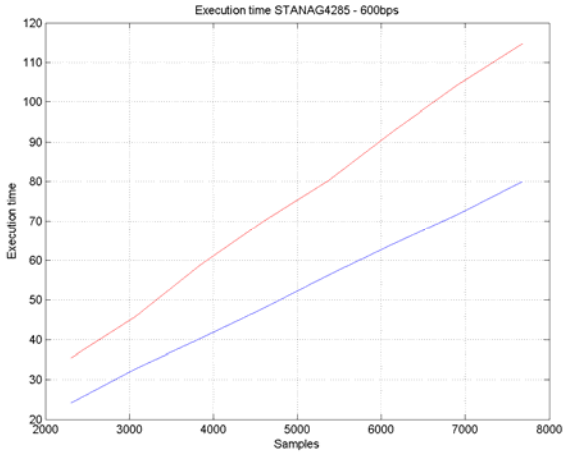


Fig. 1 – Comparison between compact and fragmented waveform in terms of execution time

In order to simplify the implementation and to enable future improvements, we implemented each component of the transmitter and receiver chains as OSSIE components.

This way to operate has brought several advantages and disadvantages: we can exploit each component for creating other waveforms without writing again the codes, so we got a suite of useful components, usable in each moment. Furthermore generic components are able to adapt to several conditions, setting only a few parameters.

In this manner we maximize the flexibility of our components, but penalize it from the point of view of efficiency. Indeed, a generic component pays a trade-off between flexibility and efficiency. Therefore, starting from generic version, we implemented dedicated components for each case in which we optimized codes to obtain better performance.

This paradigm has been extended to waveform composition. We can build a waveform using generic components chosen from our suite, connecting and setting theirs in correct manner. This method made us waste many computational resources, and degrade the performance in terms of throughput and latency, inasmuch each component allocates a process into logical device, such as the GPP processor.

CORBA is the main responsible for this behavior. Throughput and latency are factors of both CORBA and the underlying transport used by CORBA, and depending from message size exchanged by each component, as showed in [16] and [17]. Furthermore CORBA inserts a heavy overhead for each component employed for running the waveform.

Fragmentation of waveform enhances this trend and gets worse performance. Measurements of CORBA computation overhead for a GPP system with the Ossie CF and OmniORB have been provided in [18].

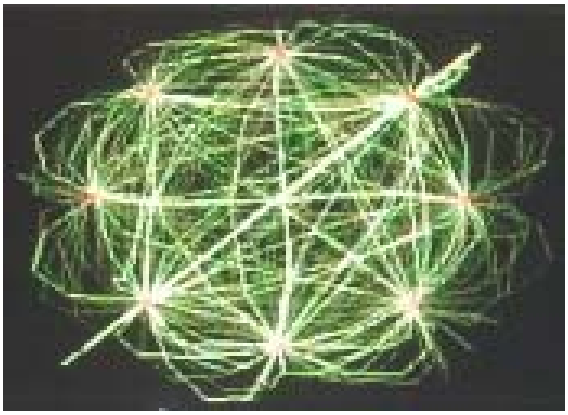


Fig. 2 - 8PSK Constellation of Stanag 4285 from digital spectrum analyzer

Learning from these works, we build a waveform in compact mode, composed by only two components, one for producing/elaborating data and one for transmitting/receiving theirs. In fact, the extended waveform is not able to transmit and receive real-time data, but only to produce a dump file for offline communications. A performance comparison between these two types of waveform will be shown in the next chapter.

6. SIMULATION AND TEST

We have tested the waveforms described above in the LANCERS Laboratory [19]. There, exploiting simulation tools and instrument sets, RF measurement instruments, and human capabilities, we have tested the tactical waveforms described in the Section 2, starting from the test and evaluation (T&E) procedure.

After analyzing documents of the military radio standard, we have implemented C++ codes of each component that compose both transmission and receiver chains. As mentioned in Section 5, we first implemented waveforms by the employment of generic components, and then dedicated components. In this way, already at the time of the simulation, we tested the two implementation modes.

In order to stress the waveform elements, we test each one end-to-end, or rather, assaying a chain composed by only specific element and by its counterpart. We also verify the entire waveform with varying channel features starting from the additive white Gaussian noise (AWGN) channel, up to more complicated models.

After this first phase, we modeled OSSIE components, in both a generic and a dedicated fashion. After testing these elements, we designed the entire waveform, first in a fragmented mode, composed by several elementary elements, and then in a compact mode.

Simulations have been running on nodes composed by only GPP. In these simulations we evaluated the bit error rate (BER) for several channel models and as a function of the signal-to-noise ratio (SNR) for each implemented waveform.

In order to evaluate also the performance in terms of execution time, we run N=400 times the STANAG-4285 waveform at 600 bit/s mode with short interleaver varying the amount of data, and we got the compacted waveform results about 1.4 times faster than fragmented waveform, as shown in Fig.1. Furthermore each component of the fragmented waveform or each function that implements the component in the compact waveform provides a log file, in which we can find data input, data output and other features that can suggest a correct working or a malfunctioning.

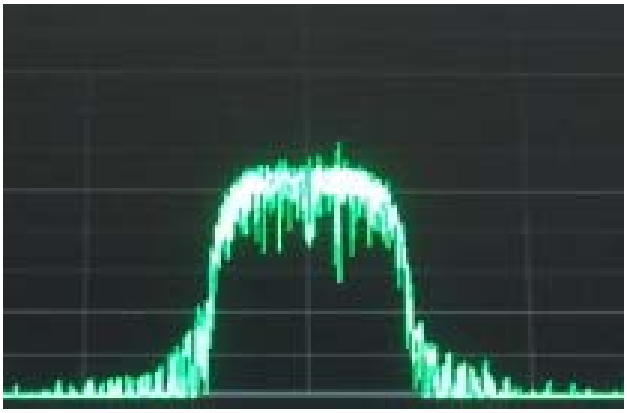


Fig. 3 - Stanag 4285 Spectrum

When each component behaves as expected, we can change the node, passing to another one, composed by GPP and UHD device. The first one will process the baseband samples, whereas the second will handle the up or down conversion to RF. Here, we perform the "over-the-air" testing, verifying the quality of the generated signal in terms of band occupation, filter shape, modulation correctness and out-of-band emission, as you can see in Fig.2 and Fig.3.

During these tests, Ettus USRP platforms driven by OSSIE appeared to present some problems in terms of spurious in-band emission. Indeed, the carrier signal produced by the local oscillator is present in the useful band during the receiving phase. Partial presence of carrier signal is also present after the end of transmission. The first problem has been solved by modifying the UHD driver, whereas the second problem is yet to be solved.

7. CONCLUSION AND FUTURE WORK

In this paper, we showed our fully-software implementation of tactical waveform on low-cost SDR platforms, such as Ettus USRP platforms, by means to the open-source SCA-compliant framework called OSSIE. We analyze implementation methods about fragmented and compact waveform, describing pros and cons, also supported by test results.

As a future activity, we are going to extend the implementation of several additional waveforms, also including upper layers, such as TCP/IP and application layers, into the simulation platform and also evaluate frequency hopping capabilities. We are also planning the testing of the implemented platforms in a real scenario, also including the interoperability control among the features of our simulation suite.
Migration to newest SCA-compliant framework RedHawk is also expected.

8. REFERENCES

[1] V.Pellegrini and M.Luise, "Fully software OFDM modulation in vehicular, highly time-variant channels. An implemented technology and its results," Wireless Communication Systems, 2009. ISWCS 2009. 6th International Symposium on , vol., no., pp.550,554, 7-10 Sept. 2009

[2] NATO, Military Agency for Standardization (MAS), "STANAG 4285: Characteristics of 1200/2400/3600 Bits Per Second Single Tone Modulators/Demodulators for HF Radio Links", 1989.

[3] NATO, Military Agency for Standardization (MAS), "STANAG 4539 (Edition 1), Technical Standards for Non-Hopping HF Communications Waveforms", 8 June 2006.

[4] U.S.Department of Defense, "MIL-STD-188-110A: Interoperability and Performance Standards for Data Modems", 30 September 1991.

[5] U.S.Department of Defense, "MIL-STD-188-110B: Interoperability and Performance Standards for Data Modems", 27 April 2000.

[6] "OSSIE" http://ossie.wireless.vt.edu/

[7] "GNU-Radio" www.gnuradio.org

[8] "Ettus Research" home.ettus.com/

[9] "Rtl-sdr" http://rtlsdr.org/

[10] Mathworks "http://www.mathworks.it/"

[11] "SCA" http://jpeojtrs.mil/sca/Pages/sca1.aspx

[12] "Software Communications Architecture Specification", version 2.2.2, 15 May 2006

[13] "RedHawk" www.redhawksdr.org

[14] "Liquid DSP library" http://liquidsdr.org/

[15] "Fftw library" http://www.fftw.org/

[16] F.Casalino, G.Middioni, and D.Paniscotti, "Experience report on the use of CORBA as the sole middleware solution in SCA-based SDR environments," in SDR'08 Technical Conf. Product Exposition, Oct.2008.

[17] T.Ulversøy and J.O.Neset, "On workload in an SCA-based system, with varying component and data packet sizes," in RTO-MP-IST-083 Military Commun. Special Focus Tactical Commun. Netw. Centric Operations,Apr.2008.

[18] Z.Jianfan, D.Levy, and A.Liu, "Evaluating overhead and predictability of a real-time CORBA system," in Proc. 37th Annual Hawaii International Conf. Syst. Sciences - 2004, Jan. 2004.

[19] F.Arreghini et al, "Test and Evaluation of Military SDR Platforms and Waveforms: Initial Outcomes from the Laboratory funded by the Italian Ministry of Defense", IST-123 Symposium on "Cognitive Radio and Future Networks",14 May 2014

LOW COST GSM/GSM-R INTERFERENCE DETECTOR AND PLMNS DISCOVERY USING SOFTWARE DEFINED RADIO TECHNOLOGIES

Ottavio M. Picchi[(1)], Marco Della Maggiora[(1)], Irene Menicagli[(2)], Marco Luise[(2)]

(1) WISER S.r.l, Via Fiume 23 57123, Livorno, Italy

(2) Department of Information Engineering, University of Pisa, Pisa, Italy

ABSTRACT

Interferences over GSM/GSM-R networks are suspected to increase in the near future, due to the expected growth of GSM-R network deployment and the potential growth of public cellular networks. The problem of interference over GSM-R spectrum has become a very sensitive theme since high speed train information is conveyed over GSM-R radio signals. In this paper we investigate a set of algorithms, which can be executed on a Software Defined Radio (SDR)-based sentinel to be deployed on the field. This sentinel is able to detect interference signals on the GSM/GSM-R bands as well as discover the Public Land Mobile Networks (PLMN) transmitting on the band under analysis.

1. INTRODUCTION

Recently, some GSM-R operators have observed operational limitations caused by interferences from public networks emissions. The interference issue is suspected to increase in the near future, due to the expected growth of GSM-R network deployment and the potential growth of public cellular networks. The problem of interference over GSM-R spectrum has become a very sensitive theme since high speed train information is conveyed over GSM-R radio signals. This clearly implies that an interference signal over the GSM-R band becomes a public safety criticality. In fact an undetected interference might lead to undesired service blocks or even worst to railways disasters. For all these reasons, the European Community has highlighted the need for some regulations [1], which foresee an efficient interference detection system as well as a reliable mitigation mechanism. The European Community has also proposed some possible countermeasures for mitigating the risks of interferences, using a preventive approach. Some solutions have been identified in [1], [2].

Instead in China a different interference scenario has been identified. Chinese railways provider uses a band, which is a sub-portion of the public GSM spectrum. According to [3], the 885÷889/930÷934 MHz EGSM radio resource can be used by both public GSM operators and GSM-R systems depending on different geographic areas. Specifically, public GSM operators are allowed to transmit on 885÷889/ 930÷934 MHz bands if their BTSs are geographically separated by the railways of, at least, 3 km in rural areas and of, at least, 6 km in urban areas [3]. This solution of co-using a radio band is a precedent in the world of wireless communications. This has led to severe interference conditions and transmission collisions, since, even obeying geographical regulation, interference between public GSM and GSM-R is not avoided.

The main contributions of this paper are: i) a novel Interference Detection Algorithm (IDA) for GSM/GSM-R signals; ii) a set of software algorithms intended for PLMNs Discovery (PLMND).

All these algorithms are developed for SDR purposes and have been tested on real-signals, using a Universal Software Radio Peripheral (USRP) front-end. The novelty of the algorithms for PLMND is mainly related to the SDR-target implementation, i.e. a software implementation designed to run over a GPP.

IDA and PLMND are designed to work jointly. In fact, after switching on the sentinel, a first stage of initialization and networks discovery is carried out. After the initialization stage, the spectrum is continuously monitored by IDA in order to detect possible interference. Periodically the PLMND algorithm is applied in order to verify that no anomalies happened on the bandwidth under analysis.

This paper reports the performance of both IDA and PLMND in terms of reliability in case of absence of interference. Specifically, we will provide the probability of successful PLMND stage for real signals recorded in typical urban scenario. Moreover, we will provide the performance of IDA in terms of interference false alarm probability and GSM signal missed detection. Then we report the performance of IDA under interference conditions. Specifically, two types of interferences have been considered, i.e. continuous waves and narrow-band interference. The interference power has been tuned in order to provide the algorithms performance at different level of signal-to-interference ratio (C/I).

2. SENTINELS DEPLOYMENT

Basing on the previous considerations we have been strongly motivated to investigate the topic of interference detection over the GSM-R systems in the European scenario as well as the Chinese one. Our proposal for mitigating the risk of interference is based on interference detection sentinels, which can be deployed on the field continuously monitoring

the GSM-R signal integrity. In case of interference, the sentinel could report the anomaly to a dedicated Data Control Centre (DCC), so that the proper countermeasures can be applied before a service block happens. Such massive sentinel deployment might have a significant cost for Railways Societies and National Governments. For this reason the use of SDR technologies could reduce the overall deployment cost by limiting the sentinel recurrent and unitary cost. Specifically, in our vision a sentinel can be composed by a low cost RF front-end, like the Ettus USRP and a computational back-end, i.e. a General Purpose Processor.

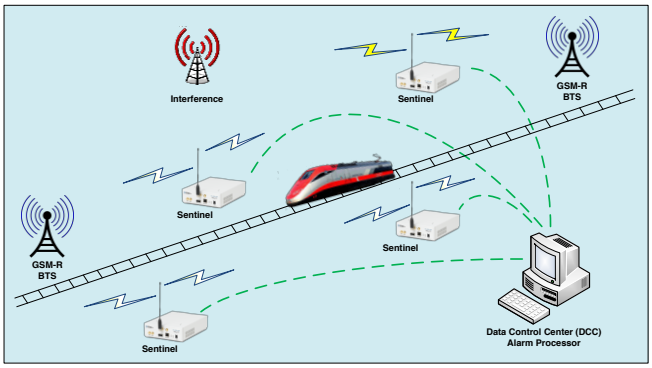


Figure 1 – Sentinels deployment

These sentinels manage to continuously monitor the GSM/GSM-R spectrum by using a combination of PLMND and IDA procedures. Specifically, we assume that PLMND is applied during sentinel initialization stage and during some periodic check on hourly base. During the remaining time, IDA is executed on the sentinel, continuously monitoring any anomaly.

3. PLMNS DISCOVERY AND IDA

The operations performed during the initialization stage, aiming at achieving the whole spectrum knowledge, are summarized in Figure 2 (at the end). Let us detail each block of this figure.

3.1. Time buffering and channel filtering

The block of Time buffering receives I,Q samples from a front-end. The selected sample rate is R_{sa} = 4 Msps in our case, since we were interested in monitoring the GSM-R 4 MHz downlink bandwidth. Once we have collected 941760 complex samples (N_{sa}), this signal chunk is conveyed into the FFT block. After the FFT operation we have 941760 spectral components, representing a 4 MHz bandwidth. Hence each GSM-R channel includes a number of spectral components ($N_{sp/ch}$) equal to

$$N_{sp/ch} = \frac{N_{sa}}{20} = 47088 \quad (1)$$

where the number 20 comes from 19 GSM-R channels plus one 200-kHz-wide section composed by two frequency guards. The frequency guards are placed one on the left and the other on the right of the GSM-R downlink band. Since we want to process each GSM-R channel at a sample rate of 1.083 MHz, i.e. four times the GSM symbol rate (the oversampling factor is $N_{ov} = 4$), we use FFT operation to jointly perform filtering and rate adaptation. Specifically,

$$R_{dec} = R_{sa} \cdot \frac{13}{48} \quad (2)$$

where R_{dec} is the target sample rate. Since the Gaussian Minimum Shift Keying (GMSK) is not a band-limited modulation, for each GSM-R channel we select not only the nominal GSM/GSM-R channel width (200 kHz), but a frequency portion 400-kHz-wide. So the number of active spectral components to be considered is 2·47088=94176. However, for rate adaptation purposes we need to zero pad these spectral components, so that

$$N_{dec} = N_{sa} \cdot \frac{13}{48} = 255060 \quad (3)$$

After the inverse FFT operation we have a filtered signal, at R_{dec} sample rate and whose duration is:

$$T_{dec} = \frac{N_{dec}}{R_{dec}} = 235.4 \text{ msec} \quad (4)$$

Let us note that this duration is almost equivalent to the GSM control multiframe one.

3.2. Active channel threshold setting

Before channel selecting the signal, a mechanism is applied in order to derive a signal power, which can be considered as a threshold. Below this threshold, the channel is considered idle. The implemented mechanism is based on the practical assumption that at least one channel on the GSM-R downlink spectrum is idle. The threshold is then computed as:

$$T\Big|_{dB} = \min_{i=0\div 18}\left\{P_i\right\}\Big|_{dB} + \alpha_{dB} \quad (5)$$

where P_i is the power detected on the i-th channel and α is the power margin, which we typically set to 13 dB. The value of T is continuously updated by averaging the noise floor power. So for each signal chunk, the power over each channel is measured and compared with the threshold T: if the power is greater than T the channel is considered active

and processed, whereas if the power is below the threshold the channel is considered idle.

3.3. Interference Detection Algorithm

The active channel signals are then conveyed to the IDA block, whose output can be:

1. Traffic Channel (TCH) signal;
2. Uncertain if TCH or Broadcast Control CHannel (BCCH) carrier;
3. Unknown signal.

The key idea behind this algorithm is to check if the signal under analysis meets the GSM TDMA constraints, basing on the burst granularity.

In case of detection of a TCH channel, this stream of data is passed directly to the TCH identification block, bypassing the SW receiver core.

In case of unknown signal, the algorithm reports this event as an interference occurrence. It is clear that different strategies can be selected before signalling the presence of interference: in fact we can wait for a pre-set number of consecutive interference detections or we can report interference at the first occurrence. The selection of this strategy is clearly related to the type of interference we desire to detect as well as a trade-off between false alarm and missed detection probabilities.

In case of uncertainty between TCH and BCCH carrier the data stream is passed to the SW receiver core.

3.4. SW Receiver core

The SW receiver core is actually a real GSM receiver, which aims at reading only Local Area Identification (LAI) information from the GSM/GSM-R signal. The architecture of the SW receiver core is depicted in Figure 3 (at the end). The first block is an FM non coherent demodulator, which extracts the GMSK modulating signal.

3.4.1. FM demodulator

The input of the FM demodulator can be expressed as

$$y(n) = e^{j\varphi(n)} + w(n) \tag{6}$$

where $\varphi(\mathrm{n})$ is the GMSK modulated digital signal and $w(\mathrm{n})$ is the thermal noise. The FM demodulator works as follows

$$\hat{s}(n) = \frac{\mathrm{Im}\left\{ y'(n) \cdot y^*(n) \right\}}{\left| y(n) \right|^2} = \frac{\varphi'(n) + \nu(n)}{\left| y(n) \right|^2} \tag{7}$$

where $\hat{s}(n)$ is the GMSK signal, $y^*(n)$ is the conjugate of the received signal and $\nu(n)$ is the thermal contribution after FM demodulator. The output of this block is a real signal at a sample rate of R_{dec}.

3.4.2. Time synchronization

The signal $\hat{s}(n)$ is then passed to the Synchronization Algorithm, which first of all computes the cross-correlation function between the received signal and the local copy (real-valued) of the GSM synchronization sequence, as

$$xcf(n) = \sum_{m=0}^{M-1} \hat{s}(m) \cdot x(m-n) \tag{8}$$

where n=0,…,N_{dec}, M is the length of the synchronization sequence in number of samples (256 samples, considering the synchronization sequence length of 64 bits and that we are working at R_{dec}, i.e. four times the GSM bit rate). Instead $x(n)$ is the local replica of the synchronization sequence. After the computation of the cross-correlation function, we check whether its local maxima are timely-separated by the attended time interval. Since one cross-correlation peak occurs every synchronization sequence and one signal chunk is almost one control multiframe long, each signal chunk can have at most 5 correlation peaks. If the synchronization algorithm detects 3 consecutive significant peaks, the algorithm stops and selects the first peak index (τ_{sync}).

3.4.3. Frequency Offset Recovery and Compensation

The frequency offset recovery algorithm works on the complex signal $y(n)$, instead of the FM demodulator output. First of all the vector containing all the samples in the FCCH burst is obtained, as

$$\mathbf{y_{FCCH}} = \left\{ y(\tau_{sync} - L_{frame}), \ldots, y(\tau_{sync} - L_{frame} + L_{burst}) \right\} \tag{9}$$

where L_{frame} is the duration of a GSM frame in samples (i.e. 5000 at R_{dec}), whereas L_{burst} is the duration of a GSM burst in samples (i.e. 625 at R_{dec}). Once obtained $\mathbf{y_{FCCH}}$, we can compute its spectrum by using the FFT.

Information in the Frequency Correction CHannel (FCCH) burst is all zeroes which produces a tone at 67.73 kHz above the RF carrier centre frequency.

So first of all we measure the frequency of received tone by using Rife and Boorstyn algorithm ([4]). The difference between the measured frequency of the tone and the nominal frequency is the frequency offset (Δf) to compensate. The compensation can be performed as follows

$$\bar{y}(n) = y(n) \cdot e^{-j \cdot 2\pi \cdot \Delta f \cdot n \cdot T_{dec}} \tag{10}$$

3.4.4. Phase Offset Recovery and Compensation

The frequency-compensated signal $\bar{y}(n)$ still needs to be phase-compensated. Specifically, let us indicate as $\bar{\mathbf{y}}_{\mathbf{sync}}$ the vector of samples of the synchronization sequence, after frequency compensation and as $\mathbf{r}_{\mathbf{sync}}$ its local copy. The first step for phase estimation is as follows

$$\xi = \sum_{n=0}^{M-1} \bar{y}_{sync}(\mathrm{n}) \cdot r_{sync}^{*}(\mathrm{n}) = \sum_{n=0}^{M-1} \left| r_{sync}(\mathrm{n}) \right|^2 \cdot e^{j\vartheta} \qquad (11)$$

where ϑ is the phase offset to compensate. In the formula above we assume that the frequency offset recovery is perfect, so that ϑ is not time-dependent. The phase offset is computed by extracting the phase of ξ. After the estimation of the phase offset, the necessary phase compensation is applied not only to the synchronization sequence, but also to the Synchronization Channel (SCH) burst payload. The SCH burst, frequency and phase compensated, will be indicated as $\tilde{\mathbf{y}}_{\mathbf{SCH}}$.

3.4.5. Coherent demodulation and SCH decoding

Once the received SCH signal is properly frequency and phase compensated, the coherent demodulation can be performed according to

$$\begin{cases} z_{2n} = (-1)^n \cdot \mathrm{Re}\{\tilde{y}_{SCH}(2 \cdot n \cdot N_{ov})\} \\ z_{2n+1} = (-1)^n \cdot \mathrm{Im}\{\tilde{y}_{SCH}(2 \cdot n \cdot N_{ov} + N_{ov})\} \end{cases} \qquad (12)$$

where n spans within $0,\ldots,\frac{N_{burst}}{2}-1$, N_{burst} is the number of bits per GSM burst. Let us remark that the output of the coherent demodulation z_{2n}, z_{2n+1} is down-sampled by a factor of N_{ov}. These samples are now taken at 270.833 kHz and then hard-decided and de-mapped as

$$b_i = 1 - 2 \cdot sign(\mathrm{z}_i) \qquad (13)$$

The stream of coded bits b_i is then fed to the Viterbi hard decoder, which extracts the SCH information bits. Hence it is now possible to compute the GSM frame number, in order to compute the delay (number of samples to wait) to the closest LAI field.

3.4.6. BCCH decoding and LAI read

Once the delay to next LAI field has been estimated, the SW receiver core waits for the next occurrence of this field. As known from [5], LAI is transmitted every other two BCCH frames, so that the maximum delay is less than 3 GSM multiframes. At the following occurrence of LAI, the SW receiver core selects the chunk of signal 3 frame plus 1 burst long. In fact LAI is conveyed over 4 bursts. As shown in Figure 3, each received BCCH bursts need to be phase compensated and coherently demodulated, in the same manner explained for SCH burst in § 3.4.4 and 3.4.5. The only one difference between SCH and BCCH processing is related to the phase recovery. In fact for SCH burst the phase offset estimation and compensation is performed by using the synchronization sequence, as shown in (11). For each BCCH burst the phase offset estimation is carried out by exploiting the proper midamble sequence. Once hard decided the bit sequences for each BCCH burst, the GSM BCCH de-interleaver is applied, before conveying the de-interleaved bits into the Viterbi decoder. Finally we are able to read MCC and MNC of the transmitting BTS, so that we can state if the BCCH carrier is authorized to transmit at that frequency or not. In other words it is possible to establish if the identified provider is allowed or not allowed to transmit on the band under analysis. The output of the SW receiver core is a vector of flag, which reports for each BCCH carrier if the transmission is authorized or not.

3.5. TCHs identification

Once the SW receiver core has distinguished between authorized and not authorized BCCH carrier, we need to perform the same distinction on the TCHs. The idea of this block in Figure 2 is to detect, which BCCH carrier is synchronized with the TCH under analysis. Unlike the UMTS system, where all the BTS are time-synchronized with the GPS, the GSM BTS are not time-synchronized. Synchronization among GSM BTS belonging to the same PLMN is admitted, but it is unlikely that two BTS of different PLMNs are time-synchronized. Hence if a TCH is transmitted with the same timing of a BCCH carrier, it is most likely a signal of the same PLMN. In this way we are also able to distinguish between authorized TCHs and not authorized TCHs.

3.6. GSM tail analysis and Interference signalling

After discovering the PLMN for each active TCH and BCCH carrier, there might be a class of active channels not yet identified, i.e. GMSK tails. Since the GMSK is a not band-limited modulation, part of the power transmitted over a channel is leaked over the adjacent ones (on both sides). The block of GSM tail analysis receives from upper blocks information concerning the position of TCH and BCCH carrier within the GSM-R spectrum. This block also receives information about unknown active channels. The GSM tail analysis block checks if the unknown active channels are actually tails by checking if their power over these unknown channels obeys the emission mask (Figure 4). In case the emission mask constraint is fulfilled, the algorithm labels

this signal as GSM tails. If the GSM emission mask is not obeyed, the algorithm labels this signal as an interfered channel.

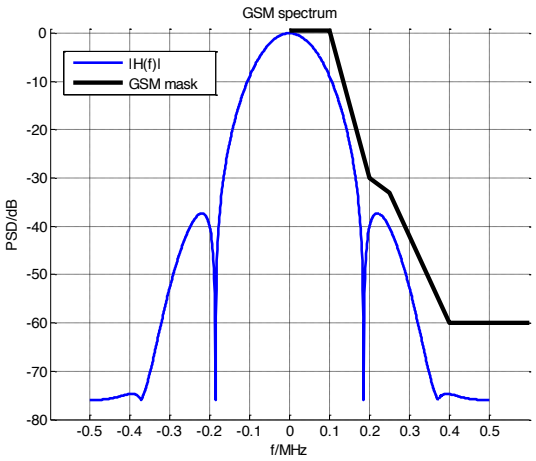


Figure 4 – GSM emission mask

5. PERFORMANCE ANALYSIS

This section reports the performance analysis for PLMND procedure as well as for IDA. For PLMND we provide the performance in absence of interference, since we assume that no interference is active during the initialization stage. Considering the short duration of the initialization stage, this hypothesis seems to be reasonable. Instead for IDA analysis we report the performance of this algorithm in absence and in presence of interference signals. In order to measure the performance of PLMND and IDA we tested both on real signals, monitoring different portions of GSM downlink spectrum from different locations. The propagation channel is typical urban, since our observation points are placed in urban scenarios. This means that PLMND and IDA can perform better in hilly terrain and rural areas, where multipath effects will be less detrimental.

5.1. PLMN Discovery performance

In this section we report the performance of the PLMND stage. This performance has been obtained by monitoring the GSM downlink spectrum (portions of 4 MHz). In order to measure this performance we assume to have the full knowledge of the spectrum under analysis. So we assume to know the channel types (BCCH carrier, TCH or GSM tail), the PLMN for each active channel and the MCC and MNC of each BCCH carrier. We also assume that no interference is affecting the spectrum under analysis during the test stage. Table 1 shows the error rate in channel type detection, i.e. the error rate in detecting, for example, a TCH instead of a BCCH carrier. Tests were performed from different urban locations, in order to provide a more realistic picture of the reliability of the PLMND in terms of channel type detection.

Table 1 – Channel type identification error rate

Location	n. Trials	n. Error	Error rate
A	31510	40	0.001269438
B	31780	60	0.00188798
C	19120	240	0.012552301
D	27790	60	0.00215905
Summary	**110200**	**400**	**0.003629764**

Table 2 reports the performance of PLMND in terms of errors in the detection of inter-channel synchronization. In other words this table shows the reliability of PLMND in understanding if two GSM channels are time-synchronized. As explained in § 3.5, for the purpose of identification of a TCH channel, the inter-channel synchronization reliability is crucial.

Table 2 – Inter-channel synchronization error rate

Location	n. Trials	n. Error	Error rate
A	13440	110	0.00818452
B	20980	100	0.00476644
C	7940	40	0.00503778
D	11970	20	0.00167084
Summary	**54330**	**270**	**0.00496963**

Table 3 reports the performance of PLMND in terms of MCC and MNC erroneous read. This statistic has been measured only on BCCH carriers and we assume that the synchronization algorithm, in § 3.4.2, succeeded. Hence the number of errors in this table takes into account the number of erroneous read of MCC/MNC, but also the number of events for which we do not manage to read them. This is due to the occurrence of something bad after the synchronization algorithm, e.g. an error on SCH payload read, or an error in time-refinement from SCH to BCCH.

Table 3 – MCC and MNC error rate

Location	n. Trials	n. Error	Error rate
A	4980	160	0.032128514
B	3570	97	0.027170868
C	720	19	0.026388889
D	8560	302	0.035280374
Summary	**17830**	**578**	**0.032417274**

Table 1, Table 2 and Table 3 show the performance of PLMND stage in terms of different parameters. Specifically, we can end up that PLMND has an error rate of about 10^{-3} in terms of channel type detection and inter-channel synchronization. Instead the error rate for MCC and MNC read is about 10^{-2}. It must be specified that these statistics have been measured on independent tests base. After the initialization stage of the PLMND algorithms, extracted

information might be averaged and combined, so that expected error rates will be much lower than the ones shown above.

5.1. Interference Detection Algorithm performance

This section reports the performance of IDA. Specifically, we present the performance in absence and in presence of interference signals.

5.1.1. Performance in absence of interference

In order to characterize IDA performance in absence of interference, we monitor portions of GSM downlink spectrum and we assume that no interference is affecting the received RF signal. As stated for the PLMND performance measurement, we assume to have the full knowledge of the spectrum under analysis.
First of all let us define different events, whose occurrences enable to measure the IDA reliability. These events have been measured by monitoring GSM spectrum from different locations in urban scenarios. The observation of IDA behaviour in different locations can supply a realistic picture about how this algorithm works.
The first event we want to monitor is the interference false alarm, which is defined as the probability of detecting an interference conditioned to the absence of interference on that channel, i.e.

$$P_{FA}^{(I)} = \Pr\{\text{Interf. Detected} \mid \text{Interf. absent}\}$$

Table 4 reports the summary of the trials performed in each location and the correspondent number of recorded interference false alarm events. We can conclude that IDA produces an this kind of event with a probability of about 10^{-3}. It is important to mention that these interference false alarm events have been registered on idle channels or on GSM tail channels. However, no interference false alarms have been detected on a GSM active channel.

Table 4 – Interference false alarm results

Location	n. Trials	n. Inter FA	Inter. FA prob
A	39749	113	0.002843
B	53784	108	0.002
C	42048	196	0.0047
D	64464	87	0.00135
Summary	**200045**	**504**	**0.00252**

The second event we monitor is the GSM missed detection, which is defined as probability of not detecting a GSM signal, conditioned to the presence of a GSM signal on that channel, i.e.

$$P_{MD}^{(gsm)} = \Pr\{\text{not GSM Detected} \mid \text{GSM present}\}$$

Table 5 reports the summary of the trials performed in each location and the correspondent number of recorded GSM missed detection events. We can appreciate that we do not manage to register a sufficient statistic, since this event occurrences are very sporadic. This shows a good reliability of the IDA in terms GSM missed detection.

Table 5 – GSM missed detection results

Location	n. Trials	n. GSM MD
A	39749	0
B	53784	2
C	42048	0
D	64464	5
Summary	**200045**	**7**

5.1.1. Performance in presence of interference

This section reports the performance of IDA when interference is present. Specifically, we monitor an active GSM BCCH carrier, combined with an interference signal generated by an AGILENT E4438C generator. GSM signal and the output of the signal generator are combined on the wire using an RF signal combiner. The first step aimed to set a desired Interference to GSM plus Noise Ratio (IGNR) is to measure the power over the BCCH carrier. The measured power is averaged over long observation intervals (on hourly-based), in order to smooth fluctuations of the power emitted by the BTS, as well as channel impairments. Once we obtain the RF averaged power over channel, we can apply the proper interference power in order to set the target IGNR value. Once set the desired IGNR, we measure the Interference Missed Detection Probability (IMDP), defined as the probability of not detecting an interference, when it is present, i.e.

$$P_{MD}^{(I)} = \Pr\{\text{not Interf. Detected} \mid \text{Interf. present}\}$$

For quantifying the performance of IDA we test it applying three different interference signals: a continuous wave (CW), a narrowband signal (NS) with 16QAM modulation and symbol rate equal to the GSM one, i.e. 270.833 ksym/s and a GMSK modulated signal with $\beta T = 0.5$, and a symbol rate of 250 ksym/s (GMSK-0.5). All the interference signals are transmitted exactly at the BCCH carrier nominal frequency. CW has the whole power focused on the BCCH carrier frequency, whereas NS and GMSK-0.5 almost equally spreads its power over the GSM channel bandwidth. We investigate IDA performance in presence of three interferences, since they can give us a better insight of the IDA capabilities under different interference signals.
Let us observe Figure 5. This shows interference missed detection probability against IGNR and for the three

interference signals. The blue line is for a CW, the red one is for NS and the green one is for GMSK-0.5. Let us focus on CW first. We can appreciate that if the interference power is 4 dB smaller than the power of the GSM signal, the interference signal is detected with a probability of about $1\text{-}3\times10^{-5}$.

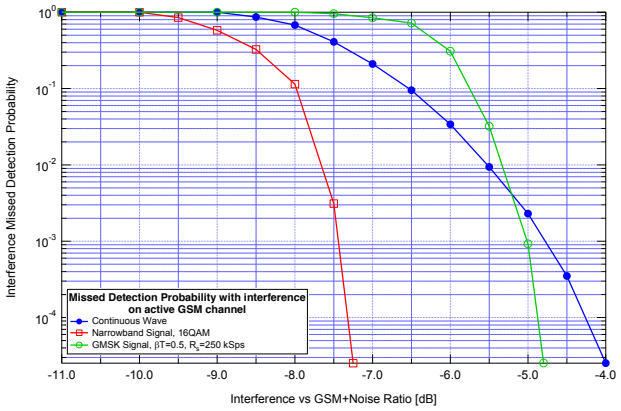


Figure 5 – Interference missed detection probability

Let us define an important parameter, i.e. the GSM Intelligibility Threshold (IT). This parameter states the minimum interference power, and consequently the minimum IGNR, over which the GSM signal is not readable, i.e. MCC and MNC cannot be extracted from the signal. This IT has been empirically measured with PLMND software for each interference signal.

The GSM IT for CW interference is placed at IGNR = 0 dB. This means that our algorithm is able to detect the presence of interference (with good probability, i.e. $P_{MD}^{(I)} = 10^{-2}$) 5.5 dB below IT.

Regarding the NS interference we can appreciate that NS is earlier (than CW) detected by IDA algorithm. In fact at IGNR = -7.25 dB the missed detection probability is 3×10^{-5}.

For NS the IT is placed at IGNR = -7 dB. This means that our algorithm is able to detect the presence of this interference (with good probability, i.e. $P_{MD}^{(I)} = 10^{-2}$) 0.75 dB below IT.

Hence the NS makes the GSM signal not readable with a lower power. This is because NS has higher (than CW) frequency components which destroy GSM signal.

For GMSK-0.5 we can appreciate that the interference is not detected by IDA up to IGNR = -6.5 dB, but its curve is steeper than the one for CW. The IT for GMSK-0.5 is placed around IGNR = 2.5 dB, which means that IDA is able to reliably detect (i.e. $P_{MD}^{(I)} = 10^{-2}$) the presence of this type of interference 8 dB below the IT.

6. CONCLUSIONS

In this paper we presented a set of algorithms for GSM PLMN discovery and interference detection algorithm using the SDR approach. The identification of whole GSM-R spectrum might be of particular interest in China, where the regulation does not foresee a dedicated spectrum for the railways provider. This led to the need of understanding if a GMSK signal is transmitted by the railways provider (authorized) or by a public provider (not authorized). All these algorithms have been designed for SDR applications and can be executed over a GPP. This makes the set of developed algorithm particularly suitable for low cost sentinels, deployed to monitor the GSM-R integrity. Considering the exploitation of SDR paradigm, the unitary cost of a sentinel might be limited, which encourages a massive deployment of sentinels. This set of algorithms is currently designed for GSM-R downlink spectrum (or GSM sub-bands 4 MHz wide), but it can be quite easily extended to the full GSM downlink spectrum.

Regarding the PLMND performance we showed a channel type identification error rate and an inter-channel synchronization error rate both of about 10^{-3}.

Regarding the IDA performance, we designed an interference detection algorithm which detects the presence of interference signals for power levels below the GSM IT. Specifically, IDA detects the presence of CW starting from IGNR = IT – 5.5 dB; it detects the presence of NS starting from IGNR = IT – 0.75 dB; it detects the presence of GMSK-0.5 starting from IGNR = IT – 8 dB. These values show that IDA is able to detect the presence of interference before than the GSM signal is unreadable. This could enable the reaction of the sentinel network, by activating the proper countermeasures.

7. REFERENCES

[1] ECC Report 162, "Practical mechanism to improve the compatibility between GSM-R and public mobile networks and guidance on practical coordination," May 2011.

[2] G. Baldini, *et al*, "An early warning system for detecting GSM-R wireless interference in the high - speed railway infrastructure", Int. J. of Critical Infrastructure Protection 3, pp.140-156, 2010.

[3] L. Zhao, X. Chen, J. Ding, "Interference clearance process of GSM-R network in China," Proc. International Conference on Mechanical and Electronics Engineering (ICMEE), Kyoto, Aug. 2010.

[4] D. Rife, R.R. Boorstyn, "Single tone parameter estimation from discrete-time observations," IEEE Transactions on Information Theory, Vol. 20, Is. 5, May, 1974.

[5] Mehrotra, Asha. GSM system engineering. Norwood: Artech House, 1997. Print.

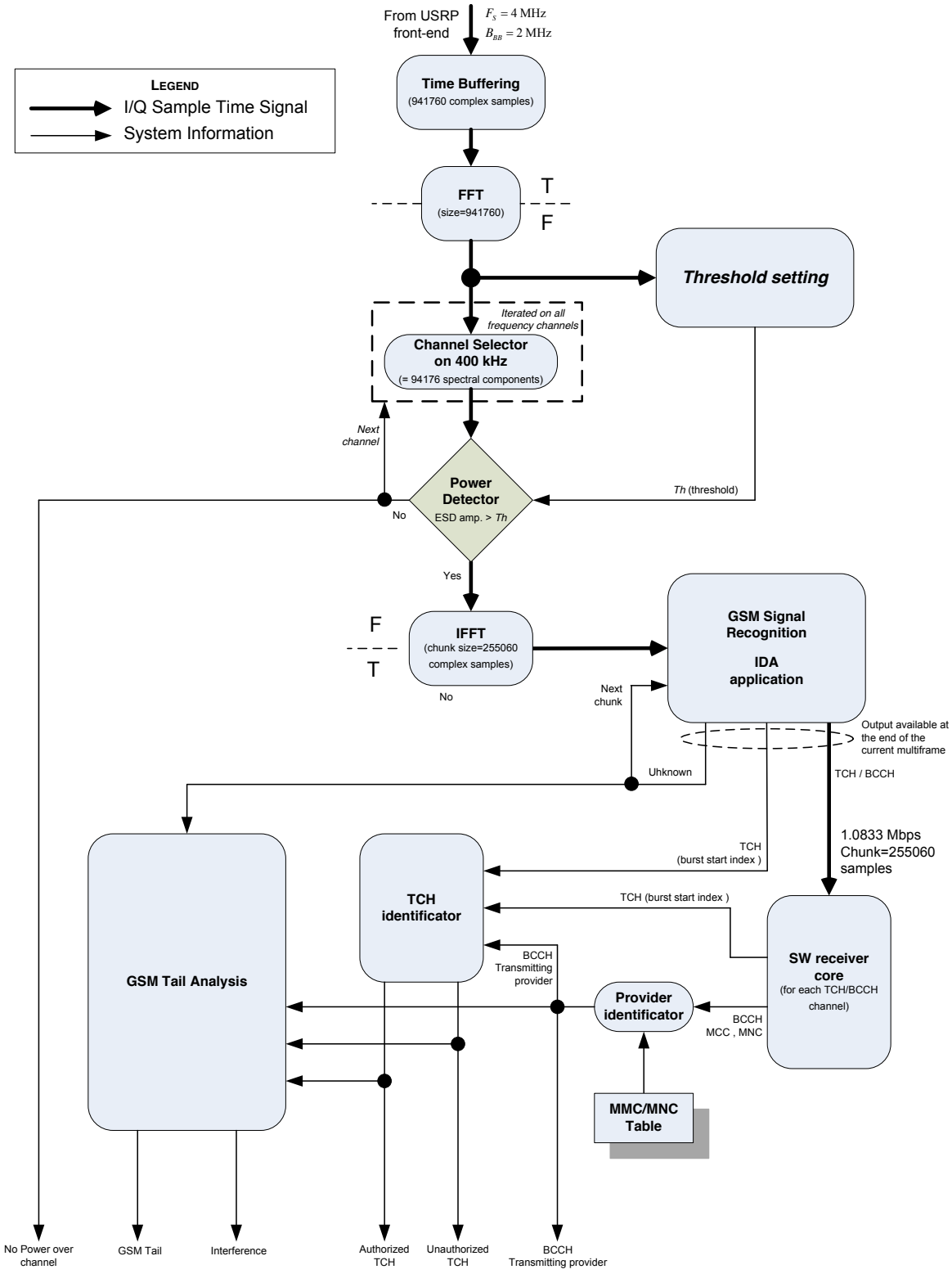


Figure 2 – Software Receiver Architecture

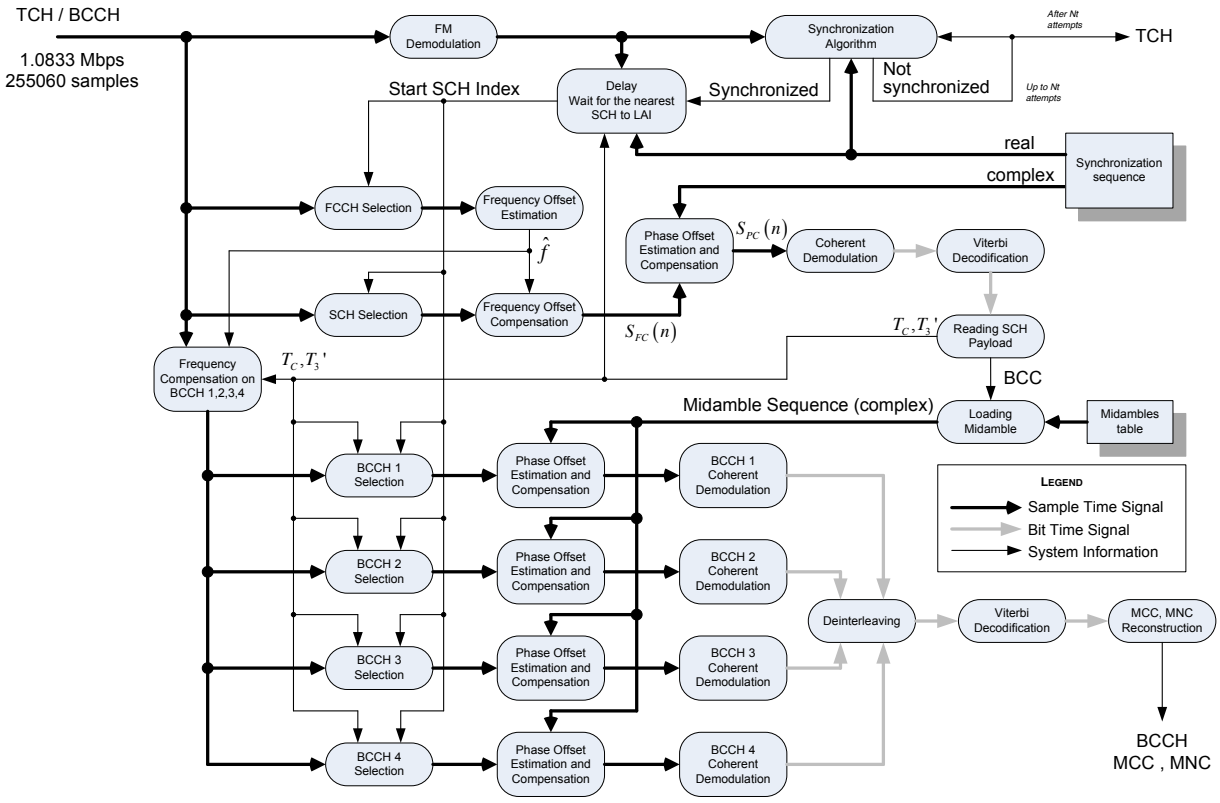


Figure 3 – Software Receiver Core

SPECTRUM SHARED WIRELESS SENSOR NETWORKS BASED ON RADIO ENVIRONMENT DATABASE

Shunsuke Takagi (takagi@awcc.uec.ac.jp), Shunta Sakai (sakai@awcc.uec.ac.jp), Koya Sato (k_sato@awcc.uec.ac.jp), and Takeo Fujii (fujii@awcc.uec.ac.jp)

Advanced Wireless Communication research Center (AWCC),
The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan

ABSTRACT

The paper presents an efficient channel selection method to enable spectrum sharing among WSNs and WLAN. The method is based on the knowledge of the topology of the surrounding radio systems given by a radio environment database. The proposed WSNs gather not only surrounding physical layer information but also MAC address of WLAN to share the spectrum effectively. Also gathered information is uploaded to the radio environment database, which can support spectrum usage of WSNs. The database is connected to the spectrum manager, and the information from distributed sensor nodes is utilized to understand the topology of access point (AP) and WLAN nodes. The spectrum manager selects the channel which does not occur hidden node problem (HNP), and gives the channel information to sensor nodes. In order to confirm the effectiveness of the proposed method, the packet arrival rate and channel utilization ratio of WSNs are evaluated by computer simulations.

1. INTRODUCTION

Current spectrum allocation is basically exclusively use in each specific radio communication system. This kind of spectrum allocation policy is able to communicate without considering interference with other systems. On the other hand, 2.4GHz band is opened to sharing among multiple systems as Industry-Science-Medical (ISM) band to aim flexible frequency utilization. Wireless LAN (WLAN) and Bluetooth are able to utilize this band. WLAN has ability for sharing the spectrum freely by following the radio regulation rule in ISM band. Wireless sensor networks (WSNs) which gather the sensed information from multiple sensor nodes are one of the wireless communication systems utilizing 2.4GHz band. Because WSNs are low cost and low energy consumption wireless communication system, it is suitable for gathering sensed information. WSNs are expected to be utilized in many kinds of applications such as home automation, smart grid and so on and are actively investigated [1][2]. The main frequency band which is allocated to WSNs is 920MHz band and 2.4GHz band. From propagation characteristic, 920MHz band is suitable for wide area communication and 2.4GHz band is suitable for narrow area communication, so it is necessary to select appropriate frequency according to applications. However, since multiple wireless communication systems exist on the 2.4GHz band, it is very crowded by WLAN due to increasing the offloading from smart phone using cellular network.

Because of the crowded environment, stressless spectrum sharing is difficult and steady communication is difficult realize on the same frequency band. WSNs utilizing 2.4GHz band may also lead to performance degradation because of the interference from other nodes. To decrease the mutual interference, IEEE802.15.4, which is a current standard of WSNs, uses Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). CSMA/CA is a method that a transmitter detects a surrounding radio condition before transmitting packet data. If an idle channel status is recognized by a transmitter, it transmits a packet data on the same frequency. As a result, a transmitter can avoid a signal collision with other transmitters. Because CSMA/CA detects an idle channel by sensing a signal based on the carrier signal level, some times the transmitter does not detect other transmitter signal due to weak carrier signal level and a signal collision occurs at the receiver node as shown in Fig.1. This problem is called hidden node problem (HNP), and it causes network quality degrades [3]. Also HNP occurs between different systems as shown in Fig.2, which shows the signal collision with the node located at outside of the carrier sense area. One of the solutions of HNP is a Request to Send/Clear to Send (RTS/CTS) [4]. This method is that when a node transmits the data to another node, the node exchanges RTS/CTS packet for checking the status of the transmitter and the receiver before signal transmission. By exchanging RTS/CTS packet, the node shares surrounding radio environment with othernodes in the same network. The transmitter node may avoid collision because of shared spectrum condition to the hidden node. However, this method may lead to throughput degradation due to increasing a control frame and waiting time. In addition, because RTS/CTS can be used the same radio system in the same network, it is difficult to solve HNP between WLAN and WSN. Therefore, a channel selection considering other surrounding radio environment recognition is necessary for supporting different systems. The transmitter and the receiver understand utilized channel by using the status recognized at surrounding ra-

dio systems and use nonutilization channel by the surrounding radio systems. Consequently, HNP is solved. However, if we consider coexistence with other system, this method wastes the resource. Also, the channel without mutual interference is not considered due to crowded spectrum. If the radio system can share the channel with other radio systems without HNP, the appropriate channel is assigned to the radio system. Therefore, the radio system which cannot share the channel without HNP, use the idle channel.

The probability of a signal collision caused by hidden nodes is decreased by reducing the carrier sense level. However, if the carrier sense level is reduced simply, the wireless communication system refrains from packet transmission even if the packet collision does not occur. Therefore, the throughput may degrade severely.

Another packet collision reduction technique shares RTS/CTS between WLAN and WSN. The node can understand activity of WLAN by RTS/CTS [5]. This method solves HNP in WLAN, and assures transmission opportunity to transmit RTS to access point (AP). However, the throughput is materially deteriorated by the transmission period of RTS/CTS in WLAN, even if the HNP does not happen.

In this paper, we propose an adaptive channel selection method considering the topology of the surrounding radio system and mutual interference level supported by the radio environment database. The radio environment database considered in this paper records the source and destination MAC address of the surrounding radio systems, and the received power measured by sensor nodes. In WLAN, MAC address is an identity to judge a signal source and a signal destination. Therefore, surrounding radio environment which cannot be known only by the received power, can be obtained by MAC address information in a packet header of WLAN. The database is constructed by gathering the information from sensor nodes, which read MAC address in a packet and upload MAC address information and received power information to the database. Based on the constructed database, the spectrum manager that is connected to the database, selects suitable channel for a spectrum shared WSN with avoiding mutual interference.

By using the above mentioned proposed method, WSNs are able to avoid HNP to protect WLAN, and to communicate in narrow area without mutual interference. Also, because WSNs select the channel communicate with no HNP, WSNs design to improve spectral efficiency. We confirm the effectiveness of the proposed method through computer simulations with channel utilization rate and packet arrival rate.

The rest of the paper is organized as follows: we suppose a system model in Section 2. In the proposed method, the spectrum shared WSNs based on radio environment database is shown Section 3. We discuss simulation results in Section 4, and finally, Section 5 concludes this paper.

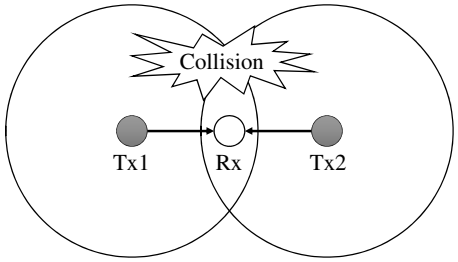


Fig. 1: Hidden node problem in the same system.

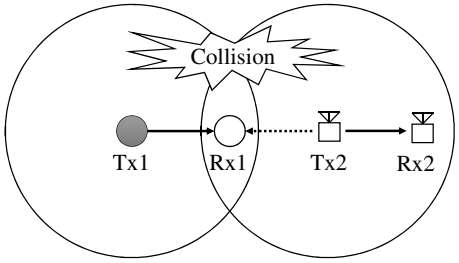


Fig. 2: Hidden node problem in the difference systems.

2. SYSTEM MODEL

In this section, the proposed method is explained in two phases. Phase1: The database construction phase as shown in Fig.3. The sensor nodes gather information from surrounding radio systems, and the radio environment database is constructed. Phase2: The database utilization phase as shown in Fig.4. The spectrum manager considers interference of surrounding radio nodes, and selects an appropriate channel.

In the database construction phase, sensor nodes upload sensed information to the database. Uploaded information is utilized in the spectrum sharing with surrounding radio system. To obtain surrounding radio system information, signal source information is required. In this paper, MAC address of signal is fully utilized, and the sensor nodes are constructed by software radio. Because software defined radio is able to change the radio communication method, the sensor nodes can gather the surrounding radio information. Uploaded information by sensor nodes is five as follows to obtain surrounding environment information.

1. Sensor node ID of itself.
2. Source MAC address of observation signal.
3. Destination MAC address of observation signal.
4. Center frequency of observation signal.
5. Instantaneous received power of observation signal.

These information are gathered from many sensor nodes. Uploading method is that the sensor nodes use the same frequency

for the surrounding nodes and communicate to the database. In database construction phase, the sensor nodes cannot avoid HNP arbitrarily as before.

In the database utilization phase, the spectrum manager utilizes the surrounding radio information stored in the database, and decides utilized channel by sensor nodes. The database has observation information measured in each sensor node. The average received power of observation signal is calculated from the database information. The spectrum manager is able to decide hidden node compared with the carrier sense level and average received power. If the average received power is higher than carrier sense level, CSMA/CA performs to avoid the interference, therefore HNP does not occur. Accordingly, the spectrum manager selects the channel which is possible to share the spectrum by CSMA/CA. If the average received power is lower than the carrier sense level, CSMA/CA does not work for avoiding interference, therefore HNP occurs. Accordingly, the spectrum manager does not select the channel that is not possible to share the spectrum by CSMA/CA. The spectrum manager notifies the selected channel to sensor nodes. After that, sensor nodes utilize the notified channel for data communication.

3. SPECTRUM SHARED WIRELESS SENSOR NETWORKS BASED ON RADIO ENVIRONMENT DATABASE

In this section, we explain WSNs that utilize radio environment database and share the spectrum. The purposes of this method are that the spectral efficiency is increased by the appropriate channel selection for communication and HNP avoidance. In order to share the spectrum considering mutual interference, it is necessary to detect the surrounding hidden nodes existence. The proposed channel selection method for spectrum sharing is indicated in Fig.5.

First, the data stored in the database are statistically processed. The uploaded information in the database, which is sensed by sensor nodes is utilized to know the topology of the surrounding nodes for hidden node decision.

Second, the surrounding nodes of the sensor nodes are categorized into the average received power. In this part, the spectrum manager detects the hidden nodes for the sensor nodes.

Third, the channels utilized for WSNs are categorized by hidden nodes and network ID. In this part, the spectrum manager decides whether the channels are on the status of HNP. Because WSNs giving interference to the surrounding radio systems have to be avoided, we select the channel to avoid HNP.

Fourth, the spectrum manager decides the channel which is utilized by WSNs. In this part, the spectrum manager selects the channel considering HNP and spectrum efficiency, and the flowchart is over.

In this section, we explain statistical data processing, categorization of the surrounding nodes and the channels. The adaptive channel selection algorithm is also discussed.

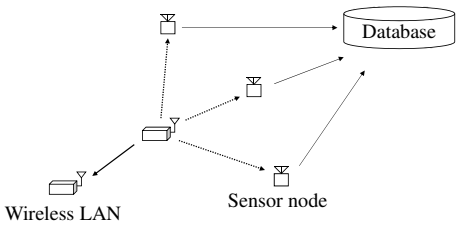


Fig. 3: The database construction phase.

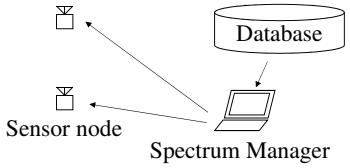


Fig. 4: The database utilization phase.

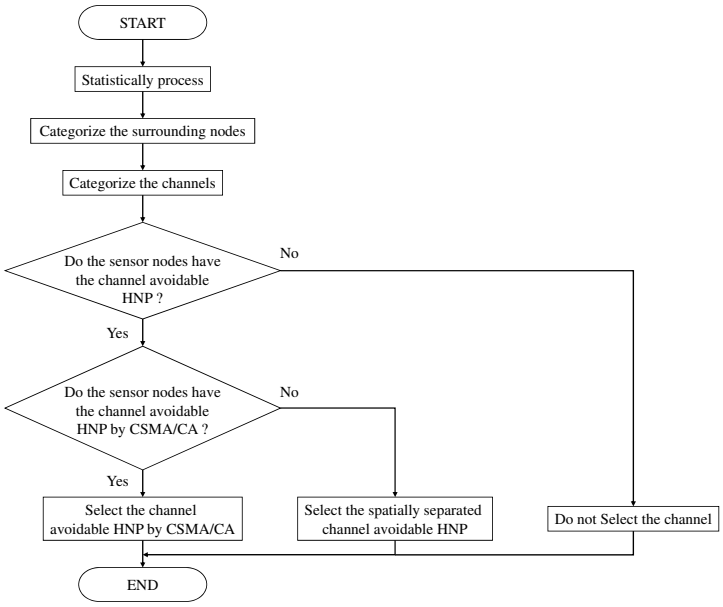


Fig. 5: Channel selection flow.

3.1. Notice to topology with statistically sensed data

If we consider the spectrum sharing with multiple systems, the existence of hidden node highly affects network reliability. Therefore, it is necessary for the spectrum manager to detect the channel with the hidden node. The gathered physical layer information from each sensor node, however, cannot understand network topology and the existence of the hidden node clearly. In order to utilize the information stored in the database, the gathered information is taken statistics processed. By using statistical sensed information, the spectrum manager makes the surrounding nodes list of each sensor node, and the topology list of

radio environment.

First, the spectrum manager makes the surrounding node list of each sensor node. A list has the MAC address of the surrounding nodes, the average received power and channel. The average received power is calculated by averaging the instantaneous received power on each source MAC address. This list is made to add the information which is received by sensor nodes.

Second, the spectrum manager makes the topology list of radio environment. The spectrum manager adds relationship between the source MAC address and the destination MAC address in the topology list, and makes network ID for each access point (AP). Network ID is an identifier of the network stored in the radio environment database. Each AP has different ID to recognize the source MAC address and the destination MAC address based on the topology list. If AP connects to some nodes, AP has the same ID to some nodes. The spectrum manager understands the topology of the surrounding radio systems by the topology list.

By comparing the two lists, the spectrum manager knows the topology of the surrounding radio system and interference power.

3.2. Categorize the surrounding nodes of the sensor nodes

In this subsection, the condition for detecting existence of hidden node is shown. The nodes which are surrounded by the sensor nodes are categorized into three cases as shown in (1),

$$\begin{cases} \text{Possible carrier sense} & (P_{\text{ave},i} > P_{\text{cs}}) \\ \text{Mutual interference,} \\ \text{Impossible carrier sense} & (P_{\text{cs}} > P_{\text{ave},i} > P_{\text{ai}}) \\ \text{Mutual noninterference} & (P_{\text{ai}} > P_{\text{ave},i}). \end{cases} \quad (1)$$

$P_{\text{ave},i}$ is the average received power from node i. P_{cs} is the carrier sense level. P_{ai} is is allowable interference power at the sensor node and the surrounding radio systems. This is the mutual interference threshold. "Possible carrier sense" means the nodes can detect the signals from the primary system for spectrum sharing. "Mutual interference, Impossible carrier sense" means the nodes is difficult to detect the primary signals for spectrum sharing, in which the hidden node exists and leads to a network degradation. "Mutual noninterference" means the nodes cannot detect the signals by carrier sense but the mutual interference is low because the primary system is far from the node. As a result, this channel is able to be utilized with spatial separation.

3.3. Categorize the channel

Unusable channel is eliminated based on the categorized node topology. As an example shown in Fig.6, the sensor node is able to share the spectrum with the same categorized system in the channel with available carrier sense without any hidden node or the channel without interference due to spatial separation. However, if the channel shared with different categorized system is

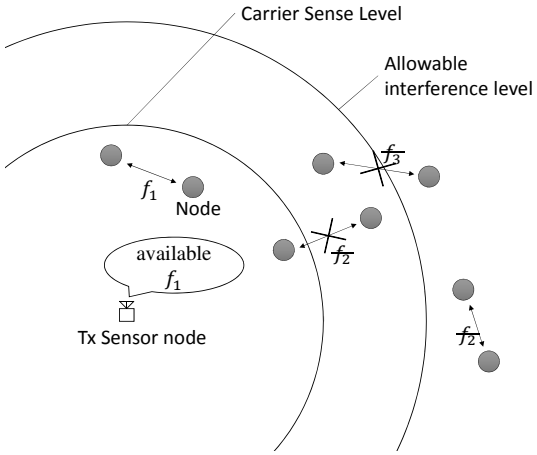


Fig. 6: Avoid hidden node problem by understood the topology.

located on the outside of the carrier sense area, HNP is happened. Therefore, the sensor node cannot utilize f_3. Because WLAN topology cannot be known based only on the received power at the sensor nodes, it is difficult to handle the HNP in different system spectrum sharing environment. On the other hand, if the node can utilize MAC address information of the source node and the destination node, it is possible for the sensor node to detect the hidden node. Therefore, if we apply the above procedure, we can select the channels without HNP and effectively share the spectrum between different systems.

3.4. Channel decision

The fulfilled channel is selected from candidate channels categorized in the transmitter sensor node and the destination sensor node. At this time, WSNs utilize the available CSMA/CA shared channel as possible, accordingly spectral efficiency is improved. If there are either channels satisfied avoiding HNP by CSMA/CA or allowed received interference level of the destination node, the channel avoiding HNP is selected to avoid interference to WLAN. From the above operation, WSNs avoid HNP to protect WLAN and establish communication without hidden node by CSMA/CA. Additionally, spectral efficiency is improved by the proposed operation.

4. SIMULATION

In this section, the proposed channel selection method is evaluated by the packet arrival rate of WLAN and WSN, and the independent channel utilization ratio. Simulation parameters are shown in Table 1. Here we assume WLAN is connected peer to peer network and the proposed method is evaluated by increasing the number of WLAN pairs. We assume only channel 1 or 2 has WLAN as primary systems. WSN is detected by the spectrum manager and the connection is established in the selected channel by the spectrum manager. It is assumed that WLAN

does not have interference from other WLANs and other WSNs in this simulation. Two channels are occupied by WLAN, and the one spatially separated channel unused by WLAN is available for WSN. Both systems WLAN and WSN share the spectrum by using CSMA/CA. If signal-to-interference-plus-noise ratio (SINR) is lower than the certain value, packet is assumed to be lost, and the lost packet will not be resent. The sensor node position is satisfied that the received power of the destination sensor node from the source sensor node is higher than -80dBm in this simulation.

The number of WLANs versus the packet arrival rate sharing the spectrum with WLAN and WSN using channels 1 and 2, is shown in Fig.7. The vertical axis is the packet arrival rate and the horizontal axis is the number of WLAN pairs in each channel. From Fig.7, it is clear that the packet arrival rate of the proposed method is better than the random channel selection regardless of the number of WLAN pairs in each channel. Additionally, the packet arrival rate is higher than 95% regardless of the number of WLAN pairs in the proposed method. This is because channel for spectrum sharing considered to the dedicateed channel is used. In contrast, the packet arrival rate of WSN decreases in the random channel selection, as the number of WLAN increases. SINR is lower than the desired SINR because the HNP is caused even using CSMA/CA. It is considered that a few packet loss is affected by the allowable interference level. In this paper, the allowable interference level is set to be -85.0dBm. However, when active nodes have low SNR, the packet arrival rate of active nodes may be interfered by the allowable interference. Therefore, the allowable interference level is necessary to be set based SNR of active nodes. The proposed method shows sharing spectrum by channel selection except low SNR.

The number of WLANs versus channel utilization ratio on each channel of WSN, is shown in Fig.8. In Fig.8, the vertical axis is the channel utilization ratio of sensor nodes and the horizontal axis is the number of WLAN pairs in each channel WSN utilized the channel 1 and channel 2 as possible because channel 3 can be remained for other systems. If there is hidden node, WSN utilizes the channel 3, which is no WLAN channel evaluated by the proposed method. When the number of WLAN is small and WLAN occupation area is sparse, WSN can share the same channel from channels 1 and 2. However, when the number of WLANs is large, WLANs occupation area is crowded and the HNP may be happened. Therefore, WSN utilizes the independent channel in most cases, and occasionally share the spectrum without hidden node. Consequently, WSN selects suitable channel corresponding to the surrounding radio environment.

From above results, the proposed method is shown that WSN utilizes the independent channel at the existence of the hidden node, and shared spatially separated idle channel without hidden node. Since by increasing the number of WLAN nodes, the HNP is happened frequently, WSN utilizes the independent channel without WLAN to avoid hidden node. However, if WSN has the available channel for sharing the spectrum with WLAN,

Table 1: Simulation parameters.

Field size	100×100 m^2
Number of sensor nodes	2
Position of sensor nodes	Random
Number of WLAN of each channel	[1,10]
Position of WLAN nodes	Random
Number of channels	3
Frequency	2.4[GHz]
Transmission power	10.0[dBm]
Channel	Propagation loss based on exponential mode, AWGN
Path-loss exponent	3.5
Carrier sense level	-62.0[dBm]
Allowable interference level	-85.0[dBm]
Average AWGN	-100.0[dBm]
Desired SINR	10.0[dB]

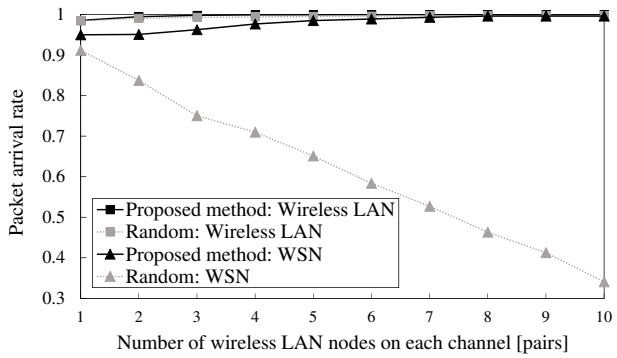


Fig. 7: The number of WLAN versus packet arrival rate.

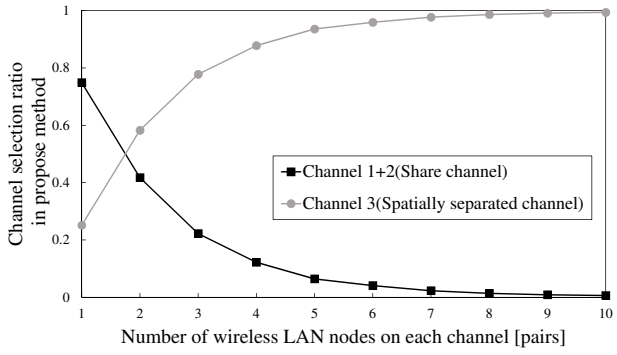


Fig. 8: The number of WLAN versus channel utilization ratio on each channel of WSN.

WSN shares the spectrum regardless of the number of WLANs. If we apply the random channel selection, WSN may transmit the data on the channel with hidden node by CSMA/CA. As a result, the required SINR is not satisfied and the packet arrival rate becomes low. From the above results, the proposed method is confirmed that WSN can avoid HNP, and can efficiently share

the spectrum with surrounding nodes under WLAN existence.

5. CONCLUSION

We propose an highly efficient wireless sensor networks by recognizing the surrounding wireless network topologies by using radio environment database in spectrum sharing with WLAN. The purpose of the proposed method is that WSN avoids the HNP and increases spectral efficiency by CSMA/CA without hidden nodes. In this paper, each sensor node gathers radio environment information, and uploads them to the radio environment database. The spectrum manager decides to share channel with WLAN according to the information of the database. The spectrum manager also utilizes MAC address for channel selection because the topology of the WLAN nodes can be utilized for improving the spectrum sharing efficiency. Then WSN shares the spectrum with WLAN without HNP. The proposed method was evaluated by computer simulation and confirmed that WSN can avoid the packet loss due to HNP, and efficiently shares the spectrum with surrounding WLAN nodes.

ACKNOWLEDGMENT

A part of this work is supported from the Ministry of Internal Affairs and Communications (MIC) of Japan under 2014 SCOPE R&D for Very High Efficient Wireless Sensor Networks with Environment Recognition.

REFERENCES

[1] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, pp. 92–101, June 2010.

[2] M. Yigit, E. Yoney, and V. Gungor, "Performance of mac protocols for wireless sensor networks in harsh smart grid environment," *First International Black Sea Conference in Communications and Networking*, pp. 50–53, July 2013.

[3] A. Rahman and P. Gburzynski, "Hidden problems with the hidden node problem," *Biennial Symposium in Communications*, pp. 270–273, 2006.

[4] A. Qayyum, M. U. Saleem, Tauseef-Ul-Islam, M. Ahmad, and M. Khan, "Performance increase in csma/ca with rts-cts," *Multi Topic Conference in INMIC* , pp. 182–185, Dec 2003.

[5] F. Inoue, M. Morikura, T. Nishio, K. Yamamoto, F. Nuno, and T. Sugiyama, "Novel coexistence scheme between wireless sensor network and wireless lan for hems," *IEEE International Conference in Smart Grid Communications* , pp. 271–276, Oct 2013.

A New Security Paradigm for SDR Terminals

Rafael Aguado, Eduardo Solana {rafael,eduardo@globalsdr.com}

***Abstract* – As Software Defined Radio (SDR) terminals evolve, their security requirements become significantly more complex. The network capabilities and the new features introduced in such terminals (such as SNMP) shorten the differences between the traditional network security and SDR-based security.**

The typical command and control headquarter has evolved during the last few years, where the hardware based terminals have been replaced by SDR terminals working together seamlessly in different network configurations supporting voice and data and operating both in broadcast and point-to-point modes.

This joint scenario results in new security requirements as the increased connectivity drive the tactical communications closer to cloud connection domain. This paper proposes a change in the security paradigm.. Many systems fail because designers protect the wrong things or even worse, the right things in a wrong way. The survey will not only study the architectural paradigms, but will also explore the main data paths established among the different subsystems, highlighting where the risks and threats are in a practical approach, identifying what has to be protected and the best ways to do so. Lastly the paper will investigate how the last version of the JTNC SCA framework, influences the security mechanisms that need to be established in order to fulfill the requirements from the standard.

***Index terms* – SDR, SCA, Security, Black Red separation, Software Radio, Signal Processing**

I. INTRODUCTION

According to [1] [2], Software Defined Radio (SDR) refers to the capabilities of the Radio Systems to be upgraded via software updates or reconfigurable through software commands. The adoption of these technologies minimizes the number of required terminals while increases their lifetime. Although is not military centric, from 1999 until nowadays the evolution of the military communications has been based on the SDR architectures, with the JPEO JTNC SCA [3] as the main exponent.

Nowadays the tactical communications deployment configurations have greatly changed their requirements and CONOPS (Concepts of Operations). A typical deployment requires different kinds of communications equipment, connected to different kinds of networks depending on:

- Throughput and topology requirements
- LPD (Low Probability of Detection) / LPI (Low Probability of Interception) requirements
- Anti-jamming and resilience capabilities
- High speed capabilities
- Legacy systems

This situation has provoked the co-existence of multiple proprietary solutions that hardly interoperate. The figure below shows the JTNC Inc 1 deployment [4] where all the different networks and Waveforms are depicted:

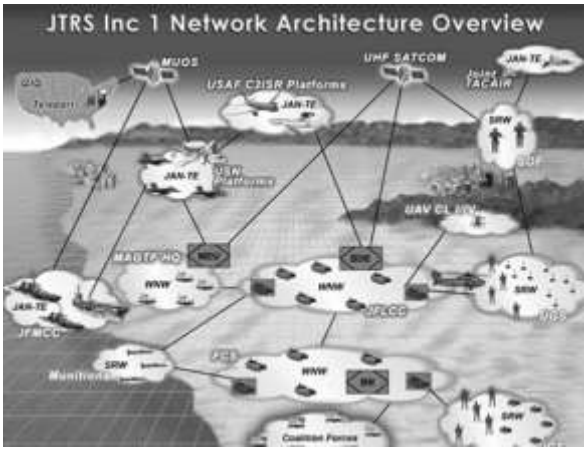


Figure 1. JTNC Inc 1 Network Architecture

According to Dennis Bauman [4], Joint Program Executive Officer for the Joint Tactical Radio System, SDR and SCA capabilities are the main enabler of the final GIG (Global Information Grid) scenario.

The US DoD [5] enforces this scenario by highlighting: "The GIG must be designed and optimized to support warfighting functions of advantaged and disadvantaged users, to include mission partners, across the full range of military and National Security operations in any operational environment. The GIG must also be resilient and able to support the missions despite attacks by sophisticated adversaries"

Working in parallel to the US DoD GIG, the NATO NNEC [6] initiative proposes the ability to federate various capabilities at all levels, military (strategic to tactical) and civilian, through an information infrastructure.

This situation shorten the differences between a cloud connected network and the combat scenario, where the tactical equipment is deployed. The introduction of new information sources like sensor networks or UAV's, or the interoperability with civilian or public safety equipment in Other-Than-War missions', enforces more the idea of an over-connected network.

As the requirements and the CONOPS change, the technology has to evolve accordingly. This over exposition of the systems provokes an increase of the threats that can alter or make an unauthorized usage the network.

There are few proposals providing a secure framework for SDR terminals [39]. On [7] a secure framework is proposed, that covers a particular threat on the field of operations, safe guarding the subsystem that the SDR terminal exposes to the network. A proposal for an implementation of a secure SDR architecture is presented in [8], making use of the main security standards for Security Services [9] and Crypto Subsystems [9]. The traditional approach for SDR security audit is based on a systematical inspection of the SDR architectonical components [10] because it was considered that the SDR equipment would be deployed in a restricted connection environment, where the definition of secure areas can be established. However, as it was presented, the radio equipment is no longer considered as an isolated node, but as part of a complex network deployment.

This survey is based as well in SDR terminals which implement the well-known JTNC SCA standard but focuses on the information that has to be shared across the network and how to protect it.

II. CURRENT SOLUTIONS FOR A SECURE SDR ARCHITECTURE

II.1 JTNC SECURITY ANNEX

The SCA standard version 2.2 includes a security supplement [18] [22] that defines the U.S. Government security requirements for JTNC radios, a security API and suggests a high level architecture for a secure SCA-compliant radio. The JTNC security architecture is composed of separate partitions: the red partition, the black partition and the cryptographic subsystem. The red partition stores and processes sensitive information unencrypted or with a low level of protection, and black partition handles non-sensitive or encrypted information. Both partitions are connected by a cryptographic subsystem, which has a bypass mechanism for data that can be transferred unencrypted between black and red partitions.

A SCA-compliant radio set that implements the JTNC security architecture is described in [36]. The security supplement suggests a physical separation between partitions, i.e., it recommends separate processors for the red and black partitions, and a third one for the cryptographic subsystem. This physical partitioning of functions should also take into account compromising emanations, which involves both the distribution of power and electromagnetic emissions. Depending on the level of confidentiality of the information processed by the red partition, electromagnetic shielding, physical distancing and electrical isolation of physical partitions are mandatory [37] [38].

Both the Red and Black domains contain a full SCA stack, and most SCA components are replicated in both partitions, with few exceptions. One major exception is the Domain Manager. In a SCA-compliant radio, the Domain Manager component controls the whole radio domain and there is one Domain Manager per radio set. There are advantages and disadvantages of allocating the radio control component either in the red or black partition [39]. Usually, the Domain Manager is instantiated in the red partition and it uses the bypass mechanism to communicate with components in the

black partition. If the black partition is compromised due, for instance, to an attack that exploits buffer overflow vulnerabilities, the confidential data stored in the red partition is not exposed. Furthermore, due to the hardware implementation of cryptographic algorithms and other security features in the cryptographic subsystem, enough bandwidth is available to encrypt/decrypt all data that are transmitted or received. The hardware components of the cryptographic subsystem provide a reliable root-of-trust for the radio set as a whole. A hardware root-of-trust is important because trusting all the radio software is an unreasonable option [39]. However, the widespread utilization of the bypass mechanism in some implementations represents a major weakness of the red-black paradigm [39].

II.2 EUROPEAN SECURE SOFTWARE RADIO

The target of the ESSOR Program is to provide the basis for development and production of Software Defined Radio (SDR) devices in Europe to meet the requirement for fielding such equipments in Europe within the timeframe of 2011-2015, but final schedule will depend on national implementations.

The main outcomes of the ESSOR program can be organized in two main areas of interests:

- ESSOR Architecture. A common architecture, shared by the Participating States that defines the framework for the development of radio platform software and associated security elements.
- High Data Rate Waveform. The HDRWF is a high data-rate multi-hop mobile ad hoc network, self-organizing and self-healing.

A milestone of paramount importance of the ESSOR program is to define a reliable secure architecture compliant with the SCA framework and the ESSOR Architecture [32], with the purpose of achieve an improvement on interoperability among EU Members States, USA, NATO and homeland security communication systems.

With the requirement of maintaining as much compatibility as possible with the publicly available specification of the JTNC SCA, the ESSOR Architecture building blocks have been organized as follow:

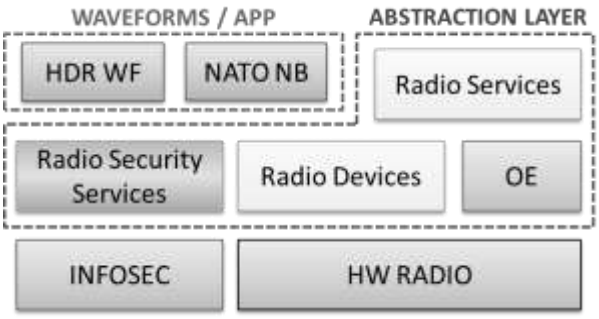


Figure 2. ESSOR Platform Building block

The ESSOR architecture takes as baseline the JTNC SCA Architecture for its different building blocks. This assumption can be extended to the Security Architecture definition, in which the JTNC Security Supplement has been taken as reference. The entities constituting the Radio Security Services will provide the security functionality defined in the scope of the ESSOR Program, taking also into consideration the requirements inputs from the HDR WF.

The ESSOR Architecture inherits from the JTNC Security Supplement the implementation of the Red (plain text) – Black (ciphered) frontier based paradigm, as stated by the platforms that will implement the European standard [33].That means that the RSS components will have to be used to access the security functionality from the Crypto Subsystem.

The constraint of being compatible with the JTNC SCA makes the ESSOR architecture fulfill the requirement of CORBA [34] usage as middleware. This means that a bypass mechanism would be implemented in the ESSOR compliant platforms, to assure communication between components located in the Red and Black subsystems.

All these conclusions result from the above mentioned references since all the material regarding security has been considered classified by the ESSOR Community.

II.3 WINNF INTERNATIONAL RADIO SECURITY SERVICES API

The release of the JTNC SCA v2.2 in 2001 supposed a significant game changer in the SDR development. This specific version of the standard is structured to fulfill two main specific goals [12]:

- Increase portability of applications amongst SCA platforms
- Reduce the WF development cost, time and resources

After more than ten years, the JTNC maintains in the new version of the SCA [3] the same goals, enforcing the importance of success in these objectives. Several initiatives both governmental [13] [14] and industrial [15] [16], have followed this mandate encouraging the certification of SCA compliant platforms.

The SCA was initially targeted for the military domain, therefore security is always present and enforced. However, this security layer has been turned into a mayor stopper for WF portability and all the above initiatives on Platform and Waveform SCA compliancy certification keep security consequently out of the scope.

In order to mitigate this problem, the JTNC included in the SCA v2.2 a Security Supplement [18], providing guidance on how to implement the Security layer of a SDR Device. However this supplement was not completely alien to comments and criticisms [19], indicating the reduced number of requirements that were covered by the supplement. The JTNC officially deprecate the Security Supplement after the release of the version 2.2.2 of the JTNC SCA [20] in favor a JTNC-specific security specification.

This situation impulses the creation of the Security Working Group at the Wireless Innovation Forum, which in 2011 releases the International Radio Security Services (IRSS) API [17]. The working group focuses during the development of this API on the military and tactical domain. The API is intended to be deployed on tactical radios implementing the JTNC SCA specification, though SCA is not a requirement for its use.

Following the aforementioned objective on WF portability, the IRSS API intention is to maximize the portability degree between various radio platforms that provide the same API. This API enforces also the framework paradigm from the JTNC SCA standard, and allows its deployment in non SCA compliant platforms.

II.3.1 API Organization

It's impossible to obviate the fact that the security layer in the military tactical communications has been historically considered as classified material and any effort on standardization has always been withdrawn.

The new effort from the Wireless Innovation Forum relies on the usage of the three categories of security coined by the EDA [31]. This model assumes the existence of three levels of classification:

- Open. Public standard that is potentially accessible by everyone.
- Coalition. This category is for more sensitive purposes and would be accessible only be trusted partners.
- National. Classified information only accessible by national stakeholders.

Taking into account these considerations, the way this API is intended to be used is to allow access to the first category, or the other two through a transformation layer. The picture below describes how the access to each category can be performed:

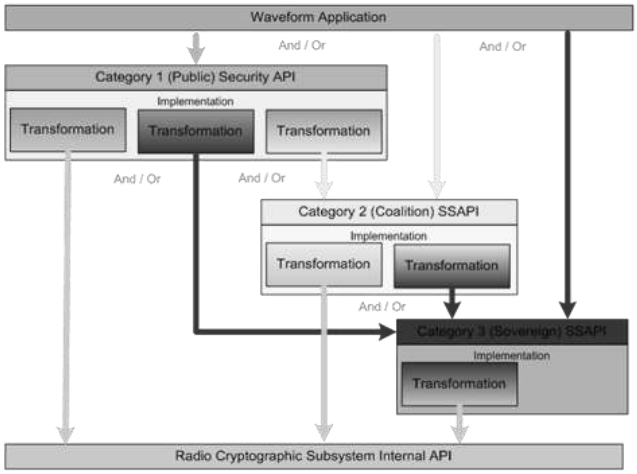


Figure 3. IRSS category model

The IRSS API is centralized on the usage of the different channels (cryptographic, TRANSEC, platform, bypass) that can be established between the Crypto Subsystem and the security domains. This statement has driven the group to divide the API in the following groups [17]:

- The *control service* group details interfaces used to establish, configure, and otherwise

manage channels for services provided by this API.

- The *Infosec service* group details interfaces for usage of cryptographic channels and TRANSEC channels.
- The *bypass service* group details interfaces for usage of bypass channels used to transfer waveform control information between security domains (e.g. Red and Black subsystems) without encryption.
- The *integrity and authentication service* group details interfaces for features such as generating hashes, generating message authentication codes (MACs), generating and verifying digital signatures, and generating random numbers.
- The *protocol service* group details interfaces that allow waveforms to interact with Cryptographic Applications (CAs), using a generic protocol to perform CA-specific functions.

The IRSS API doesn't make any assumption on how many security domains the final SDR Device has and provides different components connections configurations for each situation. The figure below represents the IRSS SCA component connections configuration with a WF user in a typical two security domains situation:

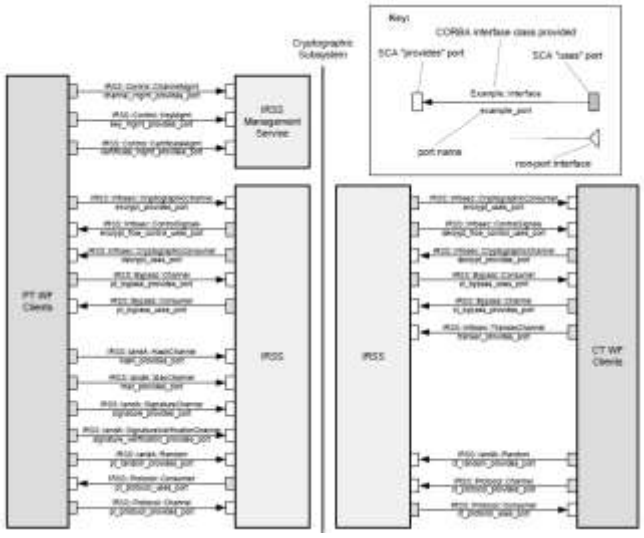


Figure 4. Connection schema between IRSS and WF components

The specification has been developed by the consensus of the working group members, focusing on WF portability constraints, however there are some improvements that can be taken into account for future releases.

The certificates are generally used in background to support other secure operations and are part of the basic key management protocols. The structure of the certificate and its format is out of the scope of the API as it is waveform dependent. Alternatives for its structure can be found at ITU [21].

A channel is understood as a communication path between a WF client and the Cryptographic Subsystem. The different channels that can be created are:

- TRANSEC channels.
- Bypass channels.
- Hash channels.
- MAC channels.
- Signature channels.
- Signature verification channels. channels are used to verify a signature
- Protocol channels.

Although it has been said that JTNC has been pulled back, the Security Supplements both in [18] and in [22] specify the usage of PTF channels for certain operations like bypassing platform specific information or configuration.

Most of the commercial solutions [23] [24] available in the market provide also bypass data channels for waveform specific functionality.

As discussed in the case of certificates, the support of the IRSS API standard for key management is reduced to what the platform supposed to support, leaving to waveform or application specific usage.

From an operational scenario perspective, some basic black-key management [25] [26] would be desirable to be gathered in the standard, to achieve certain degree of reusability among different waveforms.

II.3.2 COMPARISION AGAINST SECURITY SUPPLEMENT

As has been aforementioned the International Radio Security Services has been published to foster and improve waveform portability. This approach has been already followed by the Security Supplement. However

there are significant differences among one solution and the other. The following table synthesizes the differences between both solutions. In order to understand the legends:

¨X¨ means the API supports completely the functional group

¨□¨ means the API supports partially the functional group

– means the API doesn't support the functional group

Group/Primitive	IRSS	SS
Management::Zeroization	□[1]	X
Algorithm::Management	–	X
Bypass::Channel	X	X
Control::ChannelMgmt	X	X
Control::KeyMgmt	X	□[2]
Control::CertificateMgmt	X	X
Infosec::CryptographicChannel	X	X
Infosec::TransecChannel	X	X
IandA::HashChannel	□[3]	X
IandA::MacChannel	X	–
IandA::SignatureChannel	X	X
IandA::SignatureVerificationChannel	X	–
IandA::Random	X	–
Protocol::Channel	X	–
Security::Management	–	X
Fill::Port	–	X
Alarm::User	–	X
Time::Management	–	X
GPS::Management	–	X

Table 1. Comparition between IRSS and JTNC Security Supplement

Architectural

In general terms, the Security supplement considers the API as a monolithic component and assumes two security domains, named Red and Black sides for plain text and ciphered text respectively.

On the other hand the IRSS API proposes a more structural solution allowing the creation of several components even considering some of them as optional. The API considers also the possibility of having one or two security domains.

According to [27] [28] it's a requirement for all the JTNC equipment to be able to *zeroize* sensitive information contained by the crypto, such as keys, certificates, algorithms, security policies or users.

The Security Supplement [22] provides through the management service a `ZEROIZE_ALL` command, which allows the user to zeroize all the sensitive information. Further investigation on these topics reveals that in [29], the JTNC states that not only zeroization is a required functionality, but also Over-The-Air-Zeroization (OTAZ) is expected.

There's no discussion [27] [28] on the need for implementing a Fill interface for a tactical radio. As a platform dependent the security supplement proposes a set of functions that covers the operational requirements for such requisite.

The International Radio Security Services does not consider the management of the algorithms as a requirement. The general consensus is to consider algorithms as the core of the Crypto functionality as they support most of the operations [29].

Although it can be discussed that the suitability of managing the whole lifecycle of the algorithms, from loading from an external device to its installation in the crypto module, the API should offer the management of the algorithm's ID.

The Security supplement provides a strong support for security policies in order to secure the access to the crypto and to manage all the possible contingences and exceptions. The IRSS takes the other lane leaving all the security policies to WF management.

Conflicts

There are several modules that are specified in the Security Module not gathered in the IRSS:

- The Security Supplement supports the management of Alarms as stated in [30] [22]. This is a consequence of the lack of support for security policies.
- The Security Supplement specifies also the possibility of using GPS and Timing support. It's important to highlight the differences between this functionality modules and the

[1] Only Key zeroization
[2] Not possible to update the key with a given algorithm
[3] Not sign of hash streams

analog JTNC SCA Components defined in [3]

Finally the IRSS proposes different modules to be implemented to provide further support for waveform portability:

- The IRSS provides a Random generation module, to support the management of random numbers as a support other modules.
- In order to support waveform specific needs, the IRSS provides a Protocol channel.
- The IRSS also provides MAC functionality support.

As a concluding remark, it seems clear that both specifications share most of the functionality provided by the platform to ensure waveform portability. It is precisely the existence of the Protocol channel functionality and the transformation layer mechanisms what puts the IRSS API in the frontline for a true standardization of the access to the Secure Subsystem. It is also clear for the authors that the API has to be extended to consider platform needs.

II.4 CRYPTO API STANDARDS

On the tactical domain, the Crypto API shares with the Radio Security API the same problematic, most of the available documentation is considered confidential by the governments and radio manufacturers don't disclose their API solutions.

There is another consideration that has to be made before entering in further details that also affect WF portability. Nowadays, the Crypto Subsystem is not part of the SCA standard; hence it doesn't follow the constraints imposed by the SCA framework.

This situation increases the portability efforts from a waveform development stand point. However there are different publicly available solutions that achieve a compromise alternative between portability and security. The transformation layer concept mentioned in §II.3 can also be applied to this standards to achieve a secure implementation of the Crypto subsystem.

Nowadays, the most successful initiative on the field is the CICM (Common Interface to Cryptographic Modules) standard [10]. Although this standard is not specifically tailored for SCA or SDR devices, it can be adjusted to fulfill the constraints required for this kind of equipment. As it was mentioned in chapter §I. on [8] the CICM is studied in order to identify what can be used as a reference and what functionality has to be increased to be able to implement it in SDR devices.

Besides detailed and specific questions on technical details there is a major controversial on the usage of bypass mechanisms. It is not foreseen in the CICM specification the usage of bypass mechanisms to allow plaintext data flows between different subsystems. This is a major stopper since the SCA architecture specifically allows, and requires, such communications.

III. SDR THREATS AND RISKS

As the functionality and connectivity capabilities of SDR equipment tend to converge into flexibly configurable and networked IT devices, one should apply the lessons learned in the computing and internet security arena.

Most of the security breaches and vulnerabilities we have witnessed for the last two decades result from poorly designed architectures considering security as a feature or in the worst cases, as last minute patch following a devastating attack. For all these years a number of authors, security experts and IT practitioners have emphasized on the need to consider security as a design principle for building solutions rather than a feature to be added to an existent system conceived with no security in mind.

Unfortunately the IT mass market and the Internet as a global network are clear examples on how things should not be handled from a security perspective. Initial PC hardware designs (still fundamentally valid nowadays) didn't take security arguments into consideration and the same applies to operating systems both commercial and open source.

The last few years, as security concerns were growing in the society, have brought forward new architectures based on trusted devices that are properly supported by widely available operating systems. The same applies to the Internet, a stack of protocols initially designed with "insecurity" in mind that has become the perfect playground for an infinite number of all sorts of blended attacks. The undergoing transition versus the

security sensitive protocol set present in IPv6/IPsec constitutes a promising direction but still threatened by very significant challenges and with relatively limited scope of application as of today.

A number of excellent surveys on SDR security [11] [35] have extensively defined SDR security requirements, together with the most significant threats and corresponding countermeasures. The solutions presented (certification, secure download of waveforms, software validation, tamperproof modules, entity strong authentication, parameterized security zones, etc.) are well known and tested mostly in IT network environments.

Although we consider that classical security solutions will be needed in any serious secure SDR architecture, we consider that at these early stages of secure SDR, a prominent effort should be devoted to emphasize the "security as design principle" paradigm and consequently define solutions and architectures with security in mind.

As an example, the SDR classical architecture featuring a crypto module separating the black and red zones presents clear advantages in terms of concentrating all the key material and sensitive data in a well-defined module performing all the cryptographic operations. Unfortunately, the need for establishing management channels between the physically separated red and black zones introduces the need to create bypass tunnels that compromise the isolation principle and as a result, the security of the whole system. Furthermore, a closer look at the different information flows in the red zone shows that, in some cases, confidential data flows in the clear and that any encryption solution would need the intervention of the crypto module, resulting in significant complexity added to the whole system. An in-depth analysis of the information flows associated with a risk-based approach would be needed to redefine the cryptographic protection needed to secure these flows and the appropriate architecture needed to store and manage the cryptographic keys based for instance in trusted modules providing the appropriate (hardware) protection to this cryptographic material.

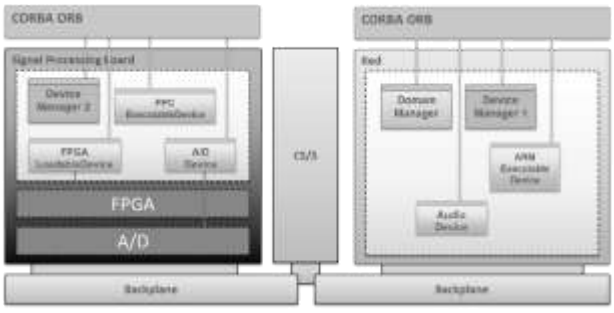
Another example of an insecure architectural issue that needs to be considered is the ability to remotely manage the equipment through the SNMP protocol. It is widely known that this protocol, especially in its very early implementations has resulted in important vulnerabilities to the host systems. A risk-based analysis would be needed to balance the trade-off between the simplified management advantages that this protocol brings and the security risks it creates, especially in public safety and military environments.

As a final remark, one cannot draw an accurate picture on SDR security without considering realistic scenarios where SDR equipment are subject to serious attacks and stress conditions in terms of security. Classical IT and network security has made its most important advances in a very hostile framework of "real-life" attacks. The extremely sensitive nature of the data handled by these SDR systems together with the multiple implications of the service availability and accuracy will make it the target of choice for politically and economically motivated adversaries. So we consider that together with the architectural and design considerations presented here, a comprehensive and realistic set of real condition tests will need to be conducted.

IV. A NEW PROPOSAL

In the current JTNC SCA [3] specification there is no reference on how to provide information assurance in a SCA compliant SDR equipment. Having said that, there are sufficient indications in [18] [19] or in [8] to establish the well-known Red and Black architecture as a *de facto* solution for this kind of military graded equipment.

The picture below shows the basic diagram of the architecture under discussion:



The diagram shows an architecture based on a secure domain (Red) in front of a public area (Black) protected

by a perimeter (CS/S). This perimeter acts as a Zone of control, which means (military definition):

"The perimeter is the outer edge of a zone of control that enables adequate resupply, protection, coordinated communications and movement"

However equating Red Domain to Zone of control can be dangerous and erroneous. The system is partitioned in two domains (Red and Black) with different tasks and purposes. However, both domains share components (or components types) that can have small differences (or even different implementations), deriving in a duplicated source code management and maintenance of those components.

The Red / Black Architecture forces the implementer to two separate boards for each domain. Both subsystems have different needs and requirements

- Red – That is focused in upper layers of the communications protocol stack, Management, and data acquisition
- Black – Lower levels of the communications protocol stack and signal processing

This architecture requires the existence of a cryptographic subsystem (in most of the cases NON CORBA-capable) element between the processing boards forcing the developer to provide a bypass mechanism. This situation increments the number of resources of the development and may have impact on the COTS solutions available in the market.

At this point, it's of paramount importance to highlight that most of the Security Annex of the JTNC SCA [18] focuses on this bypass mechanisms, but due to the lack of support on the CS/S proprietary solutions shall be provided.

Even with a domain separation approach, the literature on SDR security [11] [35] identifies most of the threats on the Black domain of the terminal:

- Insertion of malicious code
- Alteration / destruction of: configuration data, RTOS software, WF software, CF software, Middleware Software
- Artificial consumption of resources
- Unauthorized use of SDR services

Therefore, the main objective of the attackers of a Tactical network is precisely to shut down the terminal and/or other networks.

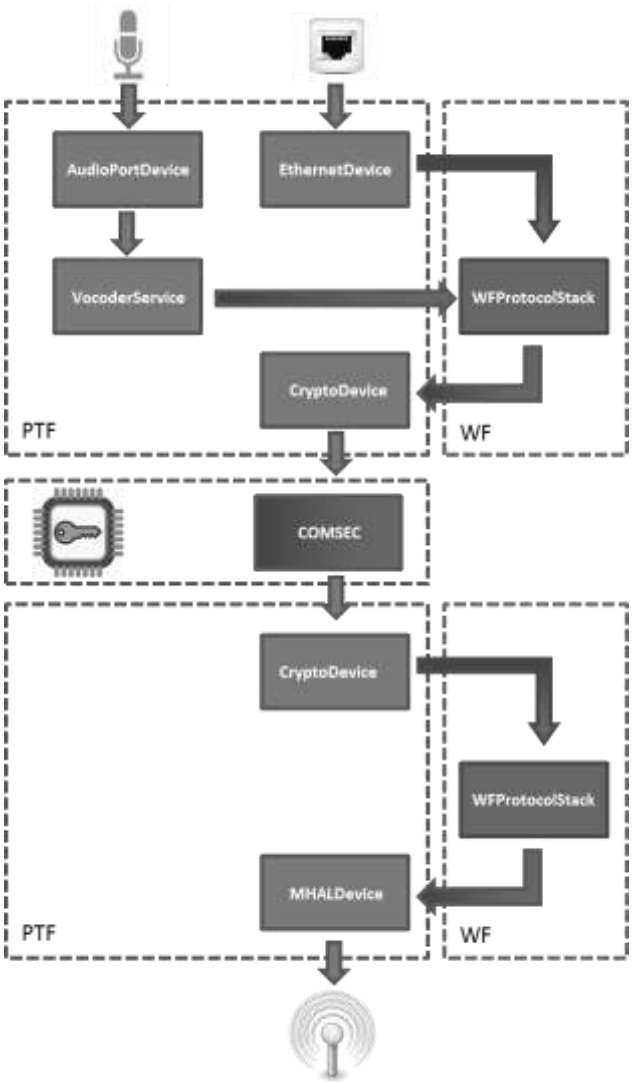
It's has been identified that Black components shall get or set information on Red components, that even assuming those component are trustable, can derive in dangerous situations (Resource DoS). So the question we are highlighting here is whether the Red domain components get closer to the Black domain or *vice versa*. Where the line between the red and black domains should be drawn?

In order to answer these questions, this security proposal is be based on the study of the different data flows that may be established within the boundaries of the SDR equipment. In the scope of this study, not all the scenarios will be described.

The voice and data flows share some similarities in their study, where only the stream acquisition changes. Following the JTNC SCA standard, the components involved in the data and voice paths are:

- Data Path: The *EthernetDevice* is in charge of acquiring the data from the actual Ethernet port. This acquisition is supposed to be secure.
- Voice Path: The *AudioPortDevice* and *VocoderService*

After the acquisition of the data the components used to transmit or receive the information are the same. The stream is directed to the WF protocol stack for its routing and from there to the *CryptoDevice* and through the Crypto Subsystem. The data is received by the *CryptoDevice* that complete the cycle sending the information to the waveform protocol processing components and once the data is routed, to the *MHALDevice* (if DSP or FPGA are present in the system).



In the tactical communications environment, the most common objectives are:

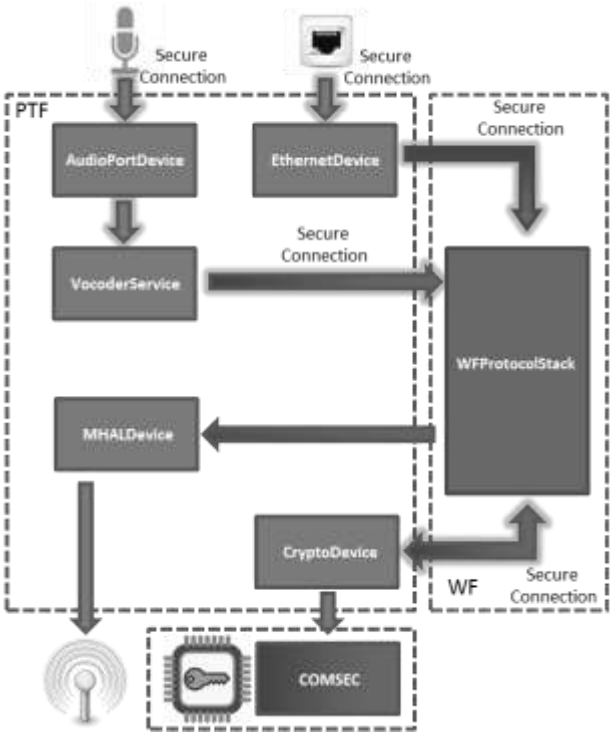
- Intelligence agency: To retrieve information from the enemy communications
- Operational agency: To jam enemy communications.

However, as the COMSEC capabilities are getting more and more complex, the discussion between the agencies end soon. The content of the communications can't be retrieved, so the efforts are now on jamming the radio communication signal to shutdown the network.

All these statements drove us to establish a more simplistic assumption on the SDR architecture but increasing the resilience of the components and the communications among the components.

The view that concentrates the security risks in the black domain is quite simplistic in the opinion of the authors. One can expect that ethernet, serial and even microphone interfaces could represent threats vehicles that could compromise the system security "from the inside". One clear example is the above mentioned SNMP protocol that has proved to be a significant security danger by topping the list of exploited network vulnerabilities for years. Furthermore, in a foreseeable future other protocols allowing to enhance usability, management and control of SDR systems will possibly be introduced and deployed. No doubt that these protocols will piggyback their own set of vulnerabilities that may potentially be exploited by enemies and motivated adversaries. Our architectural proposal focusing on component and data flow security protection provides a powerful means to address this risk scenario whereas the black-red dichotomy falls short.

The proposal is to consider the boundary between red and black domains at component level, leaving the overall architecture domainless.



The most obvious consequence of engaging this solution is a huge improvement on equipment´s SWaP But also, simplifying the design, the development cost is reduced dramatically.

V. CONCLUSIONS AND WAY AHEAD

The paper has gone through the security solutions that are become mandatory in the development of military graded equipment.

Those solutions may have resolved the security problems that appeared with the birth of the SDR technologies, but as the tactical networks become more and more complex, the threats and vulnerabilities also evolve.

It has been proved that an architecture based in a secure domain in front of a public domain may not bring as many benefits as expected, because in essence all the main attacks of the SDR equipment are focused in the public domain.

These assessments drove us to define a domainless model in which the Red / Black boundaries are defined at component level, rather than at board level.

This solution pretends to focus in three main areas:

- Update the security solution to nowadays problems
- Optimize the hardware design of the equipment
- Streamline the software development, allowing the team to focus in one domain only.

Future work will be focus on the implementation of the security mechanisms that will have to be deployed to establish communications among the components, including algorithms, key management and trusted computing bases. More precise policies will need to be established among the different components allowing the implementations to define invocations more precisely.

VI. REFERENCES

[1] Mitola, Joe. The software radio architecture. Communications Magazine, IEEE May 1995

[2] What is Software Defined Radio? Wireless Innovation Forum. http://www.wirelessinnovation.org Last accessed 08/30/2010

[3] JPEO JTNC SCA. http://jpeoJTNC.mil/sca/Pages/default2.aspx. Last accessed 08/30/2010

[4] Sharon Anderson, Steven A. Davis. The Joint Tactical Radio System – Reloaded. September 2006.

http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=3076

[5] US DoD The Global Information Grid (GIG) 2.0 Concept of Operations Version 1.1

[6] NNEC Portal http://nnec.act.nato.int/default.aspx. Last accessed 08/30/2012

[7] Murotake, Martins, 2009. A high assurance wireless computing system (HAWCS™) for software defined radio.

[8] Aguado et al, 2010. Settling a SDR Reference Security Architecture, Wireless Innovation Forum Technical Conference

[9] Leubner, Aguado, et al, 2010. A technical overview of the International Radio Security Service API for tactical radios. Military Communications Conference, 2011 - MILCOM 2011

[10] Lanz and Novikov, 2011. Common Interface to Cryptographic Modules v3.0.

[11] Baldini et al. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead

[12] Software Communications Architecture Specification MSRC-5000SCA V2.2 November 17, 2001 Joint Tactical Radio System (JTNC) Joint Program Office

[13] JTNC Test and Evaluation Laboratory http://jtnc.mil/Pages/AboutJTEL.aspx Last accessed 09/07/2014

[14] European Defence Agency. European SDR Standardization and Certification feasibility study (ESSaC).

[15] Wireless Innovation Forum. Test and Certification Guide for SDRs based on SCA, Part 1: SCA. SDRF-08-P-0007-V1.0.0

[16] Wireless Innovation Forum. SCA Certification Guide #2. WINNF-10-P-0012-V1.0.0

[17] Wireless Innovation Forum. International Radio Security Services API Task Group.

IRSS API Specification. WINNF-09-S-0011-V1.0.0

[18] Joint Tactical Radio System (JTNC) Joint Program Office. Security Supplement to the Software Communications Architecture Specification. MSRC-5000 SEC v1.1. November 17, 2001

[19] Bunnell and Trinidad. The Challenge in Developing an SCA Compliant Security Architecture that Meets Government Security Certification Requirements.

[20] JPEO JTNC. JPEO JTNC Approves New Release of the Software Communications Architecture June 16, 2006

[21] ITU X.509 : Information technology http://www.itu.int/rec/T-REC-X.509 Last accessed 09/06/2014

[22] Joint Tactical Radio System (JTNC) Joint Program Office. Security Supplement to the Software Communications Architecture Specification. JTNC-5000 SEC v3.0. August 27, 2004

[23] Aeronix - ASM Programmable Crypto Module Reference Design. http://www.aeronix.com/services/high_assurance_crypto_reference_design/asm_crypto_reference_design. Last accessed 09/07/2014

[24] Harris - Communications Security & Encryption Products. http://rf.harris.com/capabilities/communications-security/embeddable-encryption.asp Last accessed 09/07/2012

[25] Attila Gulyás - Hungarian Defence Forces - Enable command and control (C2) for Special Operation Forces through SDR applications

[26] Ross Anderson – Security Engineering Second Edition.

[27] Joint Tactical Radio System (JTNC) - Operational Requirements Document (ORD) April 2003

[28] Multiservice Communications Procedures for Tactical Radios in a Joint Environment – June 2002

[29] Performance Requirements Document (PRD) for Joint Tactical Radio System (JTNC) Rifleman Radio Full Rate Production – February 2012

[30] Information Technology – Open Systems Interconnection – Systems Management; Security Alarm Reporting Function – ITU Recommendation X736

[31] Towards SDR standardisation for military applications – European Defence Agency

[32] SDR and CR standardization and certification – A4ESSOR – ISPRA 2011

[33] TERSO - Spanish Research Platform Ready For Service http://www.afcea.org/content/?q=node/1383 Last accessed 25/09/2012

[34] ESSOR Architecture - Motivation and Overview – WinnF Technical Conference 2010

[35] System Threat Analysis For High Assurance Software Defined Radios – Murotake D., Martin T.

[36] Kurdziel, M. Beane, J. Fitton, J.J.. An SCA security supplement compliant radio architecture. In: Proceedings of the Military Communications Conference, 2005. MILCOM 2005. IEEE

[37] TEMPEST Tempest Fundamentals, NSA-82-89, NACSIM 5000, National Security Agency, 1982. Available at http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm

[38] TEMPEST NSTISSAM TEMPEST/2-95, Red/Black Installation Guidance, 12 December 1995. Available at http://cryptome.org/jya/tempest-2-95.htm

[39] Davidson, J.A. On the Architecture of Secure Software Defined Radios. In: Proceedings of the IEEE Military Communications Conference, 2008 (MILCOM 2008)

[40] Gallo, R., Kawakami, H., Dahab, R. On Device Establishment and Verification. In the Proceedings of the EuroPKI 2009.

[41] Swanson,M., Bartol, N., Moorthy, R. Piloting Supply Chain Risk Management Practices for Federal Information Systems. Draft NIST IR 7622.

[42] Standaert, F.-X., Malkin, T.G., and Yung, M. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In: Advances in Cryptology – Eurocrypt 2009. Lecture Notes in Computer Science, 2009, Volume 5479/2009, pp. 443-461

FIELD TESTS OF DATABASE-ASSISTED V2V COMMUNICATIONS OVER TV WHITE SPACE

Onur Altintas, Koichi Seki, Kohsuke Nakagawa,
Toshihiko Watanabe, Haris Kremo and Hideaki Tanaka

TOYOTA InfoTechnology Center Co., Ltd.
6-6-20 Akasaka, Minato-ku, Tokyo, Japan
{onur, ko-seki, nakagawa.k, nabe, hkremo, hi-tanaka@jp.toyota-itc.com}

ABSTRACT

Using a centrally authorized geolocation database is recently being ruled as the preferred method of primary user protection in certain markets. The secondary user must be location aware, and must periodically access the database querying the information regarding available white space. In centralized network topologies, base stations can query the database on behalf of individual users. In an ad-hoc vehicle-to-vehicle communications setting, additional wireless connectivity to query the database would be necessary in each vehicle. On the other hand, depending on the market, the regulators require that a mobile node perform a database query whenever it moves for more than 100 meters. If this rule is adopted for vehicular networks, a vehicle traveling at 100 km/h would create one database query every 3.6 seconds. A better way of accomplishing this could be to have one vehicle act as a proxy to obtain information from the database and distribute it among its peers, not only for the current location but also for "future" locations, by taking hints from the vehicles' velocity vectors. In this paper, we first describe the general architecture which makes dual use of a geolocation database and spectrum sensing. In this architecture, whenever a database query result is available, that information is prioritized over sensing results and when the database access is disrupted, vehicles rely on the spectrum sensing results. After describing the general concepts, we present the middleware-centric implementation and field test results of a multi-hop vehicle-to-vehicle communications over the licensed TV-band. We present results regarding multi-hop throughput, delay, jitter, channel switching and database access latencies.

1. INTRODUCTION

"Connected vehicle" and communications among vehicles are not anymore future concepts with the automobile manufacturers increasingly employing wireless communications technologies in new vehicles. Advanced driving support applications which rely on wireless communications among the vehicles, aiming to increase driver awareness and situation perception are being envisioned to help decrease accidents. Similarly, traffic flow efficiency is expected to improve by using such technologies [1].

In 1999, the U.S. Federal Communication Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz band for dedicated short-range communications (DSRC) to be used by intelligent transportation systems (ITS). Ever since then, applications of one-way or two-way vehicle-oriented communications have evolved into various forms. Recently, 9 MHz of spectrum centered at 760 MHz band has been allocated for ITS in Japan. Europe has allocated 30 MHz of spectrum in the 5.8 GHz band for ITS. Furthermore, several standards supporting vehicular communications have already been designed, e.g., ARIB STD-T109 in Japan, IEEE 1609 and IEEE 802.11p elsewhere.

Currently, the number of vehicles which are capable of performing wireless communications is a mere fraction of the total current market. Furthermore, the spectrum requirements of these vehicles presently are relatively low compared to wireless applications deployed in other sectors. However, not only the communications among vehicles, but also the communications between people, objects and vehicles are expected to become ubiquitous in the future, resulting in a significant increase in the accompanying spectrum and capacity requirements. This requirement of spectrum may further be enhanced by the developments in automated driving systems where autonomous vehicles might need to exchange significant amount of sensor and image data in real-time. Eventually, vehicular applications might suffer from spectrum scarcity and overcrowding, as has already been experienced by other mobile wireless communications sectors. For example, one recent study [2] looks into the spectrum requirements of vehicular communications for safety applications in which more than

80 MHz of spectrum is deemed as necessary for a packet error ratio of 1%.

To this end, one candidate solution will be to look for spectral resources elsewhere, as in the dynamic spectrum access (DSA) paradigm where unlicensed devices temporarily borrow licensed but spatially and/or temporally unused spectrum. In the rest of this paper, we will first briefly touch upon our previous work regarding DSA for vehicular communications in general, and V2V communications over TV white space in particular. Following that, we will continue with the description of the database assisted vehicular communications system underlying concepts, and a brief description of the architecture. Finally, we will present the middleware-centric implementation and field test results of a multi-hop vehicle-to-vehicle communications setup over the licensed TV band. Results regarding multi-hop throughput, delay, jitter, channel switching and database access latencies will be presented.

2. PREVIOUS WORK

Applying the dynamic spectrum access concepts to mobile environments brings additional challenges due to the mobility of the participating hosts. All of the existing standards center around a fixed or nomadic base station (or access point) in which a master-slave relationship exists. In vehicle to vehicle communications, this type of architecture becomes less relevant since most of the communications occur among vehicles in a geographically confined but continuously moving area.

Broadcast television spectrum becomes one possible candidate for dynamic spectrum access in vehicular environments thanks to its relatively static channel utilization. In order to opportunistically access the unused spectrum, vehicles must be aware of their spectral environment. This can be accomplished by incumbent user signal sensing or by geolocation database lookup, neither of which works perfectly in a vehicular setting [3].

In [4] we described the system architecture and reported field test results of multi-hop vehicle to vehicle communications over TV white space among three moving vehicles. The system relied on limited spectrum sensing capabilities of the emulated TV signals in the test area. A set of autonomous and distributed control and data channel selection algorithms for vehicle to vehicle communications which can work in an unknown spectral environment were developed and demonstrated.

Complementing the system in [4], in [5] we extended the system design so as to include dual use of sensing and database information. We presented the general design and operation principles of a vehicle to vehicle system in which the TV white space information is obtained from a centrally authorized white space database. In the following section we will briefly review that architecture as well as the system operation, and describe implementation of the middleware that governs the flow of events.

3. ARCHITECTURE AND SYSTEM OVERVIEW

Using a centrally authorized geolocation database is recently being ruled as the preferred method of primary user protection in certain markets. The secondary user must be location aware, and must periodically access the database querying the information regarding available white space. In centralized network topologies, base stations and access points can query the database on behalf of individual users. In an ad-hoc vehicle-to-vehicle communications setting, additional wireless connectivity to query the database would be necessary in each vehicle.

Additionally and depending on the market, the regulators require that a mobile node performs a database query whenever it moves more than 100 meters. If this rule is adopted for vehicular networks, a vehicle traveling at 100 km/h would create one database query every 3.6 seconds. A better way of accomplishing this could be to have one vehicle act as a proxy to obtain information from the database and distribute it among its peers, not only for the current location but also for "future" locations by taking hints from the neighboring vehicles' velocity vectors.

3.1. Dual Use of Geolocation Database and Spectrum Sensing

Since the centrally authorized geolocation database is (at least at present) the preferred method of primary user protection [6][7], the vehicles must be able to identify their location and query the database for available white space. In addition to the database access, we allow for spectrum sensing as the fallback option in case that the database access is lost, owing to high mobility of the network nodes (Figure 1).

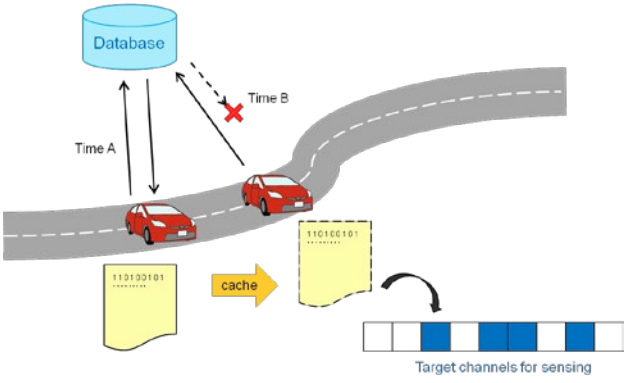


Figure 1. Dual use of database and sensing.

When flipping to spectrum sensing as the method of spectrum awareness, the sensing subsystem obtains the list of vacant channels in the cache (effectively the last database access results) and builds a channel sensing plan by skipping the occupied channels.

If, for some reason, database access cannot be restored for a prolonged time, the system might end up starving spectrum in the worst case. This happens due to the sensing subsystem not visiting the previously occupied channels and continuously detecting other occupied channels as the vehicle changes location in time. To avoid spectrum starvation, we come back to the occupied channel list in the cache and select *n* channels randomly to include in the target channels for sensing list. Details of this scheme are explained in the flowchart in Figure 2.

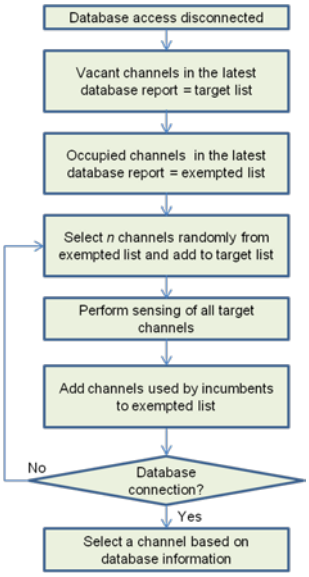


Figure 2. Database and sensing flip-over with spectrum starvation hedging.

To reduce load on the wireless 3G/4G network used to query the database, we implemented two procedures: 1) the vehicles which constitute the network swarm (described below in Section 3.2) select a proxy in charge of communication with the database and dissemination of the spectrum availability within the swarm; and 2) the proxy downloads spectrum availability information for multiple locations on the road in advance.

The proxy is selected based on its *x*-*y* Cartesian coordinates. The area map is divided into a mesh. All vehicles compare their location within a square field in the mesh (which we call the "distribution area") to the center of that area. A vehicle which is presently at, or close to the center of the distribution area queries the database. This information is periodically announced on the distribution control channel (DCC). Since we assume congestion of the 760 MHz/5.9 GHz licensed band, it cannot be used to distribute the database information. Thus, the proxy simply selects the white space channel which will be available for the longest distance, as the DCC. Other nodes simply sequentially listen all TV channels, starting from the lowest index, until they discover the DCC. Conveniently, this discovery procedure must be performed only in case of a "cold start", or when a vehicle travels over a completely new trajectory. This concept is presented in Figure 3.

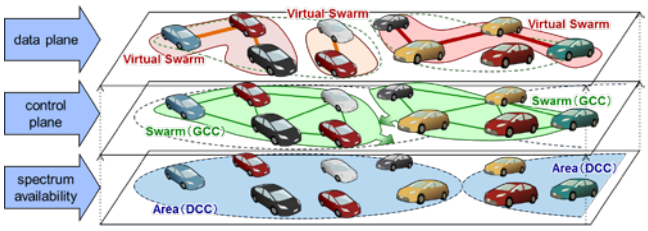


Figure 3. General concept showing the control and data plane separation with actual and virtual swarms of vehicles.

Current FCC regulations require that a mobile white space node perform database query whenever it moves for more than 100 meters [6]. To act as a simple remedy for excessive queries to the white space database in case of high mobility of the nodes, the regulations allow for prefetching of data. As the trajectory of vehicles, at least to the next intersection, is highly predictable, the proxy can trade a number of per–point database queries for a single query addressing multiple locations. The query process can further be made efficient by filtering out the "cells" that the road curvature is clearly not passing through, thus decreasing the amount of information that needs to be shared with other swarm members. From another point of view, by excluding the irrelevant cells from the query, a longer "look ahead" in terms of available spectrum might be possible.

On the other hand, if a proxy is querying the database on behalf of the others, as in a swarm, then a more comprehensive pattern which includes other vehicles' position and speed vectors is required. This relevant-cells-only concept combined in case of three vehicles is illustrated in Figure 4.

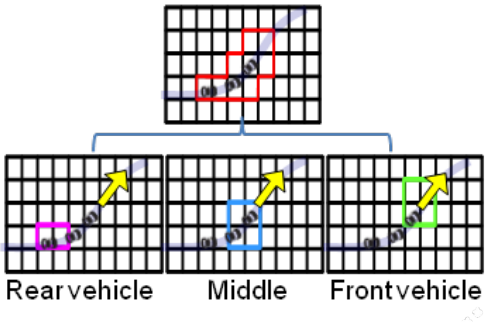


Figure 4. Database query area for a three-vehicle swarm

3.2. Formation of swarms

In addition to querying the database, the information about location of nodes is needed to establish and maintain network topology. Suitably, localization is already an important part of the licensed DSRC network design. To fulfill traffic safety assistance tasks, the vehicles broadcast their data including their identifier, location, speed, heading, and acceleration in the licensed 760 MHz or 5.9 GHz band. These messages are broadcasted periodically, for instance ten times per second, as defined in the SAE J2735 [8], the ETSI ITS [9], and the Japanese Advanced Safety Vehicle (ASV) Message Set specifications [10]. From the information received about its neighbors, each vehicle can create and maintain a swarm table. These swarm tables are not maintained with perfect accuracy, because high mobility of nodes causes frequent changes in the network topology as vehicles travel with different speeds and frequently merge and leave roads.

Given that the role of DCC is to share (announce) channel availability information, and that padding of additional information on the DSRC broadcast packets is not in compliance with the relevant standards mentioned above (i.e., SAE J2735, ETSI ITS, J-ASV), the remaining issue is how to exchange swarm related information among the swarm members. A mechanism is needed on the application (data) plane to form "virtual swarms" of nodes which run a certain application and requires data exchange. The virtual swarm nodes must congregate to the same white space channel and select a data route in the case of multi-hop exchanges. In our design, the necessary information is shared over the group control channel (GCC). Note that these control and distribution channels can be logical or physically allocated channels.

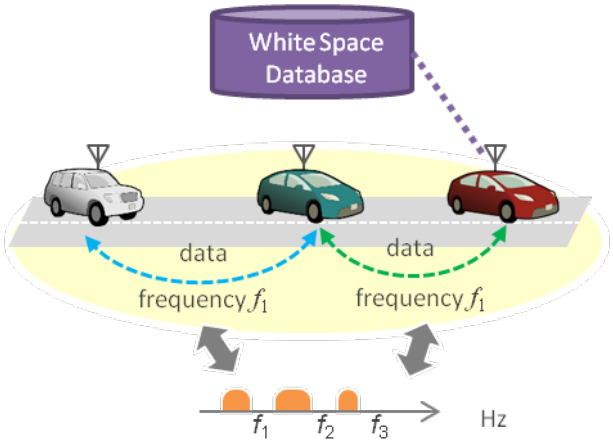


Figure 5. Outline of the field tests.

3.3. Database Design

The database used during the field tests is developed and implemented by the National Institute of Information and Communication Technology (NICT) of Japan. It was implemented in such a way that divided the entire Japanese archipelago into cells of 100m x 100m resulting in approximately 550 million cells in which the incumbent TV station information is calculated per channel. Cells were identified by their latitude and longitude identifiers in addition to a cell number. The database was located in Yokosuka City, approximately 900 km away from the test site, and was accessed via the 3G/LTE networks.

4. FIELD TESTS AND RESULTS

We obtained experimental licenses for five TV channels, through channel 13 to 17 of 5.7 MHz of width each, centered at 473, 479, 485, 491 and 497 MHz. The license was effective for several weeks until the end of March 2014, covering a 5 km stretch of the public roads in Miyazaki, southwestern Japan. The power limit for the TV band devices was approximately 80 mW over these five channels. TV band devices employed OFDM without channel bonding. Relevant parameters are summarized in Table 1.

Location	Misatocho, Miyazaki
Channels	TV Ch 13 to 17 (470-500 MHz)
Bandwidth	5.7 MHz/channel
Output Power	79 mW
Modulation	OFDM 64QAM
Database	NICT-Yokosuka, access via 3G/LTE

Table 1. TV band device operation parameters.

The tests involved three vehicles with a camera installed on the headrest of one of them as shown in Figure 6. An application that transferred real-time video images from the car with the camera to other vehicle(s) was implemented and used during the tests. Vehicles traveled at or below 40 km/h, the speed limit for the public roads in the test area. Note that, while the camera is installed in only one of the cars, the sequence of the vehicles need not be as shown in Figure 6 as the location based routing scheme implemented in the middleware core uses a so-called georouting algorithm. In other words, depending on the position of the source and destination(s) of the application, the routing scheme builds and maintains a route that takes into account the actual coordinates of the vehicles. This scheme was also tested by changing the sequence of the vehicles without changing the source and destination of the application to confirm that the position of the source (car with video camera) triggers a makeover of the routing table in all cars.

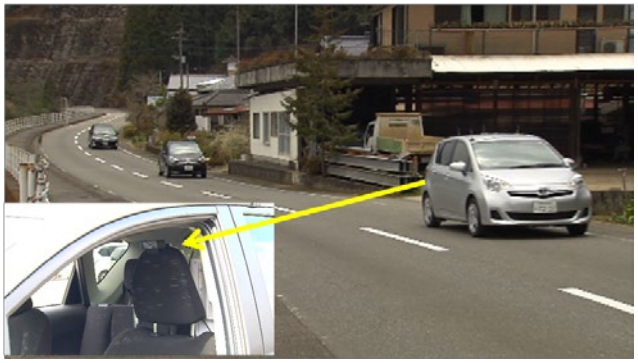


Figure 6. Field tests with a front-view camera installed in the lead car transferring real-time video images to others.

4.1. Throughput and Delay

We first measured the throughput of the system without the relay car in between the source and destination (i.e. single hop). The values vary depending on the distance between the cars, however the average is roughly 5 Mbps. When the relay car is introduced in between the source and destination (i.e. two hops) the average throughput drops to around 2 Mbps. This is a known issue stemming from the shared media access of all three cars. Theoretically, end-to-end throughput can be maintained the same in multi-hop structures if each hop uses a different channel, however this requires extra hardware and/or other sophisticated schemes such as full-duplex radio. The throughput results for TCP and UDP, as well as the packet loss percentage and end-to-end delays are summarized in Table 2 for a packet size of 1470 bytes. The distance between the cars in the single hop measurements was around 140 meters, and was 185 meters in total with two hops.

	Throughput (TCP)	Throughput (UDP)	Packet Loss (UDP)	e2e delay
One hop	4.64 Mbps	6 Mbps	-	3.1 msec
Two hops	2.24 Mbps	2.7 Mbps	1%	7.2 msec

Table 2. Throughput, delay and loss performance results for single hop and two hops.

Figure 7 presents a snapshot of the display inside the rear car showing the near real-time video feed being received from the lead car. Video codec delays in these tests were much more significant than the packet transmission delays (2 seconds versus 7 msecs).

Figure 8 zooms into the user interface inside the rear car showing real-time operating parameters. Upper portion shows the data route active in between the cars, middle portion shows the spectrum sensing results, and the lower portion shows database query results coming from the proxy car overlaid onto the actual map of the test area. More will be said about sensing performance below.

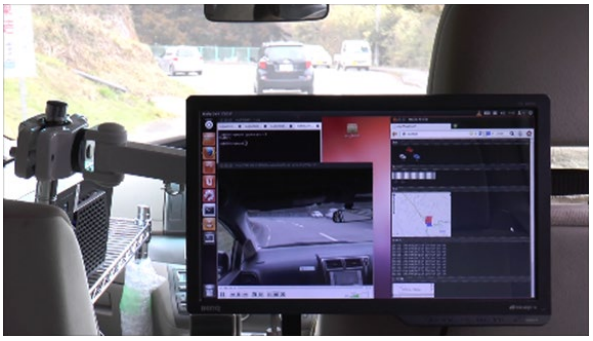


Figure 7. Snapshot of the view inside the rear car showing video feed from the lead car.

Figure 8. User interface in the rear car showing routing, sensing and database overlay.

4.2. Incumbent Sensing

As for the sensing of incumbent signals, we implemented a cross-correlation method that looks into a single segment of the 13-segment Japanese digital terrestrial broadcast scheme (ISDB-T). In ISDB-T, HDTV broadcast signal occupies 12 segments, and the remaining single 428 KHz segment is used for mobile terrestrial digital audio/video and data broadcasting (the so-called 1seg service). Our sensing implementation was tuned to detect signals on this 1seg service band which sits in the center of the TV channel. Sensing capability of the radios was -108dBm/430KHz (-111.3dBm/200kHz). Figure 9 presents results pertaining to detection probability of the 1seg signals. These results were obtained when the vehicles were stationary. For comparison, we provide spectrum analyzer screen shots of the corresponding channels in Figure 10. We also observed false alarm rates of 15%, 7% and 1% for channels 43, 44 and 46, respectively. The false alarm usually spreads to other channels too when the vehicles are not stationary.

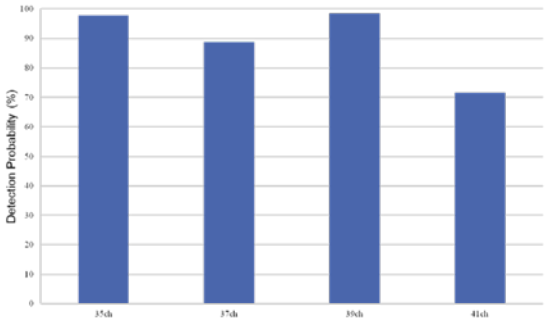


Figure 9. Incumbent detection probability for channels 35, 37, 39 and 41.

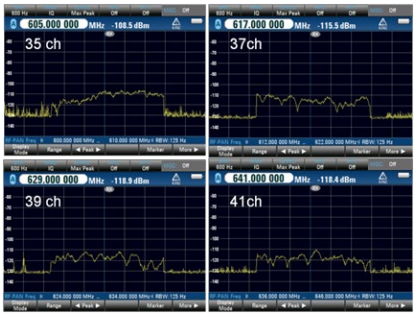


Figure 10. Spectrum analyzer screen shots of the corresponding channels in Figure 9.

4.3. Database Access and Channel Switching Latencies

Database access takes 9 seconds for cold start for 3G which includes connection setup times and 0.3 seconds for LTE, respectively. For the subsequent queries, response time decreases to 0.4 seconds for 3G and to 0.12 seconds for LTE on average per query.

As the vehicles traveled from an area with no incumbent signal on the borrowed channel, to another area with incumbent activity on that channel, they switched channels by negotiating over the group control channel (GCC). We measured the time to switch in between the channels. Vehicles traveled at approximately 40km/h and with 40-50 meters of separation during channel switchover tests. Switchovers were performed for the following patterns: Ch 14 → Ch 16, Ch 16ch → Ch 15, Ch 15 → Ch 16, Ch 16 → Ch 14. The time that the channel on the first hop change from a soon-to-be occupied channel to a vacant one, on the average, is 2.69 seconds and the time it takes for both hops change the channel is 2.70 seconds. Most of this delay comes from the radio to "settle" on a new channel.

4.4. Delay Jitter Analysis

Finally, we present results of delay jitter analysis. As mentioned previously, end to end delay times are 3.1 and 7.2 msec for one-hop and two-hop scenarios, respectively. Jitter varies similarly for both topologies. Average jitter in single hop topology is 2.35 msec and that of two-hop topology is 5.88 msec. Corresponding distribution patterns of the jitter for one-hop and two-hop topologies are given in Figure 11 and Figure 12. Note the wider distribution with two humps in case of the multi-hop topology.

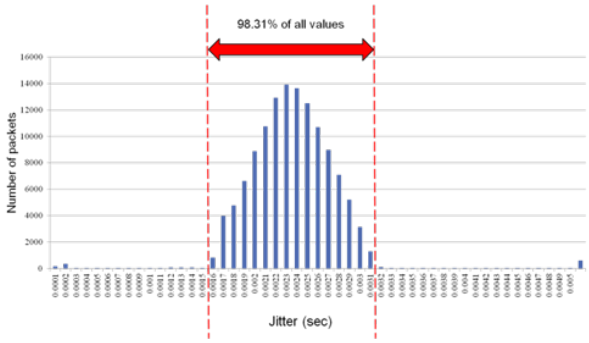


Figure 11. Jitter distribution for one-hop topology.

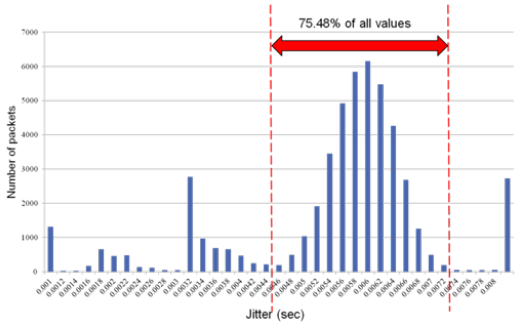


Figure 12. Jitter distribution for two-hop topology.

5. SUMMARY

In this paper, we have presented an architecture that makes use of a centralized TV white space database to determine the spectrum opportunities for V2V communications. We implemented and tested the system in the field by using licensed TV channels and presented results pertaining to throughput, sensing, channel switchover, database access latencies, end-to-end delays and jitter. Future work would look into scalability of the inter- and intra-swarm schemes with proxy elements distributing the database information.

6. ACKNOWLEDGEMENT

Part of this work was supported by the "FY2012 Revised Budget for Research and Development into Expanding Radio Wave Resources" of the Japanese Ministry of Internal Affairs and Communications.

7. REFERENCES

[1] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," *IEEE Communications Surveys & Tutorials*, Vol. 13, Issue 4, pp. 584–616, 2011.

[2] L. Shi and K. W. Sung, "Spectrum Requirement for Vehicle-to-Vehicle Communication for Traffic Safety," in *IEEE Vehicular Technology Conference 2014 Spring*, Seoul, S. Korea, May 2014.

[3] H. Kremo and O. Altintas, "On Detecting Spectrum Opportunities for Cognitive Vehicular Networks in the TV White Space," *Springer Journal of Signal Processing Systems*, Vol. 73, Issue 3, pp. 243-254, Dec 2013.

[4] Y. Ihara et al., "Distributed Autonomous Multi-Hop Vehicle-to-Vehicle Communications over TV White Space," *Proc. 10th IEEE CCNC 2013*, pp. 330-338, Las Vegas, NV, USA, Jan. 2013.

[5] O. Altintas et al., "Database Assisted Vehicle-to-Vehicle Communications over TV White Space," in *Wireless Innovation Forum Conference on Wireless Communication Technologies and Software Defined Radio*, Schaumburg, IL, USA, Mar. 2014.

[6] Federal Communications Commission, "FCC 10–174: second memorandum and opinion and order in the matter of unlicensed operation in the TV broadcast bands, additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band," Washington D.C., 2010.

[7] Ofcom, "Implementing Geolocation," *http://stakeholders.ofcom.org.uk/consultations/geolocation/*

[8] Dedicated Short Range Communications (DSRC) Message Set Dictionary, *http://standards.sae.org/j2735_200911/*

[9] ETSI TS 102 637-2: Intelligent Transport Systems (ITS) Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, 2013.

[10] Advanced Safety Vehicle Message Set, *http://www.mlit.go.jp/jidosha/anzen/01asv/resourse/data/asv4pamphlet_seika.pdf*

TRANSMISSION DECISION ALGORITHM FOR UPDATING SENSING INFORMATION

Mai Ohta (Department of Electronics Engineering and Computer Science, Fukuoka Univ., Fukuoka, Japan; maiohta@fukuoka-u.ac.jp); Osamu Takyu (Interdisciplinary Graduate School of Science and Technology, Shinshu Univ., Nagano, Japan); Takeo Fujii (Advanced Wireless Communication research Center, The Univ. of Electro-Communications, Tokyo, Japan); and Makoto Taromaru (Department of Electronics Engineering and Computer Science, Fukuoka Univ., Fukuoka, Japan)

ABSTRACT

This paper proposes a decision method for transmitting a sensing information according to a surrounding environment. The sensing node autonomously decides the transmission timing based on detection result of a change of the measured environment. Then the receiving fusion center can update a stored statistical information. However there is a relationship between the transmission interval and the detection probability of the change of the environment, because the transmission interval is regarded as the measurement period. By using this relationship, the sensing node can avoid using the wireless resources wastefully. This paper clarifies the relationship and evaluates the proposed method by using computer simulation.

1. INTRODUCTION

Recently, a scarcity of the wireless resources is one of the problems in the world. A cognitive radio system, which is one of solutions for its scarcity has been researched from many researchers [1]. In particular, a spectrum sensing is one of very important technologies in cognitive radio systems. By using the spectrum sensing for the cognitive radio system, the cognitive system can utilize a white space, which is a spatial and temporal vacant spectrum allocated to the existing primary systems. Then, the channel utilization efficiency is improved by the cognitive radio system. However, the cognitive system needs to gather a lot of information because the wireless environment changes over time and with location. A cooperative spectrum sensing is that a fusion center collects the wireless environment information from its surrounding sensing nodes. Then, the cognitive system requires many sensing nodes. In this network, the fusion center comprehensively decides whether the channel is the white space or not by using the sensing information observed at multiple sensing nodes [2] – [4].

Similarly, in a sensor network, the observed information is gathered from a sensor node to a sink node [5]. Because the observed environment also changes over time and with location, the sensor node transmits a lot of information to the sink node. The sensing information has various characteristics. In this paper, we consider the sensing information whose volume of information is low, whereas the number of the sensing information which is transmitted from many sensor nodes or sensing nodes is large. Then the receiving sink node or fusion center statistically process the gathered information and store the information at a database. In order to update the stored statistical information, the node which observes the environment transmits the sensing information at regular intervals [6] – [8]. In this case, however, the change of the environment depends on time, location, situation, frequency and so on and the fusion center cannot detect the change of the environment in real time. Therefore, this paper deals with the method that the sensing node autonomously decides the timing to transmit the sensing information.

This paper proposes a transmission decision method for avoidance of wasteful channel utilization for transmitting of sensing information, which depends on the measured environment. The proposed method changes a transmission interval according to the speed of environment change over time. The transmission interval is very important. For example, when the interval is too long, there is possibility of the environment change in the long interval. In this case, the fusion center cannot follow the environment change, because the stored statistical data at the fusion center is updated by old data which is measured at the sensing node due to its long measurement interval. On the other hand, if the interval is too short, the data transmission times become large. In addition, if the surrounding environment is likely to not change in the short interval, the wireless resources are wastefully used for transmitting the current data that is equal to the previous measurement data. Because the scarcity of the spectrum resources is becoming the serious problem, the wasteful transmission has to be avoided for the economical wireless communications.

Then, in this paper, the proposed method decides dynamically adapting the timing of transmission based on the change of the surrounding environment. As a result, the sensing nodes can autonomously avoid the wasteful use of the wireless resources for transmitting the environment information. In addition, the fusion center can rapidly update the stored statistical data by using the environment information based on the wireless environment change. However, there is a relationship between the interval of the information transmission and an amount of the error of the measured results. This paper confirms the relationship and evaluates the proposed method.

The rest of the paper is organized as follows: Section 2 shows the system model in this paper. The proposed method that autonomously decides the transmission interval is explained in Sect. 3. Section 4 presents the simulation results. Finally, Sect. 5 concludes this paper.

2. SYSTEM MODEL

In the cognitive radio system, each sensing node observes and recognizes a surrounding wireless environment. In this paper, an energy detection method is used for detecting a white space. This paper assumes that the sensing node observes the received power during a measurement period and calculates a channel occupancy ratio (COR), R^{co}, which is obtained by summing the number of detected result and divided by the number of the measured slots. This calculated COR is distributed on a true value. Each sensing node observes the received power per slot. The measurement period consists of M slots. In this paper, the slot is defined as term that the channel utilization trend does not change. Here, we assume the channel is occupied with a two-state Markov chain model. As shown in Fig. 1, the two-state Markov chain model is represented by a channel occupancy ratio that the channel is occupied (i.e., the channel state is ON), P_{on}, and a state transition ratio, P_{st} and P'_{st}. The channel occupancy ratio is calculated by using the results of the energy detection every slot. There are many sensing nodes, and then a fusion center gathers much information of the channel occupancy ratio from the surrounding multiple sensing nodes. The fusion center has a database, which stores statistical information of the channel occupancy ratio gathered from many sensing nodes.

In the proposed method, the sensing nodes transmit the information, (i.e., the local channel occupancy ratio, R^{co}) for updating the statistical channel occupancy ratio stored in the fusion center after the channel observation during the measurement period, M. In this case, we assume the measurement period is the same as the interval of the information transmission for updating the statistical information of the fusion center. In this paper, the transmission slot is not considered, and the cognitive radio system has a table with an amount of the error depended on

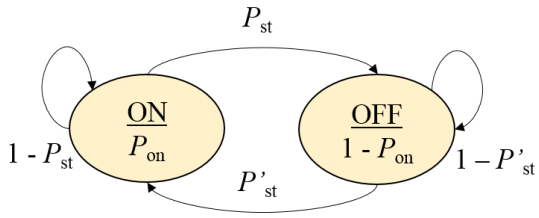


Fig.1 Two-state Markov chain model

the measurement period for the channel occupancy ratio. Then, the sensing node autonomously decides the timing to transmit its own measured channel occupancy ratio (local information) toward the fusion center. However the amount of the error are included in the channel occupancy ratio which is due to detection error by the energy detector depends on Signal-to-Noise Ratio (SNR) at each sensing node. For simplicity we assume that all of them have the same SNR. In addition, we assume that the table with the amount of the error which depends on the length of the measurement period can be obtained by experimental observation results of the surrounding wireless environment in the past.

Each sensing node selects the error limits of the local information by using the table. In this paper, we assume that the sensing node knows an allowable error of the local channel occupancy ratio in the cognitive radio system. Because there is a relationship between the interval of the information transmission and the amount of the error included in the local channel occupancy ratio, the boundary of the allowable error included in the local channel occupancy ratio is decided from the received SNR at the sensing node and the measurement period. Here, when the amount of the allowable error is a certain value α, 1 - α is called the confidence coefficient. Then the confidence limits are used for deciding the transmission of the local channel occupancy ratio, which is observed at each sensing node. In this paper, we do not consider collision between the transmissions of the sensing information.

3. DECISION OF TRANSMISSION

In this section, we explain the proposed method for transmitting a sensing data, i.e., local channel occupancy ratio (LCOR) by autonomously detecting the change of the environment and the reliability of the LCOR. In the relationship between the interval of the information transmission and the amount of the error of the measured LCOR, if the interval of the information transmission is short term, the fusion center can frequently update the statistical information. However, at the same time, the measured LCOR during the short term might include the error with high probability. Then, even if the sensing node detects the change of the environment in a short measurement period, it is high probability that the calculated

LCOR is wrong. That is, when the measurement period is too short, a variance of the error becomes larger than case of long measurement period.

On the other hand, if the interval of the information transmission is long term, because the measurement period also is long term, the fusion center can gather the reliable information. However, if the channel utilization trend changes rapidly, the transmitted information to the fusion center is different from actual condition over the long measurement period. Therefore, the sensing node has to decide to send the observation information, i.e., LCOR, for updating the statistical information stored in the fusion center by considering the amount of the error concluded in the sensing result.

At first, this section explains the confidence limits, which are used for autonomously deciding the sensing information transmission at the sensing node. Then we present the procedure of the proposed method with the derived confidence limits.

3.1. Confidence Limits

The proposed method utilizes the confidence limits for deciding the LCOR information transmission at the sensing node. We assume the fusion center has the desired confidence coefficient, 1 - α. The sensing node decides the confidence limits by using the desired confidence coefficient, which is informed in advance from the fusion center. In this paper, the sensing node repeats the spectrum sensing every slot during the measurement period, M. The local channel occupancy ratio (LCOR) during the measurement period is calculated from these energy detection result per slot at each sensing node. As is clear from the law of large numbers, the calculated LCOR depends on the number of slots in the measurement period. If the number of the measurement slots is small, the calculated LCOR includes large error contrary to actual channel occupancy ratio of its channel. The difference between the calculated result and the actual value decreases with the increasing the number of the measurement slots. For example, Fig. 2 shows three cases when the actual channel occupancy ratio is 0.5. First case is the measurement period is five slots. In this case, the calculated LCOR is 0.8, which includes large error. Moreover, in second case and third case, the measurement period is updated 10 slots and 15 slots, respectively. The third case denotes the calculated result is more closely to the actual value than that of first case and second case. As shown in Fig. 2, the case of long measurement period can obtain less error of the channel occupancy ratio than other short period cases.

As seen above, there is the relationship between the number of the measurement slots and the amount of the error of LCOR. Then, we can generate the table including

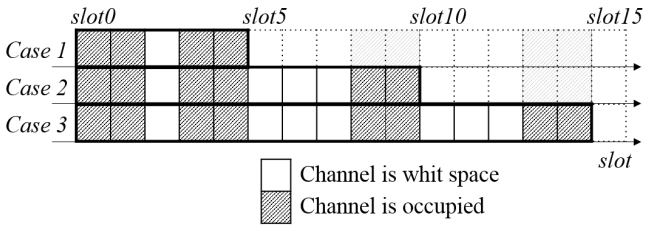


Fig. 2 Calculation of channel occupancy ratio based on measurement period

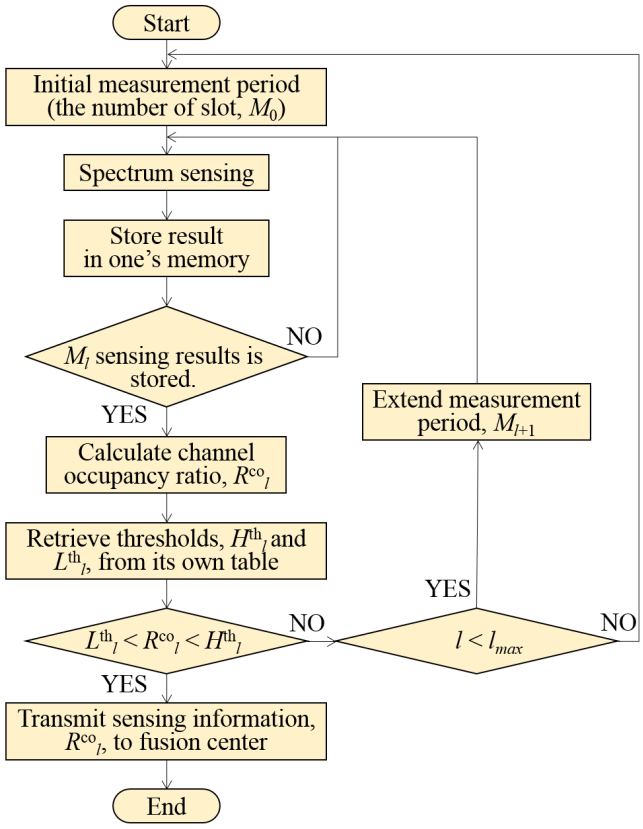


Fig. 3 Flowchart of transmission decision

the amount of the error based on the number of measurement slots by the computer simulation, whereas it is difficult to model the error because it is not always true that the distribution of the error included in LCOR is Gaussian distribution. In this paper, it is assumed that the sensing node has the table on which the amount of the error according to the measurement period is written in advance.

The sensing node decides the confidence limits by the error table. For example, if the desired confidence coefficient of the fusion center, 1 - α, is 0.1, the upper probability and the lower probability are 5% respectively. We assume that the sensing node knows the previous statistical channel occupancy ratio (SCOR) stored at the fusion center. Then, the sensing node selects the confidence limits according to its measurement period on the assumption that its own LCOR is equal to its SCOR. If the

calculated LCOR is out of the confidence interval, the sensing node decides that the environment is changed and transits its LCOR information toward the fusion center.

Thus, the sensing node can transmit the information without wasteful use of the wireless resources with satisfying the desired accuracy of the channel occupancy ratio at the fusion center by using the table as explained next subsection.

3.2. Procedure of Information Transmission

Figure 3 shows the flowchart for deciding the sensing information transmission. Each sensing node follows this flowchart. At first, the sensing node sets the measurement period to M_0 slots. Then, the sensing node performs the spectrum sensing on the certain channel and stores its result in its own memory. When the number of the sensing results is equal to M_0 slots, the sensing node calculates the channel occupancy ratio, R^{co}_0. As previously mentioned, because the sensing node has the table to detect whether the result of the measured LCOR is allowable or not, the limits, L^{th}_0 and H^{th}_0, can be retrieved from its own table according to the measurement period (M_0 slots). Here, these limits are called the confidence limits, and the interval between the lower and upper limit is called the confidence interval. In this paper, the sensing node decides the confidence limits and interval by previous SCOR which is stored at the fusion center. Then, the sensing node compares the calculated R^{co}_0 with the confidence interval generated by the retrieved limits. If the result R^{co}_0 exists between the lower limit, L^{th}_0, and the upper limit, H^{th}_0, the sensing node increases the number of slots which is performed the spectrum sensing and then the measurement period is extended to M_1.

Then the sensing node achieves to the next stage for obtaining higher reliable result, as shown in Fig. 4. In this way, if the LCOR calculated by the spectrum sensing is within the confidence interval, the sensing node regards that the observed channel occupancy ratio does not change and then repeats the cycle of the spectrum sensing to obtain the reliable result by extending the measurement period. On the other hand, if the result of the comparison is that the R^{co}_0 is out of the confidence interval between the lower limit, L^{th}_0, and the upper limit, H^{th}_0, the sensing node transmits its LCOR information to the fusion center. As shown in Fig. 3, the sensing node repeats the spectrum sensing for detecting the change of the channel occupancy ratio. Here, when the repetition achieves maximum number, l_{max}, the result of the spectrum sensing and the measurement period are reset to zero and initial value, respectively, because too many repetition causes the deadly error.

In this way, the sensing node decides the transmission of the sensing information. Therefore, the fusion center can gather the information that the channel occupancy ratio is changed. Moreover, the sensing node can effectively utilize the white space by autonomously controlling the transmission timing according to its change.

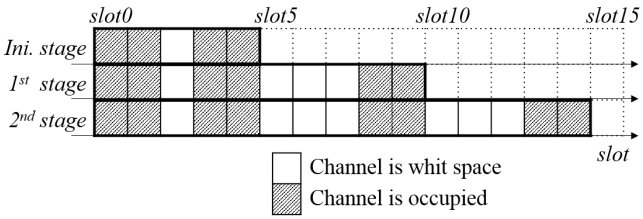


Fig. 4 Extension of measurement period by each stage

3.3. Characteristics of Proposed Method

The proposed method can transmit the local channel occupancy ratio information with the low number of times by detecting the environment change. The sensing node compares the confidence limits, which are derived from the previous SCOR and the confidence interval, with the measured LCOR for autonomously deciding to transmit its LCOR information by detecting the change of the channel occupancy ratio. The sensing information is transmitted to the fusion center only if the measured result is out of the confidence interval. In this way, the proposed method can avoid the wasteful use of the wireless resources. In addition, the fusion center can follow the environment change because the sensing node transmits the current sensing information based on the detection of the change of the channel occupancy ratio.

As previously explained, when the measurement period is short, the result may include the large error. In contrast, when the measurement period is long, the measured result can obtain high reliability. That is to say, the confidence interval is narrow on the long measurement period, whereas the short measurement period derives the wide confidence interval, when the desired confidence coefficient is satisfied. Therefore the sensing node can decide the environment change with the desired confidence coefficient, as explained in the previous subsection.

4. SIMULATION RESULTS

In this section, we show the simulation results and discuss the performance of the proposed method. In order to evaluate the performances, this section compares the proposed method with the conventional method, which transmits the information at regular intervals. In this paper, the transmission interval is the same as the measurement period. The channel occupancy ratio is changed at a certain interval, which consists of static slots. If the number of the static slots is large, the channel utilization change is slow. On the other hand, if the number of the static slots is small, the frequency of channel change is quick. The sensing node

performs the spectrum sensing at every slot. Then, the LCOR is calculated by its results over the measurement period. For simplicity, we assume the calculated LCOR does not include an influences of fading and shadowing, whereas it includes the influence of the lack of measurement result. In the proposed method, we assume that the sensing node can obtain correct SCOR from the fusion center when the change of the LCOR is detected correctly, even if the calculated COR is wrong. That is to say, if the change is true and the sensing node correctly detects the change, we assume that the sensing node can obtain the SCOR without error from the fusion center. We set the actual channel occupancy ratio changes three times in this section. Each channel occupancy ratio is continued over the same number of slots. For example, the number of the static slots is 500, 1000, 2000 and 3000. In this paper, the state transition ratio, P_{st}, which is described in Fig. 1 is 0.5.

At first, we explain the derivation of the confidence limits before the proposed method is evaluated.

4.1. Confidence Limits

The proposed method utilizes the confidence limits for deciding the LCOR information transmission at the sensing node toward the fusion center. The confidence limits are tabulated with an amount of the error which is depended on the measurement period of the spectrum sensing. However, the amount of the error depends on a received SNR at the sensing node and the actual channel occupancy ratio (COR). From the law of large numbers, the distribution is approximately normal distribution, which is centered on the true channel occupancy ratio. However, in fact, the distribution is inconsistent with normal distribution. Then, the first simulation evaluates a cumulative distribution function when the sensing node observes the channel occupancy ratio.

Figure 5 shows the cumulative distribution function when the actual channel occupancy ratio is 0.5, 0.7 and 0.9. We consider that the measurement period (MP) is 50 slots and 300slots. It is assumed that the received SNR is 30 dB. As we can see from Fig. 5, each median of the measured LCOR does not correspond to each true value. This effect is derived from bias of the distribution and limitation of the channel occupancy ratio, [0, 1]. Moreover, when the same true COR lines are compared, the result that MP is 50 slots is higher in variance than the result that MP is 300 slots. These results are also clear from the law of large numbers.

In the next simulation, these results are used for deciding the LCOR information transmission in the proposed method. From Fig. 5, the sensing node can obtain the confidence limits, which satisfy the desired confidence coefficient, $1 - \alpha$. In this paper, we assume the desired confidence coefficient, $1 - \alpha$, is 0.9 and the confidence limits are decided from two-sided test.

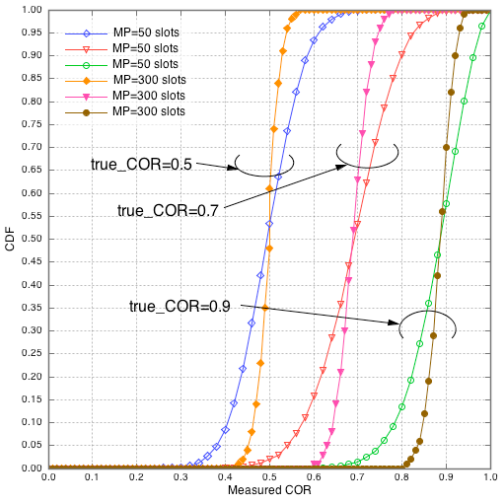


Fig. 5 CDF of Measured LCOR

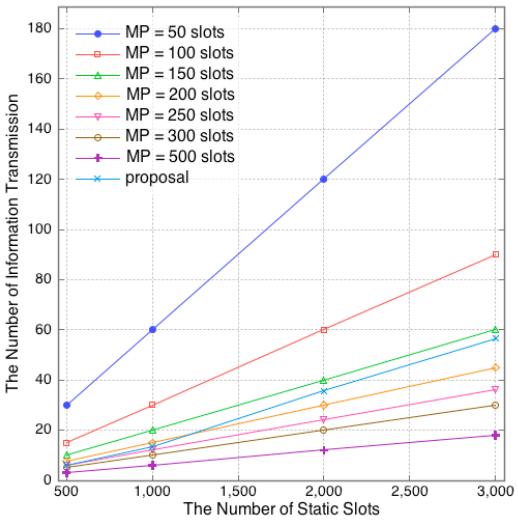


Fig. 6 The Number of LCOR Information Transmission

4.2. The Number of Information Transmission

Hereafter is assumed that the actual COR is transited from 0.5 to 0.7, and then from 0.7 to 0.9. Figure 6 shows the number of LCOR information transmission by using the proposed method and conventional methods that the measurement period (MP) is 50, 100, 150, 200, 250, 300 and 500 slots, respectively. From this figure, we can see that the proposed method decreases the number of information transmission than the conventional methods (MP = 50, 100, 150 slots, and MP = 200 slots when the number of static slots is low).

On the other hand, Fig. 7 shows the difference between the calculated LCOR and the actual COR with different methods, the proposed method has larger difference than the results of the compared method. However, as shown in Fig. 8, when the number of the static slots is low, the probability

of correct detection is high. Here, the correct change detection probability is derived from the result that is divided the number of correct detection of COR change by the number of transmission when the sensing node uses the proposed method. This result indicates the proposed method can follow the quick change.

Moreover, Fig. 9 shows the result of the average measurement period by using the proposed method. From this result, we can see the proposed method has maximum measurement period. Figuer 9 indicates that case that the number of static slots is 1000 slots has the longest measurement period (transmission interval). Therefore, the sensing node should decide the maximum measurement period based on the number of the static slots. As a result, these results indicate that the proposed method can transmit the sensing information according to the change of the environment with satisfying the confidence coefficient.

5. CONCLUSION

In this paper, we propose a method of decision of information transmission for avoiding using the wireless resources wastefully. By using the proposed method, the sensing node can transmit the information based on the environment change. We compare the simulation results of the proposed method with the simulation results of the conventional method, which transmits the observed information at regular intervals. From the simulation results, we confirm that the proposed method can transmit the information according to the environment change.

6. ACKNOWLEDGMENT

A part of this work is supported from the Ministry of Internal Affairs and Communications (MIC) of Japan under 2014 SCOPE "R&D for Very High Efficient Wireless Sensor Networks with Environment Recognition."

7. REFERENCES

[1] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Commun.*, Vol.6, No.4, pp.13–18, Aug. 1999.

[2] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," *Proc. ICC2006*, pp.1658–1663, June 2006.

[3] E. Peh and Y. Liang, "Optimization for cooperative sensing in cognitive radio networks," *Proc. WCNC2007*, March 2007.

[4] J. Ma, G. D. Zhao, and G. Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, Vol. 7, No. 11, pp. 4502–4507, Nov. 2008.

[5] Z. Liang, S. Feng, D. Zhao, and X. Shen, "Delay performance analysis for supporting real-time traffic in a cognitive radio sensor network," *IEEE Trans. Wireless Commun.*, Vol. 10, No. 1, pp. 325-335, Jan. 2011.

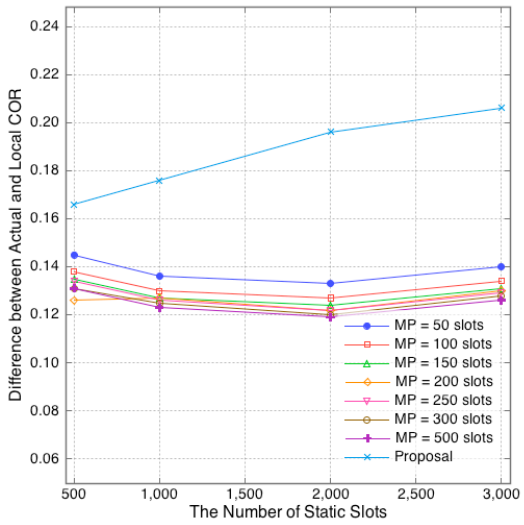


Fig. 7 Difference between Actual and Local Channel Occupancy Ratio

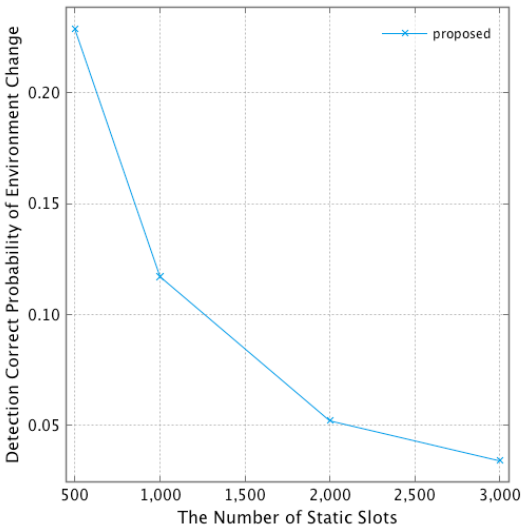


Fig. 8 Probability of Correct Detection

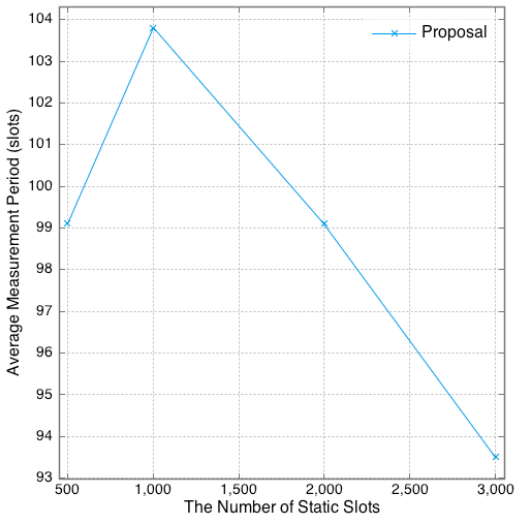


Fig.9 Average Measurement Period

[6] Y.-C. Liang, Y. Zeng, E. Peh, and A.T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, Vol. 7, No. 4, pp. 1326-1337, Apr. 2008.

[7] S. Stotas, and A. Nallanathan, "Optimal sensing time and power allocation in multiband cognitive radio networks," *IEEE Trans. Commun.*, Vol. 59, No. 1, pp. 226-235, Jan. 2011.

[8] A. D. Domenico, E. C. Strinati, and M. G. D. Benedetto, "A survey on MAC strategies for cognitive radio networks," *IEEE Commun. Surveys & Tutorials*, Vol. 14, No. 1, pp. 21-44, First Quarter 2012.

DISTRIBUTED SPECTRUM SENSING USING LOW COST HARDWARE

Stefan Grönroos (Turku Centre for Computer Science TUCS/Åbo Akademi University, Turku, Finland; stefan.gronroos@abo.fi); Kristian Nybom (Åbo Akademi University, Turku, Finland; kristian.nybom@abo.fi); Jerker Björkqvist (Åbo Akademi University, Turku, Finland; jerker.bjorkqvist@abo.fi); Juhani Hallio (Turku University of Applied Sciences, Turku, Finland; juhani.hallio@turkuamk.fi); Jani Auranen (Turku University of Applied Sciences, Turku, Finland; jani.auranen@turkuamk.fi); Reijo Ekman (Turku University of Applied Sciences, Turku, Finland; reijo.ekman@turkuamk.fi)

ABSTRACT

A distributed spectrum sensing network is prototyped using off the shelf hardware consisting of Raspberry Pi minicomputers and DVB-T receivers with software defined radio capabilities. Using the prototype network, coordinated, distributed wideband spectrum sensing is performed in a geographical area. The spectrum sensing data from the nodes is collected in a database. Well established low-complexity algorithms for distributed spectrum sensing are applied, and the results are compared against a professional spectrum sensing system. We show that with this simple low-cost setup, the decisions made on the availability of spectrum using the distributed sensing data correspond well with the decisions made on the reference data.

1. INTRODUCTION

It is well known that the radio frequency (RF) spectrum is a scarce resource. Currently, RF spectrum is allocated to license holders and services by governmental agencies who generally assign these spectra for large geographical regions on a long-term basis. With the rapidly increasing number of users, services, and wireless communication systems, however, and with the VHF and UHF bands almost completely allocated already, it is unlikely that the spectrum allocation methodology will keep up. Furthermore, while most of the spectrum is allocated, it is underutilized [1].

Cognitive radio (CR) is a technique that addresses this issue by allocating spectrum dynamically to users. It is fairly easy to see that a dynamic allocation approach can improve the utilization of the RF spectrum, as communication systems are not bound to use a pre-defined frequency range for their communication anymore. However, CR introduces several new challenges. One of these challenges is how to determine what spectrum is available and what spectrum is in use. At first glance, this may seem trivial, since a quick scan of the RF bands will reveal where communication is active and where it is not. If the RF environment is truly cognitive, however, there will be a high variability on the availability of the spectrum, since spectrum, by definition, is allocated dynamically. Hence, this calls for continuous scanning of spectrum and efficient algorithms for determining the availability of the spectrum.

Spectrum sensing – one of the most important components of CR – is the technique for obtaining awareness about the spectrum usage in a geographical region. The main objective when doing spectrum sensing is to detect primary users (PU) in the RF spectrum, where a PU is one who has higher priority or legacy rights on the usage of a specific spectrum. Correspondingly, secondary users (SU) are those who have lower priority and who exploit the spectrum in such a way that they do not cause interference with the PUs [2]. Without spectrum sensing dynamic allocation of spectrum would not be feasible, because if specific RF spectrum was allocated to a SU which was already in use by a PU, the SU would cause high interference with the PU.

In this paper we investigate the feasibility of using low cost hardware for distributed sensing. We note that the distributed sensing considered in this paper corresponds to non-coherent wideband centralized co-operative sensing, as defined in [3]. We prototype the distributed sensing network using a number of Raspberry Pi (RPi) devices with USB DVB-T (Digital Video Broadcasting - Terrestrial) dongles connected to them, where the DVB-T dongles function as software defined radio (SDR) receivers. With this setup, each sensor node costs roughly 50 USD at the time of writing. We compare our prototyped sensing network to dedicated professional equipment and to sensing with a single device. We use simple algorithms for analyzing the sensing data and for making decisions on the availability of spectrum.

The paper is structured as follows. Section 2 presents the general methodology for distributed sensing, while section 3 describes the prototyped distributed sensing network. In section 4, details on how spectrum sensing methods are used are given. Section 5 presents the results from measurements and

concluding remarks are given in section 6.

2. DISTRIBUTED SPECTRUM SENSING

The main goal with spectrum sensing is to obtain awareness about the spectrum usage in a geographical area. When the spectrum sensing is distributed, several sensing nodes are spread out over the area of interest where each node senses the spectrum on its own. After the sensing is completed, the nodes combine their sensing data by transmitting it to a fusion center (FC) where various combination strategies can be applied. This process is covered in more detail in Section 2.2.

With distributed sensing, a more detailed observation can be made as compared to sensing with a single node only. Figure 1 illustrates the distributed spectrum sensing scenario, where a number of SUs in the neighborhood of a PU sense their surrounding area, whereafter they transmit their data to a FC. Note that in the scenario considered in this paper, the FC contains a measurement database (MDB) where the measurements are stored. When the FC is required to decide on the presence and absence of signals, it extracts the measurement data from the nodes from the MDB and uses it for making the decisions. The decision making process is covered in more detail in Section 2.1.

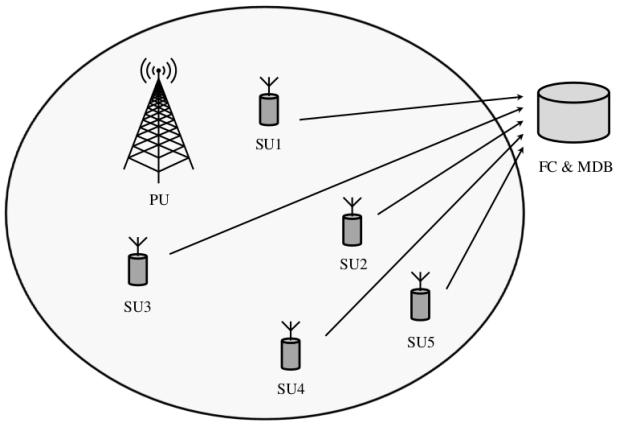


Figure 1: Illustration of the distributed spectrum sensing scenario considered.

In the remainder of this section, we describe some of the methods used in spectrum sensing, and distributed spectrum sensing.

2.1. Signal Detection Techniques

Spectrum sensing is the method for determining whether a signal is present or not in the measured spectrum. This is often formulated as a binary hypothesis testing problem where we have two hypotheses H_0 and H_1 as follows:

$$y(t) = \begin{cases} n(t), & H_0 \\ s(t) + n(t), & H_1 \end{cases} \quad (1)$$

where $y(t)$ is the received signal, $s(t)$ is a transmitted signal, and $n(t)$ is noise. Thus H_0 is the hypothesis that only noise is present, while H_1 is the hypothesis that a signal and noise is present.

A major influence on the choice of technique for detecting the presence of a signal in the spectrum is whether we have a priori information about the signal we are trying to detect or not [3]. If we do have a priori information about the characteristics of a signal we may for example use matched filters or cyclostationary detection [4]. Matched filters are used to correlate for example known pilot patterns with the signal to discover the desired type of signal. Cyclostationary detection exploits the periodicity of man-made signals.

Another factor that influences the choice of technique is whether the sensing is for narrowband or wideband detection. For wideband detection, compressed sensing [5, 6] may be a more attractive choice than the techniques mentioned above, mainly because it has a lower computational complexity.

The performance of the detection algorithm chosen can be described using two probabilities: the probability of detection P_D and the probability of false alarm P_F. As the name suggests, P_D is the probability of detecting a signal that truly is present. P_F, on the other hand, is the probability of reporting the presence of a signal which in reality is not present. The probabilities are defined as [7]

$$P_D = \mathbf{Pr}(Y > \lambda | H_1) \quad (2)$$

$$P_F = \mathbf{Pr}(Y > \lambda | H_0) \quad (3)$$

where Y is the decision metric and λ is the decision threshold. Based on these definitions, the probability of missing a signal, i.e., the probability of a false negative P_M can be defined as

$$P_M = 1 - P_D \quad (4)$$

Clearly, a good detection algorithm is one that has a high P_D and a low P_F. However, it is noteworthy that a high P_F means that the FC will incorrectly decide on H_1, which in turn means that the corresponding frequencies will not be allocated to users in a CR network, since the FC believes they are already occupied. Although this is not optimal, it is still better than the FC missing a signal and allocating the already used frequencies to another user.

2.2. Data Fusion

Data fusion is the process of combining sensing data gathered at nodes. Combining of data can be done in one of the three following ways: soft combining, quantized soft combining, or hard combining [2]. When using soft combining, the sensing nodes transmit their entire sensing data to the fusion center (FC), where the data is combined. With quantized soft

combining, the sensing data is simply quantized before transmission, thus saving on the required transmission bandwidth. Hard combining saves even more on the required transmission bandwidth between the nodes and the FC by making decisions on the presence and absence of signals before transmitting the data to the FC. In this case, the hard decisions from the nodes are combined at the FC using either AND, OR, or majority rules.

Using the AND rule, the global decision on the presence of a signal is set to true if all sensing nodes agree on this. Correspondingly, when using the OR rule, the decision will be set to true if at least one of the nodes is of this opinion. The majority rule, on the other hand, is a more flexible rule in that it requires that at least a certain number of the involved nodes agree on the presence of a signal. The number of nodes to agree on the presence is typically at least half the number of involved nodes, but it can also be set more strictly, e.g. $2/3$ or $3/4$ of the involved nodes.

The idea of distributed sensing is also to find local PU's that are not visible to centrally located sensing nodes. For instance, ad-hoc networking nodes might communicate locally such that they are only visible to a single spectrum sensing node in a distributed sensing network. In this case the data fusion must be done in a way that also recognizes the possiblity of local PU's. A more general data fusion model which takes into account geographical distribution and signal propagation models is needed, but it is not in the current scope of this study.

3. MEASUREMENT SETUP

In this section, we describe the various components, both hardware and software, of our experimental spectrum sensing network. First we describe the sensor nodes and the RFeye reference equipment, after which the implementation of the measurement database, and our test network are explained.

3.1. Sensor nodes

The sensor nodes consist of a Raspberry Pi mini-computer, which is equipped with a single-core 700 MHz ARM11 CPU and 512 MB of RAM. The SDR receiver is a USB dongle intended for the reception of DVB-T, DAB, and FM radio broadcasts. The dongle contains a Realtek RTL2832U demodulation chip and a Rafael Micro R820T tuner chip. It has been discovered that the demodulation chip is capable of outputting raw 8-bit I/Q samples in addition to decoding DVB-T on-chip. This capability was originally used to decode DAB and FM radio, but has lately made these dongles highly popular as low-cost SDR receivers [8]. The dongles are capable of streaming samples at approximately 2.5 MS/s reliably. A sample sensor node is shown in figure 2. The Raspberry Pi model used for the sensor nodes costs roughly 35 USD, while the DVB-T dongle costs less than 15 USD, yielding a total cost of roughly 50 USD for the bare hardware and a low-quality antenna. Peripherals such as storage media (a Secure Digital card is required for the Raspberry Pi), power supplies, enclosures and perhaps higher quality antennas add to this price.

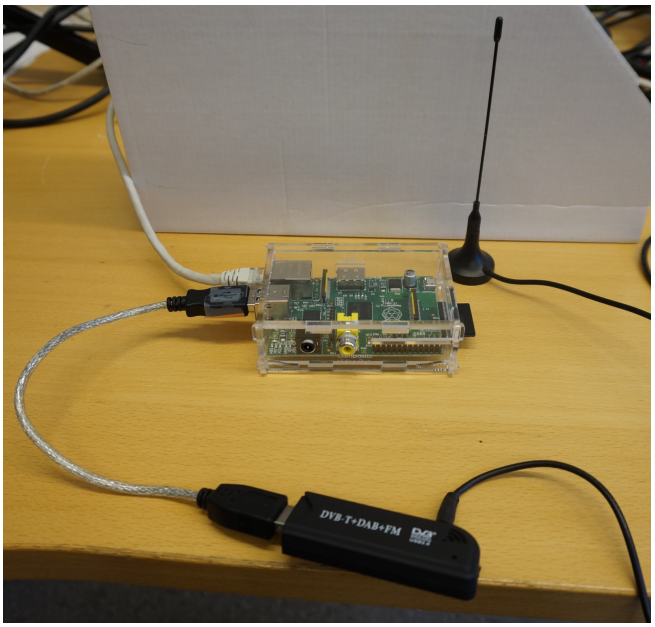


Figure 2: A Raspberry Pi-based sensor node, with SDR capable USB dongle attached.

In our experiments, we analyze the frequency spectrum between 110 MHz and 1300 MHz with a resolution bandwidth (RBW) of 39.0625 kHz. The software setup consists of a modified version of the rtl_power software, which is included with the Osmocom RTL-SDR driver package [8]. This software scans the spectrum by hopping through the frequency interval and performing an FFT operation of each interval to calculate a dBm value for each FFT bin. Our modifications to the software mostly consist of making the software insert measured frequency sweeps into a remote database in addition to writing the values to a local file. We chose a sampling rate of 2.5 MS/s (megasamples per second), i.e. we capture a 2.5 MHz slice of spectrum at a time. We do however discard half of the measured spectrum interval, 625 kHz at each side of the measured interval, since the frequencies farthest from the center frequency tend to have a quite high attenuation. Thus, we effectively measure only 1.25 MHz intervals at a time, however we compensate by measuring intervals with a 50% overlap to get the full spectrum of interest. Each sweep of the 1190 MHz wide spectrum takes approximately 70 seconds to finish. We did not focus on minimizing the sweep time in this work, and it might be possible to lower it, if one accepts fewer samples per sweep. This might how-

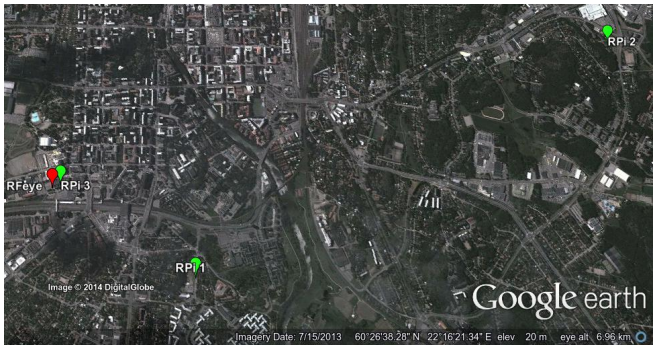


Figure 3: Placement of the RPi-based sensor nodes (RPi 1 to 3 in figure), as well as the reference RFeye Node in Turku, Finland.

Table 1: Description of the various nodes seen in fig. 3

Node	Antenna	Placement
RPi 1	Wideband double discone	On balcony
RPi 2	Small TV whip	Window sill
RPi 3	Wideband antenna	Roof of office bldg.
RFeye	Wideband double discone	5-th floor terrace

ever lead to unstable results, as the receiver requires some time to settle after a retune.

3.2. RFeye reference sensor

The CRFS RFeye Node is a spectrum monitoring node supporting the monitoring of spectrum between 10 MHz and 6 GHz (in some models even higher) [9]. The RFeye equipment is being used in a spectrum observatory, lead by the Illinois Institute of Technology, in which Turku University of Applied Sciences participates, providing measurements from the Turku area.

For our experiments, we set the parameters of one RFeye device to cover the same spectrum width as the RPi nodes and 39.0625 kHz RBW. The RFeye did however sweep through the entire spectrum in only 3 seconds, giving a much higher temporal resolution for each frequency. The captured data from the RFeye serves as our reference data.

3.3. Spectrum Database

We use a central MongoDB document database [10] (also called a NoSQL database) to store measurements from the various sensor nodes. In our setup, each document inserted into the database consists of the data from one measurement of a 1.25 MHz interval. The document contains fields for time, sensor ID, start and stop frequencies, RBW, number of bins, the gain used, as well as an array containing the dBm value for each measured FFT bin. This data can then be queried and combined by computers performing fusion and other analysis tasks.

3.4. Distribution of receivers

For this experiment, we distributed three RPi-based sensor nodes across the city of Turku, Finland. Figure 3 shows the locations of the three RPi nodes, as well as the reference RFeye Node. The node "RPi 3" was located in the same building as the RFeye, however different antennas were used. The distance from the RFeye (and RPi 3) to RPi 1 was approximately 1.2 km, and to RPi 2 approximately 4.3 km. Table 1 shows further information on the antenna type and placement of the various measurement nodes. Note that RPi 2 was only equipped with a standard small TV whip antenna, and placed on a window sill of a concrete apartment building, while RPi 1 and 3 were connected to superior antennas, with better placement.

4. METHODOLOGY

This section focuses on methods used within this work and how they are applied. We are interested in detecting signals without a priori information. For this purpose, a common and simple detection method is energy detection [3, 4], where we detect a signal based on whether the measured signal-to-noise ratio (SNR) exceeds a set threshold. Energy detection is thus not dependent on the type of signal present.

4.1. Noise Floor determination

In order to perform energy detection, we often need a method of estimating the noise floor of the received spectrum, as it may be different for different receivers, and may also vary with frequency and time. In [11], three suitable algorithms are discussed, namely rank-order filtering, Akaike information criterion, and minimum description length methods. We chose to use rank-order filtering in this study. The use of rank-order filters in noise floor estimation was inspired by morphological image processing in [12]. A rank-order filter $R(N, K)$ takes N values as input, and outputs the K'th smallest value. The noise detection method iteratively filters the signal with an $R(N, 1)$ filter followed by an $R(N, N)$ filter, where N is increased by one for each iteration. With increasing values of N, wider peaks in the spectrum are filtered out, until eventually we are left with a single level over the entire spectrum. In our case, we set a maximum N, that followed relatively fast changes in the noise floor quite well, without also considering for example wide OFDM (orthogonal frequency-division multiplexing) signals as changes in the noise floor.

4.2. Data processing and fusion

In order to analyze the data, we query the spectrum database for measurements from a certain time interval from the Mon-

goDB database. We approximate the noise floor through the use of a rank-order filter, as explained in section 4.1. The rank-order filter parameters were tuned in such a way, that it would follow relatively quick fluctuations in noise floor over the frequency range, while not counting for example wide 8 MHz DVB broadcasts as a large change in the noise floor. The noise floor was calculated separately for each receiver, and was subsequently subtracted from the signal.

We used two approaches to data fusion, hard combining with various voting rules and soft combining using a simple equal gain combining (EGC) method [3]. In the hard combining approach, we first make hard decisions for each sensor node, where a signal is assumed to be present if the power in an FFT bin exceeds a certain threshold above the estimated noise floor. According to a voting rule, we then set a threshold for the number of receivers that must have detected a signal in order for it to be considered present. In the soft combining approach, we take the average of the measured power from each receiver (for each FFT bin), and set a threshold above which the average signal strength should be in order to count as an actual signal.

5. RESULTS AND DISCUSSION

Using the three RPi-based nodes described in section 3, we collected measurements into the database for analysis. We also collected data from the RFeye reference node to be used as a reference.

5.1. Results

We used two threshold levels of 6.5 dB and 12 dB over the estimated noise floor for the reference data from the RFeye. This means that for each FFT bin, we accept H_1 (declare that there is a signal) if the signal power in that bin exceeds the floor detected by the rank-order filter by 6.5 or 12 dB. The 6.5 dB point was found by manual observation of the regions where H_1 was accepted, to be a suitable level where noise was no longer likely to result in a false alarm. The 12 dB threshold on the other hand was chosen as a robust detection point, where the weakest signals are not necessarily detected. We would like to point out that the focus of this work is on the comparison of the RPi network to the RFeye node, rather than on the selection of good threshold values for energy detection.

For the data from the RPi node network, we used detection thresholds between 0 and 15 dB. We also tested various combination techniques for the measurement data from the three nodes. When using hard decision, we decide to accept or reject H_0 for each node individually, and then combine the binary decisions according to AND, OR, and 2/3 majority rules. When using soft-combining, for each bin, all three measurements were summed together and divided by 3, after which the sum was compared to the threshold (0-15 dB) to either reject or accept H_1.

In order to combine sweeps from different points in time, we either used a peak-hold method, where the maximum value of each bin was used to produce the combined result (to preserve bursty signals), or signal averaging, where the FFT bins were averaged over time (to reduce noise peaks). This combination was performed for each node individually before any thresholds were applied.

We used approximately one hour of measurement data from each receiver to produce the results. Due to practical issues, the measurements from the RFeye and the RPi nodes were captured during different days. The RFeye measurements were captured in the afternoon on June 6th, 2014, while the RPi measurements were all captured during the afternoon on June 12th, 2014. Due to both measurements being quite long, and taking place on a workday afternoon, we do not expect the differing dates to affect the results much. An overview of the captured spectrum is shown in figure 4, where data has been combined using the peak-hold method over time, and also to combine the data from the three RPi nodes. The detected noise floor has been subtracted from the signal in figure 4. It is worth noting that the rank-order filter used for noise floor estimation tends to follow the "bottom" of the noise floor. This was corrected for by choosing higher threshold levels.

Figures 5 and 6 show the results from these measurements. The only setting differing between the figures, is that in figure 5, the peak-hold combining method is used to combine sweeps, while in figure 6, averaging is used. Note that the legend shown within subfigure (b) applies to all subfigures (a)-(d). The x-axis in the figures is the threshold for hard or soft decisions when combining measurements from each RPi node.

Subfigures (a) of figures 5 and 6 show the agreement rate between the RFeye, and the distributed RPi network as a percentage, i.e. how often decisions between H_0 and H_1 match. Subfigures (b) show the total measured spectrum occupation. Note that the two horizontal lines in (b) show the occupation seen by the RFeye when using the 6.5 and 12 dB thresholds. In subfigures (c), we measure the rate of false alarms, if we consider the decision made on the RFeye data to be correct. The false alarm rate is the number of cases where H_1 was accepted for the RPi measurements, when H_0 was accepted for the RFeye compared to the total number of RPi H_1 decisions. 100% would mean that for each H_0 decision for the RFeye, the corresponding decision for the RPi network was H_1. In subfigures (d), we measure the rate of missed signals, assuming the RFeye decision to be correct. I.e. it is the ratio of H_0 decisions when the RFeye decision was H_1, to the total number of RFeye H_1 decisions.

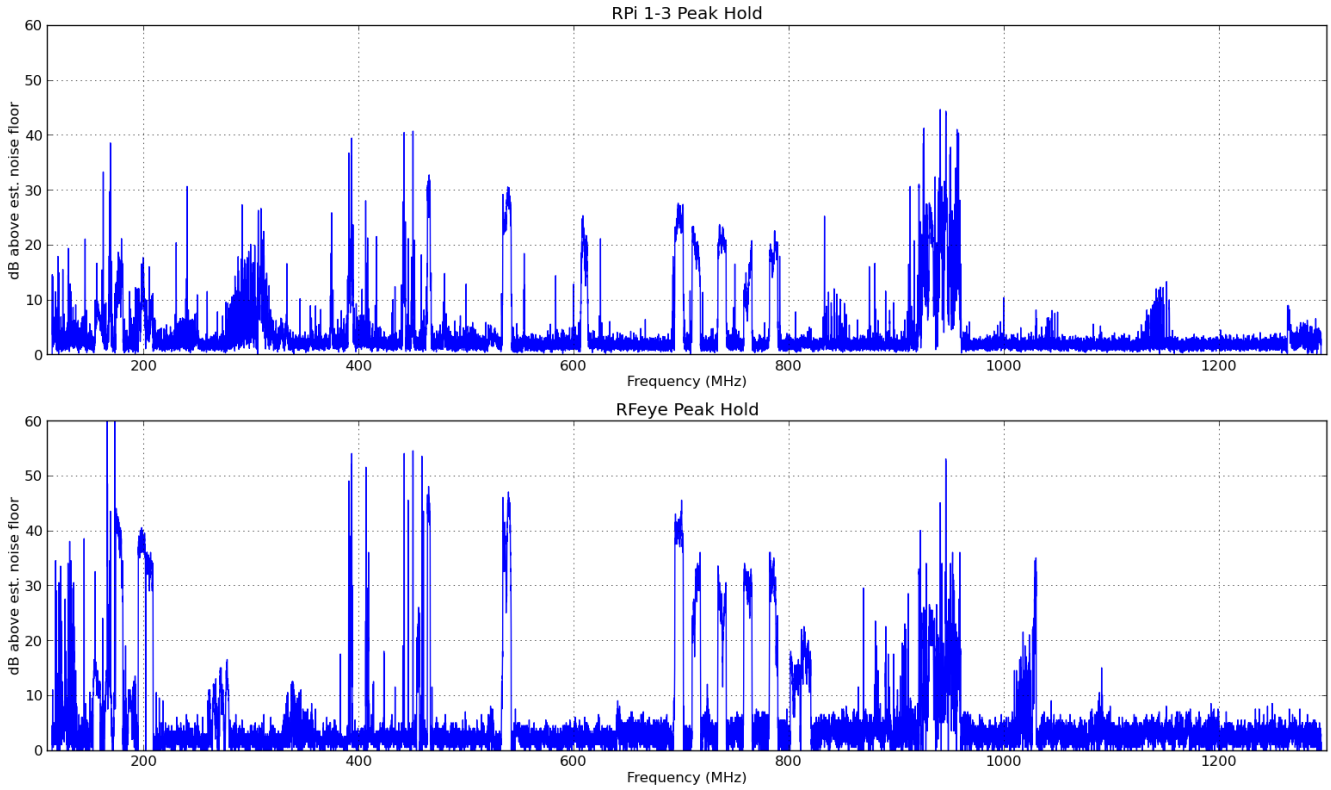


Figure 4: An overview of the captured spectrum from the RPi nodes, as well as from the RFeye reference node. The data from the three RPi nodes has been combined by retaining the maximum value over time and over all nodes (peak hold).

5.2. Discussion

From figure 5, we can see that the decisions made based on the RFeye and RPi measurement data are the same for about 85-95% of the spectrum, depending on which configuration and thresholds are used. When the threshold for detection on the RFeye data is high, we get a higher rate of agreement, which is likely due to the fact that the higher threshold discards weaker signals, which can likely not be picked up by the less sensitive USB dongles. In terms of agreement on decisions, the highest rate of agreement is reached with the hard decision rule based on 2/3 majority votes, followed by the soft combining method. The OR-rule gives the worst agreement rates in this case. We can also see that we benefit from the cooperative sensing here, as both the 2/3 majority vote and soft combining approaches yield a higher peak agreement rate than the best RPi node (RPi 1) on its own.

While the 2/3-vote rule gives the overall best agreement rate, one might want to choose another rule, when optimizing for low rates of missed signals or false alarms. If one wants to have few missed signals, which is likely the case in cognitive radio applications [13], the OR rule gives the best performance, as seen in figure 5(d), as it does not filter out any H_1 decisions from RPi nodes.

Figure 6 yields similar results overall, but the 6.5 dB limit is already quite high in this case, as noise and bursty signals have been averaged out. Thus the performance measures using the 6.5 dB and 12 dB thresholds for the RFeye are quite similar.

It is important to note that while the RFeye is treated as a reference here, it is possible that the RPi nodes detect signals that the RFeye does not due to the different locations and the different time of measurement. One example of this can be seen in figure 4, where a low-power cognitive radio test signal at 610 MHz has been captured by one RPi node, however it was not present at the other nodes (hence was filtered out by for example the 2/3 majority rule), and was also not present at the time of capturing the RFeye signal.

It was noticed during measurements, that setting a high internal gain in the USB dongle resulted in various forms of interference and stability issues, while a low gain made the dongle too insensitive. It might therefore be beneficial to connect an external amplifier between the antenna and USB dongle, in order to improve the received signal quality. The internal clock of the dongle was also found to generate interference on multiples of 28.8 MHz.

While not perfectly demonstrated with our initial limited

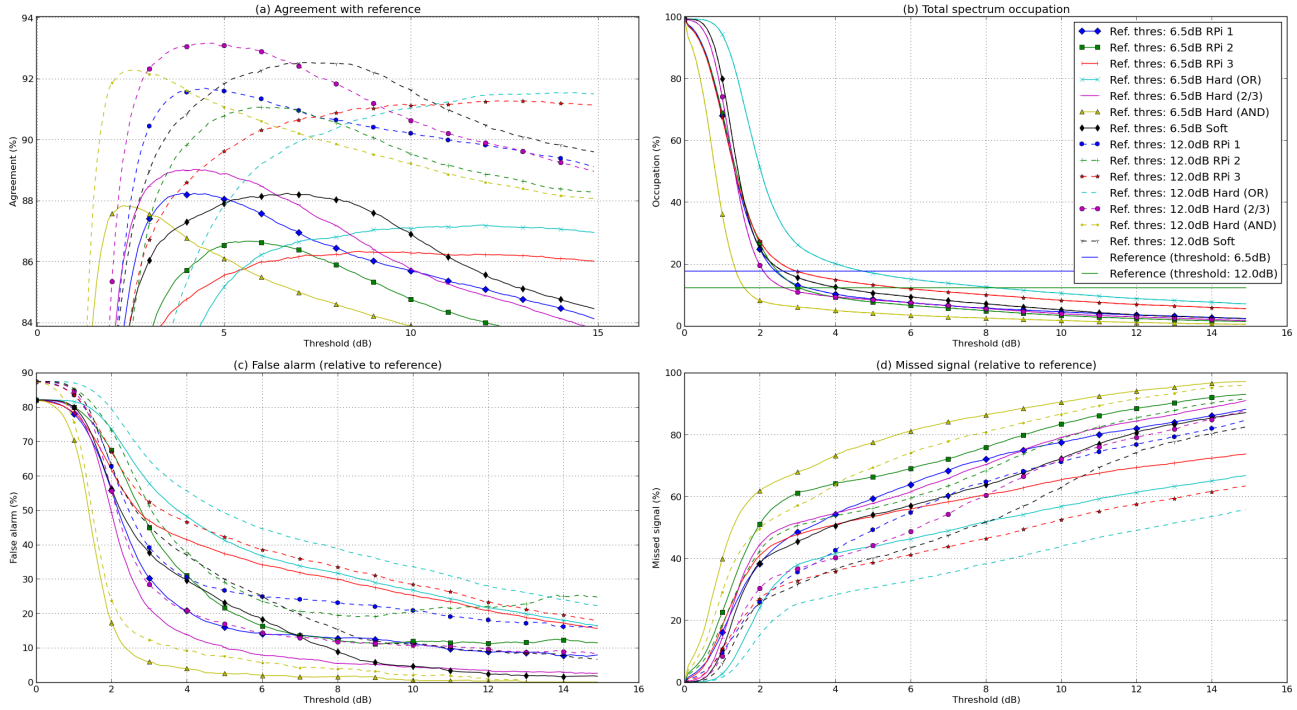


Figure 5: Statistics for 110-1300 MHz on (a) agreement between RFeye and RPi network, (b) total spectrum occupation, (c) false alarms (relative to the RFeye reference), and (d) missed signals (relative to RFeye), using peak-hold method of combining sweeps over time.

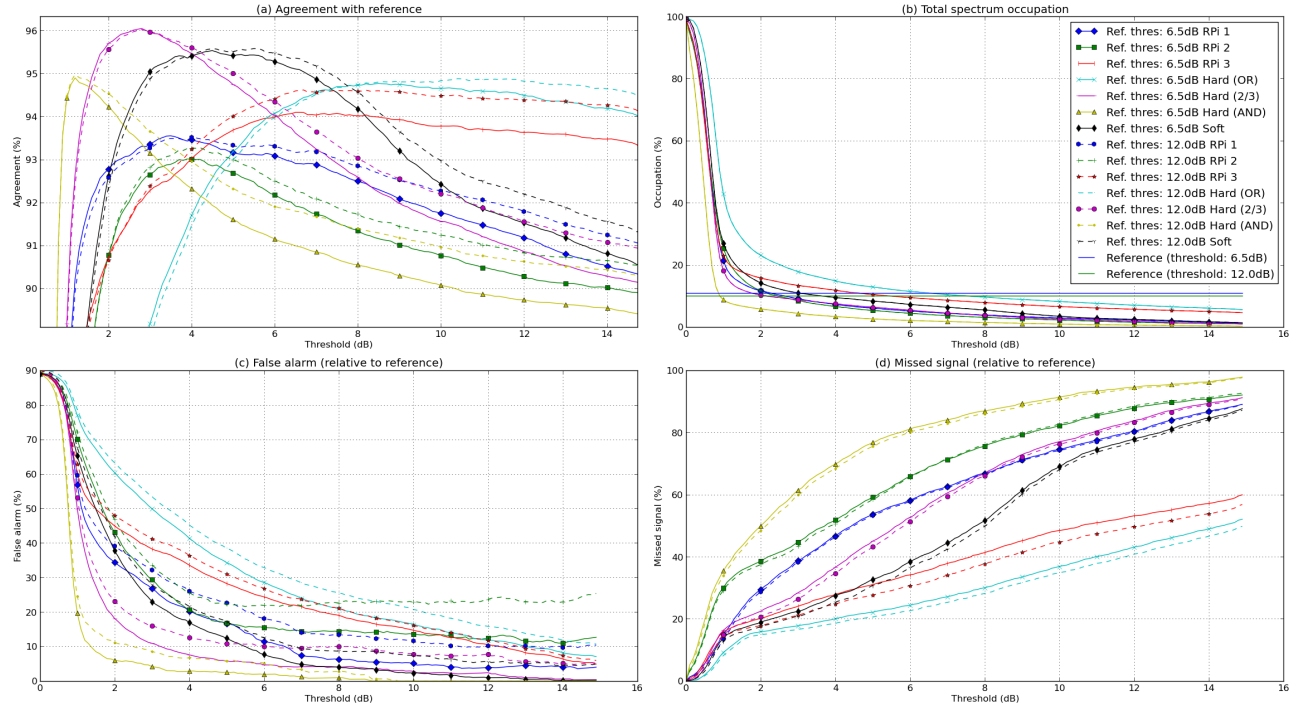


Figure 6: Statistics for 110-1300 MHz on (a) agreement between RFeye and RPi network, (b) total spectrum occupation, (c) false alarms (relative to the RFeye reference), and (d) missed signals (relative to RFeye), using averaging method of combining sweeps over time.

number of sensor nodes in the Turku field trials, a large network of these low-cost nodes could outweigh some of the disadvantages that a single node has compared to a higher-end device such as the RFeye. As mentioned the time required to perform one sweep of the spectrum is quite high (an order of magnitude higher than the RFeye), which will result in lower detection probability of burst signals. This can be at least partly compensated for by having a larger number of nodes, and perhaps also multiple dongles attached to each node. The lower sensitivity of the DVB dongles can also be compensated for by having a wide network of nodes, reducing the requirements on sensitivity of a single node, as there will likely exist nodes closer to each transmitter. Furthermore, a network of sensor nodes could also likely aid in locating the source of a transmission, to help in for example locating rogue transmitters.

6. CONCLUSION

The motivation for the research performed in this paper was to analyse if a low-cost off the shelf digital wide-band receiver can be used for effective spectrum sensing. The follow up question was: if the single low-cost sensing node is not good enough, can we compensate for this by having a network of geographically distributed low-cost nodes? In order to answer these questions, a small network of low-cost nodes was set up, with each node reporting the observed energy levels to a central database. The observations from this network were compared to an RFeye reference receiver. Antennas and their placement are important for good communication, but with the low-cost DVB-T dongle sensing node, only a very simple whip antenna is included. Clearly the largest amount of signals were missed using this antenna, whereas the best antenna at the best location had the closest match to the signal detection of the reference RFeye. The difference was however not that large, i.e. already a simple whip antenna gives useful information. A challenge comparing spectrum occupancy using energy levels is to select thresholds for detection, i.e. to separate signals from noise. In our case, manual heuristics were used, which is not optimal for the general case where it should be very easy to automatically deploy new nodes. This was an initial setup of low-cost sensing nodes, where we showed that the general idea works, i.e. we get useful information from the nodes. However, compared to the reference node, the low-cost node is inferior. The combination of several low-cost nodes gives better correlation to the data of the reference node, while placing more importance on the design of the data fusion model. In that area work must still be done to enable robust and precise signal detection in the time-frequency-space.

7. REFERENCES

[1] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks*, 50(13):2127 – 2159, 2006.

[2] T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *Commun. Surveys Tuts.*, 11(1):116–130, January 2009.

[3] Ian F. Akyildiz, Brandon F. Lo, and Ravikumar Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: A survey. *Phys. Commun.*, 4(1):40–62, March 2011.

[4] Jun Ma, G.Y. Li, and Biing-Hwang Juang. Signal processing in cognitive radio. *Proceedings of the IEEE*, 97(5):805–823, May 2009.

[5] David L. Donoho. Compressed sensing. *IEEE Trans. Inform. Theory*, 52(4):1289–1306, 2006.

[6] E. J. Candes, J. Romberg, and T. Tao. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. Inf. Theor.*, 52(2):489–509, February 2006.

[7] Fadel F. Digham, Mohamed-Slim Alouini, and Marvin K. Simon. On the energy detection of unknown signals over fading channels. *IEEE Transactions on Communications*, 55(1):21–24, 2007.

[8] Osmocom. OsmocomSDR (Wiki). `http://sdr.osmocom.org/trac/wiki/rtl-sdr` (Accessed 13.06.14), 2014.

[9] CRFS Ltd. RFeye Node. Data Sheet NOD-EYE0002, `http://media.crfs.com/uploads/files/1/crfs-md00011-c07-rfeye-node.pdf` (Accessed 15.06.2014), 2014.

[10] MongoDB, Inc. mongoDB. `http://www.mongodb.org` (Accessed 13.06.14), 2014.

[11] S. Sequeira, R.R. Mahajan, and P. Spasojevic. On the noise power estimation in the presence of the signal for energy-based sensing. In *Sarnoff Symposium (SARNOFF), 2012 35th IEEE*, pages 1–5, May 2012.

[12] M.J. Ready, M.L. Downey, and L.J. Corbalis. Automatic noise floor spectrum estimation in the presence of signals. In *Signals, Systems amp; Computers, 1997. Conference Record of the Thirty-First Asilomar Conference on*, volume 1, pages 877–881 vol.1, Nov 1997.

[13] Daniel Willkomm and Adam Wolisz. Is oversensitive spectrum sensing the door opener for initial cognitive radio deployments? In *Proceedings of the 2010 ACM Workshop on Wireless of the Students, by the Students, for the Students*, S3 '10, pages 21–24, New York, NY, USA, 2010. ACM.

SPECTRUM SHARING AND CRITICAL INFRASTRUCTURE PROTECTION: OPPORTUNITIES AND CHALLENGES

Daniel Devasirvatham (Idaho National Laboratory, Idaho Falls, ID, U.S.;
daniel.devasirvatham@inl.gov)

ABSTRACT

The paper examines some of these scenarios and challenges to security in spectrum sharing, especially when applied to critical infrastructure. It should help heighten awareness of potential real world consequences that need to be taken into account as these systems are designed and deployed. The concept of "Practical Session Security" is introduced, and the idea of "Wireless Cyber" is explored. The necessity for testing these concepts in a safe, test infrastructure ecosystem is also discussed.

1. INTRODUCTION

Spectrum sharing has become an area of great interest in future communications. It has been accelerated in the U.S. by the President's directive to the U.S. Government to share portions of its spectrum with the commercial world. A key step in this direction was embodied in the U.S. by the President's Council of Advisors on Science and Technology (PCAST) report on spectrum sharing [1] and the subsequent Presidential Memorandum [2]. Similar efforts are being undertaken in Europe as well. This paper examines the broader consequences of this class of technologies from the point of information security and service disruption.

2. WIRELESS AND CIP

Wireless is now an integral part of Critical Infrastructure (CI). Therefore, Critical Infrastructure Protection (CIP), by necessity, requires the protection of vulnerabilities in Wireless Communications as well [3], especially those that can be used to disable key sectors in CI, such as nuclear, oil and gas power plants, refineries, pipe lines, bridges, and dams. The move toward a "smart grid" model for power generation and distribution is heavily reliant on tight communications between centralized and distributed generation, energy distribution and loads, to optimize the utilization of all elements of the chain and maximize efficiencies and reduce pollution. Supervisory Control and Data Acquisition (SCADA) networks and more advanced

Figure 1. Potential wireless security targets.

forms of machine-to-machine (M2M) communications are now integral to the operation and safety of CI. This traffic could be carried by wired or wireless networks, or a combination of both. Wireless also facilitates communications with maintenance crews along utility corridors, which could be instrumental in service restoration after major incidents. Even power plants, which have nominally eschewed the use of wireless and used analog control in critical control circuits, are installing digital controllers. Ideally, these controllers must be isolated. However, as a practical matter, they may be connected to the outside world for maintenance and updates or share common physical communications paths with only virtual isolation. Wireless may be used for displaying status for operating and maintenance crews to give them mobility. Even if a specific operations group chooses not to actively use these wireless functions, many modern components embed the features in the product creating latent communications capability just waiting to be activated, often with just a software change. Any chink in this armor, which was assumed to be providing protection, could be potentially exploited with cyber-attacks. Figure 1 shows the multiplicity of systems, many of them interconnected, that could be targeted by the attacker.

Wireless is now also woven into the fabric of most people's daily life, whether they reside in the developed world or an emerging economy. Indeed, wireless is, in many cases, the catalyst to economic development, since its use scales well from micro-finance and small businesses all the

way to very large businesses and warehouses. The advent of wireless in a small village could mean the opening of new opportunities to the least of its inhabitants, spurring economic activity, hope, upward mobility, and independence. The main reason for wireless deployments has moved beyond just the convenience of mobility and untethered communications; it has enabled many nations to leapfrog the need for the slow and expensive erection of wired telephony and internet connectivity to be replaced by wireless broadband communications. It is estimated that even in the United States, one-third of the households get both voice and data communications using only wireless. When a major storm strikes, for example, further compromising wired and wireless infrastructure, millions of people are cut off from their families, whose attempts to re-establish contact only compounds the problem further. However, wireless does not stand by itself. Wireless is now an almost inseparable extension of the wired network. It may be said that "Wireless isn't."

The accelerating wireless traffic, coupled with the marketing of unlimited use data plans, has resulted in an unprecedented spectrum crunch. Wireless spectrum for mobility and for fixed access is a limited resource, especially in bands that propagate well over varied terrain and topography to serve rural areas. Wireless service providers have moved toward a combination of increasingly smaller cells, which increase the utilization in terms of Mbit/sec and MHz/sq. kilometer, as well as bandwidth aggregation (combining the capacity of different bands into one data stream to serve the demand for data). However, opening up new spectrum to serve this market is getting increasingly more difficult. The cost of relocation of services into other bands to free up spectrum can run into the billions of dollars, easily swallowing up the profits from any sale of spectrum. More importantly, it is a slow process, which cannot keep pace with the accelerated demand for wireless access and spectrum. In an attempt to preserve network integrity and communications in times of event stress, the United States, for example, is trying to build its own nationwide network, FirstNet, for public safety and critical communications. This effort cannot be universally replicated for all critical services.

The next step in capacity enhancement, beyond bandwidth aggregation using dedicated bands, is to share spectrum dynamically. It is believed that large capacities could be unlocked at the expense of modest system and terminal complexity when it is determined that a secondary user could share spectrum sufficiently without creating unacceptable interference to the primary occupant or compromising its network. It is also believed that, as new versions of incumbent systems become spectrum-use aware, sharing efficiencies would increase dramatically.

When some major incident happens, and hence, traffic volume goes up, congestion and delay could have deleterious consequences on the safe and stable operation, or at least the optimum operation, of CI. In cases where there is significant damage to some element of CI, re-routing of functions (or power in the case of the smart grid) requires reliable and well-understood traffic paths to execute the required protection and disconnection strategies.

3. SPECTRUM SHARING AND SECURITY

Spectrum sharing throws other potential vulnerabilities into the mix, especially when it is used to supplement capacity for critical infrastructure communications. It could also provide additional ways in which someone wishing to do harm could magnify the effects of the incident by additional cyber-attacks via the connections and protocols that are provided in spectrum sharing.

Wireless systems have not, at least to date, been inherently built with very high levels of security, and most security is added in higher levels of the communications stack. In addition, wireless is bandwidth and capacity limited. Security mechanisms use up precious bits in the air interface stream, and the additional computation could throttle what is already a relatively slow medium, compared to fixed wired networks. Hence, wireless security mechanisms are a compromise between data security and traffic capacity. More importantly, mobility precludes the locking up of channels with extended security establishment phases in the protocol. Each access attempt by the mobile user exposes the security fabric of the air interface by broadcasting at least some information necessary for establishing the connection, even if encrypted. Additionally, air link hand-off due to user mobility may require the regeneration of session keys, especially when one roams between sub-networks or different systems. Hence, it is relatively less difficult to attack the air interface protocols of commercial mobile wireless systems. It is then often up to the user to provide end-to-end security; but this, again, reduces the usable traffic capacity and is a sub-optimal security solution. Furthermore, end-to-end security provides no protection against service interruption caused by overloading or interruption of communications due to an attack on the wireless air interface, even if it is only a relatively simple jamming attack or collective interference that does not breach data or protocol security. Many CI attacks are more concerned with physical effect or functional denial of service than theft of information.

Data bandwidth aggregation using the individual capacities of different systems in different bands is a form of spectrum sharing. However, it is only as good as the security of the weakest system. Systems that share spectrum dynamically have additional challenges in maintaining security, since they may have access to portions of spectrum for only relatively small slices of time. This adds to the pressure to use the available bits to maximize user traffic,

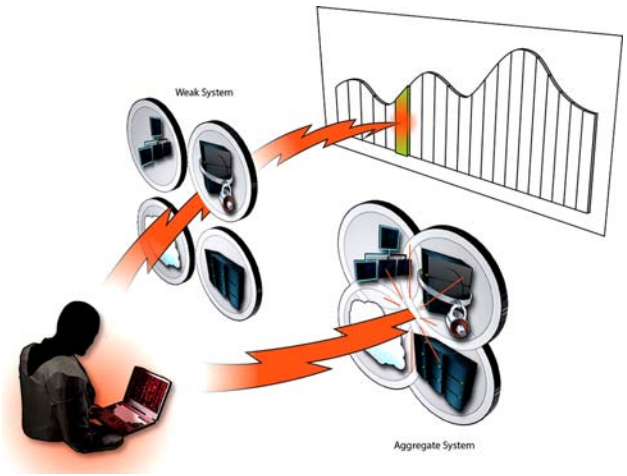


Figure 2. A weak link compromises an aggregate system.

further restricting security mechanisms. More importantly, given the limited shared spectrum access time, the overhead of establishing a traditional strong security envelope could add too much complexity and take too much time to effectively establish and use the connection before it has to be given up. Some of the initial negotiation may also have to be sent in the clear, opening additional chinks in the armor. This is illustrated in Figure 2, where even though an attack on a complex aggregate system might fail, the system could still be compromised by attacking a weak spectrum sharing component.

Hence, dynamic spectrum sharing systems may require capacity aggregation of different data streams. Other elements that could compromise spectrum sharing systems that aggregate bandwidth, be they dynamic or using static bandwidth aggregation, could include (a) different versions of IP protocols, (b) the use of IPV4 and IPV6 in the different systems, (c) different IP security software and management systems, (d) different security protocols employed by the different operators, or even the lack thereof. Additionally, it is being recognized that the IPV6 may introduce other vulnerabilities which may, as yet, be unknown due to its newness. In many cases, the greater dangers may not be in the individual air interfaces themselves, but in the interfaces between the systems or protocol stacks where they join or concatenate the data streams.

It could be argued that dynamic spectrum access and sharing could make it harder to intercept or compromise the wireless stream, effectively making this look like a frequency hopping spread spectrum system. The effective "hopping sequence" is now dependent on observations at the individual receivers and may not be replicated at the location of the attacker. Hence the prediction by the attacker of the next frequency the system would hop into could be in error, blunting the attack. This is illustrated in Figure 3. However, proposed spectrum sharing systems are also expected to use some form of sharing database to guide and regulate their activity. Hence, compromising the database and tapping into its communications could provide a blueprint for the spectrum sharing methodology being used by the potential victim, especially in denial of service or similar jamming/interference attacks where physical effect is more important than information theft. In effect, it provides another place where it could be potentially penetrated to be compromised.

At the same time, more components and processing stages internal to the "radio design" are moving to software and firmware based solutions. As performance of such hybrid software/hardware approaches increases and as more functions are shifted from dedicated hardware into various forms of digital signal processors, the greater the threat of lower-level embedded software attacks. Early forms of software attacks will likely start as simpler denial of service or by interfering with transmission protocols. As interest in "Wireless Cyber" vulnerabilities grow, the embedded attack techniques, impacts, and complexities of mitigations will also grow.

Finally, it must always be remembered that security can never be a "bolt on" solution if maximum integrity is to be maintained. Spectrum aggregation using different systems precludes a unified and totally planned security mechanism. It is no longer possible to impose a comprehensive security architecture on the whole. It has also been shown above that dynamic spectrum sharing may result in a weaker security envelope.

4. TESTING AND MITIGATION

The ingenuity of the cyber-attack community is legendary. It has not been possible, at least to date, to provide a formal proof of the invulnerability of any digital communications system, whether wired or wireless. Hence, an operating axiom in communications security is that any system could be penetrated at some point; the goal, then, being to increase the amount of time it takes to penetrate it to the point that the communication traffic being attacked has already ended or a more resilient alternative for the end function is established. Ideally, the next communications session would require a re-start of the attack and, if properly designed, make any progress made in the previous attack useless. Another goal is to ensure that any malware introduced during the penetration is useless to inhibit the next session. This may be called "Practical Session Security." It is worthwhile noting that most known long-term interceptions and surveillance have used the cooperation of the service provider. The only way to validate this goal of practical session security, as opposed to absolute security, is to test the system by attacking it using the full ingenuity of the penetration community and using the full computational power available to the attacker. This could, of course,

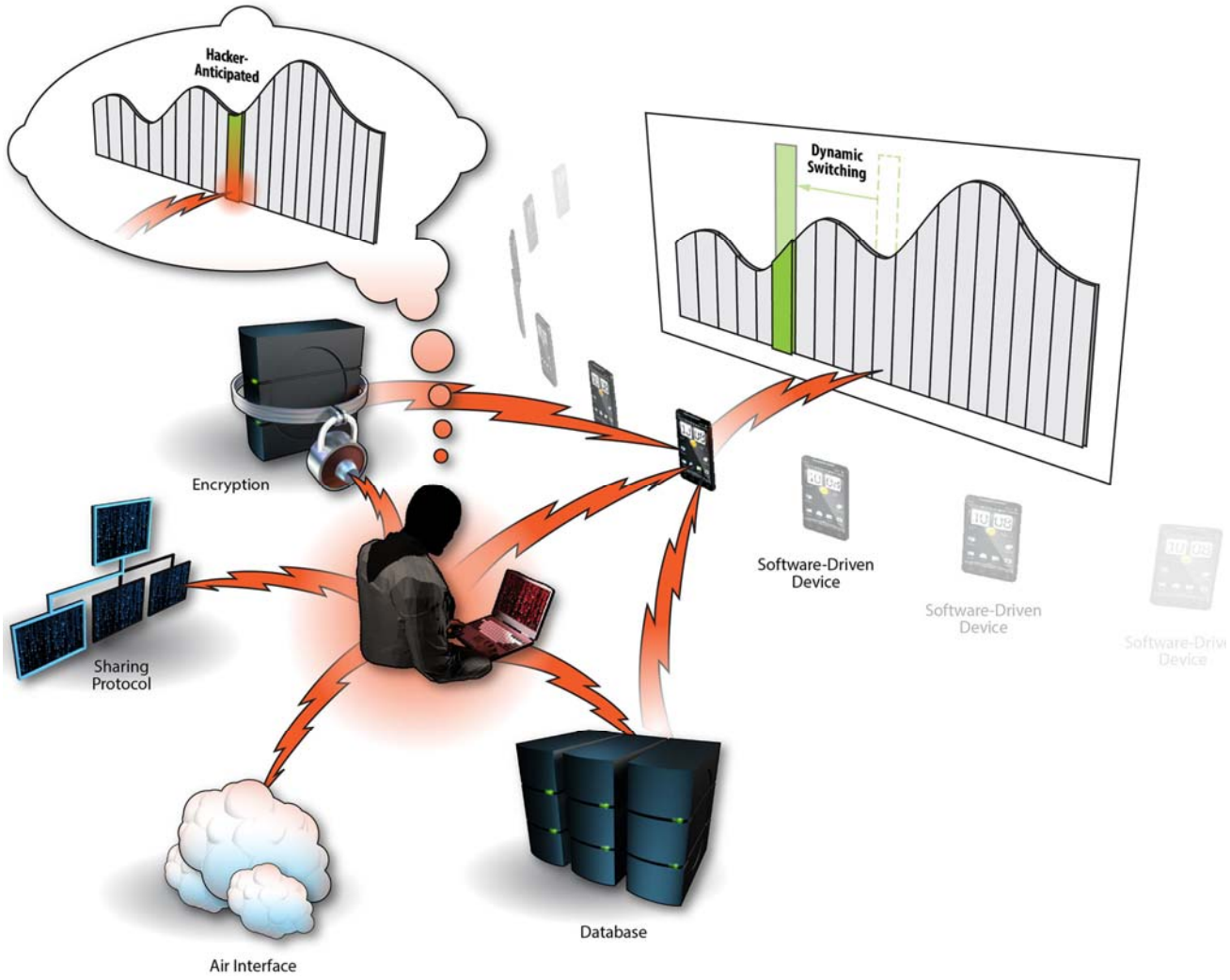


Figure 3. Security benefit of dynamic spectrum sharing and possible compromise by a point attack on the common database.

depend on whether the attacker is a script kiddie at home, a sophisticated loner, or a sovereign entity. However, ingenuity is a leveling factor, and no assumptions can be made as to the potency of the attack just based on the class of the attacker and available facilities.

Fortunately, the cyber defense community also includes many equally capable orthodox and unorthodox experts. They form two main streams. The first does vulnerability assessment/development, and the second endeavors to provide countermeasures. Hence, any CIP system must be tested by the cyber defense experts in a realistically complex environment that is reasonably isolated – its own CI ecosystem. Additionally, the inclusion of wireless in the mix can require a different class of experts or at least teams who are familiar not only with cyber security, but also with physics, propagation, and protocols of wireless and its impacts on cyber security, physical transmission environment, and the affected CI (e.g., electrical system, chemical process, physical unit). Hence, the term "Wireless Cyber" may be coined to encompass such systems whose air interfaces are increasingly implemented with software/firmware approaches affecting physical functions beyond the information transmitted. This could require the addition of Wireless Cyber Monitoring over the air, in addition to conventional cyber monitoring and defense. It may form a discipline of its own. Additionally, it requires wireless cyber expertise to design appropriate security mechanisms that may need to be designed into the wireless systems and tested in a realistic ecosystem before they are even built and deployed.

5. CONCLUSIONS

The paper examined some of the scenarios and challenges to security in spectrum sharing, especially when applied to critical infrastructure. It should help heighten awareness of

potential real world consequences which need to be taken into account as these systems are designed and deployed. As wireless becomes more pervasive, it presents more and easier targets to attack, even in critical infrastructure. Getting large data throughputs in spectrum sharing systems may require aggregating data from several systems, which will introduce several new vulnerabilities, and make the overall system only as strong as the weakest of these. Dynamic Spectrum sharing may make it harder for an attacker to predict where in spectrum space the system might go next, making it harder to compromise. However, other elements, such as a common database used to control the system could prove to be an easier target, negating this advantage. Finally, the concept of "Practical Session Security" was introduced, and the idea of "Wireless Cyber" was explored. The necessity for testing these wireless concepts in a safe infrastructure ecosystem was also discussed.

Hence, while spectrum sharing is a very attractive concept, caution needs to be exercised that its security is considered as an integral part of the design from inception, and not as a "bolt on" afterthought.

6. ACKNOWLEDGEMENT

The author gratefully acknowledges and thanks Wayne Austad and Kurt Derr, of Idaho National Laboratory, for their detailed comments and suggested revisions, and David Combs for his illustrations.

7. REFERENCES

[1] President's Council of Advisors on Science and Technology, "Report to the President: Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth," July 2012. http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf

[2] Obama, B., "Presidential Memorandum – Expanding America's Leadership in Wireless Innovation," June 14, 2013. http://www.whitehouse.gov/the-press-office/2013/06/14/presidential-memorandum-expanding-americas-leadership-wireless-innovatio

[3] Devasirvatham, D., and Austad, W., "Wireless Adds Vulnerability to Cyber Threats," Mission Critical Communications Magazine, May 2014.

ADAPTIVE PARAMETER CONTROL FOR COOPERATIVE SPECTRUM SENSING FOR WIRELESS VEHICULAR NETWORKS BASED ON MEASUREMENT-BASED SPECTRUM DATABASE

Kohsuke Nakagawa (nakagawa.k@awcc.uec.ac.jp) and Takeo Fujii (fujii@awcc.uec.ac.jp)

Advanced Wireless Communication research Center (AWCC),
The University of Electro-Communications, Choufu-shi, Tokyo, Japan

ABSTRACT

Recently, spectrum sharing with cognitive radio for wireless vehicular networks (WVN) has been emerging. For achieving spectrum sharing, spectrum sensing is used to protect primary user (PU) communications. However, simple spectrum sensing is affected by variable surrounding environment caused by mobility of secondary users (SU). The detection performance degrades in low signal to noise ratio (SNR) environment because a simple spectrum sensing cannot adapt surrounding environment. Therefore, a cooperative spectrum sensing improving detection performance has been studied. In the cooperative spectrum sensing, since many costs such as power and wireless resources need to share observed information, setting appropriate sensing parameters is important to reduce costs. In order to realize resource efficient spectrum sensing, an adaptive parameter control scheme for cooperative spectrum sensing based on a measurement-based spectrum database is proposed in this paper. In this scheme, firstly secondary user gets location information and sends it to the database. The database searches the average received power information of PU signal at the location SU and reports it to the SU. The SU can estimate the PU detection performance according to sensing parameters such as sensing period, presence or absence of cooperation, cooperative area and so on based on the information from database. SU decides sensing parameters to fulfill the desired criterion values such as detection probability and false alarm rate. As a result, the proposed scheme ensures the desired detection performance with minimum costs on a mobile environment such as WVN and the stable communication performance of PU can be protected.

1. INTRODUCTION

Recently, lots of applications works over wireless vehicular networks (WVN) have been studied for not only safety driving support but also entertainment. In near future, demand on additional spectrum resources for WVN will increase because WVN requires higher speed and larger capacity communication than other mobile communication systems. However spectrum resource is scarcity because of the increasing the applications of wireless systems such as smart phone and wireless LAN. In order to solve the spectrum scarcity problem, cognitive radio (CR) [1] is expected to employ for spectrum sharing in WVN, which is an opportunistic and efficient communication technology. Here, a mobile terminal recognizes surrounding radio environment and adapts to suitable communication parameters based on CR concept. In spectrum sharing with CR, secondary user (SU) detects and uses spatial and temporal unused spectrum band of primary user (PU) called white space (WS) to improve spectrum efficiency. A SU must avoid interference to PU with radio environment recognition technologies because PU and SU share the same spectrum. There are two types of major radio environment recognition technologies. One is a radio environment database, which is constructed from information of location. The database can know whether a SU can share the spectrum or not according to the estimated communication area of PU and the estimated interference from SU. Then the database returns spectrum usage information of location at SU when SU sends own location information. Such kind of database is considered to be used in the United States defined by FCC. However, the current radio environment database cannot support realistic radio propagation because the stored information in database is estimated by using propagation model. Therefore, the extra margin for protecting PU is required and the current database leads to degradation of spectrum sharing efficiency. The other major radio environment recognition technology is spectrum sensing. An SU detects whether PU is idle or busy based on the real time spectrum observation by SU. There are many kinds of spectrum sensing methods such as energy detector, cyclostationarity[2], matched filter [3] and so on. The energy detector (ED) is one of the spectrum sensing method which does not require large amount of calculation. In ED, SU determines whether PU is idle or busy based on observing the signal power of PU [4]. The problem of ED is the detection performance becomes worse in low SNR

environment because the power of the detected signal is fluctuated due to fading. As a solution, cooperation of multiple SUs for detecting PU called cooperative spectrum sensing has been studied. It has higher detection performance than an individual sensing. Multiple SUs share observed information and integrate it to judge state of PU. The received signal at each SU propagated through different channel because of variety of locations. The detection performance of cooperative sensing is higher and more robust than that of individual sensing because SU can use multiple information. However, SU needs additional cost such as power and wireless resources to share the measured information among sensor nodes. Thus, it is important to reduce the number of cooperation nodes as few as possible. If SU performs individual sensing with enough performance at the point, SU selects an individual sensing to keep to the minimum costs of sharing information.

Therefore, this paper proposes a novel cooperative spectrum sensing which decides sensing parameters supported by measurement-based radio environment database. The database is constructed by the average received power when PU is ON according to location from the past observed information. SU adapts sensing parameters based on information provided from the database. In this scheme, SU sets sensing parameters to fulfill desired detection probability and false alarm rate. SU obtains the information of the average received power from the database and decides the appropriate parameters by estimating detection performance. Therefore, the desired detection performance is achieved with minimum costs. In this paper, firstly, radio environment recognition technology is explained in detail, next, the relation between energy detector on WVN and Rayleigh fading is explained. After that, an adaptive parameters control for cooperative spectrum sensing based on measurement-based spectrum database is proposed. Conventional sensing and proposed sensing are compared to show the effectiveness of the proposed sensing. Finally, the paper is concluded.

2. RADIO ENVIRONMENT RECOGNITION METHOD

2.1. Radio environment database

Currently, radio environment database is considered as one of the typical radio environment recognition technologies. SU recognizes surrounding radio environment of SU by using pre-registered database. Almost all conventional databases estimate PU communication area by using radio propagation model and provide information for SU. However, it is difficult to perfectly reflect the influence of geography and surrounding buildings. Thus the database constructed by measured information represents the spectrum environment with high accuracy can be achieved.

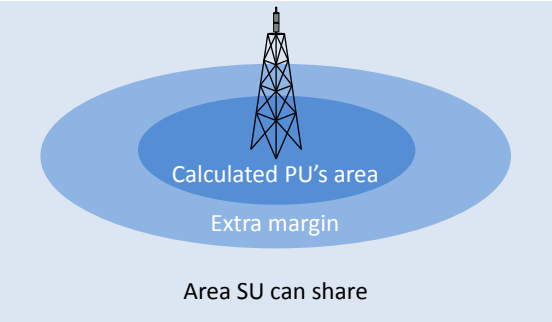


Figure1 Sharing areas based on propagation model.

2.1.1. Propagation model based database

Federal communication commission (FCC) promotes spectrum sharing over TV white space using radio environment database as a solution to scarcity of spectrum resources. Some associations construct radio environment database according to FCC guideline. In the guideline, communication area of PU is estimated from parameters of PU such as transmit power, location and so on and the propagation model is defined by FCC. Thus, the database is constructed by information whether SU can use the spectrum of PU or not according to SU location. FCC defined database cannot perfectly reflect the influence of the geography and buildings because of using a radio propagation model. Hence, extra margin for protecting PU should be added to the estimated PU area defined in the guideline. In this margin, SU cannot use the spectrum of PU regardless of the fact that SU does not give interference to PU. The margin degrades the efficiency of spectrum usage for SUs.

2.1.2. Measurement-based database

It is desirable that the database has information expressing real radio environment with more precise for effective spectrum sharing. However, the database based on radio propagation model cannot perfectly reflect the influence of geography and buildings. Thus, the database constructed by measured radio environment information has been proposed [5 6]. The vehicle equipped with sensor drives to measure and to gather the received power with its location for constructing the database. Gathered information is split into mesh of a given size and the received power information is processed statistically. Therefore, the database is constructed by statistical information of PU signal according to the location. The database can estimate a higher accuracy of real PU communication area than the database based on propagation model because the measured information reflects to the unique effect of the propagated environment. Estimation with high accuracy information enables SU to use the spectrum of PU without interference and achieves more efficient spectrum sharing.

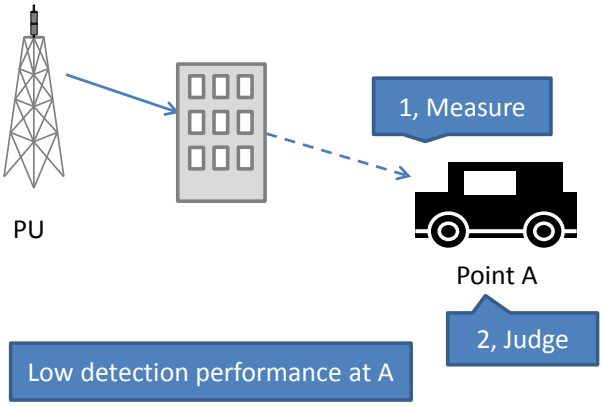


Figure2 Individual energy detector.

2.2. Spectrum sensing

Spectrum sensing is one of the typical radio environment recognition technology based on radio observation. SU can get real time information because SU recognizes and observes radio environment at the same time. From the reason, the spectrum sensing can detect the temporal WS of PU has ON and OFF states on time domain different from the database. A simplest spectrum sensing scheme called Energy detector has been studied extensively. Additionally, a cooperative spectrum sensing by using energy detector is studied to solve the problem of performance degradation of the individual sensing due to wires channel environment. Those are explained as follows because the proposed scheme in this paper is based on energy detector.

2.2.1. Energy detector

An energy detector is the simplest spectrum sensing scheme which only needs small amount of calculation without prior information about PU. In energy detector, spectrum sensing problem can be considered as a hypothesis testing problem to determine whether PU is idle or busy. In hypothesis testing, hypothesis is made and determined statistically whether it is correct or not. In ED, the idle state of PU is defined as hypothesis H_0. The busy state of PU is defined as hypothesis H_1,

$$\begin{aligned} H_0 &: PU\ is\ ilde \\ H_1 &: PU\ is\ busy \quad . \end{aligned} \tag{1}$$

Then, SU determines the present state whether H_0 or H_1 [7]. Each state is expressed in the following equation (2),

$$\begin{aligned} H_0 &: x[n] = w[n] \\ H_1 &: x[n] = h \cdot s[n] + w[n] \quad , \end{aligned} \tag{2}$$

where, $x[n]$ denotes the received signal of SU. $n = 1,2, \dots, \mathrm{N}$ is the sample index of and N is total number of collected samples. $w[n]$ is additive white Gaussian noise (AWGN) which has zero mean and variance σ_w^2 , h is channel coefficient, $s[n]$ is transmitted signal from PU. The test statistic $T(x)$ calculated by $x[n]$ is used to determine the state of PU. $T(x)$ is calculated by following the equation (3),

$$T(x) = \sum_{n=1}^{\mathrm{N}} (x[n])^2 \quad , \tag{3}$$

The test is compared to the size of $T(x)$ and detection thresholdλ. The criterion formula is (4).

$$T(x) \underset{>}{\overset{\leq}{}} \lambda : \begin{matrix} H_0 \\ H_1 \end{matrix} \tag{4}$$

$P(H_1 \,|H_1)$ denotes the detection probability P_{D} and $P(H_1 \,|H_0)$ denotes false alarm rate $\mathrm{P_{FA}}$. High P_{D} means SU has a high possibility of detecting PU communications. High P_{FA} means high probability that PU state is determined as state H_0 when PU is busy. Thus, it is desirable to fulfill higher P_{D} and lower P_{FA} in ED. However, it is difficult to fulfill together because there is a trade-off relation between P_{D} and P_{FA}.

Generally, detection threshold λ sets to fulfill desired P_{FA} based on noise levels of receiver.

If the number of samples is large enough, the distribution of test statistic can be approximated to Gaussian distribution by the central limit theorem. Thus, λ is calculated by equation (5),

$$\lambda = \sqrt{\mathrm{N}}\sigma_w^2 Q^{-1}(P_{FA}) + \mathrm{N}\sigma_w^2 \quad , \tag{5}$$

where, $Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{t^2}{2}} dt$. P_{FA} is calculated by equation (6) when ED performs with λ,

$$P_{\mathrm{FA}} = Q\left(\frac{\lambda - \mathrm{N}\sigma_w^2}{\sqrt{\mathrm{N}}\sigma_w^2}\right) \quad . \tag{6}$$

2.2.2. Cooperative spectrum sensing

ED easily determines the state of PU communication. However, the detection performance of an individual ED degrades because the received power degrades because the received power fluctuates due to fading, geography and buildings effect. Thus, a cooperative spectrum sensing with performing multiple observed information of SUs and integration for determining have to be studied. SU gains spatial diversity effect because SU can use observed information not only at SU location but also at other cooperation nodes (CN). Therefore, it performs with higher

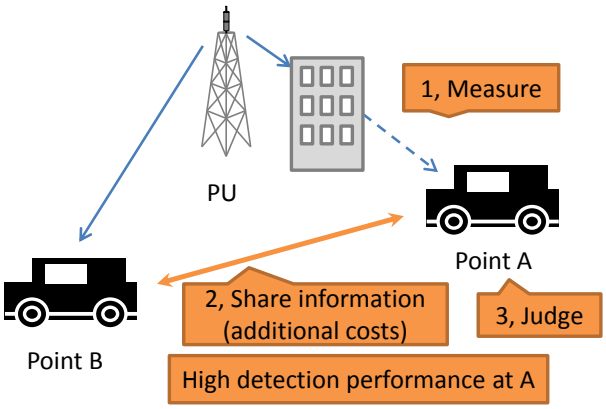


Figure3 Cooperative energy detector.

detection probability than individual ED. Some integration scheme for cooperative sensing are studied. Most general approach has extended equation from individual ED. The hypothesis on node number $m = 1,2,\dots,\mathrm{M}$ are expressed by equation (7),

$$\begin{aligned} H_0 &: x_m[n] = w_m[n] \\ H_1 &: x_m[n] = h_m \cdot s[n] + w_m[n] \end{aligned} \quad , \qquad (7)$$

where $x_m[n]$ is the received signal, $n = 1,2,\dots,\mathrm{N}$ is the sample index and N is the total number of collected samples on SU or CN has node number m. $w_c[n]$ is AWGN which has zero mean and variance σ_{wm}^2. h_m is channel coefficient. Nodes share the observed information with each other to calculate Test statistic $T_c(x)$ by using $x_m[n]$. $T_c(x)$ in cooperative sensing with M nodes is calculated by the following equation (8),

$$T_c(x) = \sum_{m=1}^{\mathrm{M}} \sum_{n=1}^{\mathrm{N}} (x_i[n])^2 \ . \qquad (8)$$

The decision is processed by comparing $T_c(x)$ with detection threshold λ_c. If the number of sample is large enough, the distribution of test statistic $T_c(x)$ can be approximated to Gaussian distribution by central limit theorem. Thus, λ_c in cooperative sensing with M nodes is calculated by the equation (9),

$$\lambda_c = \sqrt{\mathrm{NM}}\sigma_w^2 Q^{-1}(P_{FA}) + \mathrm{NM}\sigma_w^2 \ . \qquad (9)$$

Cooperative sensing can improve detection performance. However costs to share observed information such as power and wireless resources increase with increasing the number of cooperation nodes. Therefore, SU needs to set appropriate number of cooperation nodes adaptively for preventing excessive increase of sensing costs in cooperative sensing.

3. ENERGY DETECTOR ON WVN AND RAYLEIGH FADING

The surrounding environment of SU changes because of mobility on WVN. The fading channel and the received power at SU variation depend on SU's location. The detection performance of ED degrades caused by temporal degradation of the received power on slow fading environment. The reason is that the detection performance is determined by SNR and the channel coefficient does not vary for a sensing duration in slow fading environment. Thus, detection performance of ED is unstable because it is affected by mobility on WVN.

The distribution of instantaneous SNR γ is expressed in equation (10) when the amplitude of received signal on SU follows Rayleigh distribution [8],

$$f(\gamma) = \frac{1}{\bar{\gamma}} \exp\left(-\frac{\gamma}{\bar{\gamma}}\right) \ , \qquad (10)$$

where $\bar{\gamma}$ is the average SNR. Thus, detection performance P_{Dray} of cooperative ED with m nodes is shown in equation (11),

$$P_{\mathrm{Dray}} = \alpha \left[G_1 + \beta \sum_{n=1}^{m\mathrm{N}-1} \frac{\left(\frac{\lambda}{2}\right)^n}{2n!} {}_1F_1\left[m; n+1; \frac{\lambda}{2}\frac{\bar{\gamma}}{1+\bar{\gamma}}\right] \right], \qquad (11)$$

where m is the number of cooperation nodes, ${}_1F_1(.;.;.)$ is the confluent hyper geometric function and α, β, G_1 are described in Appendix A.

4. ADAPTIVE PARAMETER CONTROL FOR COOPERATIVE SPECTRUM SENSING BASED ON MEASUREMENT-BASED SPECTRUM DATABASE

In conventional energy detector, SU has unstable detection performance on WVN because SU sets detection threshold based on noise levels. The cooperative spectrum sensing is proposed to improve the detection performance. However it must need costs such as power and wireless resources. So, it is better to set minimum number of cooperation nodes. Thus, this paper proposes an adaptive parameters control scheme for minimize costs of cooperative spectrum sensing by using measurement-based radio environment database.

SU previously sets criterion values of lower limit of detection probability P_{Ddis} and upper limit of false alarm rate P_{FAdis}. Then SU sets sensing parameters to fulfill criterion values together by using the average received power information stored in database according to location. Therefore, stable sensing performance can be achieved regardless of locations. The process of this method is shown below.

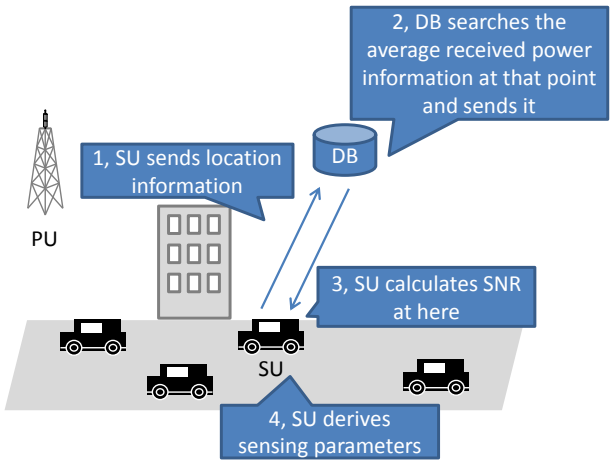


Figure4 Proposed spectrum sensing.

1. SU sends the own location information to database for sharing spectrum to PU.
2. Database sends the average received power information of SU location to SU when PU is ON states.
3. SU estimates average SNR and P_{D} on its own location based on the average received power and own receiver's noise level.
4. SU sets appropriate sensing parameters based on SNR to fulfill desired P_{Ddis} and P_{FAdis} together.

The parameters configuration is based on P_{FA} in the conventional sensing scheme. However in our proposed scheme, the parameters configuration based on P_{D}.Thus, the proposed scheme is able to ensure the stable detection performance and spectrum sharing with stably protecting PU regardless of surrounding environment. In this paper, the number of sample of each node is constant value and detection threshold and the number of cooperation nodes are changed to achieve desired sensing performance.

4.1. Detection threshold for individual energy detector

Firstly, SU judges whether the detection performance can achieve desired performance or not by using individual ED because it is the sensing scheme has minimum costs. SU estimates λ when the detection probability achieves $\mathrm{P_{Ddis}}$ by using estimated SNR and detection probability equation (11). Then SU calculates P_{FA} when SU performs individual sensing ($m = 1$) with λ. SU decides to perform individual sensing if calculated P_{FA} is lower than P_{FAdis}. Then, SU can achieve desired detection performance using individual ED with λ. SU decides to performs cooperative sensing if calculated P_{FA} is higher than P_{FAdis}. Then, SU cannot achieve desired detection performance using individual ED.

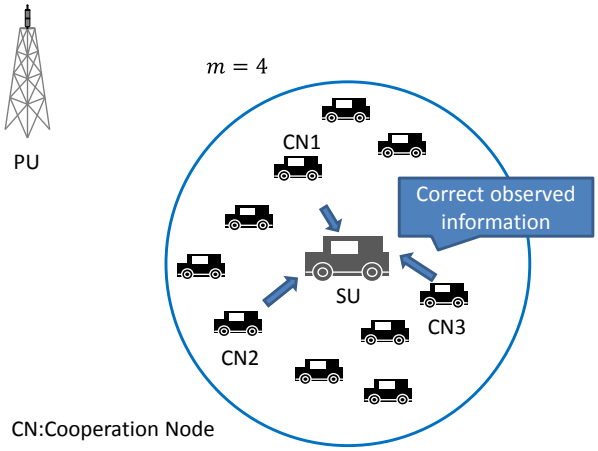


Figure5 simulation model.

4.2. The Number of cooperation node setting

After SU decides to perform cooperative sensing, SU calculates the minimum number of cooperative nodes to fulfill desired sensing performance to perform sensing with minimum costs. To calculate appropriate number of cooperation nodes, firstly, m is assigned to 2 and SU calculates λ to fulfill P_{Ddis} by using detection probability equation (11). Then SU calculates P_{FA} with λ. If calculated P_{FA} is lower than P_{FAdis}, SU sets λ and perform cooperative sensing with m nodes. If calculated P_{FA} is higher than P_{FAdis}, m is assigned to $m + 1$ and calculate λ again. These steps perform repeatedly to set minimum m can fulfill the criterion values. Therefore, SU performs cooperative sensing with λ and m.

If SU cannot fulfill criterion values when m is assigned to maximum number of cooperation nodes M, SU calculates λ to fulfill $P_{\mathrm{FA}} = P_{\mathrm{FAdis}}$ and performs cooperative sensing with λ and M.

5. SMULATION RESULTS

Computer simulation is used to show the efficiency of the proposed scheme. Figure 5 shows the simulation model. SU exists in the center of the circle with radius r and CNs are randomly distributed around SU in the circle. Each CN sends the test statistic to share observed information. SU determines state of PU based on integrated each CN's information. In the proposed scheme, criterion values of sensing performance are lower limit of detection probability $P_{\mathrm{Ddis}} = 0.9$ and upper limit of false alarm rate $P_{\mathrm{FAdis}} = 0.1$. The cooperation area of SU is the circle of radius 200m. 10 CNs are randomly distributed in the circle. The detection performance using the individual energy detection, the cooperative sensing and the proposed scheme are compared. There are 4 cooperation nodes selected from 10 CNs in conventional cooperative sensing.

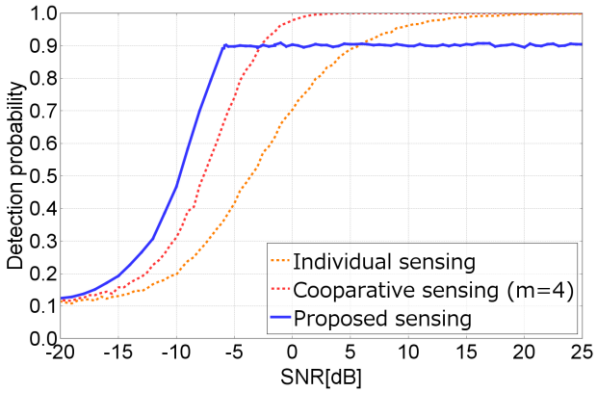


Figure6 SNR versus detection probability.

5.1. Detection probability evaluation

The detection probability variation of SNR at SU is shown in Fig. 6. The detection probability degrades in low SNR using individual sensing because individual sensing decides detection threshold based on the noise levels of SU's receiver. Cooperative sensing achieves higher detection probability than individual sensing. However in high SNR, cooperative sensing uses additional costs to share information despite enough performance available without sharing costs. On the other hand, the proposed sensing sets sensing parameters based on detection probability. The proposed scheme shows higher detection performance than desired detection probability 0.9 in the environment of SNR more than 6dB. This is because the proposed sensing can fulfill criterion values such as P_{Ddis} and P_{FAdis} together with minimum costs in this environment. However from 6dB, the detection probability gradually decreases because in this environment. SU cannot fulfill criterion values together caused by limitation of maximum number of cooperation nodes. This decrease can be curbed to increase the number of samples or cooperation nodes. The proposed sensing enables SU protect PU stably regardless of surrounding environment.

5.2. False alarm rate evaluation

The number of false alarm rate variation of SNR at SU is shown in Fig. 7. It shows false alarm rate is constant regardless of SNR in conventional individual and cooperative sensing because SU sets detection threshold to fulfill constant P_{FA} in conventional sensing. While in the proposed sensing, P_{FA}.varies according to SNR, P_{FA} is always lower than upper limit of $P_{\mathrm{FAdis}} = 0.1$. Lower P_{FA} means SU has stronger potential to find WS. In this way, the proposed sensing gets as many chances as possible with ensuring the protection of PU's communications.

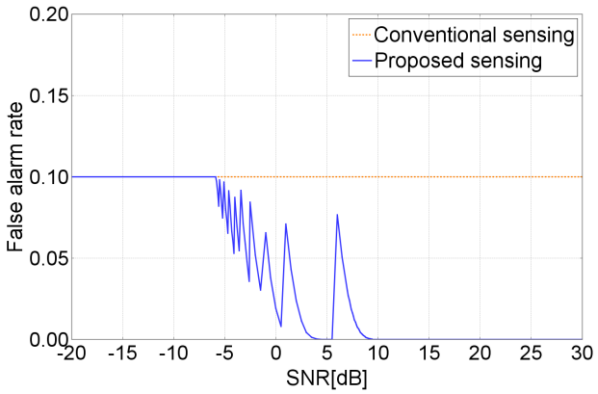


Figure7 SNR versus false alarm rate.

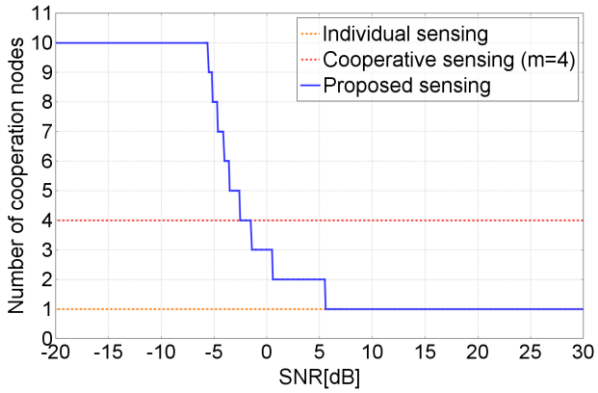


Figure8 SNR versus number of cooperation nodes.

5.3. The number of cooperation nodes evaluation

The number of cooperation nodes variation of SNR at SU is shown in Fig. 8. Although the conventional individual and the cooperative sensing have the constant number of cooperation nodes regardless of SNR. On the other hand, the proposed sensing adapts it based on SNR. The number of cooperation nodes is small in high SNR environment and it is large in low SNR environment. This adaptation makes constant detection performance from low to high SNR environment with minimum costs. The conventional cooperative sensing and the proposed sensing have enough performance in high SNR environment as shown in Fig. 6. The conventional cooperative sensing has 4 cooperation nodes. It means information sharing costs are needed. However the proposed sensing has only 1 cooperation nodes. It means SU performs individual sensing without sharing costs. The proposed scheme can reduce information sharing costs as possible with stable detection performance.

6. CONCLUSIONS

This paper considers the problem of the conventional energy detector in WVN and a novel parameter adaptation spectrum sensing based on radio environment database for WVN is proposed. The proposed sensing achieves desired detection

performance with minimum costs by setting sensing parameter based on SNR according to location. Thus, the detection performance is evaluated to show the effectiveness of the proposed sensing by simulation. Therefore, the results indicate that the proposed sensing can achieve more stable protection of PU's communication than the conventional sensing with minimum costs regardless of location.

ACKNOWLEDGMENT

This work was supported by JSPS KAKENHI Grant Numbers 24246067, 25630158.

APPENDIX A

α, β, G_1 in equation (11) describe as follow,

$$\alpha = \frac{1}{\Gamma(m)2^{m-1}}\left(\frac{1}{\bar{\gamma}}\right)^m , \tag{12}$$

$$\beta = \Gamma(m)\left(\frac{2\bar{\gamma}}{1+\bar{\gamma}}\right)^m e^{-\frac{\lambda}{2}} , \tag{13}$$

$$G_1 = \frac{2^{m-1}(m-1)!}{\left(\frac{1}{\bar{\gamma}}\right)^m}\frac{\bar{\gamma}}{1+\bar{\gamma}}e^{-\frac{\lambda}{2(1+\bar{\gamma})}}\left[\left(1+\frac{1}{\bar{\gamma}}\right)\left(\frac{1}{1+\bar{\gamma}}\right)^{m-1} \times L_{m-1}\left(\frac{\lambda}{2}\frac{\bar{\gamma}}{1+\bar{\gamma}}\right) + \sum_{n=0}^{m-1}\left(\frac{1}{1+\bar{\gamma}}\right)^n L_n\left(\frac{\lambda}{2}\frac{\bar{\gamma}}{1+\bar{\gamma}}\right)\right] , \tag{14}$$

where $L_n(.)$ is the Laguerre polynomial of degree n.

REFERENCES

[1] J. Mitora and J. Maguire, G.Q., "Cognitive radio making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4 pp. 13-18, Aug. 1999.

[2] M. Oner, F. Jondral, "Air interface recognition for a software radio system exploiting cyclostationary," *Proc. PIMRC2004*, vol.3, pp.1947–1951, Sept. 2004.

[3] W. A. Gardner, "Signal interception: A unifying theoretical framework for feature detection," *IEEE Trans. Commun*., vol. 36, pp. 897–906, Aug. 1988.

[4] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE,* vol. 55, no. 4, pp. 523–531, Apr. 1967.

[5] T.Fujii, K.Inage, M.Kitamura, O.Altintas, H.Kremo and H.Tanaka, "Short Paper: Probing the Spectrum with Vehicles: Towards an Advanced Spectrum Database," *IEEE VNC*, pp. 226-229, Dec 2013.

[6] H.R.Imam, K.inage, M.Ohta and T.Fujii, "Measurement based radio environment database using spectrum sensing in cognitive radio," *IEEE iCOST in Mobile and Wireless Networking*, pp. 110-115, Oct. 2011.

[7] Song, J., Feng, Z., Zhang, P. and Liu, Z "Spectrum sensing in cognitive radios based on enhanced energy detector," *IET Communications,* vol. 6, issue 8, pp.805-809. May 2012,

[8] Wei. Jiang and Huizhu, Ma. "Cooperative spectrum sensing for cognitive radio in rayleigh channels," *IEEE ICISE,* pp.2595-2598 Dec 2009.

WIDEBAND COGNITIVE WIRELESS COMMUNICATION SYSTEM: IMPLEMENTATION OF AN RF-ETHERNET BRIDGE FOR CONTROL APPLICATIONS

Pedro Manuel Rodríguez* (pmrodriguez@ikerlan.es), Raúl Torrego* (rtorrego@ikerlan.es), Felix Casado* (fcasado@ikerlan.es), Zaloa Fernandez* (zfernandez@ikerlan.es), Mikel Mendicute** (mmendikute@mondragon.edu), Aitor Arriola* (aarriola@ikerlan.es), Iñaki Val* (ival@ikerlan.es)
*Communications department: IK4-IKERLAN, Arrasate-Mondragón, Spain
**Signal Theory and Communications Area: University of Mondragon, Arrasate-Mondragón, Spain

ABSTRACT

Ethernet and Industrial Ethernet are widely used nowadays in control applications due to the bandwidth, robustness and scalability they provide. However, when dealing with complex systems, the use of these standards generates complex wirings, and the necessity of devices that penalize the size and weight of the system (e.g. access points, routers, switches, etc). Besides, depending on the application (e.g. moving or rotating elements) it may not be possible to route a wire to all the elements to control. The use of wireless control networks is therefore the solution for these issues. However, this type of applications requires a reliability not provided by classical wireless communication systems. Software Defined Radio and Cognitive Radio are technologies that enable the implementation of wireless communication systems with enough bandwidth and reliability so as to replace this type of wired control networks. On this basis, this paper presents the implementation of a wideband RF-to-Ethernet bridge for its use in control applications. The bridge has been fully implemented on an FPGA device and includes cognitive features in order to achieve the reliability and interference avoidance that control applications require.

1. INTRODUCTION

Nowadays there is a trend towards replacing wired communication systems by wireless solutions, since the reduction of the number of wires is an appreciated characteristic in any type of installation. This especially happens in industrial environments on which the size, weight or maintenance easiness of the installation has further economical impact (i.e. aeronautics, rail transport, etc.) Besides, the use of wireless communications becomes compulsory when the application contains moving or rotating elements in which it is not possible to route a wire.

Traditional wireless communication systems can be used in those subsystems in which communication reliability is not critical (e.g. multimedia delivery in passenger transport). However, other data transfers, such as the ones needed for control applications, require robustness and reliability levels not reachable by these traditional systems. This fact is precisely more noticeable in industrial environments due to the harsh conditions present in them (metallic objects causing multipath, interferences, etc). Software Defined Radio and Cognitive Radio are the technological answer that can overcome these limitations and enable the use of wireless communications in control applications.

Ethernet, and its industrial variations such as Industrial Ethernet or EtherCAT, are some of the most used standards in control applications. Therefore, this paper aims to present a solution for easily replacing a wired Ethernet link by a wireless one, and, continuing with previous works [1,2] implements an RF-to-Ethernet bridge using a wideband cognitive wireless communication system. The cognitive RF-to-Ethernet bridge captures the input Ethernet frames, transmits them over-the-air in an interference-free frequency, receives and reconstructs the frames in the receiver and puts them back into the wired interface. The main contributions with respect to the previous works are the redesign of the reception and transmission algorithms and the implementation of the Ethernet frame processing IP. These modifications allow the presented communication system to interchange frames with an Ethernet interface and increase the data rate from 1.6 Mbps to 12.8 Mbps, hence achieving a wideband communication. Moreover, it is now able to transmit short frames instead of a continuous stream, and the reception algorithms have been designed

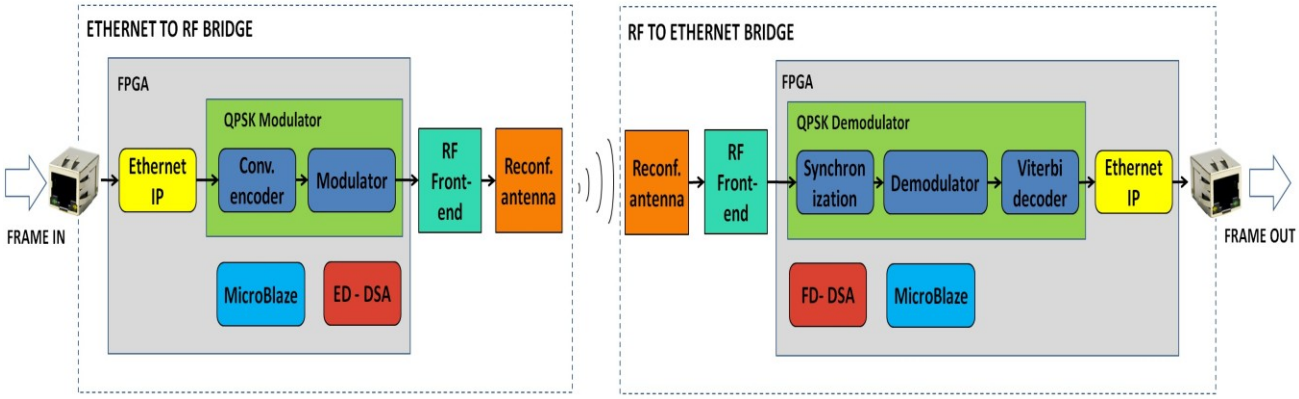


Figure 1: Wideband, cognitive, wireless RF-Ethernet bridge

accordingly so that synchronization is carried out during the preamble that precedes each frame.

The system has been fully implemented on an FPGA device, thanks to the high performance and flexibility offered by this type of devices. The baseband data processing algorithms have been designed, tested and implemented using System Generator for DSP, Xilinx's rapid prototyping tools. Besides, a commercial adjustable RF front-end and a custom-designed reconfigurable antenna make the system capable of working in the Industrial, Scientific and Medical (ISM) bands of 868 MHz and 2.45 GHz.

The remainder of this paper is organized as follows. Section 2 describes the complete system and presents the most significant blocks that make it up. System performance is analyzed in Section 3 presenting the measurements that have been carried out in the RF-to-Ethernet bridge. Finally, concluding remarks are summarized in Section 4.

2. SYSTEM DESCRIPTION

The designed cognitive RF-to-Ethernet bridge consists of two FPGA-based nodes, being each of them able to carry out both the Ethernet-to-RF and RF-to-Ethernet conversion. The system works in a half duplex mode; this means that each time one of the nodes will act as an Ethernet-to-RF bridge, while the other one will act as an RF-to-Ethernet bridge. In order to achieve the reliability needed in communications for control applications, the system implements a Dynamic Spectrum Access (DSA) algorithm. Taking advantage of the capability of the system for transmitting in two ISM bands (868 MHz and 2.45 GHz), the DSA algorithm selects the most suitable frequency in order to avoid interferences. An overview of the whole system can be seen in Figure 1.

2.1. Ethernet-to-RF Bridge

The node acting as RF-to-Ethernet bridge implements three functions: the Ethernet frame processing IP, the QPSK modulator and the Dynamic Spectrum Access algorithm.

2.1.1. Ethernet frame processing IP

The Ethernet frame processing IP is in charge of receiving the frames from the Ethernet PHY in a Media Independent interface (MII), reconditioning them and routing them to the QPSK modulator. It implements an Ethernet MAC, two dual port RAMs (implemented using FPGA BRAMs for improved speed) and a control Finite State Machine (FSM).

The Ethernet MAC manages the communication between the PHY and user logic. It receives the frames in an MII interface and translates them into a byte-by-byte format. Due to the different data rates used by the incoming data and the modulator, it is not possible to connect these two blocks directly. The dual port RAMs enable this connection by

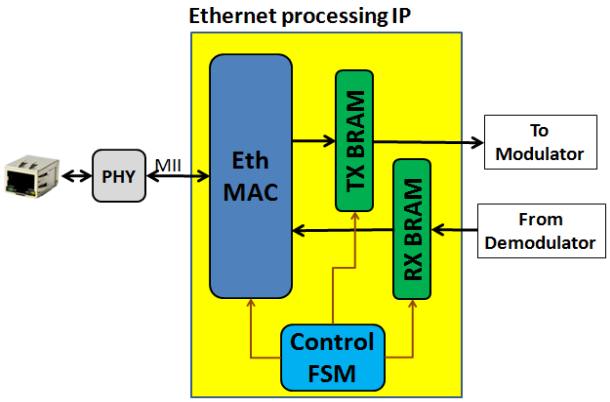


Figure 2: Ethernet frame processing IP

allowing asynchronous and independent read/write operations in each of their ports. The control of these operations is carried out by the control FSM.

It should be noted that although only the Ethernet to modulator transition has been mentioned, the Ethernet processing IP works in a bidirectional way. A single Ethernet processing IP is implemented per node; hence, in the node acting as RF-to-Ethernet bridge, this block is in charge of properly encapsulating the demodulated data into a frame and delivering it to the Ethernet PHY. A block diagram of this IP is shown in Figure 2.

2.1.2. QPSK modulator

The QPSK modulator is in charge of two functions: data encoding, in order to increase the reliability of the communication, and the modulation function itself. Data is first processed by a convolutional encoder with a ½ rate, and then delivered to the modulator in which a 256-symbol preamble is added for start of frame detection and frequency and phase recovery in the receiver. A 32-symbol Start Frame Delimiter (SFD) is added as well.

Received Ethernet frames may have different lengths. In order to properly transmit them, the length is measured and included in two bytes (8 QPSK symbols) before the payload. The complete frame to be transmitter over the air is represented in Figure 3:

PREAMBLE	SFD	LEN.	DATA
(256 symbols)	(32)	(8)	(-)

Figure 3: Frame format

Finally, data is mapped over the QPSK constellation and the signal is oversampled by a factor of 4. After that, the signal is filtered with a raised cosine filter (roll-off = 0.35) prior to being sent to the reconfigurable front-end.

2.1.3. ED Dynamic Spectrum Access algorithm

In parallel, an Energy Detection (ED)-based DSA algorithm is also implemented in the FPGA [2]. This algorithm looks for the available frequencies within the spectrum, based on energy presence, and selects the transmission frequency accordingly. The system is completed with a MicroBlaze soft processor in charge of reconfiguring both the RF front-end and the antenna, based on the information provided by the DSA algorithm. This processor is also in charge of the initialization of the whole system.

2.2. RF-to-Ethernet Bridge

Similarly, the node that carries out the inverse operation, i.e. the RF to Ethernet conversion, also implements three functions: the Dynamic Spectrum Access algorithm, the QPSK demodulator and the Ethernet frame processing IP.

2.2.1. FD Dynamic Spectrum Access algorithm

The DSA algorithm in the receiver has no information about the transmission frequency that the Ethernet-to-RF bridge is using. Hence, it must be capable of distinguishing between the transmission targeted for the RF-to-Ethernet bridge and the interferences present in other frequencies. Therefore, a Feature Detection (FD) DSA algorithm [3] is implemented in which cyclostationary features (dependant on signal characteristics such as modulation or symbol period) are used in order to distinguish the target transmission.

2.2.2. QPSK demodulator

Once the system is configured in the correct frequency band, baseband IQ data coming from the RF front-end is processed by the QPSK demodulator. First, the system detects a transmitted message by means of a preamble detector, which triggers the feed-forward timing recovery algorithm, based on Maximum Likelihood estimation [4]. A Farrow structure interpolator filter is used to get optimal symbol value. Later, a data-aided coarse frequency estimator is used to compensate the carrier frequency drift [5]. Joint phase and SFD estimation [6] is done first detecting where the frame starts and then the phase offset is estimated based on the preamble training data. Once the data symbols are correctly aligned, the payload data is decoded using the Viterbi algorithm and routed to the Ethernet frame processing IP.

The demodulator is also composed of an Automatic Gain Controller (AGC). This block uses the preamble to compute the incoming signal power and sets the analog amplifiers present in the RF front-end accordingly so that the received signal at the ADC converters reaches a 90% of full scale. Once a frame has been properly demodulated, the AGC sets back the amplifiers to their maximum gain in order to obtain the highest possible sensitivity. The dynamic range for the receiver is specified from -95 dBm to -30 dBm.

2.2.3. Ethernet frame processing IP

In the node configured as an RF-to-Ethernet bridge, the Ethernet frame processing IP is in charge of managing the communications between the demodulator and the Ethernet PHY. In order to complete the RF-to-Ethernet conversion, this IP encapsulates properly the received data into an Ethernet frame, adjusts the data rates with the double port RAMs and delivers it to the Ethernet PHY via a Medium Access Control (MAC) IP. As mentioned before, a single Ethernet processing IP is present in each node, hence being able to manage a bidirectional communication. Similarly,

Table 1: Typical requirements for industrial wireless sensor and actuator networks in the process automation domain

Sensor Network Applications	Delay	Range	Battery Lifetime	Update Frequency	Security level
Monitoring and supervision					
Vibration sensor	s	100 m	3 years	sec - days	low
Pressure sensor	ms	100 m	3 years	1 sec	low
Temperature sensor	s	100 m	3 years	5 sec	low
Gas detection sensor	ms	100 m	3 years	1 sec	low
Closed loop control					
Control valve	ms	100 m	> 5 years	$10 - 500$ ms	medium
Pressure sensor	ms	100 m	> 5 years	$10 - 500$ ms	medium
Temperature sensor	ms	100 m	> 5 years	500 ms	medium
Flow sensor	ms	100 m	> 5 years	$10 - 500$ ms	medium
Torque sensor	ms	100 m	> 5 years	$10 - 500$ ms	medium
Variable speed drive	ms	100 m	> 5 years	$10 - 500$ ms	medium
Interlocking and Control					
Proximity sensor	ms	100 m	> 5 years	$10 - 250$ ms	medium
Motor	ms	100 m	> 5 years	$10 - 250$ ms	medium
Valve	ms	100 m	> 5 years	$10 - 250$ ms	medium
Protection relays	ms	100 m	> 5 years	$10 - 250$ ms	medium

the Microblaze soft processor, in charge of transmitter functions, is also in charge of managing frequency changes in the receiver and initializing the demodulation system.

To conclude, each of the nodes contains a commercial adjustable RF front-end and a custom-designed reconfigurable antenna. These devices make the system capable of working in the Industrial, Scientific and Medical (ISM) bands of 868 MHz and 2.45 GHz [2].

3. MEASUREMENTS

This section will detail the measurement tests that have been carried out over the RF-to-Ethernet bridge presented in this contribution.

3.1. Effective data rate

The baseband data processing algorithms implemented in the FPGA and the IQ ADC/DAC converters in the adjustable RF front-end are both clocked at a 25.6 MHz frequency. An oversampling rate of 4 has been used in the system, what leads to a 12.8 Mbps raw data rate in the wireless link.

However, the inclusion of a ½ rate convolutional encoder in order to increase the reliability of the communication reduces by half the effective data rate of the system. Besides, the 256 symbol preamble and 32 symbol SFD included in each of the frames to be transmitted also degrade this effective data rate. Taking into account that the length of these two sections of the frame is fixed, this degradation will become more significant for small frames.

Figure 4 shows the effective data rate achievable by the system versus the frame length. Despite the degradation suffered by the data rate, typical update frequencies in industrial wireless sensor and actuator networks in the process automation domain are between 10 and 500 ms, as can be observed in Table 1 [7]. Therefore, and considering that the amount of data to be transmitted in this type of applications is not very large, the achieved data rate is suitable for them.

3.2. Latency

Table 2 shows the latency introduced by the different blocks of the system, as well as the overall latency. It should be noted that the air propagation delay, although negligible, should also be added to the measured times in order to obtain an exact latency. The presented times have been measured from the first 4 parallel bits (RXD[3:0]) arriving through the MII interface of the Ethernet-to-RF bridge to the same 4 bits being written to the TXD[3:0] signals of the MII interface of the RF-to-Ethernet bridge.

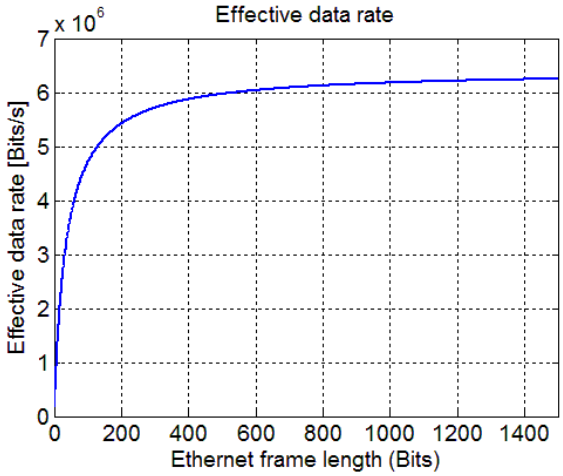


Figure 4: Effective data rate vs. Ethernet frame length

Table 2: System latency

System latency (us)									
	Block								
Frame length (Bytes)	Eth MAC RX	Eth BRAM RX	Modulator	Front-end TX	Front-end RX	Demodulator	Eth BRAM TX	Eth MAC TX	Total
32	1,52	5,20	24,00	0,10	0,50	67,00	42,80	0,70	141,82
128	1,52	11,80	24,00	0,10	0,50	67,00	163,00	0,70	268,62
512	1,52	42,50	24,00	0,10	0,50	67,00	643,00	0,70	779,32
1024	1,52	83,80	24,00	0,10	0,50	67,00	1280,00	0,70	1457,62
1356	1,52	110,00	24,00	0,10	0,50	67,00	1700,00	0,70	1903,82

It can be observed that due to the double port BRAMs needed in order to adequate the data rate in the Ethernet to FPGA and FPGA to Ethernet transitions, the latency is also dependent on frame length. Besides, these transitions are the ones that introduce the biggest latencies in the system. Unfortunately, due to system topology and selected FPGA working frequency it is not possible to remove these transitions and their latencies.

3.3. Frequency reconfiguration times

Frequency reconfiguration times have also been measured and can be seen in Table 3. The measurement represents the time from the moment in which MicroBlaze generates the reconfiguration order to the moment in which the physical frequency change happens.

It must be noted that in order to carry out a transmission frequency change when an interference is detected, it is necessary to reconfigure both the RF front-end and the antenna. Taking into account that both operations are performed in parallel, the worst case will indicate the time during which the system is not available.

In order to reconfigure the antenna it is necessary to change its DC polarization. This change is achieved through a GPIO from MicroBlaze and glue logic. The presented reconfiguration time measures the delay of the complete process. In order to reconfigure the front end, MicroBlaze carries out some calculation with the new frequency as input parameter (PLL parameters, amplifier gains…), programs them into the front-end through a SPI interface and commands the front-end for calibrations. When all this process is finished the physical frequency change takes place.

3.4. RX/TX change time

The presented system works in a half-duplex mode, i.e. each of the nodes alternates the transmitter and receiver mode over time. Besides, the node acting as a transmitter needs to analyze channel availability prior to transmitting, hence also switching from TX to RX mode. On the other hand, both the baseband processing algorithms and the RF front-end are able to work in a full duplex mode. However, as each of the nodes has only one antenna, it is necessary to include an RF switch that selects its connection to the RX or TX path of the front-end. This selection is carried out with a GPIO of the MicroBlaze processor and glue logic. The complete process takes 50 us.

Table 3: Frequency reconfiguration time

Frequency reconfiguration time		
Antena	Front end	
-	Programming and calibration	Physical change
53 us	1,83 ms	12 ns

3.5. Bit Error Rate / Packet Error Rate performance curves

In order to evaluate the performance of the receiver, Packet Error Rate (PER) and Bit Error Rate (BER) parameters have been measured over a range of SNR values. A channel emulator has been used for this purpose, which tracks the transmitted power and adds noise to the signal based on its bandwidth. 32 Byte data frames have been used for these tests.

The PER performance for an additive white Gaussian noise (AWGN) channel over an SNR range is shown in Figure 5 while the Bit Error Rate is depicted in Figure 6. Notice how the PER value of 0.01 is obtained when the SNR value is 16 dB.

3.6. FPGA resource utilization

Table 4 shows the FPGA resource utilization of the system. Assuming the number of SLICES as the most representative value of the design's size, each of the nodes in the Ethernet-to-RF bridge occupies slightly more than half of the

Table 4: FPGA resource utilization of the system

FPGA resource utilization					
	SLICES	LUT	Flip-Flop	BRAM	DSP48
Ethernet IP	394	866	790	2	0
QPSK Modulator	554	250	1197	4	168
QPSK Demodulator	9496	29579	14840	12	265
DSA algorithm	491	1506	2276	3	34
MicroBlaze	11321	24551	22800	78	19
TOTAL	23551	60258	43035	104	504

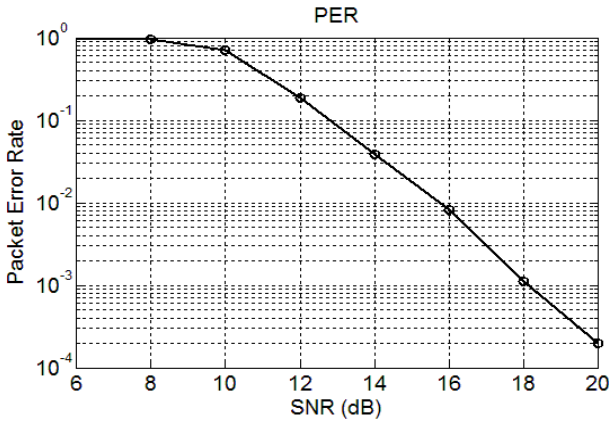


Figure 5: AWGN Packet Error Rate

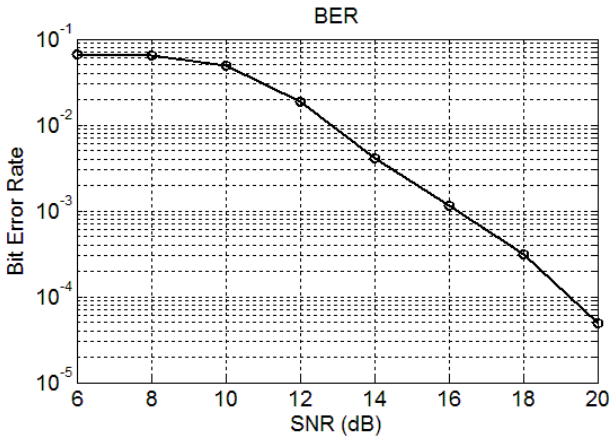


Figure 6: AWGN Bit Error Rate

XC6VLX240T Virtex 6 FPGA (37680 SLICES). With regards to the DSA algorithm, it occupies less than 500 SLICES, which means that an efficient tool for avoiding interferences and obtaining reliable communications is achieved at a very low cost.

As expected, due to the complexity of the new signal processing algorithms, the receiver is the most resource-hungry block of the system, with the exception of the MicroBlaze processor. This soft processor is only used in this application in order to control the configurable front-end and to execute some minor control tasks. However, it has enough processing power so as to implement more complex functions that justify its resource utilization (e.g. a Media Access Control (MAC) for multi-point wireless networks).

4. CONCLUSIONS

An RF-to-Ethernet bridge for control applications has been presented in this article. This bridge achieves a 12.8 Mbps half-duplex communication, and implements a Dynamic Spectrum Access algorithm that ensures that the over-the-air transmission takes place in an interference-free frequency. This way, the communication achieves the reliability needed by control applications. The system is based on FPGAs, with the data-processing algorithms implemented using Xilinx's System Generator rapid prototyping tool. Moreover, in order to achieve frequency reconfiguration, a commercial RF front-end and a custom designed reconfigurable antenna have been integrated into the system.

ACKNOWLEDGMENT

This work has been partly supported by the MOVITIC project from the ETORTEK framework program of the Basque Government (Spain) for Strategic Research Projects. The authors would like to acknowledge the invaluable contribution of Iñaki Iparragirre on FPGA implementation.

REFERENCES

[1] Torrego, R., Val, I., Muxika, E.: 'Small form factor Cognitive Radio implemented via FPGA partial reconfiguration replacing a wired video transmission systems'. Proc. Wireless Innovation Forum Conference on Communications Technologies and Software Defined Radio (SDR-WInnComm'12) , Washington (US), Year 2012

[2] Casado, F., Torrego, R., Arriola, A., Val, I.: 'Fully reconfigurable FPGA-based cognitive radio platform for reliable communications'. Proc. Wireless Innovation Forum European Conference on Communication Technologies and Software Defined Radio (SDR'13 – WInnComm – Europe), Munich (Germany), Year 2013

[3] Turunen, V., Kosunen, M., Kallioinen, S., Pärssinen, A. and Ryynänen, J.: 'Spectrum sensor hardware implementation based on cyclostationary feature detector'. Majlesi Journal of Electrical Engineering, 2011, 5(1).

[4] N. Vo, T. Le-Ngoc: 'Maximum Likelihood (ML) Symbol Timing Recovery (STR) Techniques for Reconfigurable PAM and QAM Modems'. Wireless Personal Communications, vol. 41, pp. 379-391, 2007.

[5] Luise, M.; Reggiannini, R.: 'Carrier frequency recovery in all-digital modems for burst-mode transmissions' Communications, IEEE Transactions on , vol.43, no.2/3/4, pp.1169,1178, Feb./March/April 1995

[6] Meyr, H., Moeneclaey, M., Fechtel, S.A.: 'Digital Communication Receivers, Synchronization, Channel Estimation, and Signal Processing'. John Wiley & Sons, Inc., New York, NY, USA. 1997. Chapter 8.4.3

[7] Akerberg, J.; Gidlund, M.; Bjorkman, M., 'Future research challenges in wireless sensor and actuator networks targeting industrial automation' Industrial Informatics (INDIN), 2011 9th IEEE International Conference on , vol., no., pp.410,415, 26-29 July 2011

ENERGY OPTIMIZATION USING MSK MODULATION TECHNIQUE IN WIRELESS SENSOR NETWORK

Rajoua Anane[1,2], Mehdi Bouallegue[1,3] ([1]Laboratory of Acoustics at University of Maine, LAUM UMR CNRS n° 6613, France, [2]Innovation of Communicant and Cooperative mobiles Laboratory Innov'COM, Tunisia, [3]System of Communication Laboratory , 6'com, ENIT , Tunisia) ; Ridha Bouallegue (Innovation of communicant and cooperative mobiles Laboratory Innov'COM, Tunisia); Kosai Raoof (Laboratory of Acoustics at University of Maine, Le Mans, France)

ABSTRACT

As wireless sensor networks use battery-operated nodes, energy efficiency is a very important metric. In this context, optimally selected modulation is an extremely vital technique in wireless sensor networks. This paper presents a comparative analysis of different modulation techniques in order to find the best modulation strategy to minimize the total energy consumption. The digital modulation schemes that we have studied and compared on the basis of total energy consumption are M-ary Quadrature amplitude modulation (MQAM), M-ary Frequency-shift keying (MFSK), M-ary Phase-shift keying (MPSK) and minimum-shift keying (MSK). Simulation results are presented to illustrate the performance of MSK modulation technique compared to its counterparts in Additive White Gaussian Noise (AWGN) channel conditions.

We confirm, through mathematical formulation and simulation that energy consumption per information bit can be improved by optimizing constellation size and transmission time at a specific distance.

1. INTRODUCTION

In battery-operated devices, power consumption is a critical design aspect. Indeed, a Wireless Sensor Network (WSN) consists of a large number of sensor nodes with limited energy resources and can be operated over an extensive set of applications such as military surveillance, structural health monitoring, and environmental monitoring. Therefore, energy efficiency is the primary objective to increase the lifetime of sensor networks.

Over the last few years, many efforts have been taken to improve the energy efficiency of sensor networks by optimizing physical layer parameters.

The modulation technique played an important role to decrease energy consumption and increase bandwidth efficiency of WSN.

Our main objective is to derive the optimal modulation technique and the optimum parameters that achieve minimum energy consumption for a given distance between sensor nodes.

The contribution of this paper is the comparative analysis of four types of modulation namely MQAM, MPSK and MFSK. The performance of MSK modulation is analyzed and compared with the other modulation to improve the energy efficiency and bandwidth efficient in a wireless sensor network.

The remainder of this paper is organized as follows: Section II presents the preliminary assumptions and system parameters. Section III describes the constraint analysis. Section IV provides a detailed analysis of different modulation techniques. In section V comparison results is discussed. Finally, section VI concludes the paper.

2. PRELIMINARY ASSUMPTIONS AND SYSTEM PARAMETERS

2.1. Scenario

Suppose that a source node S_1 send L bits of data to a destination node S_2 in a deadline T seconds.

The communication link between two sensor nodes will be modeled by an additive white Gaussian noise (AWGN) channel.

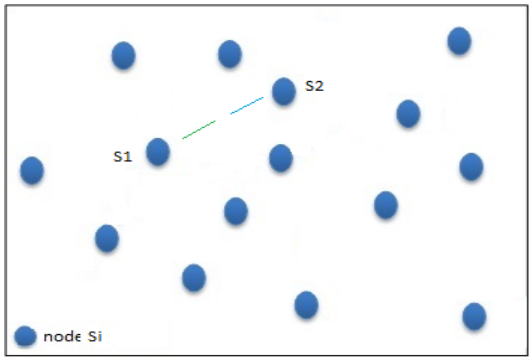


Fig. 1. An example of wireless sensor networks

2.2. Transceiver Model

In this paper, we adopt the transmitter and receiver hardware model as introduced in [1].

The transmitter block is composed of a digital to analog converter (DAC), a filter, a frequency synthesizer, a mixer and a power amplifier (PA).

At the receiver side, a filter, a Low noise amplifier (LNA), frequency synthesizer, a mixer, an intermediate frequency amplifier (IFA) and an analog to digital converter (ADC) are implemented.

The energy consumed by both the transmitter and the receiver blocks will be evaluated for calculating the total energy consumption in the network. We assume that powers consumption of filter at the transmitter blocks and receiver blocks are the same.

Case of frequency modulation schemes (MFSK and MSK), power consumption of both the DAC and the mixer will not be included in the calculation of the total power consumption [1].

2.3 Preliminary assumptions

It's assumed that transceiver circuit of a sensor works according to three modes [2][3]:

- When there is data to transmit the sensor operates in the active mode so all these circuits are active.
- If there is no information to send the circuits switch to standby mode. This contributes to energy saving and power consumption is negligible.
- Knowing that switching from standby mode to active mode, the energy overhead caused by start-up transients is also significant and must be taken into account. This temporary state called transient mode which is used to set up the frequency synthesizer of the local oscillator.

To sum up, the energy consumed during the transient mode is considered constant for a specific hardware but in a sleep state we can assume that it is equal to zero. In this paper we emphasis our analysis on minimizing the active mode power consumption.

According to the above assumptions, the transmission period T is given by:

$$T = T_{start} + T_{on\_time} + T_{stby} \tag{1}$$

Where:

- T_{start} is the time of the transient mode.
- $T_{on\text{-}time}$ represents the time spent to transmit L bits.
- T_{stby} is the duration of the standby mode.

Powers consumption associated to the described modes are denoted as:

- P_{start}: Power consumed for mode changing.
- $P_{on\text{-}time}$: Power consumed for transition
- P_{stby}: Power consumed during standby mode (assumed to be null for simplification)
- P_x is the power consumption of device x.

Expressing each term:

$$P_{tx\_cc} = P_{DAC} + P_{filt} + P_{mixer} + P_{syn} \tag{3}$$

$$P_{rx-cc} = P_{ADC} + P_{filt} + P_{mixer} + P_{syn} + P_{LNA} + P_{IFA} \tag{4}$$

The power of the amplifier is expressed as:

$$P_{PA} = \left(\frac{\xi}{\eta} - 1\right) P_{tx} \tag{5}$$

Where:

- η represents the drain efficiency of the amplifier.
- ξ is the peak to average ratio that depends on the modulation technique and is expressed as a function of constellation size M as [4]: $\xi = 3\left(\sqrt{M}-1 \,/\, \sqrt{M}+1\right)$

$\xi = 1$ for frequency modulations i.e. MFSK, MSK.

The total energy consumed is expressed as:

$$E_{total} = \left(1 + \left(\frac{\xi}{\eta} - 1\right)\right) P_{tx}\ T_{on-time} + \left(P_{components}\right) T_{on-time} + 2\, P_{syn}\, T_{start} \tag{6}$$

Where:

$$P_{components} = P_{tx-cc} + P_{rx-cc}$$

3. CONSTRAINT ANALYSIS

The major constraints to minimize the total energy consumption are the delay constraint and the peak-power constraint. So the energy constrained modulation can be modeled as:

$$\begin{aligned} &0 \le T_{on-time} \le T - T_{strat} \\ &0 \le \left(1 + \left(\frac{\xi}{\eta} - 1\right)\right) P_{tx} + P_{tx-cc} \le P_{\max-tx} \\ &0 \le P_{rx-cc} \le P_{\max-rx} \end{aligned} \tag{7}$$

Where:

- $P_{max\text{-}tx}$ represents the maximum power available at the transmitter
- $P_{max\text{-}rx}$ represents the maximum power available at the receiver

4. PERFORMANCE ANALYSIS OF MODULATION SCHEMES

In this section a communication link connecting two wireless sensor nodes is considered. Simulations shown below are performed with MATLAB.

4.1 M-ary Quadrature Amplitude Modulation

For M-ary QAM, we define $M=2^b$ where b is the number of bit per symbol. A sensor node must transmit L bits within a period $T_{on\text{-}time}$.

On the one hand we define the number of transmitted symbols by: $L_s = L/b$.

On the other hand, $L_s = T_{on\text{-}time} / T_S$ where T_S is symbol duration.

Therefore,

$$b = L\,T_s / T_{on-time} \tag{8}$$

Let us assume that, square pulses are used for all modulation techniques.

The channel bandwidth B equals $1/T_s$. Thus, the number of bits per symbol can be expressed by:

$$b = \frac{L}{BT_{on-time}} \tag{9}$$

With the data rate R_b and the channel bandwidth B, we may express the bandwidth efficiency, as:

$$\rho = \frac{R_b}{B} = \frac{b/T_s}{B} \tag{10}$$

Using (8) and (10) we deduce that: $\rho \approx b$

The error probability evaluated in the case of AWGN channel is expressed in terms of average value of the transmitted energy [4] as:

$$P_e \approx 2\left(1-\frac{1}{\sqrt{M}}\right) erfc\left(\sqrt{3SNR/2(M-1)}\right) \tag{11}$$

SNR is the signal-to-noise ratio equal to Eb/N0. The function erfc(.) denotes the complementary error function; The error probability could be also expressed as:

$$P_e \approx \frac{4}{b}\left(1-\frac{1}{\sqrt{M}}\right) e^{\left(-\frac{3}{M-1}\right)\frac{SNR}{2}} \tag{12}$$

The signal to noise ratio is approximated by:

$$SNR = P_{rx} / (2B\,N_f\,\sigma^2) \tag{13}$$

Where:

- P_{rx} is the received power.
- N_f is the receiver noise figure.
- σ^2 is the AWGN power spectral density

Hence, the received signal power can be written as:

$$P_{rx} = \frac{4}{3} B\,\sigma^2\,N_f\,(M-1)\ln\left(4\left(1-\frac{1}{\sqrt{M}}\right) \Big/ b\,P_e\right) \tag{14}$$

The power of the signal in the output of the transmitter is calculated by the equation of K^{th} path loss model [6]. We can state that:

$$P_{tx} = P_{rx}\,G_d \tag{15}$$

Or, $G_d = G_1 d^k M_1$ represents the power gain factor, G_1 is the gain factor at 1m, M_1 is the link margin and d (meters) is the distance that separate two communicating nodes . The exponent order k is between 2 and 4, in this paper $k= 3$ is selected.

The transmission energy is given by:

$$E_{tx-MQAM} = P_{tx}\,T_{on-time} = \frac{4}{3} N_f\,\sigma^2\,(M-1)\ln\left(\frac{4-4/\sqrt{M}}{b\,P_e}\right) T_{on-time} G_d\,B \tag{16}$$

Using (6) and (15), the expression of total energy consumption is:

$$E_{MQAM\_tot} = \frac{4}{3}\left(1+\left(\frac{\xi}{\eta}-1\right)\right) N_f\,\sigma^2\,(M-1)\ln\left(\frac{4-4/\sqrt{M}}{b\,P_e}\right) G_d\,B\,T_{on-time} + P_{components}\,T_{on-time} + 2\,P_{syn}\,T_{start} \tag{17}$$

The energy consumption per information bit is calculated as follows:

$$E_{\inf bit} = E_{total} / L$$

$$E_{MQAM\_\inf Bitt} = \frac{4}{3}\left(1+\left(\frac{\xi}{\eta}-1\right)\right) N_f\,\sigma^2\,(M-1)\ln\left(\frac{4-4/\sqrt{M}}{b\,P_e}\right) G_d\,B\,T_{on-time} \Big/ L + \frac{P_{components}\,T_{on-time} + 2\,P_{syn}\,T_{start}}{L} \tag{18}$$

Derived relationships between energy consumption and transmit-on time ($T_{on\text{-}time}$) are simulated and shown in Fig.2.The vertical axis presents the energy in terms of decibels relative to a 10^{-3}joule : $10log_{10}\ (E_{infbit}\ 10^3)$ *dB mjoule*, and the horizontal axis is the normalized transmission time ($T_{on\text{-}time}/T$).

The setting data used in simulation are tabulated in Table I [5].

Parameters	Values
T_{start}	5 10^{-6} s
T	0.1 s
L	10^3 bit
σ^2	$3.981.10^{-21}$
k	3
η	0.35 for MQAM/MPSK, 0.75 for MFSK /MSK
B	10^4 Hz
Carrier frequency	2.45 GHz
P_e	10^{-3}
G_1	10^3
M_t	10^4
P_{ADC}	6.70 mw
P_{DAC}	15.40 mw
P_{filt}	2.5 mw
P_{syn}	50 mw
P_{LNA}	20 mw
P_{IFA}	3 mw
P_{mixer}	30.3 mw
N_f	10 dB

Table I. *Simulation parameters*

The variation of optimum transmit-on-time for different values of transmission distance is shown in Fig.2.

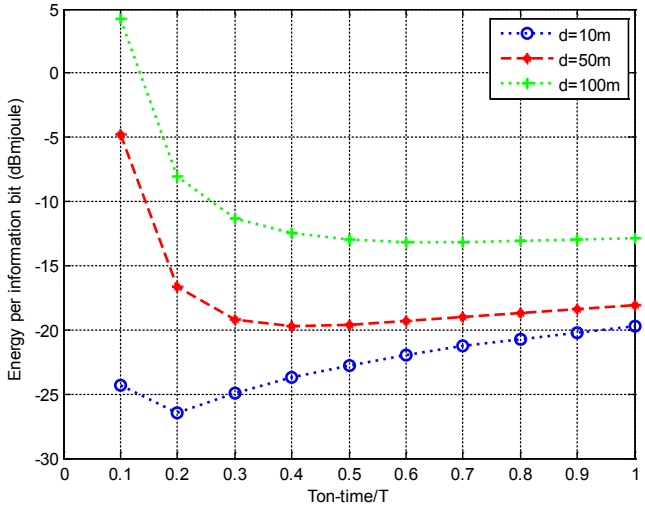


Fig. 2. Total energy consumption per bit information as a function of transmission time, (AWGN)

These curves were plotted for $0<T_{on\text{-}time}<1$ which corresponds to constellation size between 2 and 16. We can see that there are a large number of changes in the variable $T_{on\text{-}time}$ for long distance as compared to short distance and that the total energy consumption is not a monotonically decreasing function. For fixed B and L we can deduce an optimum $T_{on\text{-}time}$ for AWGN channel using this simulation. Indeed for d= 10m and at the optimal case when $T_{on\text{-}time} < T\text{-}T_{start}$ ($T_{on\text{-}time} \approx 0.2T$) the total energy consumption per information bit is about 7 dB lower than the case where $T_{on\text{-}time} \approx T$. At d = 50m we notice also about 2 dB energy saving under optimized case.

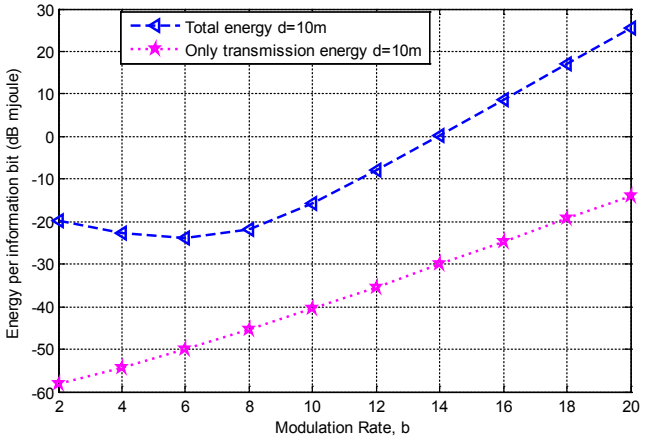


Fig. 3. Energy per information bit as a function of modulatio rate, for MQAM (AWGN)

Energy consumption per information bit $E_{infbit\text{-}MQAM}$ and transmission Energy $E_{tx\text{-}MQAM}$ are drown over modulation rate b for d=10m in Fig.3.

We can note that when we consider the total energy consumption the optimal number of bit per symbol b_{opt} = 6 and when only transmission energy is taken into account b_{opt}= 2.

4.2 M-ary Phase-shift keying (MPSK)

The bit per symboll b for MPSK modulation scheme depends on the time spent to transmit L bits $T_{on\text{-}time}$ as defined for MQAM modulation.

Let us assume that MPSK uses the same hardware configuration as the one used for MQAM.

The bit error probability for AWGN channel is expressed as follows [4]:

$$P_e \approx erfc\left(\sqrt{SNR}\,\sin(\pi/2M)\right) \tag{19}$$

Using equations (6), (9), (13), (15) and (19), the total energy consumption is derived as:

$$E_{MPSK\_tot} = 2\left(1+\left(\frac{\xi}{\eta}-1\right)\right)N_f\sigma^2\left(\ln\left(\frac{2}{bP_e}\right)\Big/\left(\sin\frac{\pi}{M}\right)^2\right)G_d B T_{on-time} + P_{components}T_{on-time} + 2P_{syn}T_{start} \tag{20}$$

We deduce the total energy consumption per information bit:

$$E_{MPSK\_\inf Bit} = 2\left(1+\left(\frac{\xi}{\eta}-1\right)\right)N_f\sigma^2\left(\ln\left(\frac{2}{bP_e}\right)\Big/\left(\sin\frac{\pi}{M}\right)^2\right)BG_d T_{on-time}/L + \frac{P_{components}T_{on-time}+2P_{syn}T_{start}}{L} \quad (21)$$

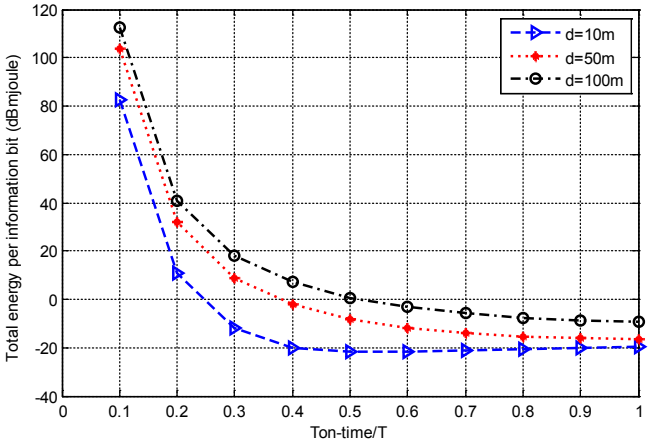


Fig. 4. Energy per information bit versus normalized transmission time for MPSK (AWGN)

The total energy consumption as a function of $T_{on\text{-}time}$.for transmission distances d=10, 50 and 100m are shown in Fig.4. The numerical values considered for these curves are the same as those used for MQAM technique.

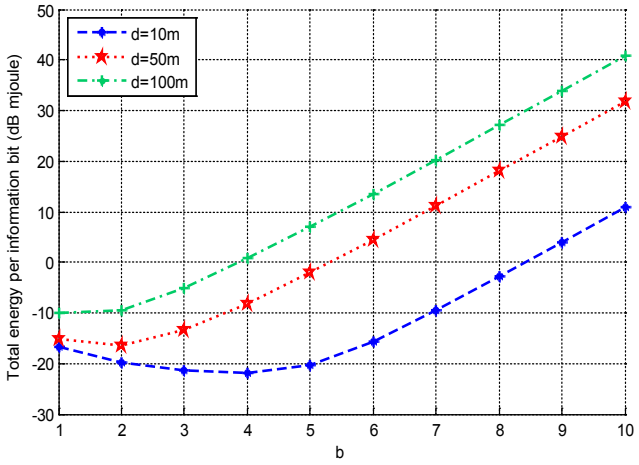


Fig. 5. Energy per information bit versus modulation rate, MPSK (AWGN)

From Fig.5, we deduce that the optimum modulation rate b for the difference distance: d=10, 50, 100m are respectively equal to 7, 4.7 and 2.

4.3 M-ary Multiple frequency-shift keying (MFSK)

Remember that, for MFSK we must eliminate the two components noted earlier, the DAC and the mixer of the hardware configuration since FSK can be implemented by a simple direct modulation. In this section analysis is done for non-coherent MFSK [5].

Let us assume that signals are orthogonal and the adjacent signals are separated by *1/2Ts*.
The bandwidth channel is defined as: $B=M/2Ts$.
Therefore, $B= R_bM/2log_2M$. .

Using the previous equation and (10) we can derive bandwidth efficiency expression as:

$$\rho = \frac{2\log_2 M}{M} = \frac{2b}{2^b} \quad (22)$$

The bit per symbol of MFSK modulation can be related to the transmit on-time as following:

$$\frac{2b}{2^b} = \frac{L}{BT_{on-time}} \quad (23)$$

The probability of error for no-coherent MFSK detection is expressed as [4]:

$$P_e \le \frac{(M-1)}{2} erfc\left(\sqrt{SNR}\right) \quad (24)$$

Hence,

$$P_e \le 2^{b-2} e^{-SNR/2} \quad (25)$$

We can deduce that:

$$\gamma = 2\ln\left(\frac{2^{b-2}}{P_e}\right) \quad (26)$$

On the other hand we find that [4_]:

$$\gamma = bE_{rxb}/2\sigma^2 N_f \quad (27)$$

Where E_{rxb} represents the energy per information bit at the receiver:

$$E_{rxb} = \left(P_{rx}T_{on-time}\right)/L \quad (28)$$

We deduce the received signal power as follows from (25-28):

$$P_{rx} = 4N_f\sigma^2\ln\left(2^{b-2}/P_e\right)\frac{2B}{M} \quad (29)$$

Knowing that $P_{tx}= P_{rx}G_d$ and $E_{tx}= P_{tx}T_{on\text{-}time}$
We obtain:

$$E_{tx-MFSK} = 4N_f\sigma^2\ln\left(2^{b-2}/P_e\right)G_d L/b \quad (30)$$

Then the total energy is:

$$E_{MFSK\_tot} = 4\left(1+\left(\frac{\xi}{\eta}-1\right)\right)N_f\sigma^2\ln\left(2^{b-2}/P_e\right)G_d L/b + P_{components}T_{on-time}+2P_{syn}T_{start} \quad (31)$$

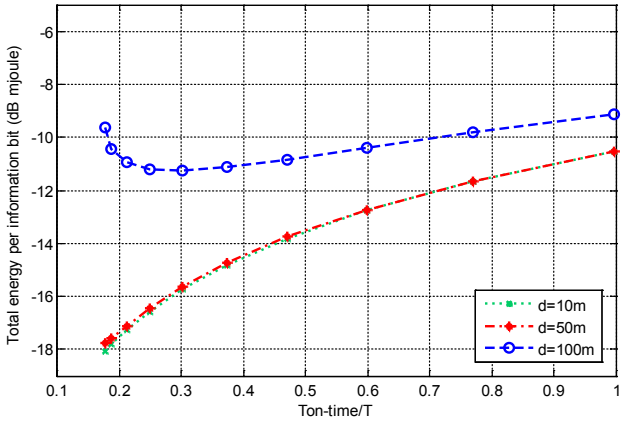


Fig. 6. Energy per information bit versus normalized transmission time, (AWGN)

In these simulations, we use the same values for the bandwidth B and the packet size L and we change the value of drain efficiency to 0.75 and that of transmission period T to 1.10s. In fact, MFSK modulation needs a longer transmission time to send L bits due to its lower bandwidth efficient comparing to MQAM and MPSK modulations. Fig.6 shows that the total energy is an increasing function of $T_{on\text{-}time}$ for short distance and under optimized case ($T_{on\text{-}time} \approx 0.18T$) we observe about 7dB energy savings compared to the case where ($T_{on\text{-}time}=T$).

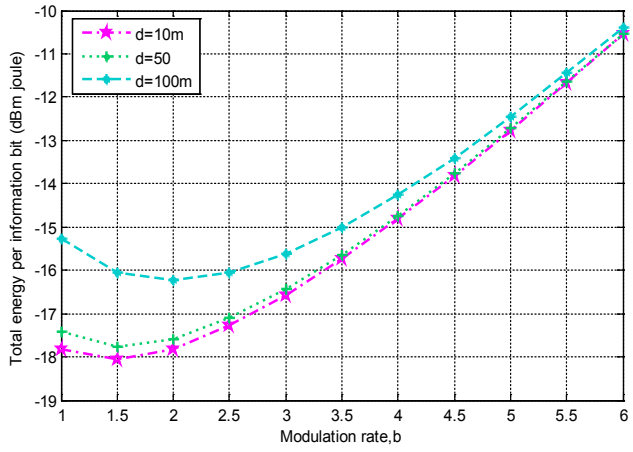


Fig. 7. Energy per infirmation bit versus Modulation rate,(AWGN)

Curves plotted in Fig.7 represent the total energy as a function of modulation rate. Based on the total energy measurements, the optimal value of b is 1.5 for d=10m, d=50m and 2 for d=100m. Approximately 7.5 dB energy savings is achieved by using optimal $b_{opt}=1.5$ compared with the non-optimized case where $T_{on\text{-}time}=T$ ($b=6$).

4.4 Minimum-shift keying (MSK)

MSK can be viewed as a special form of continuous phase-frequency shift keying, (CPFSK) where the deviation index is precisely equal to ½. A modulation index of 0.5 corresponds to the minimum frequency spacing that allows two FSK signals to be coherently orthogonal.

Where we consider the same configuration as that used for MFSK modulation. The frequency difference is equal to $1/2T_s$.

A bound on the probability of error for MSK is written as [4]:

$$P_e \approx \frac{1}{2} erfc\left(\sqrt{SNR}\right) \tag{32}$$

Therefore, we can deduce:

$$P_e \approx e^{-SNR} \tag{33}$$

Next the energy per information bit at the receiver is:

$$E_{rxb} = N_0 N_f SNR \approx 2\sigma^2 N_0 N_f \ln\left(1/P_e\right) \tag{34}$$

By following the same process used for previous modulations:

$$P_{tx} = \frac{E_{rxb}}{T_s} G_d = E_{rxb} G_d \frac{L}{T_{on-time}} \tag{35}$$

And,

$$E_{tx-MSK} = 2 N_0 N_f \sigma^2 \ln\left(1/P_e\right) G_d L \tag{36}$$

Energy consumption per information bit is written as:

$$E_{MSK\_\inf Bit} = 2\left(1+\left(\frac{\xi}{\eta}-1\right)\right) N_0 N_f \sigma^2 \ln\left(1/P_e\right) G_d + \frac{P_{components} T_{on-time}}{L} + \frac{2 P_{syn} T_{start}}{L} \tag{37}$$

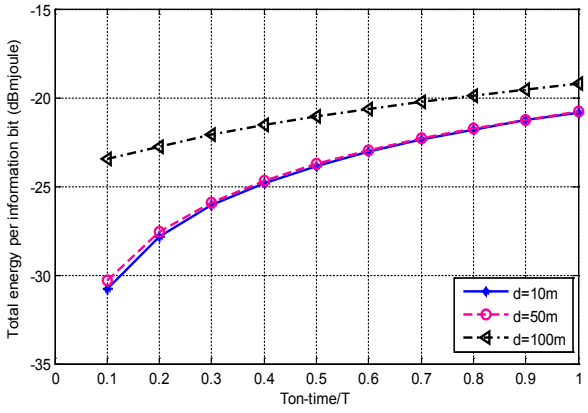


Fig. 8. Total energy per information bit ,MSK (AWGN)

The plot of total energy per information bit over normalized transmission time in the case of MSK technique is presented in Fig.8.

Not surprisingly, energy consumption is also an increasing function of transmit-on time and optimal $T_{on\text{-}time} = 0.1T$. Furthermore, in the optimal case, for d=10, 50 and 100m we respectively obtain about 10, 9.5 and 5.5 dB of energy savings compared to the non-optimized system ($T_{on\text{-}time} = T$).

5. COMPARATIVE RESULTS

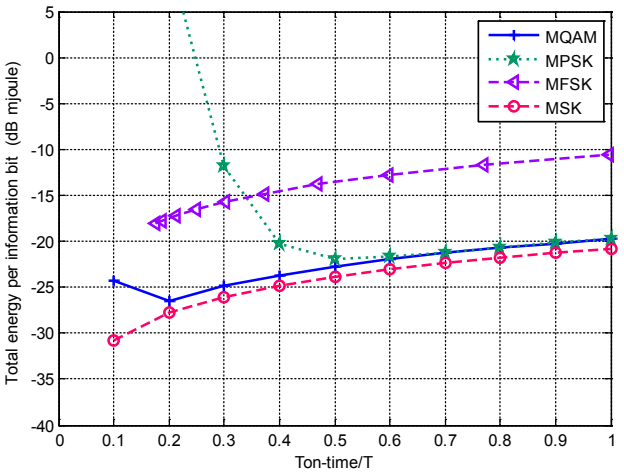


Fig. 9. Comparison of different modulation techniques for point-to-point communication, d=10m.

The total energy per information bit versus transmit-on time curves are shown in Fig 9. The simulations are presented in the case of four modulation techniques. We deduce that MSK permits for the best energy consumption comparing to the other modulation techniques.

Through this simulation, we observe about 4 dB energy savings compared to MQAM, 9 dB compared to MPSK and 12 dB compared to MFSK, during a point to point communication.

6. CONCLUSION

It has been shown that for transmitting a given number of bits in a node-to-node communication link, it is possible to minimize the total energy consumption by optimizing the constellation size and the transmission time under an operating range for the fourth modulations techniques.
Furthermore, the result shows fully open eyes that MSK modulation is more energy efficient comparing to the other modulation techniques. This modulation presents a constant envelope and a high bandwidth efficient. In the other hand, the MSK techniques can be viewed as a special form of frequency shift keying, where the deviation index is precisely equal to ½, so MSK can be simple to generate and simple to demodulate.

7. REFERENCES

[1] Mukesh .S. M. Iqbal, Z. Jianhua, Z. Ping, and Inam-Ur-Rehman, "Comparative analysis of M-ary modulation techniques for wireless adhoc Networks," in Proceedings of the IEEE 2007 Sensors Applications Symposium, 2007.

[2] G. Anastasi, M. Conti, M. Di Francesco and A. Passarella, "Energy conservation in wireless sensor networks: A survey," IEEE J. on Selected Areas in Comm., vol .7, no .3, pp. 537–568, 2009.

[3] Himanshu Sharma, Vibhav Kumar Sachan and Syed Akhtar Imam "Energy Efficiency of the IEEE 802.15.4 Standard in Wireless Sensor Networks :Modeling and Improvement Perspectives" InternationalJournal of Computer Applications (0975 – 8887) Volume 58– No.9, November 2012.

[4] J. G. Proakis, Digital Communications, 4th ed. New York: McGrawHill, 2000.

[5] Felipe M., Costa and Hideki Ochiai,,"A Comparison of Modulations for Energy Optimization in Wireless Sensor Network Links" in proceedings of the IEEE Globecom conference,2010.

[6] Theodore S. Rappaport , "Wireless Communications Principles and Practice" , second edition

A SDR Implementation of CoMP Transmission on GPP Platform

Bobo Cheng[1],Xiang Mi[1],Zhan Xu[4],Limin Xiao[2,3],Xibin Xu[2,3],Ming Zhao[2,3,*]
[1]Department of Electronic Engineering,Tsinghua University,Beijing 100084, P.R.China
[2] Tsinghua National Laboratory for Information Science and Technology,Beijing 100084, P.R.China
[3]Research Institute of Information Technology (RIIT),Tsinghua University,Beijing 100084,P.R.China
[4]School of Information and Communication Engineering,Beijing Information Science and Technology University,Beijing,China
Email:{cbb12,mix12}@mails.tsinghua.edu.cn,{zhaoming,xuxb,xuzhan}@tsinghua.edu.cn,xuxxmail@163.com

***Abstract*—CoMP (Coordinated Multiple Points) has been verified to be an effective way to improve the throughput of cell-edge users in LTE-Advanced. Due to high computational and intensive data exchange, Many CoMP systems are implemented on hardware platforms such as DSP, FPGA, etc. In this paper, We implemented a real-time downlink CoMP joint processing system on GPP platform based on TD-LTE R8/R9. We adopt socket connection as data exchange interface between soft CoMP base stations and optimized data exchange strategies to cut unnecessary data communication. To enable real-time processing, we accelerate our programs with some parallel processing techniques such as multi-threads,SIMD,etc. The test results show that the running time of our system can ensure real-time CoMP processing.**

***Keywords*—SDR;CoMP;GPP;SIMD**

I. Introduction

CoMP is a key technique in LTE-Advanced. In LTE system, adjacent cells can transmit data to users on the same frequency, this may bring some inter-cell co-channel interference to users, especially cell-edge users. To alleviate interference, CoMP is proposed in LTE-Advanced. With this technique, multi adjacent base stations can transmit data to the same cell-edge users and the inter-cell co-channel interference can be alleviated through CoMP precoding.

To implement downlink CoMP transmission, base stations should exchange some important data including user data and downlink CSI(Channel State Information). Base stations can calculate precoding matrices using CSI. This process needs much computation work. Due to high computational and intensive data exchange, Many CoMP systems are implemented on hardware platforms such as DSP, FPGA, etc. However, hardware platform is not flexible enough and it's difficult to be upgraded.

GPP platform is a common platform which is easy to migrate and upgrade. Due to its advantages, many SDR(Software Defined Radio)[1] programs are trying to implement communication system on GPP platform rather than conventional hardware platform. However, as mentioned before, Due to high computational and intensive data exchange, it's really a challenge to implement real-time CoMP processing on GPP platform. The good news is that the fast development of processor techniques has enhanced the computation ability of GPP greatly.

A lot of work has been done to exploit the feasibility of SDR on GPP platform. In[2], Sora, a fully programmable software radio platform on commodity PC architecture was proposed. In [3], Using Sora platform, authors gave a real-time software radio implementation of 2*2 MIMO system based on 802.11n. In [4], authors presented a SDR platform based on GPPs which is capable of running various wireless communication standards like Wireless LAN, LTE, WiMAX, etc. A novel GPP-based SDR architecture was proposed in [5]. It introduced PCI Express (PCI-E) bus and RTOS(Real-Time Operating System) to satisfy real-time processing requirement. In [6], authors compared several SDR platforms and proposed the general architecture of GPP-based soft base stations. Finally, the authors realized and verified a prototype of GPP-based soft base stations referring to LTE.

To the best of our knowledge, this is the first work that implements real-time downlink CoMP joint processing on GPP platform. We adopt PCI-E bus as the interface between hardware and GPP server to support high data transmission speed. Besides,we take advantage of multi-threads and SIMD techniques to achieve parallel processing and accelerate programs. Our implementation is based on TD-LTE R8/R9 and thus fully compatible with TD-LTE R8/R9 users.

The rest of this paper is organized as follows. Section I describes the CoMP architecture of our implementation.III presents our design in detail. This section includes three parts: hardware platform, soft base stations design and SIMD optimization. Some test results are shown in IV. V concludes this paper and lists some work to do in the future.

II. Architecture

As illustrated in Fig.1, There are three CoMP base stations and two CoMP users in our implementation scene. The time-frequency resources allocated to the two CoMP users are the same. The interference can be alleviated through CoMP precoding. The bandwidth of our system is 20MHz and We adopt downlink transmission mode7 defined in TD-LTE R8/R9. The uplink-downlink configuration is DSUUD DSUUD (D represents downlink subframe, S represents special subframe, U represents uplink subframe)[7].

Fig.2 presents the architecture of our soft base stations. There are three RRUs with 4 antennas. Each of them is connected to a FPGA board through an optical fiber. The FPGA board receives signals from CPRI interfaces and then

* Ming Zhao is corresponding author.

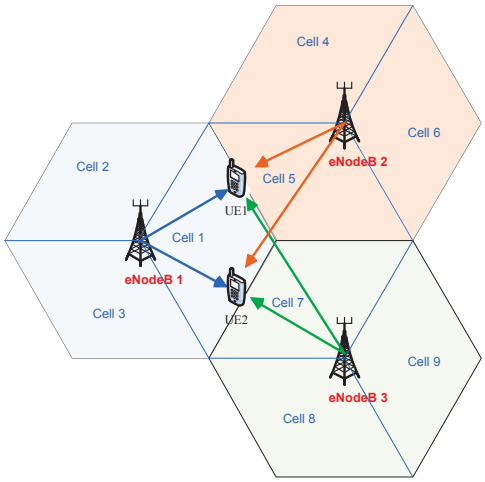


Fig. 1. Implementation scene

transmit data to GPP server through PCI-E interface. A GPS clock module is connected to the FPGA board, this module can provide precise clock and ensure timing synchronization of the whole system.

There are three soft base stations running on the GPP server and they are connected to the three different RRUs respectively. To be more scalable, every soft base station is an isolated process and can only receive user data from the corresponding RRU. So there should be some connections between these processes to support data exchange. We adopt socket connection because of its universality and scalability. There are some dedicated socket connections between every two processes.

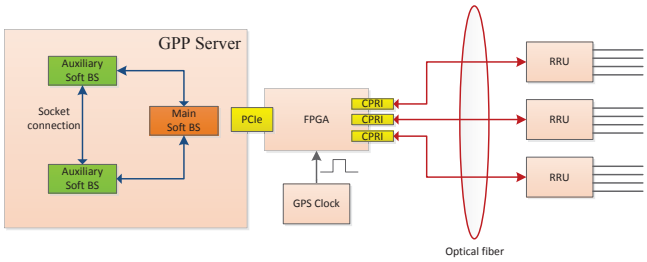


Fig. 2. Architecture of implementation

Among these three base stations, there is a main base station, others are called auxiliary base stations. The main base station is responsible for receiving CSI from others and calculating CoMP precoding matrices for all.

We adopt SRS feedback mechanism to get uplink CSI in our architecture, which has been agreed as one of three main CoMP feedback strategies in LTE-Advanced[8]. Because of the channel reciprocity of TD-LTE, these uplink CSI can be used to calculate downlink CoMP precoding matrices. Considering both the algorithm performance and computation complexity, MMSE is selected to be CoMP algorithm.

The design of socket connections, SRS and CoMP algorithm is explained in [9] in detail. This paper focuses on the design of FPGA board and soft base stations.

III. Design & Implementation

A. FPGA board

As illustrated in Fig.3, there are three CPRI interfaces and one PCI-E interface on the board. Between CPRI interfaces and FPGA memory, there is a module which can perform IFFT/FFT and CP addition/remove functionality. Besides, there is a timer counter on the board which can receive clock from the GPS clock module. The GPS clock module can provide a precise 10MHz clock and is used to enable synchronization of the whole system.

Through the PCI-E interface,FPGA board provides three APIs(Application Program Interface) to soft base stations: 1)Datawrite interface is used to transmit data from GPP server to FPGA board. 2)Dataread interface is used to read data from FPGA board memory.3)Timer interface is used to read the value of timer counter to get global synchronization information.

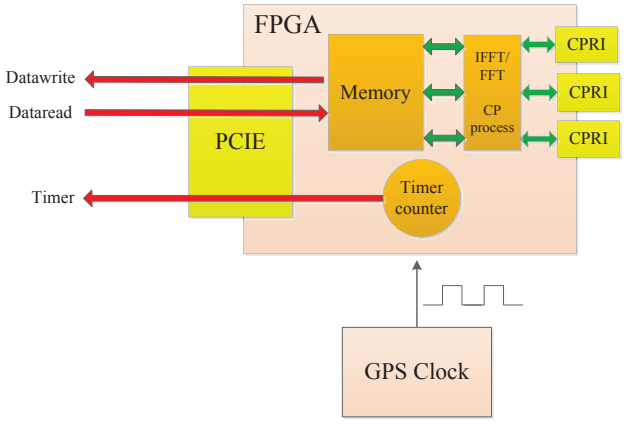


Fig. 3. Design of FPGA board

B. Design of Soft Base Stations

Fig.4 illustrates the architecture of soft base stations. There are three processes running on the GPP server. Two auxiliary processes refer to the two auxiliary soft base stations mentioned before and the main process refer to the main soft base station.

As for main base station, the data processing flow of uplink subframe is as follows: it firstly call the Dataread interface and get uplink digital baseband signals. If there are SRS signals in the last SC-FDMA symbol of current subframe, it transmits frequency-domain SRS signals to CSI estimation module. These signals are used to calculate uplink CSI and then these CSI is used to calculate precoding matrices together with the CSI of auxiliary base stations which are transmitted to main to base station through socket connections. When finish calculating all precoding matrices, main base station transmits corresponding precoding matrices back to auxiliary base stations.

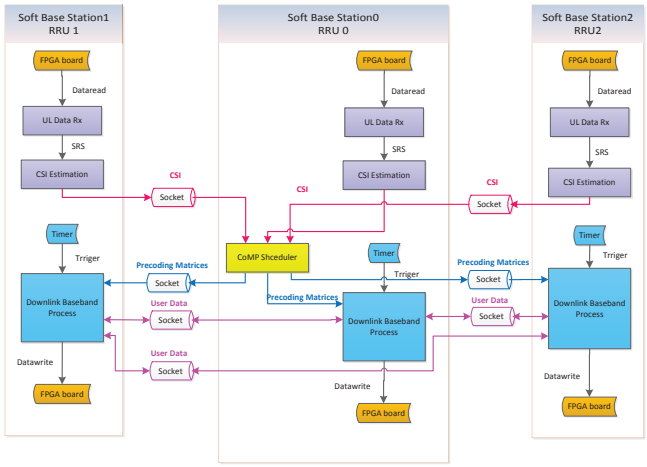


Fig. 4. Design of soft base stations

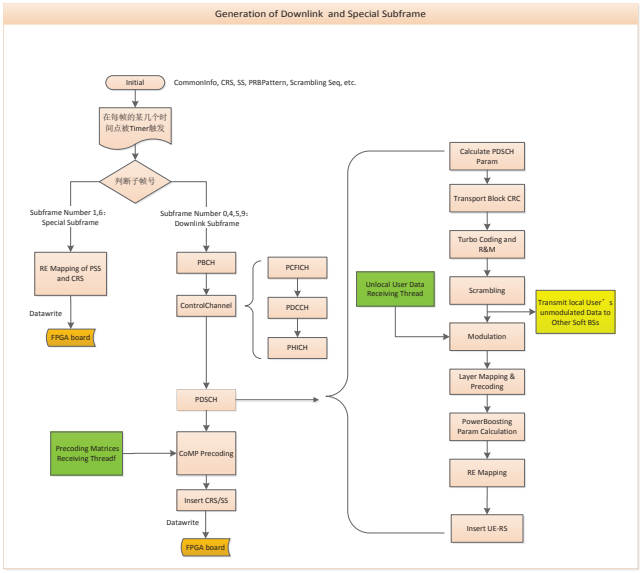


Fig. 5. Downlink data processing flow

The downlink subframe data processing flow of main base station is illustrated in Fig.5, when trigged by timer, it firstly judges subframe number. If current subframe is a special subframe, it calls corresponding module to generate special subframe. Otherwise, it generates downlink subframe as follows: First, it generates PBCH and all control channels(PDCCH, PHICH,PCFICH), then PDSCH. As mentioned before, there are three CoMP base stations and two CoMP users locating in different cells, so for a particular base station, there may exit one user or on users. If this cell has a user, during PDSCH generation procedure, soft base station firstly perform baseband processing to local user's data. Then at modulation step, it stops and waits for the unlocal user's data. Unmodulated data of the unlocal user will be transmitted to this base station together with its modulation scheme(This design is explained in [9] in detail). These data is modulated locally and then mapped to the RBs allocated together with local user's data. After that, these data is precoded using precoding matrices. Finally, the precoded data is transmitted to FPGA board by calling Datawrite interface. If there is no users locating in this cell, during the procedure of PDSCH, base station just waits for the unmodulated data of two unlocal users and then performs the following operations.

The data processing of auxiliary base station is almost the same with main base station. The only difference is that it should transmit CSI to main base stations and receive precoding matrices from it.

The above data processing flow of soft base stations is very complexity. To enable real-time processing, we adopt multi-threads technique to do some optimizations and improve processing efficiency. Take the main base station as an instance, the multi-threads design is illustrated in Fig.6. The functionality of each thread is explained as follows:

- Thread 1 is a socket receiving thread which receives user data from auxiliary base station 1.
- Thread 2 is also a socket receiving thread which receives user data from auxiliary base station 2.
- Thread 3 is a timer thread which can read timer counter value from FPGA board and get synchronization information. This thread can trigger thread 4 at appropriate time.
- Thread 4 is designed to generate downlink and special subframes. This thread is trigged by thread 3.
- Thread 5 is uplink data receiving thread. It can read uplink data from FPGA board and transmits SRS data to thread 6 to perform further operations.
- Thread 6 is SRS processing thread. It receives SRS data from thread 5 and estimates CSI. After that, it transmits CSI to CoMP scheduler to calculate precoding matrices.
- Thread 7 is a socket receiving thread which can receive CSI from auxiliary base station 1 and transmit it to CoMP scheduler.
- Thread 8 is also a socket receiving thread which can receive CSI from auxiliary base station 2 and transmit it to CoMP scheduler.

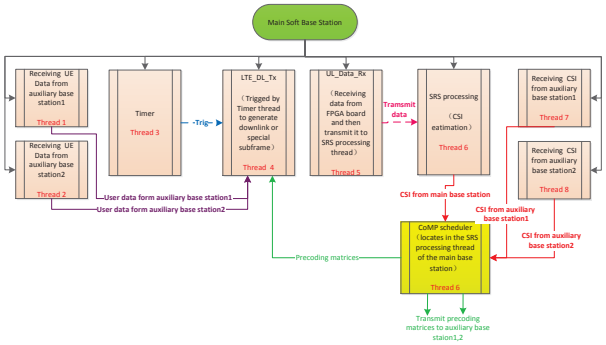


Fig. 6. Multi-threads design of main base station

What should be emphasised is that CoMP scheduler is not a dedicated thread. It is included by the SRS processing thread. If the precoding matrices haven't been updated timely, base stations directly precode user data with last preocidng matrices and don't need to wait for the latest.

Fig.7 shows the time sequence relationships of above threads. The generation of downlink subframe and special subframe starts 1ms earlier than the beginning of corresponding subframe. The generation is finished in 1ms and when it comes to the beginning of this subframe, prepared data is transmitted to RRU. In the uplink direction, data receiving thread calls Dataread interface to read the uplink subframe data from FPGA board and if there are SRS signals in current subframe, it transmits these data to SRS processing thread and trig it.

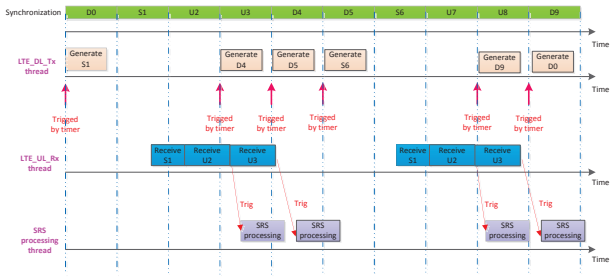


Fig. 7. Time sequence figure

C. SIMD Optimization

According to the time sequence relationships above. The generation of one downlink subframe or special subframe should be finished in 1 ms. To satisfy this requirement, we adopt SSE instructions to optimize soft base stations and accelerate programs.

SSE instructions set is first proposed in Pentium processor to support parallel processing of four 32-bit single-precision floating-point computations. It has 8 128-bit registers named XMM0,XMM1,...,XMM2. Fig.8 shows the parallel addition operation using SSE.

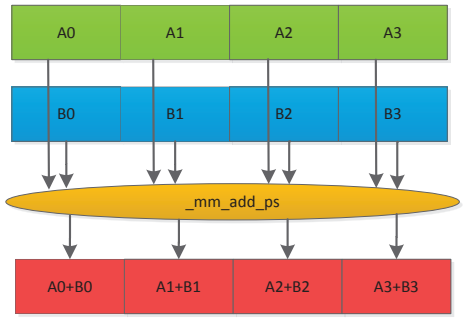


Fig. 8. Implementation scene

Besides parallel processing of four single-precision floating-point computations, SSE instructions also support parallel processing of eight 16-bit integer computations or two 64-bit double-precision floating-point computations due to its 128-bit registers.

SSE instructions can improve computation efficiency of soft base station greatly. We used it to optimize many modules including FFT/IFFT module, precoding matrices calculating module, CSI estimating module, etc. To further improve processing efficiency, We use AVX instructions to optimize CoMP precoding module. The principle of AVX instructions is almost the same with SSE. The difference is that the length of its registers is 256-bit and it can support a higher degree of parallel processing.

IV. Test Results

In our implementation, Three soft base stations run on the same GPP server, the performance parameters of which are listed in TABLE.I:

TABLE I: Server parameters

CPU Type	1*Intel(R) Core(TM) i7-2600
CPU Frequency	3.40GHz
Muti Threads per CPU	4 cores and 8 threads
Memory	4G DDR3
OS	Linux kernel 3.5.5

1) Socket Delay Test: Socket connections are adopted to support data exchange between soft base stations. Data need to be exchanged includes user data, CSI and precoding matrices. We did some experiments to test socket transmission delay. The data amount of socket transmission every time in our experiment is listed in TABLE.II. The system bandwidth is 20MHz and there are 1200 subcarriers in total. As for CSI, channel estimation result of every subcarrier is a complex number, the real and image part of wihch are both 32-bit single-precision floating-point type. So there are at most 2*1200 32-bit single-precision floating-point numbers to be transmitted at a time. For precoding matrices, because there is 4 antennas per RRU and 2 CoMP users, a 2*4 complex matrix including 2*4*2 32-bit single-precision floating-point numbers needs to be transmitted per subcarrier for every auxiliary base station. So there are at most 2*4*2*1200 32-bit single-precision floating-point numbers to be transmitted in total at a time. For user data, socket transmits unmodulated data. We set the amount to be 300*14 bytes per subframe(This result is based on the assume that user adopts QPSK modulation and occupy all RBs,14 is the number of OFDM symbols per subframe).

TABLE II: Data amount of socket transmission

Data type	Subcarriers number	Data amount per subcarrier(bytes)	Data amount in total(bytes)
CSI	1200	8	9600
User data	1200	-	4200
Precoding Matrices	1200	64	76800

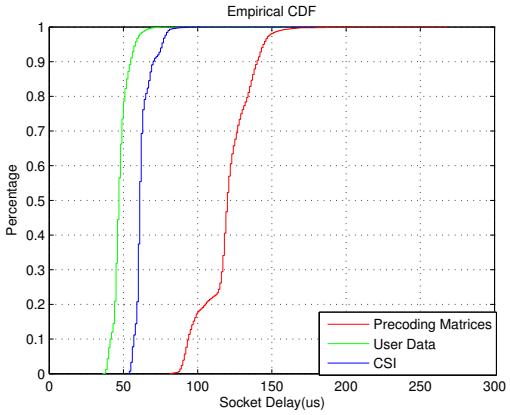


Fig. 9. CDF of socket transmission delay

Fig.9 is CDF of socket transmission delay. We did 100000 experiments to get this distribution result. We can see from the figure that at most situations, user data transmission delay is less than 70us, CSI transmission is less than 90us and precoding matrices delay is less than 170us. The amount of data to be transmitted lead to this difference.

According to SRS design in[9], CSI is transmitted at the last symbol subframe 2,3,7,8(uplink subframe). As for precoding matrices,it should also be updated 4 times every radio frame. The transmission delay of CSI and precoding matrices is acceptable because it can support timely update 4 times every radio frame. Furthermore, as mentioned before, if precoding matrices haven't been updated timely, CoMP base stations directly precode user data with last precoding matrices and don't need to wait for the update. So even if CSI and precoding matrices transmission delay exceeds threshold at particular situations, it doesn't lead to a time-out problem. For user data, it is transmitted every downlink subframe. The generation of one downlink subframe must be finished in 1ms to enable real-time processing and we can consider that 70us delay is acceptable because it occupies less than 10 percentage of 1ms.

2) Real-time test: There are two key parts in our system. The first is CSI estimation and calculating precoding matrices, the second is generating downlink subframes.

For the first part, As explained in [9], we set the subcarrier Reuse Factor to be 2, which means that for every two subcarriers, base stations only estimate CSI and calculating precoding matrix for one and these two subcarrier use the same precoding matrix. This strategy can cut computation amount, in addition, it can also cut the amount of data need to be exchanged through socket connections. TABLE.III shows the average running time of CSI estimation and calculating precoding matrices one times.

TABLE III: Time of CSI estimation and calculating precoding matrices

subcarrier Reuse Factor	CSI estimation(us)	Calculating precoding matrices(us)
2	19	820

To test the real-time generation capability of downlink subframe, we design some test cases with different configurations and throughputs. Table.IV lists the configurations and throughputs of four typical test cases.

TABLE IV: Test cases

Case number	Modulation	Number of PRBs	TB Size	Throughput per CoMP user(M bits/s)
1	QPSK	16	2536	1.0144
2	16QAM	32	5736	2.2944
3	16QAM	64	11448	4.5792
4	64QAM	32	16992	6.7968

TABLE.V shows the average running time under different cases, we test 100000 subframes to get these average results. In our test, the two CoMP users located in auxiliary base station 1 and 2, so there is no CoMP users in the main base station. For main base station, the procedure of PDSCH is just to wait for the unmodulated data of two CoMP users and perform the following operations. As for auxiliary base stations, they not only need to generate data of local user, but also need to wait for the other user's data.

In our system, special subframes only contain some CRS and synchronization signals. The total average generation time per special subframe is about 12-15us. As for downlink subframes, we can find that the average total generation time is all below 1ms under these four test cases. Comparing the running time of case 2 and case 4, we can find that the CoMP precoding time of these two cases is almost the same although the throughputs of them are different. This is mainly because the number of RBs allocated to users in these two cases are the same and this directly determines the computation amount of CoMP precoding. Another phenomenon we can find from the table is that the generation time of control channels in main base station is less than auxiliary base stations. This is because there is no local users in main base station and the generation of control channels can be simplified.

The PDSCH generation time distribution of auxiliary base stations under test case 4 is showed in Fig.10. It can be found the procedure which costs most time is modulation. This is mainly because auxiliary base stations should wait here for another user's data and there exits a socket transmission delay.

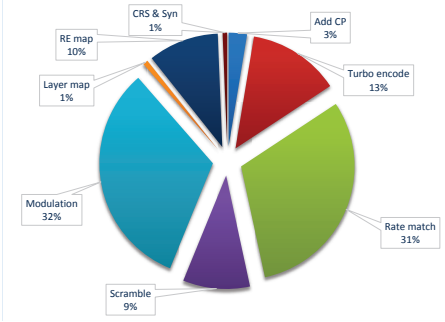


Fig. 10. Time distribution of PDSCH under test case 4

TABLE V: Data amount of socket transmission

Case number	BS	Special subframe	Downlink subframe				
			PBCH (us)	Control channel(us)	PDSCH (us)	CoMP precoding(us)	Total time(us)
Case 1	Main BS	12	8	4	118	170	301
	Auxiliary BS1	12	8	13	102	173	298
	Auxiliary BS2	11	8	12	97	171	289
Case 2	Main BS	15	8	4	243	242	498
	Auxiliary BS1	14	9	14	235	252	510
	Auxiliary BS2	12	8	13	228	242	492
Case 3	Main BS	12	9	6	327	415	757
	Auxiliary BS1	13	8	14	465	396	884
	Auxiliary BS2	13	8	13	460	390	873
Case 4	Main BS	14	8	4	433	237	684
	Auxiliary BS1	12	8	13	451	242	715
	Auxiliary BS2	12	9	15	461	252	738

V. Conclusion

We implemented a real-time dwnlink CoMP joint processing on GPP platform in this paper. With some parallel processing techniques such as multi-threads and SIMD, we optimized our program to improve processing efficiency and enable real-time processing.

In the future work, we will do some field tests to analysis the actual performance gain that users can get through our CoMP system. An other problem needs to be further studied is socket transmission delay. Because when the number of software CoMP base stations increases,the transmission delay may increase too.

Acknowledgment

This work has been partially supported by National Natural Science Foundation of China (61201192), National Basic Research Program of China (2013CB329002), Tsinghua University Initiative Scientific Research Program(2011Z02292), International S&T Cooperation Program (2012DFG12010), National S&T Major Project(2013ZX03001024-004), Key Grant Project of Chinese Ministry of Education (313005), China's 863 Project(2012AA01A502) and Tsinghua-Intel Joint Research Program.

References

[1] J. Mitola, "The software radio architecture," *Communications Magazine, IEEE*, vol. 33, no. 5, pp. 26–38, 1995.

[2] K. Tan, H. Liu, J. Zhang, Y. Zhang, J. Fang, and G. M. Voelker, "Sora: high-performance software radio using general-purpose multi-core processors," *Communications of the ACM*, vol. 54, no. 1, pp. 99–107, 2011.

[3] J. Fang, Z. Tan, and K. Tan, "Soft mimo: A software radio implementation of 802.11 n based on sora platform," in *Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on*. IET, 2011, pp. 165–168.

[4] J. Declerck, P. Raghavan, F. Naessens, T. Aa, L. Hollevoet, A. Dejonghe, and L. Van der Perre, "Sdr platform for 802.11 n and 3-gpp lte," in *Embedded Computer Systems (SAMOS), 2010 International Conference on*. IEEE, 2010, pp. 318–323.

[5] P. Guo, X. Qi, L. Xiao, and S. Zhou, "A novel gpp-based software-defined radio architecture," in *Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on*. IEEE, 2012, pp. 838–842.

[6] X.-F. Tao, Y.-Z. Hou, K.-D. Wang, H.-Y. He, and Y. J. Guo, "Gpp-based soft base station designing and optimization," *Journal of Computer Science and Technology*, vol. 28, no. 3, pp. 420–428, 2013.

[7] "Frame structure type 2," in *3GPP TS 36.211 V8.8.0 Evolved Universal Terrestrial Radio Access(E-UTRA):Physical Channels and Modulation*, 2009, p. 11.

[8] "Feedback in support of DL CoMP," in *3GPP, TR 36.814, Further Advancements for E-UTRA Physical Layer Aspects*, 2010, p. 17.

[9] B. Cheng, X. Mi, X. Xu, Z. Xu, X. Xu, and M. Zhao, "A Real-Time implementation of CoMP transmission based on Cloud-RAN infrastructure," in *Wireless Communications and Mobile Computing 2014 (IWCMC 2014)*, Nicosia, Cyprus, Aug. 2014.

AN APPROACH TO TEST AND EVALUATION OF MILITARY SDR PLATFORMS AND WAVEFORMS: THE LANCERS LAB

Fulvio Arreghini (Istituto per le Telecomunicazioni "G. Vallauri", Italian Navy, Livorno, Italy; fulvio.arreghini@marina.difesa.it); Carmine Vitiello (Ingegneria dell'Informazione, University of Pisa, Pisa, Italy, and CNIT, Parma Italy; carmine.vitiello@for.unipi.it) Marco Luise (Ingegneria dell'Informazione, University of Pisa, Pisa, Italy, and CNIT, Parma, Italy; marco.luise@iet.unipi.it); Andrea Manco (Istituto per le Telecomunicazioni "G. Vallauri", Italian Navy, Livorno, Italy; andrea.manco@marina.difesa.it); Giacomo Bacci (Ingegneria dell'Informazione, University of Pisa, Pisa, Italy, and CNIT, Parma, Italy; giacomo.bacci@iet.unipi.it); Matteo Falzarano (Istituto per le Telecomunicazioni "G. Vallauri", Italian Navy, Livorno, Italy; matteo.falzarano@marina.difesa.it)

ABSTRACT

Italian MoD is involved in SDR since 2002 and is part of the mayor multinational programs related to military SDR and waveforms, such as ESSOR and COALWNW. In addition, as an outcome of the Italian national SDR program, a complete family of SDR products is under development and some products are already available.

In 2011 the Italian Ministry of Defense (MoD) decided to develop a national test and evaluation capability of future SDR products.

In this paper we present the approach of the Italian Ministry of Defense (MoD) to the test and evaluation (T&E) process of military SDR. After describing key principles and choices made by Italy regarding military SDR, we will give a focus on the role of Italy in the International SDR Community. We will then describe the process of development of a national T&E capability for military SDR and the activities carried out at CSSN ITE Livorno to start the T&E Lab, named LANCERS. Finally the current situations of the activities of the LANCERS lab and future work will be presented.

1. INTRODUCTION

Software Defined Radio (SDR) is today one of the most appealing and challenging technology, both for the commercial and military community. The unique set of features provided by SDR in terms of flexibility and interoperability, on one side opens a lot of possibilities, on the other rises new issues.

From the technical point of view, SDR is very promising as it offers perspectives for the delivery of new services to the end users, making communications more efficient and flexible, for example using the electromagnetic spectrum in a more efficient way. This, on the other hand, asks for a new set of regulations regarding spectrum access policies, to take into account the existence of secondary users, operating in a licensed band, along with primary users. While primary users, in fact, have full access to licensed frequencies for a particular application (for example TV broadcast), regardless they are using the allocated spectrum or not, secondary users can dynamically determine if, in licensed bands there are frequencies unused by primary users, and, if needed, they can use that frequencies, on the premise of avoiding interference with licensed users.

For the military community, SDR is interesting especially as it provides a longer operational life to radios, that can be update with the installation of new waveforms to meet new needs in tactical communications, without the need of replacing the entire radio, and an easier interoperability especially in multinational joint and combined operations, making deployment of forces easier and seamless in complex scenarios.

Any new technology, anyway, including SDR, arise some issues, both from the technical and from the management point of view: in addition to the typical risks and costs that fielding new technologies implies, the intrinsic SDR can be difficult to fit into the existing regulations and operational procedures for tactical communications.

Full interoperability, in a *plug and play* fashion, is an ambitious goal that can be reached only if the efforts of all the stakeholders involved in military SDR, from the design, to production and fielding, are coordinated and harmonized. One of the mayor issues related to the development of SDR turns out to be the process of testing, evaluation and certification of the new products. This process implies activities at different levels.

In this paper we present the approach of the Italian Ministry of Defense (MoD) to the test and evaluation (T&E) process of military SDR. Section 2 describes the main challenges that the test and evaluation of military SDR has to address. Section 3 focuses on certification of SDR,

describing current efforts and trends across Europe. In section 4 the involvement of the Italian MoD in SDR at a national and multinational level is described. In this context, section 5 described the activities funded by the Italian MoD to create a test and evaluation facility for SDR Product at CSSN ITE, a research center of the Italian Navy. Section 7 describe how the test facility has been organized and which capabilities it is expected to implement. Conclusions and future work are presented in section 7.

2. CHALLENGES RELATED TO TEST, EVALUATION OF MILITARY SDR

Test evaluation and certification is the process comprising all the activities intended to verify specific features of a product versus given requirements prior to fielding. These activities are carried out at different stages of production on single components, prototypes or first-of-series products. The aim of test and evaluation is to ensure that the device under test (DUT) has a set of characteristics, required by the end user. Certification has a different perspective: it is a process intended to obtain a formal assurance that the certified product is compliant to a specified reference, being it technical or regulatory. The process of test evaluation and certification, at least governmental one, could seem related only to the final stage of the development of a product. This is actually only partially true: the evaluation process has to be taken into account from the very first stage of development, starting from the definition of the requirements. In other words, the evaluation process has to be designed together with the product or technology it is intended for: only in this way the risks and costs can be minimized when introducing a new technology. In [1]guidelines are provide to T&E personnel to identify T&E items to include in a program, starting from the early phases. An interesting sentence, clarifying the importance of thinking the T&E process together with the object to test, states that *if a T&E item or requirement is not in the SOW, it probably will not be in the RFP, and if it is not in the RFP, it probably will not be in the contract. If it is not in the contract, do not expect to get it!* The guide also points out the need to have personnel skilled in research and development assigned to write or review part of the contractual documents, together with personnel possessing a tough operational expertise.

For the military SDR, then the first driver for the development is the content of Operational Requirement Documents (ORDs) from which technical specifications are derived. A first level of verifications shall address the compliance of the products with the expectations of the ORDs. The assessment of the ORD and technical specifications ideally shall be carried out in two different moments: at first, during the definition of the documents, a technical expertise is required to assist the operational personnel so that every operational requirement is expressed in a way, suitable to be translated into one or more technical requirement. Then, during the evaluation of a delivered product, the technical personnel conducting the process shall be able to assess the correspondence of the DUT with the operational needs it is designed for. This process requires a team composed by personnel with technical expertise and deep understanding of operational needs. Anyway, a test strategy shall always include field testing of operational requirements. This can be carried out with testing directly the requirement fulfillment, when possible. When a direct verification method is not available, the test strategy shall demonstrate the compliance to operational requirements via indirect testing: as technical specifications are directly derived from ORDs requirements, lab testing can address technical specifications requirements. In order not to lose the focus on the original ORD requirements, anyway, it is necessary that the test strategy specifies what operational requirements are addressed for each test performed referring to a technical specification requirements. The correspondence between ORDs requirements and technical requirements need to be clearly defined in the test strategy. Lab testing (involving simulations, emulations and test beds) always provides a simplified model of the real operational scenario and cannot take into account every operational condition. For this reasons, whenever possible, field testing has to be considered as the primary option.

A second level of evaluation is related to performance and functionalities. When evaluating a product (platforms or waveforms) with lab tests, results of measurements are provided as outcome of the tests. Some features, investigated during the evaluation process, are related to functionalities: in this case the outcome of the test is a sort of Boolean value telling if the DUT provide the required functionality or not. Nevertheless, the DUT could provide the required functionality with different level of performance. For example, an SDR platform could provide the functionality to change the running waveform with different level of performance (requiring reboot or not, within different time, over the air or by cable etc.). For this purpose the evaluation process has to take into account, when performing a test, if the result of the test shall be assessed only in term of functionality or also in term of performance. This depends on how the requirements have been defined during the above described phase. The personnel conducting the evaluation at this stage shall be able to conduct the lab tests and to interpret the result in a correct way, according to the customer requirements. In this context it is important to define which figures have to be considered Measure Of Effectiveness (MOE) and which are instead to be addressed as Measure of Performance (MOP). MOE measures the overall impact on a mission of the tested feature, MOP gives a numerical limit that should be passed to consider the test passed. A MOP is a quantifiable

measurement that can take any number of forms. The data captured for a MOP indicates the system's achieved level of performance, and allows the analyst to determine whether the system's inherent performance requirements have been met. What they don't provide is an assessment of the impact that level of performance has in terms of being able to accomplish the goal the customer has in mind. As an example the MOP "standby time on battery" and "battery weight" can be related to a MOE like "mission duration allowed for a dismounted soldier".

A third, and perhaps more complex level of evaluation is related to interoperability and portability. As SDRs, especially military ones, are intended primarily to achieve portability of waveforms and interoperability with legacy equipment (nationally and at coalition level), several issues arise: plurality of platforms, waveforms, intellectual property rights (IPRs) of manufacturers, security policies of Governments, national and multinational regulatory aspects. When dealing with coalition and multinational programs, the process of test and evaluation gets more complicated. A team required to conduct test on products related to multinational program shall be able to manage all the related issues. This means that the evaluation personnel shall be able to access all the information required, in terms of ORDs, technical specifications, deliverable etc. related to the program. This implies that the lab shall guarantee an adequate level of security and shall be able to manage different products (even at the same time) with different requirements, treating each product according to the related security requirements. This also require that a management structure is put in place to guarantee a correct management of each workflow related to the evaluation of a specific product and the dialogue with external stakeholders at an adequate level.

3.CERTIFICATION OF SDR IN EUROPE PROBLEMS AND WAY AHEAD

Today the main program dealing military SDR in Europe are developed on the basis of National or multinational initiatives. Even if several multinational programs have among their goals the achievement of a high level of interoperability between partners, the lack of a common standard for European SDR is still a gap that needs to be filled to reach a common and shared vision on future tactical communications, enabling a real seamless integration of different programs.

In the USA military SDR has been developed under the control of the JTNC (*Joint Tactical Networking Center*). JTRS (*Joint Tactical Radio System*) program provided a reference model, the Software Communication Architecture (SCA[2]), today accepted as *de facto* standard in most of SDR programs, also in Europe. In addition the JTRS program provided guidelines to perform the evaluation of the SDR products[3]. These comprise not only the technical description of the test to be performed on a DUT to verify its compliancy to the SCA model (such as the Waveform Portability Assessment Procedure – WPAP), but also the description of the organization required to manage the entire process (the Portability Assessment Team- PAT). Finally specific tools have been developed to conduct the test. The evaluation process has then been designed together with the technology, from the early stage of development.

In Europe situation is different and somehow more complex as the European political and industrial context is more fragmented than the American one.

In 2007, the European Union was already aware that building a common approach to SDR, to make Europe able to compete with USA and Asia in the SDR market presented a number of technical and political issues [4]. These include the lack of a common standard and divergence between national SDR programs dealing with SDR. Several actions have been performed to develop a European standard for SDR, such as WINTSEC which defined the basis for a common architecture, named ESRA, and its follow-up EULER [5][6].

For this reason, among others, the procedures developed within the JTRS program, are considered to be not suitable for international application [7].

Across Europe, several entities play crucial roles for the definition of a common standard for military SDR.

The European Defence Agency (EDA) and the Wireless Innovation Forum are recognized as crucial in providing guidelines for the standardization and certification process. In addition, the European Telecommunication Standard Institute (ETSI) created technical committee dealing with the standardization of SDR, named Reconfigurable Radio Systems (RRS) addressing mainly the area of civil and public safety communications.Almost all the above listed entities tried to define a framework for the certification of SDR in Europe.

The European Defense Agency (EDA) defined the *three-basket model* [8] Each basket represents a community of stakeholders, with different regulations, requirement and with different policies concerning disclosure of classified information with other baskets. The first basket is the *open basket*, addressing the international community in a broad sense, without particular needs in terms of security or IPR. This basket is not considered particularly critical. The third basket is the national one, comprising the initiatives developed within each Nation. In this case the certification process is under the complete control of the Nation. A particularly critical area is basket2, addressing the multinational programs. Several European nations participate to a number of different coalition programs regarding SDR. Each program has different rules, depending on mutual agreements between participating nations and

often, at a national level, each program is managed by a different office (both on the Government and the Industry side). Addressing the certification of basket 2 products then require a set of independent entities able to establish links with the proper national and multinational bodies. These entities should have the security clearances and procedures to access the information of each program and to manage them according to the proper requirements.

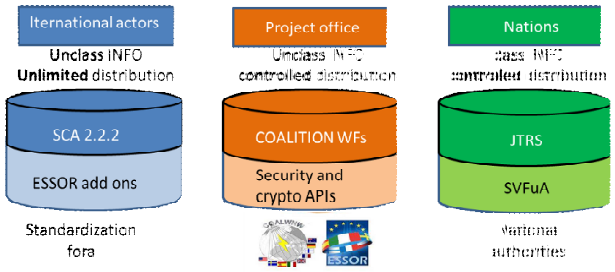


Figure 1:EDA – three baskets model for SDR standardization

The Wireless Innovation Forum defined a framework for European certification of SDR in[7]. A certification guide was expected [9] to implement the framework which, however, is not yet available.

The ETSI addressed the issue of SDR certification (with a particular focus on mobile communications and public safety in [10] where again the need of common standard as the basis to put in place a certification process is stressed.

The most likely solution for a common European certification seems to be the creation of a networks of testing facilities within different European Nations. Each laboratory should be accredited by a certification authority, providing mutual recognition of the testing activities carried out in each facility[11]. The need for a network of standardization and certification in Europe is addressed also in [12] and [13].

The networks should comprise test labs, that must have the capability and credibility to perform the testing of platform and waveform in order to verify the compliance to ORD requirements, technical specifications and national/multinational regulations. This may include experimentation and comparative testing on different combinations of platform and waveform, even in the procurement phase, to identify which one better coorregvers the operational requirements. For certification purposes, a common standard is needed and an organization as depicted in figure 2 must be implemented, to ensure mutual recognition of certification within the international community.

Up to now, among all others multinational initiatives dealing with SDR, the ESSOR program, is probably the one with the highest chance to become a European standard, for several reasons:

- ESSOR has gathered a community of Governments and Industries of six European Nations towards a common effort, for the development of a European SDR. As pointed out also in [1] a common effort and constant dialogue between Governments and Industries is a key for success in acquisition programs.
- ESSOR participating Nations are also part of the other mayor multinational programs dealing with SDR.
- ESSOR program has been focused from the very beginning on a common standard, investigating also certification matters.
- Deliverables of ESSOR program, are widely supported by experimental data (simulations) and documentation, making ESSOR, almost ready to become a common standard.

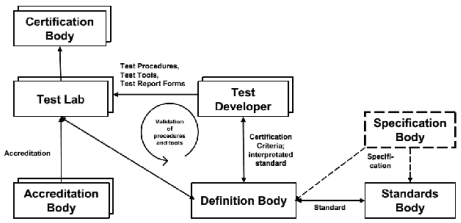


Figure 2: Wireless Innovation Forum model for European SDR certification [7]

4. ITALIAN MOD IN EUROPEAN SDR PANORAMA

SDR is one of the pillars of Network Enabled Capability (NEC) of Italian Defense.

The involvement of Italy in SDR begun in 2002, when the first R&D program, funded 50% by MoD and 50% by Selex ES, was launched. The program was intended to study the SCA, and to assess the effort to implement a compliant platform. The outcomes of the program were a technological demonstrator, a proprietary Core Framework and a naval wideband antenna.

In 2007, the ESSOR program [14] was launched. The program aimed at building a common architecture (ESSOR SCA) extending the SCA 2.2.2 and defining needed architectural components, and a wideband waveform (ESSOR HDR). The responsibility to develop national SDR platforms compliant with the ESSOR SCA architecture is up to the participating Nations. Within the program, the national platforms shall be interoperable when using the HDR waveform. Italian platforms are developed within the SDR-N program, based on ESSOR architecture.

The activities of the original ESSOR program are still ongoing and a multinational interoperability test is expected by the end of 2014. At the same time, a new phase of the

program, named ESSOR phase 2 is being initiated. The ESSOR phase 2 of the program is intended to enhance the capability of the products developed within the phase 1, especially the HDR waveform. Moreover a work package of phase 2 is dedicated to the field testing of the phase 1 waveform. This activities are intended to demonstrate that the ESSOR phase 1 outcome is a fully operational product, ready for fielding, tough planned for modifications and enhancement during the phase 2. Italian MoD personnel supported to the definition of all the technical specification of phase 2, comprising the field test ones. This was done participating to the technical working groups created within the program.

Italy is also part of the COALWNW multinational program[15], aimed to develop a wideband waveform to be used in the coalitional scenarios. COALWNW started as a development program and become later a t project addressing the acquisition of a quasi-Non Developmental Item (NDI). COALWNW requirement are mostly encompassing the ESSOR ones and ESSOR participating countries are also part of COALWNW initiative. The gap between the two sets of requirements is expected to be completely filled with the ESSOR phase 2. For this reason, and for the coherent procurement schedules, Italy supports strongly ESSOR as a candidate for COALWNW.

Moreover, Italy supports the work of NATO Line of Sight Communications Capability Team (LOS Comms CaT). Amongst other activities, the LOS Comms CaT manage the definition of the NATO Wideband waveform (WBWF). Presently the standardization of WBWF is seeking to receive input from the mayor multinational programs such as ESSOR and COALWNW. Italy supports ESSOR HDR as a candidate for NATO WBWF. In fact, not only many requirements of ESSOR HDR are suitable for NATO WBWF, but, in addition, ESSOR HDR is a product that has already been validated trough simulations (and it is expected to be soon tested on the field) and it is fully documented, so a minimum effort would be required to put existing documentation into a STANAG.

On a national side, Italian MoD in 2007 launched the SDR-N (National) program. The SDR-N program aims to develop a complete family of different national SDR platforms and waveforms, manufactured by SELEX ES. Figure 3 shows different operational platforms, some of which already available as they have been delivered, after formal acceptance by the Italian MoD. After formal acceptance by MoD, the great part of the delivered platform has been sent back to the manufacturer for the porting of ESSOR HDR (activity of ESSOR program), while a subset of platforms has been delivered to the SDR lab located in Livorno to begin a phase of Governmental testing and evaluation.

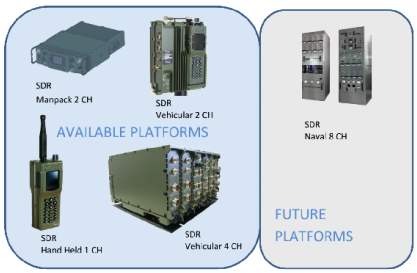


Figure 3:platforms of the Italian SDR-N program

In order to have a coherent management of all the activities related to SDR, both on the national side and on the multinational one, a dedicated Program directorate has been created within Italian MoD. The main task of this directorate is to coordinate the activities related to national and multinational programs regarding SDR and to provide guidelines for research on this topic.

A director supervise and coordinate the activity of the management groups, assisted by a deputy, responsible for the communication with industries and international cooperation.

Within the directorate three management groups are identified:

- Security management group: in charge of the development of the documents containing the security requirements of new SDR systems;
- Technical management group: in charge for the study of the technical solution responding to the operational requirements developed by the operational MG;
- Operational management group: responsible for the development and update of the Operational requirements to be inserted in the ORDs.

The Director, vice director and the chairmen of the management groups are members of the steering committee which is in charge of approving the documents provided by each management group and of issuing the adequate guidelines and policies.

Each management group can rely on working groups or tiger teams constituted to carry out peculiar tasks. In this context, a working group in charge of studying and implementing the national test and evaluation strategy is being created.

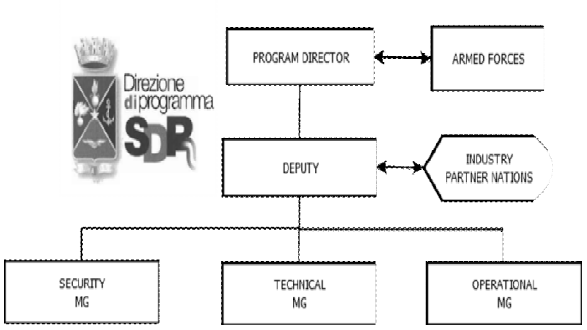


Figure 4 :SDR Progam Direction

5. THE ITALIAN APPROACH TO T&E OF SDR

Following its deep involvement in a wide range of national and multinational activities related to SDR, in 2011, the Italian MoD decided to develop a national capability of test and evaluation of SDR products. This capability is intended to reduce the risk related to the introduction of the SDR technology in operational environments through activities of Modeling and Simulation (M&S) and Test and Evaluation (T&E). A future capability of certification, after the accreditation to the competent bodies (as soon as they become available) is foreseen.

"Centro di Supporto e Sperimentazione Navale (CSSN) – Istituto per l'Elettronica e le Telecomunicazioni (ITE)", in Livorno, Italy, is the research center of the Italian Navy identified as the place to host the T&E facility.

CSSN ITE was chosen as it possesses a proven experience in the field testing of communication equipment and in experimental activities related to new military communication technologies [16],[17]. CSSN ITE personnel have been involved since 2009 in the SDR-N program, supporting MoD general Staff in the definition of the ORD and in the trials of products delivered by national industry. Moreover CSSN ITE personnel participate to the technical working groups in ESSOR and COALWNW programs and in the NATO Line of Sight (LOS) and Beyond Line of Sight (BLOS) Capability Teams (CaT). This makes CSSN ITE an excellence technical center, whose personnel is able to understand and interpret the requirements coming from the field and at the same time, is up to date with current trends and technical decisions concerning SDR. The task to form a T&E facility for military SDR was then assigned by MoD to CSSN ITE, supported by a funding program lasting until 2015. The mission of the lab, currently under construction and named LANCERS, is to develop capability in the test and evaluation of:

- Platforms (HW+OE): evaluation platform with reference to a specific standard (currently the Italian main reference is ESSOR SCA);
- Waveforms: (I) Evaluation of technical specifications of new waveforms (analysis of documentation, code and other deliverable provided during development) (II) Evaluation of base waveforms versus a given reference (III) Evaluation of the waveforms versus a legacy standard (interoperability).
- Complete systems: (I) Performance assessment of different combination of waveforms and platforms (II) Interoperability test between different SDRs and between SDR and legacy platforms (III) Performance assessment of complete systems (i.e., reconfigurability, power consumption, performance in co-sited environment, etc).

The LANCERS lab is expected to operate on products with Technology Reference Level (TRL) 5-6, to support and prepare the activity of other entities of the MoD, responsible for the final integration of the complete subsystem in the field (TRL 7-8) [18]. The LANCERS lab will not perform activities related to security certifications, as these will be done by proper national bodies, under the control of Security management group. In particular, all the activities related to security certification, will be carried out by a dedicated facility, hosted near Pisa, called CEVA (Centro VAlutazione). The CEVA depending directly from MoD general staff, is in charge for the security certifications of all ICT equipment. The CEVA lab is located in Pisa, near to the LANCERS Lab and to the University of Pisa. Testing activities carried out at CEVA is mainly focused on the certification of items, according to ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation). Anyway, CEVA can also perform testing according to ITSEC (Information Technology Security Evaluation Criteria). In addition to its *core business* dealing with security certification, CEVA is deeply investigating, with the collaboration of the University of Pisa, the security aspects of MANET, in order to identify the main threats and countermeasures that will play a crucial role during the field test of new communication technologies (including SDR) in complex, networked scenarios. It is clear that CEVA lab and LANCERS lab will be more and more deeply involved in joint activities, during the fielding of future communication technologies.

The LANCERS Lab is accredited by Italian MoD for the T&E activities. Moreover, like the others CSSN ITE Telecommunication labs, LANCERS is accredited by ACCREDIA, according to ISO 9001:2008. In the future the LANCERS lab aims to become part of an European certification networks, receiving accreditation from the competent international bodies.

As a comprehensive approach to the SDR T&E should gather the expertise from Governments, Industry and Academia, CSSN ITE settled a long-standing collaboration with the CNIT (the Italian Inter-University Center for

Telecommunications) so that the lab can rely on the academic expertise available in Pisa. The Italian Navy also funded a PhD program to be attended by a Navy Officer, and more PhD programs are expected to be activated at CSSN ITE in the near future. Furthermore, the LANCERS intends to be part of the EU certification network that is likely to be constituted and is always seeking for cooperation with other stakeholders involved in SDR technology.

The lab is equipped with:

Modeling and simulation environment: an electromagnetic propagation simulation environment, developed by the University of Pisa is available. This simulator, given a set of transmitting and receiving nodes in a propagation scenario, can provide information about the expected characteristics of the received signal, from which expected values of Signal-to-Noise Ratio (SNR) can be derived. Furthermore the propagation scenario can be created from scratch or derived from real data, coming for example from a cartographic source. This allows to build a very realistic model of the propagation in relevant scenarios. Generic modeling and simulation tools like MATLAB are used to build Platform Independent Models (PIMs) of waveforms. These models provide a reference on expected behavior of waveforms and platforms to be tested, taking into account the propagation conditions derived from the propagation simulator. A network simulator (Qualnet [19]) is available and will be used in the future to perform tests on the network level of the waveforms.

RF instrumentation: the lab has a set of generic RF instruments, such as Spectrum Analyzers, measurement antennas and channel simulators. With these instruments, tests on the RF signal can be carried out, for example to verify the compliance of the emitted signal to national regulations. A set of military (non-SDR) radios is also available to perform interoperability tests between SDR and legacy platforms. For more complex test scenarios, CSSN ITE can rely on the cooperation of naval assets provided by the Italian Navy.

Development platforms: two Universal Software Radio Peripherals (USRPs) [20] have been supplied to the lab. These platforms allow the porting of waveforms or part of them to be analyzed and tested. In the next future, the lab is expected to be supplied with professional development platforms (Prismtech Spectra [21]).

Operational platforms: at the LANCERS lab some operational platforms are available, manufactured by SELEX ES in the scope of SDR-N program. As a first step, testing activities have begun on Hand Held (HH) SDR platforms with legacy waveforms. A possible future cooperation between the LANCERS Lab and the manufacturer aimed to identify area of common interest regarding testing activities is under investigation.

6. CURRENT ACTIVITIES IN LANCERS LAB

A project containing the roadmap of the activities expected for the LANCERS lab has been started in cooperation with CNIT.

The workflow that LANCERS lab is developing is shown in Figure 5. Dashed lines refer to activities or items to be developed. in particular, the activity workflow comprise:

Analysis of the requirements/specifications: In an early procurement phase, the lab can provide support in the analysis a definition of operational requirements and technical specifications. For new existing products, the lab performs an analysis of the documentation provided.

Classification: In order to classify and to get fast and significant main information about UUT (Unit Under Test), we built a database composed by two main categories, platform and waveform respectively. For the platforms we collected hardware specifications such as General Purpose Processors (GPPs), Field Programmable Gate Arrays (FPGAs) and Digital Signal Processors (DSPs) characteristics, internal clock accuracy and stability, embedded Global Navigation Satellite System (GNSS) accuracy, maximum packet size, Peak Envelope Power (PEP), operating frequency range, RF bandwidth channelization, Tx/Rx linearity and switching time, duplex capacity, carrier frequency change time, Tx/Rx noise figure and spurious products, supported max duty cycle, battery life, operating thermal range and so on. Waveforms data specifications regarding coding, puncturing, interleaving, modulation, presence of multicarrier, scrambling, frame structure and filtering employed in the classified communication standard. The database is periodically updated in order to have a current view over the technology progress.

Modeling & Simulation: A primary modeling phase is necessary to find some reference points for the correctness of next phase tests. For each considered or supported waveform, we built a Matlab/C++ code, which will represent the “sample waveform” in the next phases. The modeling code is a Platform Independent Model (PIM), so it is reusable as a reference, regardless of the real platform where the waveform is ported. The code simulates the behavior of the waveform in several propagation scenarios, both indoor and outdoor, according to the operating environment, giving the expected values of Bit Error Rate (BER) and Frame Error Rate (FER) as function of SNR as outputs. To improve these simulations, we exploit an electromagnetic simulation tool, to calculate a real mathematical propagation model of the channel based on a real scenario, that can be built from scratch or from data extracted by cartographic tools. Using real scenarios data provide a very realistic prediction of propagation environment, without the need of setting up complex and expensive test bed directly on the field.

Nevertheless, field measurement can be performed, using mobile labs of CSSN ITE.

SCA-modeling: The original modeling code is modified to create a SCA-compliant sample waveform. This is again a PIM, but it is addressed to the subset of SCA compliant SDRs. SCA-compliant development tools, such OSSIE [22] or REDHAWK [23], are used to simplify the implementation of waveforms and its components. The code is then ported on a development platform (USRPs).

Target Waveform test: with models and benchmarks created in phase 3) UUT codes start to be tested. The target code is divided into blocks which implements a specific logical function, such as coding or mapping to create a component. Correctness of the codes is verified by stimulating the component with known input and evaluating the corresponding output, in agreement to both expected and benchmark output. Up to now, we are able to check only physical layer and MAC components.

Over-the-Air Test & black box testing: RF testing is performed on the UUT, including the assessment of the performance and the compliance to regulatory constraint. Over-the-air tests are also performed to verify that the UUT does not cause unexpected phenomena, such as signal distortion and interferences. For EMC testing we can rely on the assets of EMC division of CSSN ITE (anechoic chamber, compact range).

For RF tests a channel simulator is available. The channel frequency response can be set according to data derived in phase 3) or retrieved in the literature.

"Black box" testing can be performed to verify other requirement derived in phase 1). For example, time from boot to the operational status and time required to load a new waveform can be measured. An important category of testing concerns power consumption as a function of the waveform parameters. It is in fact known that slightly different hardware in the platform, combined with the same waveform, can show very different performance regarding power consumption [24]. Furthermore, unexpected waveforms behaviors (due to fault or design errors) can heavily affect the power consumption of the platform [25]. Power consumption is a critical performance parameter as it affects the battery duration for portable SDRs and the integration requirements for vehicular SDRs.

Interoperability Test: here we test the interoperability of UUT with other SDR devices, from the same or different

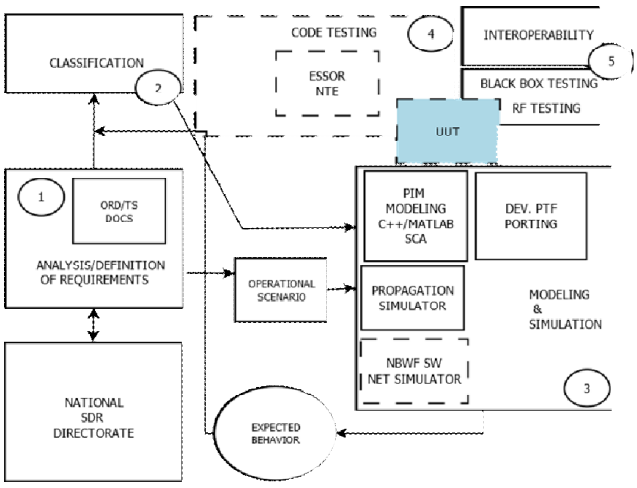


Figure 5: flows of the activities in SDR lab

manufacturer, and with classical legacy radio, wherever possible. For this purpose CSSN ITE has a complete set of legacy radios and trained personnel. Where cooperative assets are required for testing, such as surface or airborne platform, CSSN ITE can submit the request to the competent entity and manage all the activities related with the test campaign (logistics, communications, security clearances, etc.). This is particularly interesting in situations when the manufacturer cannot perform a specific set of tests, due to the lack of cooperative assets or, for instance, for tests that have to be performed in a military area. This could also be the situation of coalition interoperability (basket 2 of EDA model): in the test of products belonging to different nations within a coalition on the premise of proper agreements between involved Governments, a military area could be preferred as testing facility, for security reasons.

7. CONCLUSIONS AND FUTURE WORK

In this paper we described the activities performed by the Italian MoD for the development of national test and evaluation capability of SDR products. These encompass action both on the technical and on the management side.

The involvement of Italian MoD in the main multinational programs dealing with military SDR, along with a national SDR program, have requested the creation of a proper management structure, the SDR program directorate, which integrate all the efforts and the expertise involved in the development and delivery of the national SDR capability.

Among these expertise, the LANCERS lab, created at CSSN ITE, a Navy research center, is studying the test and evaluation strategy for the future SDR that will be fielded over the next years. LANCERS lab can rely on the expertise of personnel coming from the field and with a deep understanding of both operational and technical needs of the end users. The support from the University of Pisa gives to

the LANCERS lab, the capability to be always up to date with current research trends and ready to develop new tools when needed. The CEVA lab, in charge for security certifications, is very near to the LANCERS lab, and the activities of the two facility will soon converge to maximize the effectiveness of testing in complex scenarios.

From the technical side, in LANCERS lab we are performing investigation on SDR technologies and development of waveforms of interest, based on low cost hardware, to become part of future and more complex test beds and test procedures.

Finally, the creation of a program directorate, specifically intended for SDR, is a key element to harmonize the efforts of all national actors involved in the fielding of SDR, providing a comprehensive approach to all the issues related with this new technologies and ensuring the coherence between Italian national efforts and strategic choices made together with international partners.

8. REFERENCES

[1] Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation - Incorporating Test and Evaluation into Department of Defense Acquisition Contracts 2011

[2] JTNC Standards for Software Communications Architecture (SCA) (http://jtnc.mil/sca/Pages/default.aspx)

[3]JTRS NED Waveform portability guidelines v 1.2.1. (2009).

[4]Pullinger S: Software defined radio (2009)-Retrieved 2 2014 (http://www.europarl.europa.eu/activities/expert/eStudies.do?languageEN)

[5]WINTSEC. (2009). WINTSEC, D7.3 European Software Radio Architecture (ESRA): ESRA Framework Overview and Recommendations

[6]Sanchez A. et al. (2011). EULER deliverable 4.1 - ESRA recommendations extensions and maturation v 1.0. EULER.

[7] SDRF-08-P-0007-V1.0.0 - Test and Certification Guide For SDR based on SCA

[8]retrieved from http://www.eda.europa.eu/migrate-pages/Otheractivities/SDR/edaapproachsdr/basketmodel

[9]Leschhorn (2010): SCA Test, Evaluation and certification model realization (http://www.businesswire.com/news/home/20101014005302/en/Wireless-Innovation-Forum-Approves-Standard-Cognitive-Radio#.U0wR0RA_uUM)

[10] ETSI TR 102 838 V1.1.1 (2009-10) - Reconfigurable Radio Systems (RRS) Summary of feasibility studies and potential standardization topics

[11] ESSAC. (2001). final results. wincomm europe 2011.

[12]Symeonidis D. & Baldini, G. (2010). European Standardization and SDR Certification. Telecommunications (AICT), 2010 Sixth Advanced International Conference.

[13]Turner M. (2009). Global Military SDR Solutions – Practical Methods for SCA Radio Compliance and Deployment . Proceedings of the SDR '09 Technical Conference and Product Exposition.

[14] Retrieved from http://www.occar-ea.org/programme/ESSOR

[15]retrieved from: https://www.fbo.gov/index?s=opportunity&mode=form&id=ff1021494e3db063ae5f08b9a23616d6&tab=core&_cview=0

[16]Garroppo, R. et al (2008). Military Communications Conference, 2008. MILCOM 2008. IEEE.

[17]Garroppo, R. et al (2009). WiMAX testbed for interconnection of mobile navy units in operational scenarios. WoWMoM 2009. IEEE International Symposium

[18] "Technology Readiness Assessment (TRA) Guidance". United States Department of Defense. April 2011

[19] QualNet - Scalable Network Technologies (http://web.scalable-networks.com/content/qualnet)

[20] Ettus Research – Products (http://www.ettus.com/product)

[21] Spectra SDR Software Defined Radio SCA Software Communications Architecture Solutions - PrismTech (http://www.prismtech.com/spectra)

[22] OSSIE - SCA-Based Open Source Software Defined Radio (http://ossie.wireless.vt.edu/)

[23] REDHAWK (http://redhawksdr.github.io/Documentation/)

[24] Blair A. et al - "Porting Lessons Learned From Soldier Radio Waveform (SRW)" Military Communications Conference, 2007. MILCOM 2007. IEEE

[25] Gonzalez, C.R.A et al - power fingerprinting in SDR & CR integrity assessment - Military Communications Conference, 2009. MILCOM 2009. IEEE

Experimental Indoor Deployment of CloudRAN GSM Emergency Service

Luca Simone Ronga
CNIT, Florence Research Unit
Florence, Italy
luca.ronga@cnit.it

Enrico Del Re
Department of Information Engineering,
University of Florence, Italy
enrico.delre@unifi.it

***Abstract*— The increasing availability of computing power enables new paradigms of radio communication services. The centralized baseband processing of cellular networks reveals some interesting features such as an high degree of re-configurability, high efficiency in terms of processing power and consumed energy, fast deployment especially useful in the case of unplanned emergency networks. This paper reports an indoor multi-cell experimental deployment of GSM voice and message communications services with low-cost SDR technology. The experimental setup is characterized by a centralized processing of baseband signals, delivered with optical fiber links to RF heads. Quality of experience and resources usage analysis has been performed and reported as an evaluation of the feasibility of this approach with low-cost HW and devices.**

Keywords—Emergency cellular networks; Cloud-RAN; Software defined radio.

I. INTRODUCTION

Stepping back from previous trends pushing network intelligence from core to edges, a new tension towards the centralization of higher network functions has initiated. The Software Defined Networking concept [1] produces a separation of control-plane from data plane in routing devices. The virtualization of network access allows more flexibility and re-configurability of networking functions, increasing resiliency and robustness in case of failure. The availability of fast optical links feeding the radio base stations, suggested that a virtualization could also take place at PHY layer, by encapsulating baseband radio signals into network packets for a more efficient and flexible processing. The virtualization of radio access networks (RAN) functions in centralized abstract entities, namely Cloud-RAN [2], acts as a multiplier for features and configurations the new network can operate with. A relevant application which may benefit from this new architecture are the emergency cellular networks. Due to the circumstances of adoption, the opportunity to provide a "soft" configuration of deployed radio devices is a desired feature. In several emergency contexts the opportunity to provide emergency communication services over widespread cellular standards may result in increased rescued people and a faster reaction to events.

In this paper we report the results of an experiment of deployment of a multi base-station 2G radio network for emergency purposes in an indoor environment. The experiment shows the feasibility and required network and computing resources for a centralized baseband processing of involved radio signals. The paper is structured as follows: Section II reports the adopted system architecture and the environmental setup for the experiment along with the involved devices and radio configurations, Section III describes the measurements acquisition and comments the main results and assessments. Section IV contains some concluding remarks.

II. EXPERIMENTAL SETUP

During an emergency caused by a natural disaster of socio-political event, regular communication infrastructures could be unavailable. In order to provide a reliable communication network able to connect the population with responders and authorities, a possible solution is the activation of a temporary radio network following widespread standards like 2G/3G cellular telephony. In the experiment an emergency situation has been simulated where a software 2G (GSM) emergency network has been deployed indoor, at the second floor of the Department of Information Engineering (DINFO) at the University of Florence. The logical map of involved devices in the access segment is depicted in Fig. 1. It consists of two RF heads, one directly connected through a gigabit Ethernet link to a baseband CPU hosting OpenBTS [3], the other is remotely deployed and fed through an optical LX Gigabit Ethernet connection from a second baseband CPU unit. Both CPUs are then interconnected by a SIP PABX (Session Initiation Protocol based Private Automatic Branch Exchange), for call routing and user authentication.

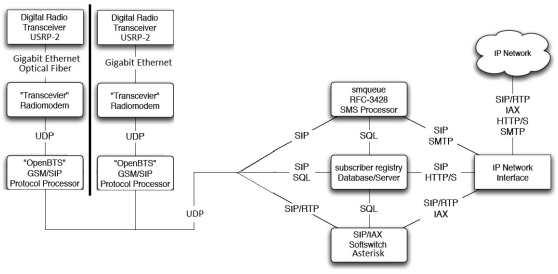


Fig. 1. System architecture used in the experiment

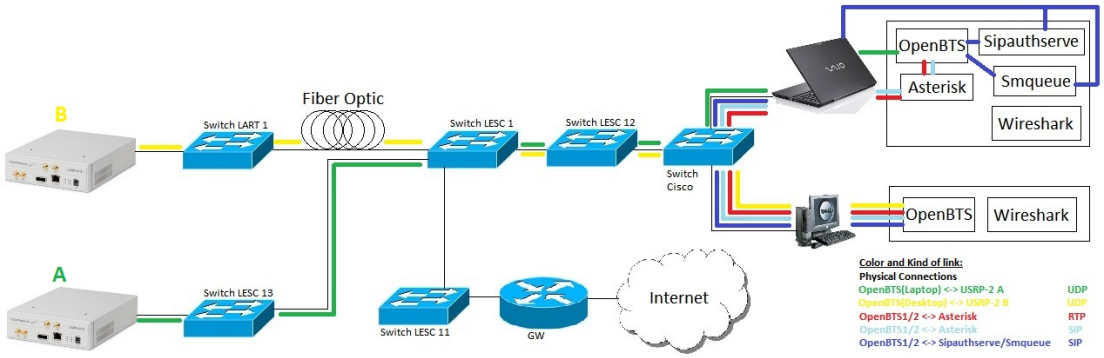


Fig. 2. Detailed traffic paths

The details of the flowing IP traffic in the experimental setup is shown in Fig. 2. Radio devices are implemented with two Ettus Research Universal Software Radio Peripheral-2 USRP2 [4] equipped with 900MHz daughter boards. The two baseband CPUs consists of a Sony VAIO (Intel I5@2.5GHz, 4 cores), namely CPU1 and Dell (P4@3GHz), called CPU2. The first CPU is hosting one OpenBTS module, the Asterisk PABX and the SIP authorization module. The second one is hosting the remote OpenBTS module. The diagram also reports the main traffic components colored depending on the link role during the radio access operation after a connection with a mobile has been established.

The deployment map is shown in Fig. 4. The stars represent the location of the two RF devices corresponding to the two GSM base stations. Numbers (1-11) indicate the location of mobiles where the measurements have been acquired.

III. Field Trials and Results

The experiment consists in providing voice and SMS service to up to 2 real GSM mobiles in the area of coverage of the two emergency cells. The main adopted parameters are represented in TABLE I. .

TABLE I. Experiment Parameters

Parameters		
name	***value***	***unit***
Downlink Frequency BS1	870,0	MHz
Uplink Frequency BS1	825,0	MHz
Downlink Frequency BS2	872,0	MHz
Uplink Frequency BS2	827,0	MHz
Noise Figure	8,0	dB
Max RF power	200,0	mW

Several voice call and text message tests has been conducted with mobiles located in various positions of the coverage area. For each setup, the exchanged IP traffic among the network functional entities has been captured and analyzed with Wireshark. The voice latency has been also measured through the analysis of the audio echoes of a sequence of audible "ping" transmitted from a modified software phone to the mobiles.

A. Aggregated Network Results

The required network resources for completing a voice call with the experimental setup is reported in TABLE II. for a single mobile and considering the outbound traffic only (from mobile to BS).

TABLE II. Voice Call Network Usage

Measurements		
name	***value***	***unit***
GSM voice payload bitrate	13,0	kbps
RTP payload bitrate	13,2	Kbps
Mean RTP packet delay	20,0	ms
RTCP overhead (5 sec)	0,41	%
Baseband IP traffic	13,0	Mbps

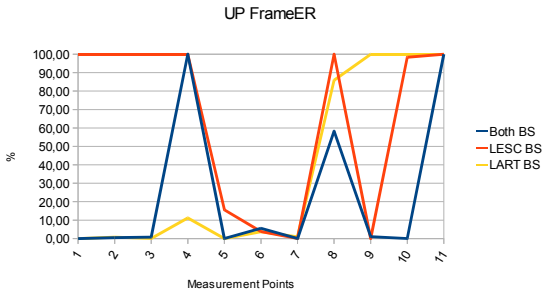


Fig. 3. Uplink Frame Error Rate with mobiles placed at different test-points

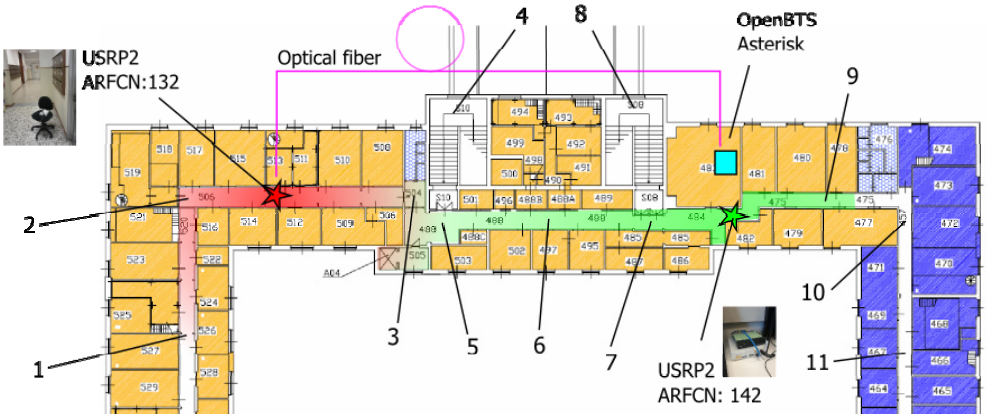


Fig. 4. Experiment deployment

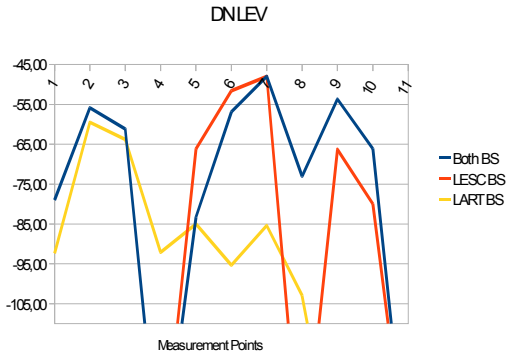


Fig. 5. Measured received signal power (dBm) at different test points

B. *Received signal and frame errors for various test points.*

For various mobile locations a series of measurements have been conducted. In Fig. 5 is reported the received signal power for the downlink in various points along the corridor and stairs. The red line shows the dependency between the measurement points and the received power from BS1 only, the rightmost in the map, while the yellow line is related to BS2. The blue line is the measured power when both BSs are available. The measured received signal strength follows the expected behavior.

In Fig. 3 the frame errors for uplink transmission during a call are reported for various test points. Again the red trace refers to the rightmost BS1 while the yellow one to BS2. As shown if a mobile is within the coverage of a BS, the related frame errors are low. During this test no automatic handover procedure has been activated. Red line also shows a signal saturation issue due to an unfavorable location of mobile with respect to the BS1 (test point 11).

C. *Computing and Energy Resources Usage*

An evaluation of computing complexity for the software realization of GSM radio access is reported in Fig. 6 and Fig. 7 for both the CPUs. The y-axis reports the CPU load fraction for various modules of OpenBTS and Asterisk (single BS). The x-axis iterates the measurements in different conditions: point 1 refers to idle operating system with no OpenBTS modules running, points 2 to 4 refer to CPU load sampling during a call. As expected the baseband processing (Transceiver) is the process with the highest load to serve.

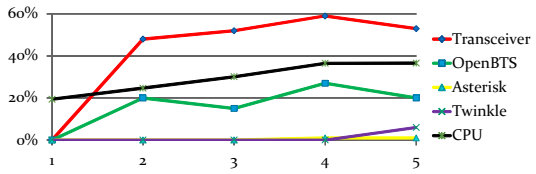


Fig. 6. Process load for the various modules in the baseband processing host (CPU1, 1=idle, 2-5 during a call).

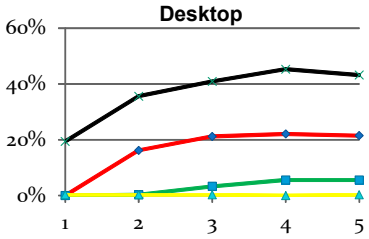


Fig. 7. Process load in the baseband secondary processing host (CPU2, 1=idle, 2-5 during a call).

In Fig. 8 the averaged power consumption is reported for CPU1. Again point 1 refers to an idle operating system conditions, while 2-5 are measured during a call.

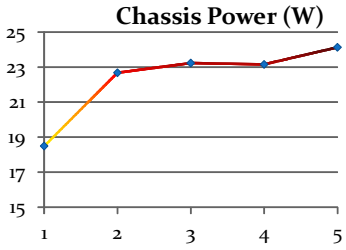


Fig. 8. Measured power consumption for CPU1 (1=idle, 2-5 during a call)

D. Audio Latency

Audio perceived delay through the experimental system has been evaluated by injecting both artificial and natural sounds and capturing the received echo produced by the analogic coupling of speakers and microphone in the mobile phone. The sounds adopted are of three kind: synthetic sounds injected by Twinkle SIP softphone, short analogic "bumps" generated on microphones and a portion of a speech during a call. By autocorrelation analysis an estimated of round-trip latency is reported in TABLE III. . Estimated one-way latency can be obtained by halving the measured RTT, resulting in values aligned with conventional digital telephony.

TABLE III. AUDIO RTT

Measurements		
name	***value***	***unit***
Twinkle mean RTT time	274,4	ms
Twinkle RTT standard deviation	64,5	ms
"Bumps" mean RTT time	172,2	ms
"Bumps" RTT st. deviation	6,5	ms
GSM mean RTT time	278,3	ms
GSM RTT standard deviation	1,6	ms

IV. CONCLUDING REMARKS

The described field trial successfully confirmed the feasibility of software virtualization of baseband signal processing with ordinary CPUs. The involved network resources in the experimented context are small (less than 15Mbps) and does not require complex devices to operate. The remote RF head has been connected with a small portion of the optical link, so that over 60 GSM base stations can share a single Gigabit optical link. Computing resources and power consumption stay within the capability of conventional laptop/desktop. With dedicated computing hardware a more computational efficiency can be achieved. The experiment considered 2G cellular technology because of the limited bandwidth and complexity of the standard. The same experimented concepts however apply to 3G and later generations with more computing and transport resources available.

REFERENCES

[1] "Software defined networking: The new norm for networks," White Paper, Open Networking Foundation, 2012.

[2] CMCC, "C-RAN The Road Towards Green RAN," CMCC white paper, Oct. 2011.

[3] Pace, P.; Loscri, V., "OpenBTS: A Step Forward in the Cognitive Direction," Computer Communications and Networks (ICCCN), 2012 21st International Conference on , vol., no., pp.1,6, July 30 2012-Aug. 2 2012

[4] Ettus Research ltd, http://home.ettus.com/

ACKNOWLEDGEMENTS

The authors thank Rodrigo Isidro Lopez for his support in the execution of the reported experiment, the director of the Department of Information Engineering (DINFO) of University of Florence for the availability of the experiment area.

EVALUATION AND ANALYSIS OF INFLUENCE FROM OTHER RADIO SYSTEMS IN WIDEBAND NON-CONTIGUOUS OFDM RECEIVER

Keiji Takakusaki Kazuhiro Kosaka Issei Kanno Akio Hasegawa Hiroyuki Shinbo
Advanced Telecommunications Research Institute International
Adaptive Communications Research Laboratories
2–2–2 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619–0288 Japan
E-mail: {takakusaki, kosaka, kanno, ahase, shinbo}@atr.jp

ABSTRACT

We are studying the Wideband Non-Contiguous OFDM (WNC-OFDM) to utilize an unused frequency band. The WNC-OFDM can realize a high-speed communication by gathering OFDM sub-carriers which are dispersively located unused frequency bands across extremely wide target bands. Since a WNC-OFDM transmission uses multiple dispersed frequency bands at the same time, its receiver needs to receive wideband signal including all dispersed bands. In this case, since the receiver receives not only the desired WNC-OFDM signals but also the undesired signals of other systems simultaneously, WNC-OFDM signals are affected by interference due to other radio systems signal. It is important to comprehend the influence from other radio systems and tolerance for them in order to design and tune the WNC-OFDM transceiver. In our previous research [1], the influences from other radio systems were evaluated through the experimentation with developed equipment and the computer simulations. The results showed bit error ratio performances were quite difference from the performance in Gaussian noise environment. In this paper, we conducted theoretical analysis and confirm validity of the interference characters observed in the previous evaluation.

1. INTRODUCTION

Recently, mobile data traffic continues to rapidly increase. Its 2013 amount is forcasted to increase over 11 times by 2018. To handle such mobile data traffic, more frequency resources are required. We focus on utilization of lower frequency bands under 1GHz, because the characteristic of radio propagation is suitable for mobile communications in a certain situation such as a mobile terminal with high mobility. It is difficult to obtain wide and consecutive frequency resources in lower frequency bands because almost of resourcess have benn already allocated to the other systems. However, there are two types of available frequency resources in lower frequency bands: (1) a gap bandwidth between allocated frequency bands and (2) allocated frequency bands but they are not used at certain places (countries and regions) and/or certain time intervals. We call (1) and (2) as “unused frequency resources”. We have observed the unused frequency resources in some places of Japan [2]. A lot of dispersed and narrow frequency resources whose utilization could not be detected were observed. If we can use the unused dispersed and narrow frequency resources and gather them, it is the same as obtaining new wide frequency resources for handling large amount of mobile data traffic.

In order to utilize such unused frequency resources effectively, there are some prior researches about the technology of Non-Contiguous Orthogonal Frequency Division Multiplexing (NC-OFDM) [3,4,5,6]. In NC-OFDM transmission, a transmitter selectively activates subcarriers on the unused frequency resources, and allocates mobile data to the activated subcarriers. A receiver gathers the activated subcarriers and obtains the large amount of transmitted mobile data. One example of implementation of the NC-OFDM receiver has been studied in [5]. The receiver supports consecutive 30 MHz bandwidth simultaneously in 5GHz ISM band.

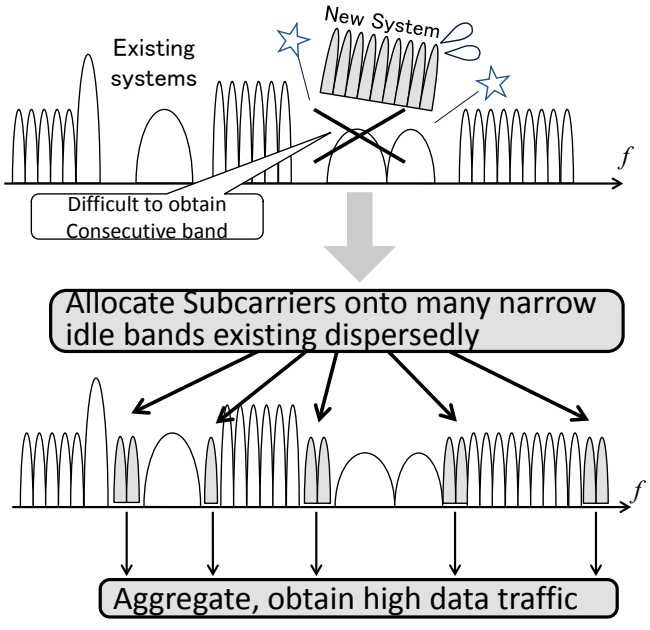


Fig. 1. Overview of WNC-OFDM

However, the supported bandwidth of NC-OFDM is not sufficient to handle the current mobile data, because the unused frequency resources in lower bands are located dispersively across extremely wide bands. We are studying Wideband NC-OFDM (WNC-OFDM) in response (Fig. 1). The main characteristic of WNC-OFDM is to utilize the unused frequency resources selected from extremely wide bands (e.g. 1GHz).

There are many issues to implement a WNC-OFDM system [6]. This paper focueses on the issue of received signal interference. One set of a radio frequency (RF) circuit and an IFFT/FFT function is defined as an "RF-unit". As shown in Fig.1, a receiver of WNC-OFDM system receives desired signals and the other radio systems signals simultaneously, because the RF-unit cannot independently receive each dispersed OFDM subcarrier. To keep a communication quality in WNC-OFDM radio link, it is important to comprehend the influence from undesired other radio system signals.

We evaluated the influence from the other radio systems in WNC-OFDM system with developed experimental equipment and computer simulations [1]. Bit error ratio (BER) vs desired signal power to undesired signal power ratio (DUR) was evaluated. The trend of the influence in WNC-OFDM system was different from Gaussian type interference environment in usual radio systems. Analysis and verification of the difference of performances had been needed, but had been set as future work in previous paper. In this paper, we conducted theoretical analysis in order to confirm the evaluated characteristic of influence from undesired CW and synchronous OFDM signal, which is different from characteristic of influence from general Gaussian noise.

This paper describes the behavior of influences of signal interference from other radio system signals with the WNC-OFDM system. Section 2 presents the detailed explanation of influences on simultaneous reception in WNC-OFDM system. Structure of WNC-OFDM experimental equipment and set-up of experiments are described in Section 3. Section 4 shows analysis results of the influence. Section 5 presents validity of the interference characters observed in the previous evaluation. And the conclusions is shown in Section 6.

2. INFLUENCE OF SIMULATONEOUS RECEPTION IN WNC-OFDM

The signal interference from other radio systems in usual radio systems is represented by adjacent channel interference. The method for the avoidance of adjacent channel interference is shown in Fig. 2. It consists of a baseband band-pass filter to adjust a signal bandwidth and a certain width of guard-band to suppress interference at transition band of the band-pass filter.

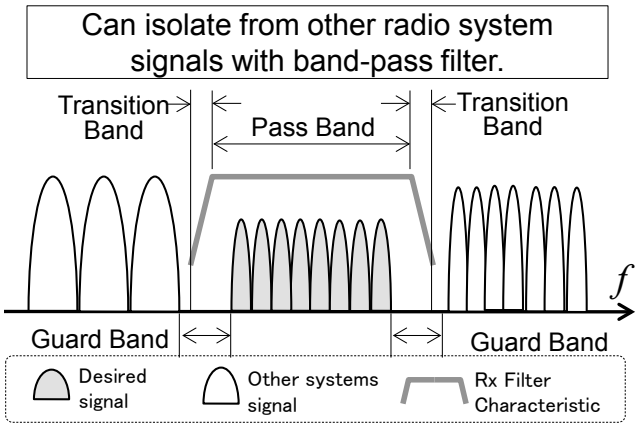


Fig. 2. Reception signals with usual radio systems

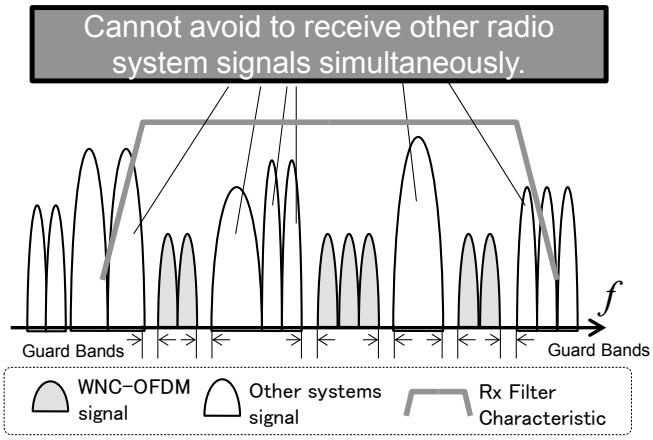


Fig. 3. Reception signals with WNC-OFDM systems

However, the signal interference in WNC-OFDM system is different from it in the usual radio systems. Fig. 3 shows received signals in WNC-OFDM systems. WNC-OFDM receiver receives both desired signals and other radio systems signals simultaneously with the same RF-unit. This situation is unavoidable, because band-pass filters for each WNC-OFDM signal, which are located dispersed and narrow frequency bands, cannot be implemented independently. In addition, since a bandwidth of each unused frequency band is very narrow, the bands cannot be utilized effectively if guard-bands with sufficient width are required for each band. That is, WNC-OFDM signals are affected by interferences from signals of the other radio systems which are received in the same RF-unit. This point is crucial difference between WNC-OFDM system and a conventional radio systems. When a total received power of other radio systems is relevant high, saturation of the analog to digital (A/D) converter and/or nonlinear distortion of the low noise amplifier (LNA) occurs. LNA distortion causes not only the signal interferences from adjacent wireless systems but also the inter carrier interference (ICI) within a

band. In addition, saturation of the analog to digital (A/D) converter generates quantization noise. Even when the total received power is low, adjacent channel interference occurs in baseband because the most of the other radio system signals are not orthogonal to WNC-OFDM signals.

The signal interference causes the degradation of communication quality in WNC-OFDM systems. To solve the issue, we must comprehend the behavior influence of signal interference from other radio systems in WNC-OFDM system.

3. EXPERIMENTAL ENVIRONMENT

In order to evaluate the influence from other radio systems to the reception of WNC-OFDM, we had conducted experiments with developed equipment. This section describes structure of the developed experimental equipment and detailed set-up of the experiments[1].

3.1. Structure of Experimental Equipment

Fig. 4 depicts schematics of the developed WNC-OFDM experimental equipment. The equipment supports extremely wide bands, from 170 MHz to 1GHz, total 830 MHz. For supporting such the wide bandwidth, we have employed divided and plural small RF-units. By employing the architecture, the hardware requirements, represented by extremely high-end wideband single RF and analog baseband circuits, are relaxed and possibility for realization of hardware increases. Concretely, the developed equipment employs four RF-units. All RF-units use the same one common intermediate frequency (IF) oscillator and all RF local oscillators use a common reference oscillator. Owing to the commonalized oscillations, frequency synchronization between all RF-units can be achieved and we have also shown that the negative effects caused by the inter-carrier interference between RF-units can be vanishingly reduced in. Baseband devices, e.g. A/D converter, D/A converter IFFT, FFT, are drove by 122.88 MHz sampling clock. Actually available bandwidth is limited to 90 MHz in order to avoid aliasing. The bandwidth of BPF implemented in analog circuit is also set to 90 MHz. The center frequencies for each RF-units can be changed

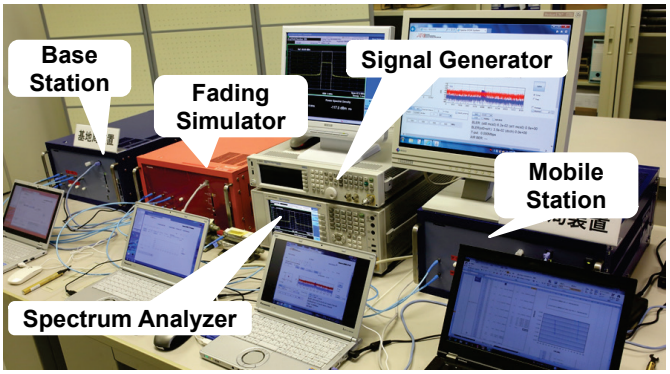


Fig. 4. External View of Experimental Environment

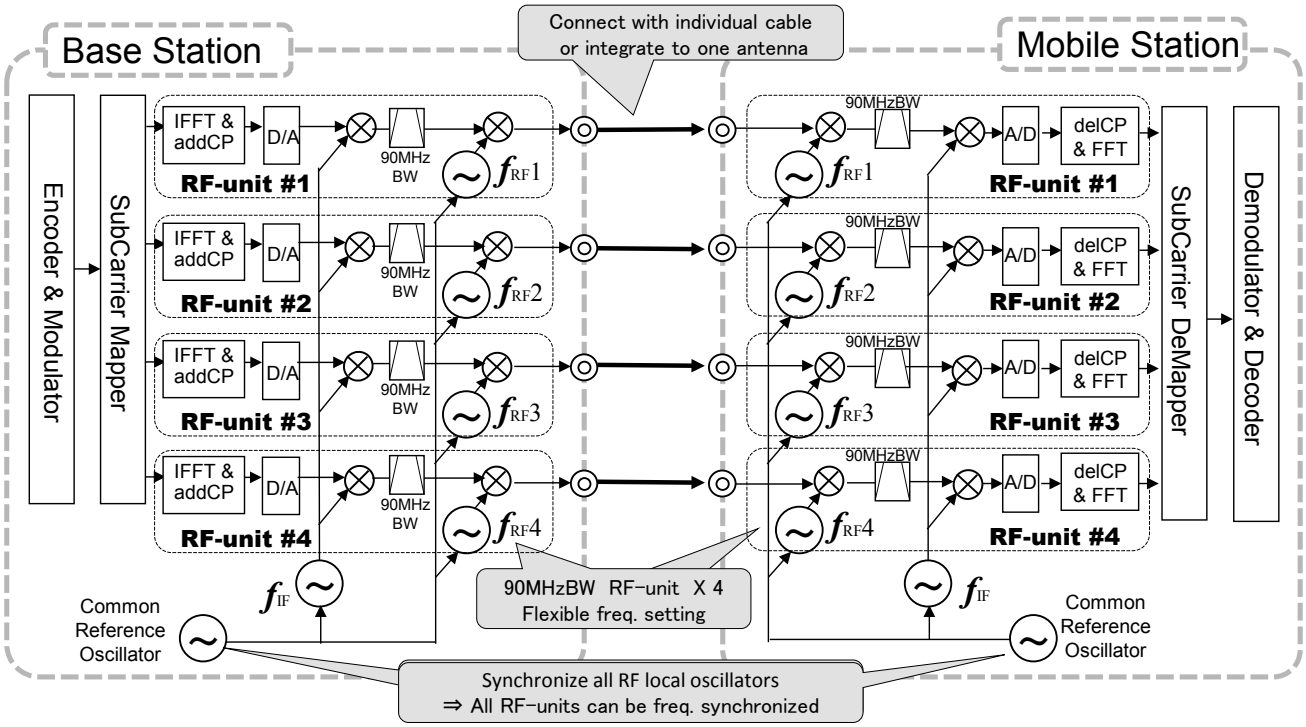


Fig. 5. Block diagram of experimental equipment (downlink part)

Table 1. Specification of signals for evalations

			Signal Format	Band width	Synchro-nization between desired signal	Generated by
Desired Signal	WNC-OFDM		Based on 3GPP-LTE Rel.8 downlink, 15kHz SC spacing, QPSK, No FEC,	9MHz (600 SCs)	-	WNC-OFDM Equipment RF-unit #1
Undesired Signal	OFDM	*Synchro nous*			Synchronous	WNC-OFDM Equipment RF-unit #2
		Asynchr onous			Asynchronous (different symbol length and timing)	Vector signal generator
	CW		Continuous wave	-	-	

flexibly and independently so as to cover the frequency band demanding allocation of WNC-OFDM subcarriers. Time domain windowing function is implemented to the equipment for the sake of out of band leakage power suppression in the transmitter. In addition, the basic parameter of the transmitted OFDM signal is set to the specification of 3GPP LTE Rel.8 [7]. That is, the subcarrier spacing is 15 kHz and specified modulation and coding schemes can be generated in the transmitter and can be demodulated and decoded.

3.2. Set-up of Experiments

In order to evaluate the influence in various scenarios, various test cases, listed in Table 1, are conducted. As the signals assuming other radio systems, synchronous OFDM, asynchronous OFDM, and continuous wave (CW) could be selected. These signals, except for the desired WNC-OFDM signal, are all defined as "undesired signal" in following description. External view of the experiment is shown in Fig. 5 and the its detailed connection diagram is described in Fig. 6. The experiment scenario can be controlled by settings of the base station, the fading simulator, vector signal generator, and step attenuators, respectively shown in Fig. 6. In the test case with undesired synchronous OFDM signal, the undesired signal is generated by different RF-units from the unit generating the desired WNC-OFDM signal because they can be synchronized. Frequency of the synchronous OFDM signal generated by RF-unit #2 can be detuned by frequency shift function of fading simulator. In other test cases, the undesired signals are added from external vector signal generator. Desired signal power to undesired signal power ratio (DUR) can be controlled by step attenuators. In all evaluations, external white Gaussian noise generator were not employed for the sake of sufficiently high signal to noise ratio (SNR), thereby it can be evaluate the pure influence of undesired signal. Frequency separation between desired signal and undesired signal is defined as Fig. 7. Channel characteristic is set to AWGN or pure Doppler (frequency shift) in this experimentation.

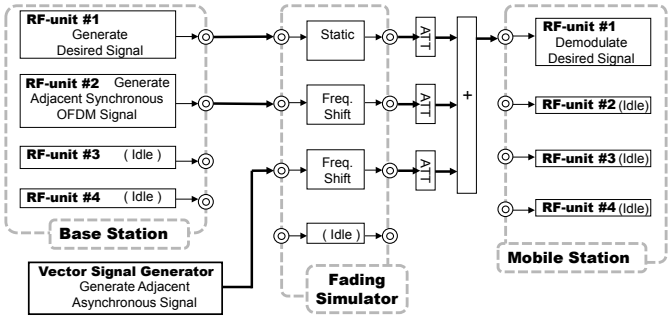


Fig. 6. Block diagram of experimental environment

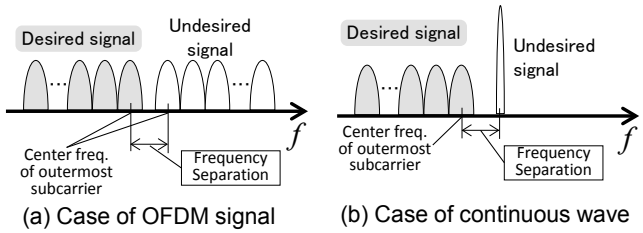


Fig. 7. Definition of frequency separation in the evaluation

4. PERFORMANCE EVALUATION AND ANALYSIS

This section describes quantitative evaluation results under the influence of various undesired signals with both the experimental equipment and computer simulations executed in previous research, which are need as targets of following theoretical analysis. This section also describes additional verification for the difference between the experimental results and simulation results.

For simplification, the computer simulations assume ideal timing synchronization and channel estimation.

4.1. Dependency on Frequency Separation

Fig. 8 shows BER performance of experimental results focused on effects of frequency separation between desired and undesired signal in AWGN channel. The types of the undesired signals are set to CW or OFDM signal and they are generated synchronous or asynchronous to the desired signal. In the figure, dependency on the frequency separation was observed clearly when undesired signal was synchronous to desired signal. The dependency can be explained as follows. When the frequency spacing is integral multiple of 15 kHz, (subcarrier spacing of desired signal, f_0) ICI from undesired signal is not generated because of the orthogonality. Meanwhile, the orthogonality is maximally collapsed and considerable ICI is generated when the frequency spacing has offset of 7.5 kHz (half of subcarrier spacing). In asynchronous case, ICI is constantly generated because of the non-cyclic characteristics of the undesired signal in the FFT interval. In the following experiments, the frequency separations were set from 15

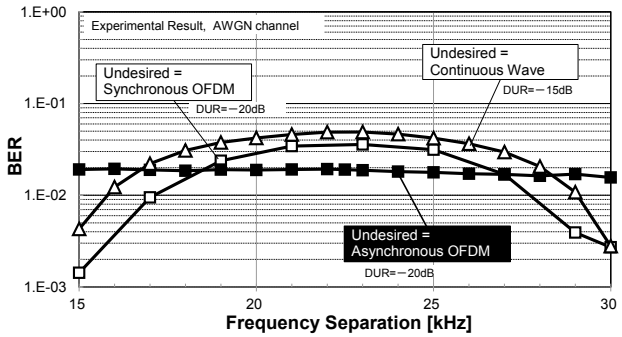


Fig. 8. BER vs frequency separation performances with various undesired signal (experimental result)

kHz to 22.5 kHz for synchronous case, and set to 15 kHz for asynchronous case by considering these results.

4.2. Influence from Synchronous OFDM Signal

Fig. 9 describes BER vs DUR performances with adjacent undesired synchronous OFDM signal obtained from experiments and computer simulations, respectively, in previous research [1]. Note that the simulation results did not take the effect of quantization noise into account. It is also noteworthy that the results themselves are obtained in previous research [1]. Indexes "Δ" denote "frequency separation" based on the definition in Fig. 7. For frequency separation 22.5 kHz, experimental results and simulation results were close. Both graphs had the same straight shape and small slopes indicating that about ten times BER improvements are obtained by increasing 10 dB DUR, and rapidly fadeout less than 1e-3. This slope was apparently different from general additive Gaussian noise environment, where its horizontal axis is SNR. The difference is theoretically analyzed in chapter 5.

It is also remarkable that when the frequency separation closes to 15 kHz, i.e. the situation with near orthogonality, the difference between simulation and experiments becomes larger. Actually, no bit error was observed for 15 kHz separation in the simulation and graph could not be drawn in Fig. 9. On the other hand, bit error remains in experiment even for 15 kHz. The cause of this remaining error can be considered as the quantization noise generated by the saturation of the A/D converter. In order to verify the hypothesis, we have conducted computer simulation with the functions of auto gain control (AGC) and generation of the quantization noise of the A/D converter. Results are shown in Fig. 10 with experimental results. The results of the simulations and experiments become very close. Hence, it can be confirmed that the dominant cause of the performance difference between experimentation and simulation shown in Fig. 9 is quantization noise generated at the A/D converter.

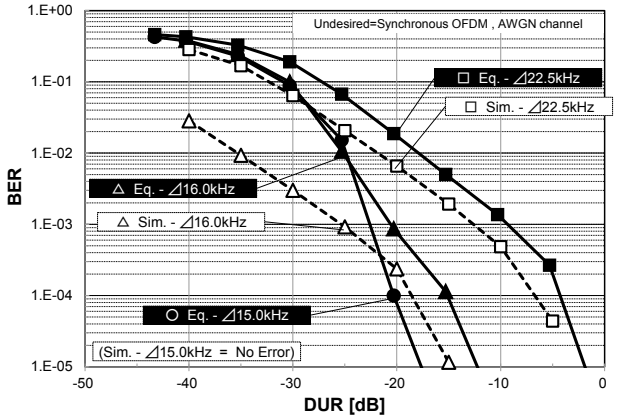


Fig. 9. BER vs DUR performance with undesired synchronous OFDM signal in various frequency separation (simulation result without A/D and experimental result, AWGN channel)

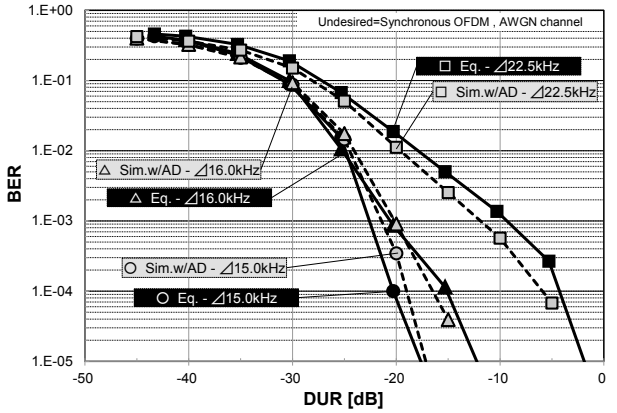


Fig. 10. BER vs DUR performance with undesired synchronous OFDM signal in various frequency separation (simulation result with A/D and experimental result, AWGN channel)

4.3. Influence from Continuous Wave

Fig. 11 describes BER vs DUR performances with adjacent undesired CW signal with various frequency separation obtained from experiments and computer simulations, in previous research[1]. Note that the simulation results do not take the effect of quantization noise into account. For frequency separation from 16 kHz to 22.5 kHz, results of experiments and simulations are very close. Both graphs have the same straight shape and small slopes indicating that about ten times BER improvements are obtained by increasing 20 dB DUR, and rapidly fadeout less than 1e-3. This slope was apparently different from general additive Gaussian noise environment, where its horizontal axis is SNR. and also different from the results for undesired OFDM signal shown in Fig. 9. The difference is also theoretically analyzed in chapter 5.

The difference between simulations and experiments has been observed. In the same manner as the previous section, we have conducted computer simulation with the

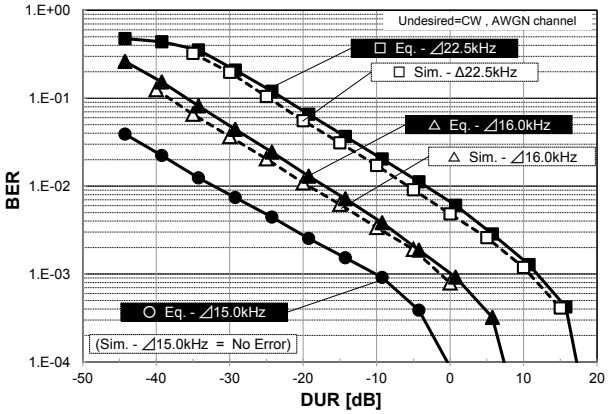


Fig. 11. BER vs DUR performance with undesired CW signal in various frequency separation (simulation result without A/D and experimental result, AWGN channel)

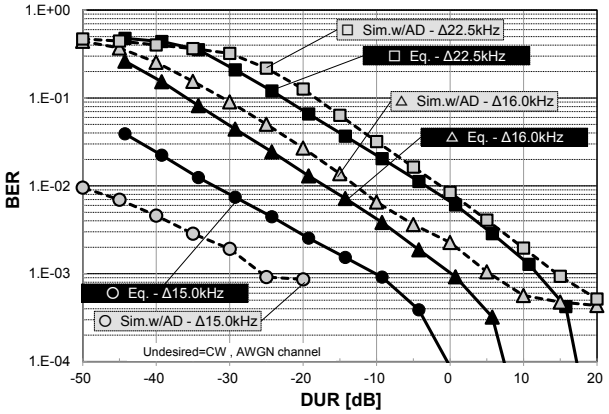


Fig. 12. BER vs DUR performance with undesired CW signal in various frequency separation (simulation result with A/D and experimental result, AWGN channel)

functions of auto gain control (AGC) and generation of the quantization noise of the A/D converter, and the results are shown in Fig. 12 with experimental results. The simulation result for 15.0 kHz frequency separation gets closer to the experimental result. However, the difference is still observed. As the causes of remaining difference, frequency error between the equipment and signal generator and un-stability of timing tracking on the equipment are considered.

5. THEORETICAL ANALYSIS OF INTERFERENCE FROM UNDESIRED SIGNAL

As shown in section 4.2 (environment with undesired synchronous OFDM) and 4.3(environment with undesired CW), BER vs DUR graphs have characteristics as follows :

- straight shape
- small slope (10X BER/20 dB DUR : CW)
  (10X BER/10 dB DUR : Sync. OFDM)
- fall steep at the region less than around 1e-3.

It was considered that this differences were caused by difference of distribution shape of interference from each undesired signal. Analysis and verification of the difference of performances were needed, but had been set as future work in previous paper. In this chapter, such the behavior is theoretically analyzed in order to comprehend the characteristics more clearly.

5.1. Histogram of Demodulated Signal

For the sake of observation for received signal distribution caused by interferences in pure and ideal environment, we executed following computer simulations.

In the simulation, received signal after FFT for all subcarriers corresponding to desired OFDM signal were recorded and histograms of their real components were made. Histograms with additive white Gaussian noise (AWGN), with undesired OFDM signal and with undesired CW are shown in Fig. 14, Fig. 15, and Fig. 16, respectively. These figures have three axis described as follows:

(1) *f*-axis : denotes subcarrier index
(2) *x*-axis : denotes magnitude of each subcarrier *x*
(3) *h*-axis : denotes histogram of *x*.

Center point of *x*-axis marked "0" denotes origin of *x*-axis (point of *x=0*). A straight dashed line which intersects *x*-axis at the origin and parallels *f*-axis is a threshold point for sign discrimination for demodulating QPSK signal of all desired OFDM subcarriers. Hereafter, this line is called "discrimination line". When distribution of *x* spreads beyond the discrimination line, transmission bit error occurs. It is noteworthy that although the analysis only deals with real part of the subcarrier, it is sufficient to analyze the behavior because the distribution characteristic of the imaginary part is also the same.

As shown in Fig. 14, when white Gaussian noise is added, Gaussian shape magnitude distribution is observed in each subcarrier and that is equivalent through all subcarriers of desired OFDM signal. However, as shown in Figs. 15 and 16, under the environment with adjacent undesired signal (CW or synchronous OFDM), different level magnitude distributions depending on position of subcarriers are observed.

In the simulation with undesired OFDM signal (Fig. 15), both desired and undesired WNC-OFDM signals consists of 600 subcarriers and QPSK modulation is employed. In addition, additive noise free static channel environment is assumed. In Fig.15, desired WNC-OFDM subcarriers are displayed from subcarrier number (SC#) 305 to SC# 600 on *f*-axis, and undesired synchronous OFDM subcarriers are allocated on residual part on *f*-axis. The outermost subcarrier of each subcarrier blocks are allocated apart 1.5*fo* (22.5 kHz). Distribution of *x* looks closed to Gaussian shaped and the magnitude distributions of each subcarrier is different according to subcarrier index, i.e.

frequency. Concretely, subcarriers close to undesired signal tend to be influenced by the higher level interference. In addition, it can be observed that the number of subcarriers which yields bit error increase as DUR got worse. Hence, the varying number of subcarriers that yield bit error by increasing undesired signal level is smaller than that in AWGN case where the noise level of each subcarrier is almost equivalent. This fact causes the results where the slope of BER vs DUR graph is smaller.

Fig. 16 shows results of simulation with undesired CW. In Fig.16, desired WNC-OFDM subcarriers are displayed from SC# 335 to SC# 600 on *f*-axis, and undesired CW is allocated apart 1.5f_o (22.5 kHz) from the outermost subcarrier (SC#600) of the desired WNC-OFDM signal. Similar to undesired OFDM signal case, higher magnitude distributions are observed for subcarriers closer to undesired signal, and the number of subcarriers yields bit error increase as DUR got worse. Then, the varying number of subcarriers that yield bit error by increasing undesired signal level is smaller than that in AWGN case. And this also causes the results where the slope of the graph is smaller.

In addition, it was observed that the distribution of *x* in Fig. 16 had quite strange shape, like a letter "M". The shape can be observed clearly in closed up figure, Fig. 17. This "M" shaped distribution has no side lobe as Gaussian distribution, thus no error occurs when interference magnitude is smaller than that of desired signal. On the other hand, suddenly error occurs when interference magnitude exceeds magnitude of desired signal. It can be guessed that the rapid growth of the steep in the region, where BER less than around 1e-3, is caused by that issue.

5.2. Theoretical Analysis for Interference from Undesired CW signal

In order to confirm validity for the interference characteristics observed in the simulation, theoretical analysis by calculating interference signal shape, distribution, and bit error ratio due to the interference has been made. Following derivations are only for undesired CW case and those for undesired synchronous OFDM case is further work. In undesired synchronous OFDM case, distribution of the interference and bit error ratio can be approximated with integration of interferences from all undesired OFDM subcarriers. In addition, the interference from one undesired subcarrier can be approximated as that from an undesired CW.

At first, CW component of FFT output is calculated. The down converted CW signal to base band are described as,

$$U(t) = A_u\{(\cos(2\pi f_\delta t + \varphi_\delta)) + j(\sin(2\pi f_\delta t + \varphi_\delta))\} \quad (1)$$

where A_u, f_δ, and φ_δ denote amplitude, frequency, and phase of the CW, respectively.

n-th subcarrier component of FFT output, *F(n)*, corresponds to CW signal (1) is calculated as following, where *N* is number of FFT points, f_o is subcarrier spacing of desired OFDM signal which equals to *1/T*, where T is the OFDM symbol duration.

$$F(n) = \int_0^T U(t)\exp(-j2\pi n f_0 t)\,dt \quad (2)$$

$$= \frac{A_u}{2}\int_0^T \left[\begin{matrix}\{\cos(2\pi(f_\delta + nf_0)t + \varphi_\delta) + \cos(2\pi(f_\delta - nf_0)t + \varphi_\delta)\} \\ \{-\cos(2\pi(f_\delta + nf_0)t + \varphi_\delta) + \cos(2\pi(f_\delta - nf_0)t + \varphi_\delta)\}\end{matrix} \right. \left. \begin{matrix}+j\{\sin(2\pi(f_\delta + nf_0)t + \varphi_\delta) + \sin(2\pi(f_\delta - nf_0)t + \varphi_\delta)\} \\ \{-\sin(2\pi(f_\delta + nf_0)t + \varphi_\delta) - \sin(2\pi(f_\delta - nf_0)t + \varphi_\delta)\}\end{matrix}\right] dt \quad (3)$$

$$= A_u\int_0^T \left\{\begin{matrix}\cos(2\pi(f_\delta - nf_0)t + \varphi_\delta) \\ +j\sin(2\pi(f_\delta - nf_0)t + \varphi_\delta)\end{matrix}\right\} dt \quad (4)$$

$$= \frac{A_u}{2\pi(f_\delta - nf_0)}\left[\begin{matrix}\sin(2\pi(f_\delta - nf_0)t + \varphi_\delta) \\ -j\cos(2\pi(f_\delta - nf_0)t + \varphi_\delta)\end{matrix}\right]_0^T \quad (5)$$

$$= \frac{A_u}{2\pi(f_\delta - nf_0)}\left\{\begin{matrix}\sin(2\pi f_\delta N + \varphi_\delta) - \sin\varphi_\delta \\ -j\cos(2\pi f_\delta N + \varphi_\delta) + j\cos\varphi_\delta\end{matrix}\right\} \quad (6)$$

$$\because 2\pi n f_0 T = 2\pi \times integer$$

This value denotes the interference affecting n-th subcarrier. When the frequency of CW f_δ is set to integer multiple of f_o, (6) equals to 0. It means the orthogonal situation. When f_δ is set to $(m+1/2)f_o$, where *m* is integer, (6) generates maximal magnitude written as (7). It means the lowest orthogonality situation.

$$F_m = \frac{A_u(-\sin\varphi_\delta + jcos\,\varphi_\delta)}{\pi f_0\left(m + \frac{1}{2} - n\right)} \quad (7)$$

The value (7) increases when A_u gets larger, i.e. DUR become worse, or focusing subcarrier frequency nf_o is set closer to f_δ.

Next, probability density function (PDF) of real part of (7) is calculated as *q(S)* as written in (10). $P(G^{-1}(S)) = P(\varphi\delta)$ denotes probability density function of $\varphi\delta$, and its value is uniformly $1/2\pi$.

$$S = Re(F_m) = \frac{A_u}{\pi(f_\delta - nf_0)}(-\sin\varphi_\delta) = G(\varphi_\delta) \quad (8)$$

$$\varphi_\delta = G^{-1}(S) = \sin^{-1}\left(\frac{\pi(nf_0 - f_\delta)}{A_u}S\right) \quad (9)$$

$$\begin{aligned} q(S) &= P(G^{-1}(S))\frac{d}{ds}G^{-1}(S) \\ &= \frac{1}{2\pi}\frac{d}{ds}\left\{\sin^{-1}\left(\frac{\pi(nf_0 - f_\delta)}{A_u}S\right)\right\} \\ &= \frac{nf_0 - f_\delta}{2A_u}\frac{1}{\sqrt{1 - \left(\frac{\pi(nf_0 - f_\delta)}{A_u}S\right)^2}} \end{aligned} \quad (10)$$

$$\frac{-A_u}{\pi(nf_0 - f_\delta)} < S < \frac{A_u}{\pi(nf_0 - f_\delta)}$$

Fig. 19 shows the graph of *q(S)* and it also can be observed the shape is like a letter "M", as observed in Fig. 17. From above analysis, it was proved that distribution of the interference from undesired CW signal had the "M" shape. In addition, distribution of the interference in undesired OFDM case can be considered as sum of the "M" shaped distributions for all undesired OFDM subcarriers, and can be considered to has characteristics of both white Gaussian noise and CW.

At last, approximated BER for undesired CW signal case is calculated. When φ_δ in (7) is set to -π/2, (7) gives the largest magnitude E(n) expressed as (11). This value is the curve of "Interference Envelope" drawn in Fig. 19.

$$E(n) = \frac{A_u}{2\pi f_0\left(m + \frac{1}{2} - n\right)} \tag{11}$$

Range for number of desired OFDM subcarriers suffer bit errors is given as (12), i.e. from N to cross point of the discrimination line and the interference envelope line(11), i.e. *nx*.

$$n_x = \left\lceil m + \frac{1}{2} - \frac{A_u}{D_0 \pi f_0} \right\rceil \le n \le N \tag{12}$$

BER is calculated by sum of value of (11) exceeding the discrimination line. PDF of the distribution is

$$BER = \frac{1}{N}\sum_{n_x}^{N}(E(n) - D_0)\frac{1}{2E(n)} \tag{13}$$

$$= \frac{1}{N}\sum_{n_x}^{N}\left(\frac{1}{2} - \frac{D_0\pi f_0}{2A_u}\left(m + \tfrac{1}{2} - n\right)\right) \tag{14}$$

$$= \left(\frac{A_u}{D_0\pi f_0}\right)\frac{1}{4N} + \left(\frac{1}{2} + \frac{1-2M}{4N}\right) + \left(\frac{D_0\pi f_0}{A_u}\right)\left(\frac{M^2 - 2M}{4N} + \frac{N+1-2M}{4N}\right) \tag{15}$$

$$where\ M = m + \tfrac{1}{2} - n$$

approximated by rectangular shape in following equations.

Finally the BER (15) can be approximated as (16), since the second term is negligible when M is close to N, and the third term is negligible when DUR=D_o/A_u is sufficiently low.

$$\approx \left(\frac{A_u}{D_0\pi f_0}\right)\frac{1}{4N} \tag{16}$$

Equation (16) proves that BER is inversely proportional to DUR, i.e. BER increases 10 times when DUR degrades 20 dB. Above analysis showed the reason why BER vs DUR graph in undesired CW case had straight shape and small slope (10X BER/20 dB DUR).

5.3. Summary of analyses for interference from various undesired signals

The results of above analyses showed that the reason of for interference from various undesired signals had the each characteristic shape of BER vs DUR graph. Conclusion of above analyses is summarized in Table 2.

6. CONCLUSIONS

Interference from other various radio systems in WNC-OFDM system had been evaluated by both experiment with implemented equipment and computer simulations. The results showed bit error ratio performances were quite difference compared to the performance in Gaussian noise environment. We conducted theoretical analysis and confirmed validity of the interference characters in WNC-OFDM system observed in the previous evaluation.

The knowledge of characteristics of interferences is valuable for designing the link adaptation algorithm based on interference in WNC-OFDM system and consideration of the employing interference mitigation technologies in the receiver.

ACKNOWLEDGMENT

This research was performed under research contract of “Research and Development on Wideband Non-Contiguous OFDM”, for the Ministry of Internal Affairs and Communications, Japan.

REFERENCES

[1] K. Kosaka, K. Takakusaki, I. Kanno, A. Hasegawa, H. Shinbo, and Y. Takeuchi, "Evaluation of Influence by Simultaneous Reception of Other Radio Systems in Wideband NC-OFDM," Proc. IEEE APWiMob 2014, Aug. 2014. (*Accepted and to be Submitted*)

[2] K. Horihata, K. Takakusaki, A. Hasegawa, T. Shibata, and M. Ohashi, “Measurement of Radio Waves in the Air for Wideband Non-Contiguous OFDM Technolog” IEICE General Conference 2013, B-17-2, Mar.2013.

[3] R. Rajbanshi, A. M. Wyglinski, and G. J. Minden, “An efficient implementation of NC-OFDM transceivers for cognitive radios,”CROWNCOM 2006, June 2006.

[4] J. D. Poston and W. D. Horne, “Discontiguous OFDM considerations for dynamic spectrum access in idle TV channels,”DySPAN 2005, pp. 607-610, Nov. 2005.

[5] J. D. Guffey, A. M. Wyglinski, and G. J. Minden, “Agile radio implementation of OFDM physical layer for dynamic spectrum access research,” GLOBECOM 2007, pp. 4051-4055, Nov. 2007.

[6] K. Takakusaki, A. Hasegawa, and T. Shibata, "Research on Wideband Non-Contiguous OFDM Technology," IEICE technical report, SR2013-16, May 2013.

[7] 3GPP, TS 36.211 (v8.9.0), “Evolved Universal Terrestrial Radio Access (E-UTRA); physical channels and modulation (Release 8),” Dec. 2009.

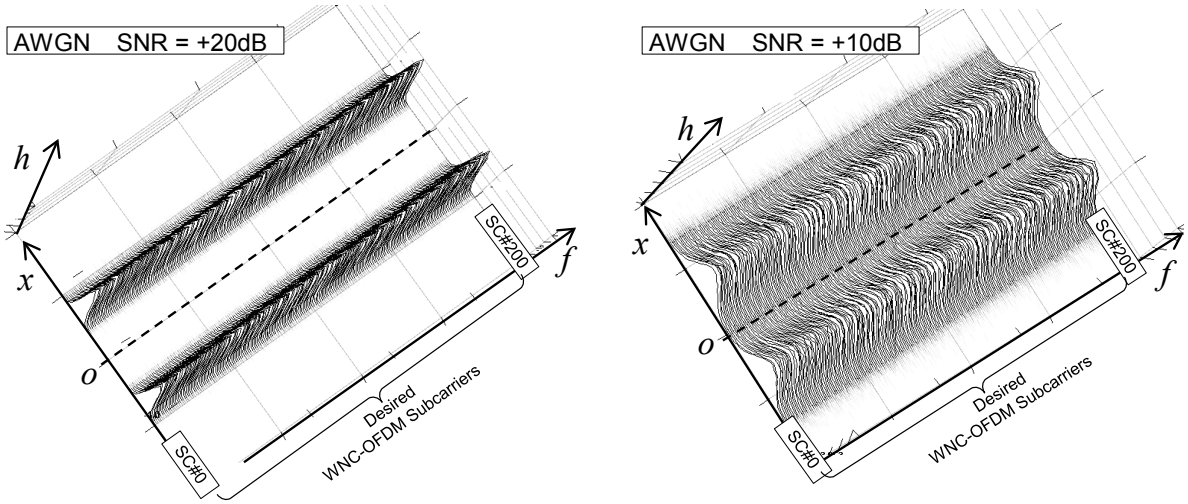


Fig. 14. Histograms of demodulated signals with AWGN

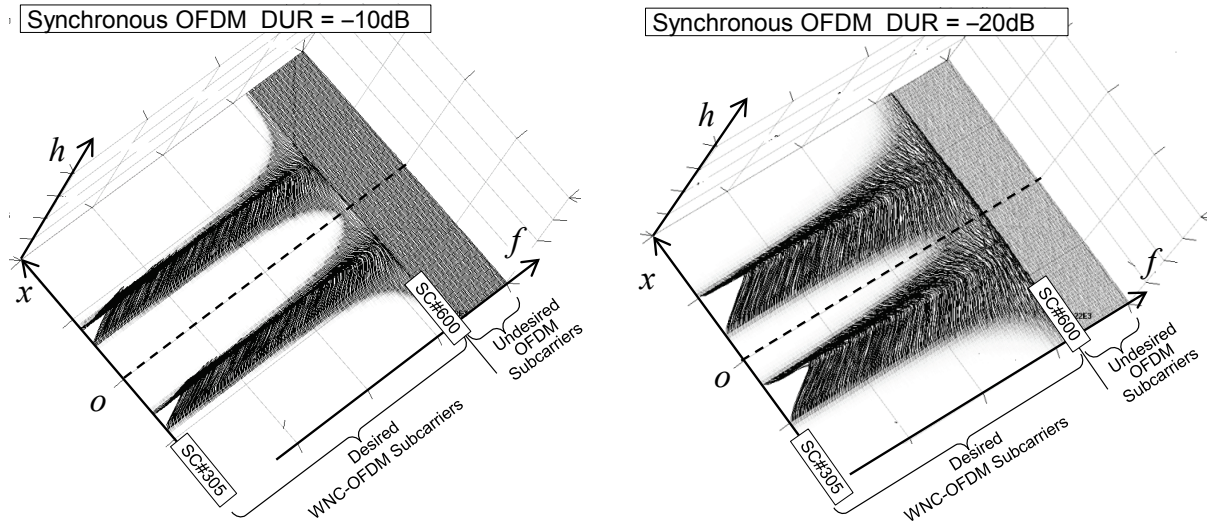


Fig. 15 Histograms of demodulated signals with undesired synchronous OFDM signal

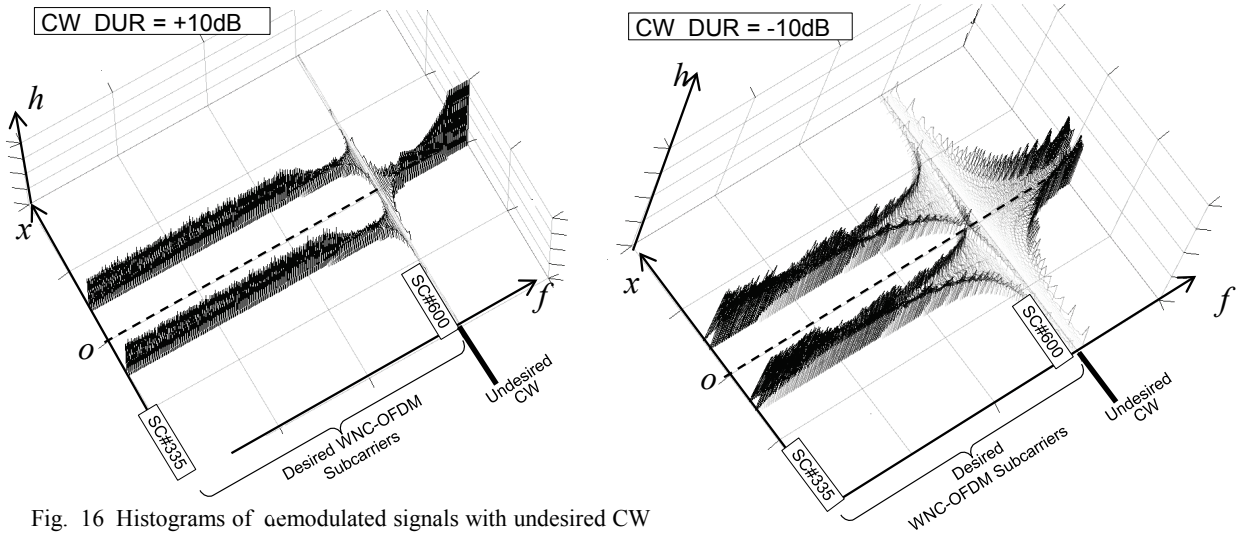


Fig. 16 Histograms of demodulated signals with undesired CW

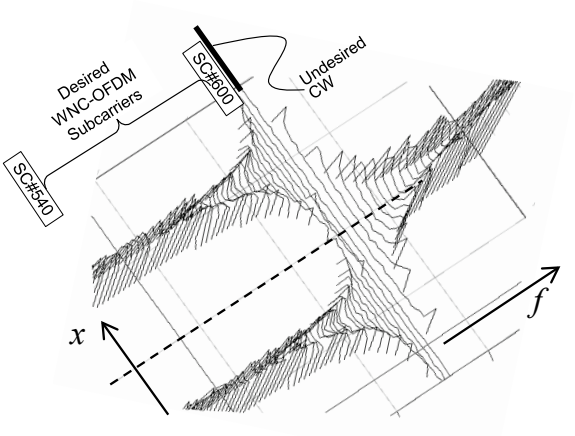


Fig. 17 Close up of Histograms of demodulated signals with undesired CW, DUR=+10dB

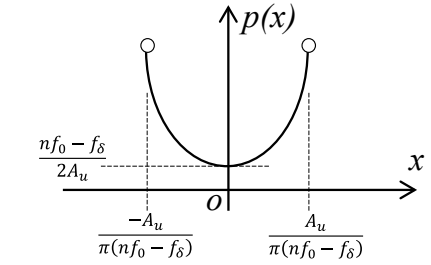


Fig. 18 Curve of the probability density function of interference from undesired CW signal

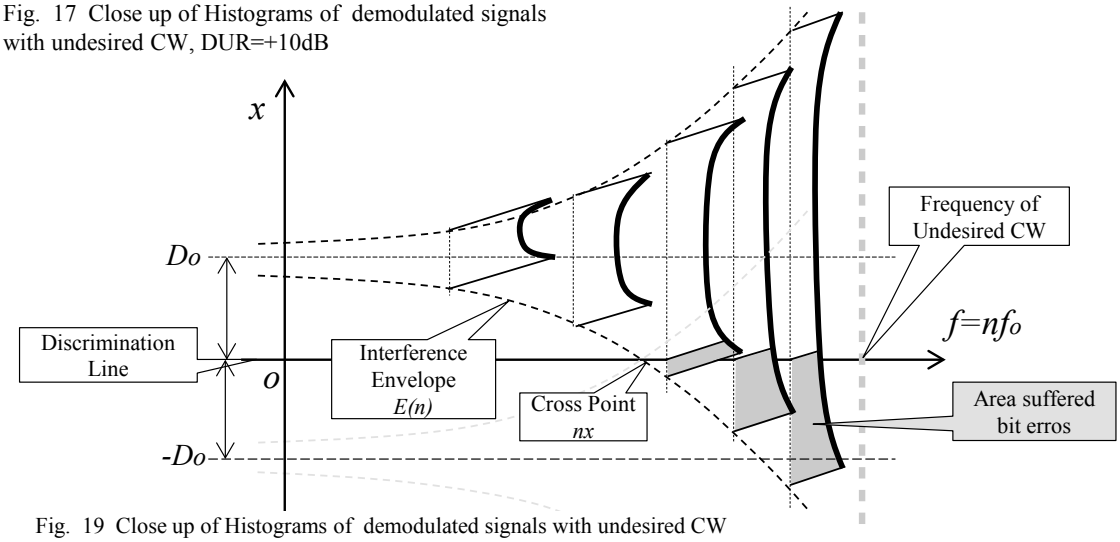


Fig. 19 Close up of Histograms of demodulated signals with undesired CW

Table 2. Comparison of influences from various types of signals

		Additive White Gaussian Noise (AWGN)	OFDM	Continuous Wave (CW)
Uniformity of Interference		Uniform additive noise - All SCs are always interfered equally	Unbalanced Interference (Larger interference for SCs close to undesired signal) - Number of interfered SCs increases as undesired signal power increases	
Magnitude Distribution of Interference		Gaussian	Like Gaussian	"M" shaped
Bit Error Occurrence at One SC of desired signal	High DUR	p(x) *A small amount of error occurs even in high DUR* –Do O +Do x	Bit error rate can be approximated with integration of all interferences from all undesired OFDM SCs. the interference from one undesired SC can be approximated as interference from an undesired CW.	p(x) *No error occurs when interference envelope is smaller than Do* –Do O +Do x
		p(x) –Do O +Do x		p(x) *Suddenly error occurs when interference envelope exceeds Do* –Do O +Do x
	Low DUR	*Error increases rapidly due to mountain shaped distribution* –Do O +Do x		*Error increases slowly due to flat distribution of interference* –Do O +Do x
Slope of BER vs DUR graph		Denoted by Error Function	BER 10 times / DUR 10dB	BER 10 times / DUR 20dB

x = Magnitude of demodulated (FFT output) signal
$p(x)$ = Probability density function of x
D_o = Constellation magnitude of desired signal at baseband
O = Origin of x, and threshold point for sign discrimination

MODEL-BASED TESTING FOR SCA CONFORMANCE TESTING

Julien BOTELLA[1], Eddie JAFFUEL[2], Bruno LEGEARD[1,3], Fabien PEUREUX[1,3]
[1] Smartesting R&D Center, France,
{julien.botella, bruno.legeard, fabien.peureux}@smartesting.com;
[2] eConsult, France, eddie.jaffuel@econsult.fr;
[3] Institut FEMTO-ST - UMR CNRS 6174, University of Franche-Comté, France,
{bruno.legeard, fabien.peureux}@femto-st.fr

ABSTRACT

The Software Communications Architecture (SCA) is a software architecture provided and published by the JTNC (Join Tactical Networking Center). Facing the multiplicity of the waveforms and the diversity of the platform architectures and form factors, the original aims of the SCA are to facilitate the waveform development in terms of portability and waveform deployments onto heterogeneous SDR platforms. In this paper, we present an approach using Model-Based Testing (MBT) to ensure the conformance of a software radio platform to SCA requirements. In this approach, an MBT model is developed on the basis of SCA specifications, and conformance tests and scripts are generated and then run on the targeted software radio platform. This approach has been developed within a National Research Project called OSeP, with results regarding modeling for automated test generation for SCA conformance testing. The techniques involved in this project focus on functional requirements and automatically generate Java executable test scripts, which aim to evaluate the functional conformance of the software implementation with respect to their associated requirements.

Keywords: Software Communications Architecture (SCA), conformance testing, model-based testing, dynamic testing.

1. INTRODUCTION

Conformance testing is done to determine whether a system meets a specified standard. One key goal of conformance testing is to ensure interoperability between systems, on the basis of agreed norms and standards. Conformance tests are designed to concentrate on areas critical to interoperability, including testing the system reaction to erroneous behavior. One specific challenge in the area of conformance testing is the design of the right test suites: how can be designed the right tests? How can be agreed, at the level of standard working group committees, on the content of the conformance test suite? How the bidirectional traceability matrix between conformance tests and the standard can be developed and maintained when the specifications change?

In this paper, we provided first results on using Model-Based Testing (MBT) [1] from UML models [2] to evaluate the functional conformance of the software implementation with respect to the Software Communications Architecture (SCA) [3]. MBT refers to the processes and techniques for the automatic derivation of abstract test cases from abstract models, the generation of concrete tests from abstract tests, and the manual or automated execution of the resulting concrete test cases [4]. Compared with a manual design approach, MBT brings the following benefits:

- MBT Modeling is a process which fosters close communication of the stakeholders.
- The forced communication process builds up a common perception and understanding of the requirements in the given domain and helps to concentrate on areas critical to interoperability.
- Reducing information and emphasizing different perspectives in the conformance MBT model makes it easier to master tradeoff and balance of the generated conformance test suite.
- It helps to reduce maintenance costs due to the "single-point" information in the MBT model and the "by-design" traceability between the model and standard.

MBT is an increasingly widely-used approach that has gained much interest in recent years. It is today getting closer and closer to an industrial reality: theoretical concepts (and associated tools) to derive test cases from specifications are indeed now mature enough to be applied in many application areas [5][6]. MBT is already in used for conformance testing in several areas of industry. We can mention for example:

- The ETSI conformance testing process – see [7].
- GlobalPlatform compliance program – see [8]. In section 2, we present the lessons learnt from applying MBT conformance testing for the compliance program of GlobalPlatform 2.2 card specification.

Therefore, our main goal was to evaluate the technical feasibility of applying a Model-Based Testing process for SCA conformance testing. This proof of concept has been done in the context of a National Research Project called OSeP[1] in partnership with DGA MI (French DoD).

The rest of the paper is organized as follows: Section 2 provides a short description of the MBT conformance testing process applied to Global Platform and summarizes the lessons learnt in this context. Section 3 gives a detailed overview of the application of this MBT process to a subset of SCA 2.2.2 specifications and summarizes the lessons learnt from our experiments. We conclude our paper in Section 4 and propose some perspectives to this work.

2. RELATED MBT INDUSTRIAL EXPERIENCE: GLOBALPLATFORM COMPLIANCE PROGRAM

GlobalPlatform is a cross industry and not-for-profit association, which members are payment organizations such as American Express, MasterCard, or Visa International, telecom operators, like AT&T, France Telecom, NTT or Verizon and industrial leaders (AMD, Apple, Blackberry, Gemalto, Nokia, Samsung, etc.).
As shown in Figure 1, GlobalPlatform identifies, develops and publishes specifications facilitating secure and interoperable deployment and management of multiple embedded applications on secure chip technology. Its proven technical specifications are regarded as the international industry standard for building a trusted end-to-end solution serving multiple actors and supporting several business models.

Figure 2: GlobalPlatform Standard Presentation

[1] OSeP - On-line and off-line model based testing of Security Properties – Applications to Security Components and Software Radio – ANR Grant n° ANR-11-ASTR-00 2 – see http://osep.univ-fcomte.fr/ (in French)

The specifications available provide the foundations for market convergence and innovative new cross-sector partnerships. The technology has been adopted globally across finance, mobile/telecom, government, healthcare, retail and transit sectors. Research conducted by Eurosmart confirmed that 2012 shipments of microcontroller smart secure devices (secure chips) is over 7 billion units, of which 2.6 billion units leverage GlobalPlatform technology.
For a standardization body like GlobalPlatform, the compliance program is a strategic mission (see Figure 2).

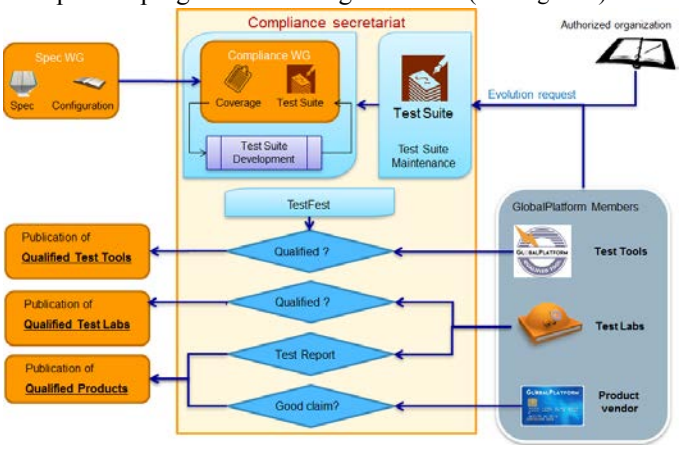


Figure 1: GlobalPlatform Certification Process

GlobalPlatform group has been using Model-Based Testing to produce its compliance test suites for more than 5 years. At GlobalPlatform, Model-Based Testing is therefore a key technology that supports the strategic conformance activity.
Figure 3 gives an overview of the Model-Based testing process to address the GlobalPlatform conformance issues. The process starts on the left at the textual requirements, from which a test designer team derive the Test Objective Charter and a UML test model. This model represents the expected behavior of the Application Protocol Data Unit (APDU) specified in the GlobalPlatform standard. A subset of UML, called UML4MBT [10], is used. It includes UML class diagrams, state machines and OCL [11] constraints to formalize the control points and observation points, the expected dynamic behavior described in the standard, the business entities associated with the test, and some data for the initial test configuration. Model elements such as transitions or decisions are linked to the requirements defined in the Test Objective Charter, in order to ensure bi-directional traceability between these requirements and the model, and later to the generated test cases and related test plan. Models are therefore precise and complete enough to allow automated derivation of tests from these models. This derivation is a fully automated process supported by the Smartesting *CertifyIt* testing tool [12], which generates abstract test cases (abstract because relying on the UML test model) to cover the items of the Test Objective Charter file.

Each generated test case is typically a sequence of APDUs, with input parameters and expected output values for each action. An adaptation layer can be used to link some abstract values from the model with some concrete test values. Such generated test sequences are similar to the high-level test sequences that would be designed manually in action-word testing [13]. They are therefore easily understood by humans, e.g., GlobalPlatform Compliance Testing Group, and complete enough to be delivered to be directly executed on a targeted system by a manual tester.

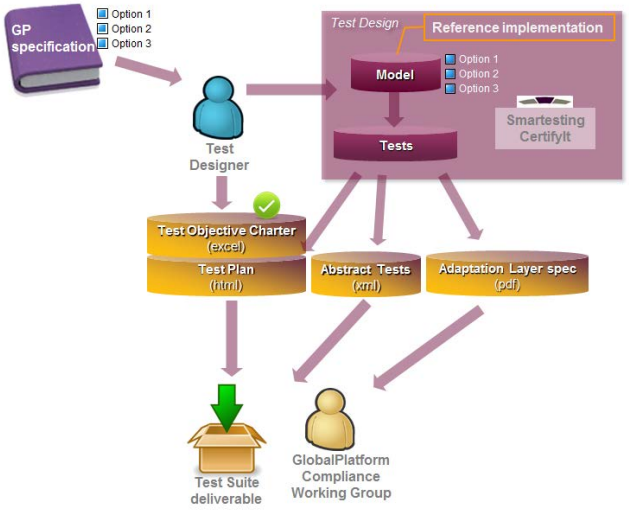


Figure 3: Model-based Compliance Test Suite

In this context, the major added value of the MBT process has been the following:

- It provides Test Suite for integration to the Product vendors in-house systems.
- It remains open to any Test Tools suppliers (let the market decide the best tools).
- It supports product variants or options (enabling to reuse all or some parts of the test model)
- It ensures and maintains the coherence between all deliverable assets of the testing process.
- The Model can be used as the unique reference implementation.

The GlobalPlatform Compliance Program has started in 2007. The metrics of the last GP Compliance Program in 2014 are the following (i.e. the previous versions of the Test Suites are not taken into account) : about 6 000 tests have been generated for 15 active Compliance Test Suites. On the basis of this success story [14], we decided to apply this MBT approach for SCA specifications conformance issues. The next section introduces this work and describes the obtained results.

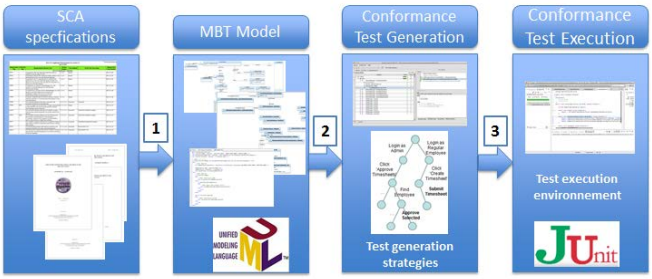


Figure 4: MBT Process for SCA Conformance Testing

3. EXPERIMENTS ON SCA 2.2 SPECIFICATIONS

The development of radio protocols, within Software Defined Radio (SDR) design context, requires the respect of the de facto Software Communication Architecture (SCA) standard [3]. To test SCA compliancy and interoperability between SDR platforms, we have studied the adaptation of the MBT approach introduced in the previous section. Figure 4 describes the overall MBT process that has been deployed on a subpart of SCA 2.2.2 specifications (functional requirements at the level of the SCA core framework). It is structured in three main steps:

1. Modeling for Test Generation from SCA specifications. From functional aspects of SCA 2.2.2, the MBT model is developed using the UML subset UML4MBT (in an eclipse-based modeling environment) and is checked for consistency. This MBT model captures the expected behavior of the SDR platform with respect to the considered perimeter of the SCA specification.
2. Automated Test Generation. Test selection criteria are chosen, to guide the automatic test generation so that it produces a test suite aligned with the test strategy. In the context of SCA conformance testing, SCA requirements are linked to elements of the model, and the coverage of these requirements drives the test generation . The precise and unambiguous meaning of the UML4MBT model makes it possible to simulate the execution of the model, to use it as an oracle by predicting the expected output of the system under test, and finally to provide traceability matrix that gives a clear functional coverage metrics. Within the project, the Smartesting test generator, namely *CertifyIt*, has been used to produce test cases and test scripts.
3. Automated Test Execution on a Test Bench. Once the test suite has been generated, the test cases are run. Test execution may be manual—i.e. by a physical person—or may be automated by a test execution environment that provides facilities to automatically execute the tests and record test verdicts. In our context, the tests are generated in Java language and automatically executed using the JUnit framework.

Requirement Tag	Criterion Tag	Requirement/Criterion Text	Section Number	Test Method	JTAP Test Case Name	Manual Test Case Number
SCA 2.2.2 Specification - Main Body						
AP0011		A log producer shall only output log records that contain an enabled CosLwLog::LogLevel value.	3.1.2.2.1	Manual		APP_TC_001
AP0012		Log producers shall use their component identifier attribute in the producerId field of the CosLwLog::ProducerLogRecord.	3.1.2.2.1	Manual		APP_TC_001
AP0013		Log producers and CF components that are required by this specification to write log records shall operate normally in the absence of a log service or in the case where the connections to a log are nil or an invalid reference.	3.1.2.2.1	Manual		APP_TC_001
AP0063		A component (e.g., Resource, DomainManager, etc.) that consumes events shall implement the CosEventComm PushConsumer interface.	3.1.2.3.1	Manual		APP_TC_029
AP0064		A component (e.g., Resource, Device, DomainManager, etc.) that produces events shall implement the CosEventComm PushSupplier interface and use the CosEventComm PushConsumer interface for generating the events.	3.1.2.3.1	Manual		APP_TC_029
AP0065		A producer component shall not forward or raise any exceptions when the connection to a CosEventComm PushConsumer is a nil or invalid reference.	3.1.2.3.1	Manual		APP_TC_029
AP0069		The connectPort operation shall make a connection to the component identified by its input parameters.	3.1.3.1.1.5.1.3	Automated	ConnectPort	APP_TC_015
AP0069	C002	A port may support several connections. The input connectionId is a unique identifier to be used by the disconnectPort operation when breaking a specific connection.	3.1.3.1.1.5.1.3	Manual		APP_TC_015
AP0070[2]		The connectPort operation shall raise the InvalidPort exception when the input connection parameter is an invalid connection for this port.	3.1.3.1.1.5.1.5	Automated	ConnectPort InvalidPort Exception	APP_TC_014
AP0070	C004[2]	The InvalidPort exception indicates one of the following errors has occurred in the specification of a Port association: 1. errorCode 1 means the Port component is invalid (unable to narrow object reference) or illegal object reference.	3.1.3.1.1.3.1	Automated	ConnectPort InvalidPort Exception	APP_TC_014
AP0071		The connectPort operation shall raise the OccupiedPort exception when unable to accept the connections because the port is already fully occupied.	3.1.3.1.1.5.1.5	Automated	ConnectPort Occupied Port Exception	APP_TC_015
AP0072		The disconnectPort operation shall break the connection to the component identified by the input connectionId parameter.	3.1.3.1.1.5.2.3	Automated	DisconnectPort Test	APP_TC_012
AP0073[2]		The disconnectPort operation shall raise the InvalidPort exception when the input connectionId parameter is not a known connection to the Port component.	3.1.3.1.1.5.2.5	Automated	DisconnectPort Test	APP_TC_012

Figure 5: Studied Excerpt of SCA 2.2.2 Application Requirements List Version 2.2.

The next subsections detail each step in the context of the SCA 2.2.2 functional specification conformance testing. This presentation focuses on the « Domain manager » function to « install / uninstall Application» nominally, including exception management as shown in Figure 5.

3.1. From SCA specifications to the MBT model

The test model is specified on the basis of the UML4MBT modeling language introduced in the previous section. It is composed of a class diagram to represent the static view of the system (using classes, associations, enumerations, class attributes and operations) and an Object diagram to list the concrete objects used to compute test cases and to define the initial state of the system. In addition, Object Constraint Language (OCL) expressions are associated with the UML class operations to provide the expected level of formalization to precisely describe the dynamical behaviors of the system. Conformance requirements traceability is managed by tagging the OCL effects of the class operations. More precisely, ad-hoc comment symbols are introduced to OCL annotations to associate the requirement identifiers with an OCL statement. When a test case covers this statement, this test case is referenced as covering the requirement defined by the annotated identifier. This tagging mechanism makes it very easy to link initial functional requirements with the corresponding model behavior. The global architecture of the model (introduced in Figure 6) conforms with the structure proposed in SCA specification: one dedicated package has been created to model each specified SCA interface. The next subsections give an overview of each artefact of the model.

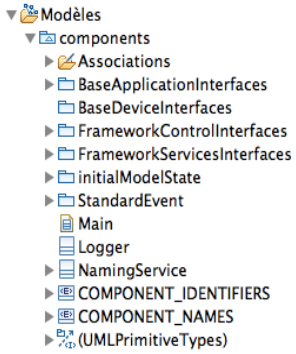


Figure 6: Model Structure using SCA Packages

3.1.1. Class diagram

Figure 7 shows the class diagram of the SCA test model. Each class may contain one or several operations (not displayed in the Figure to keep it readable), which correspond to the services that can be applied to the system.

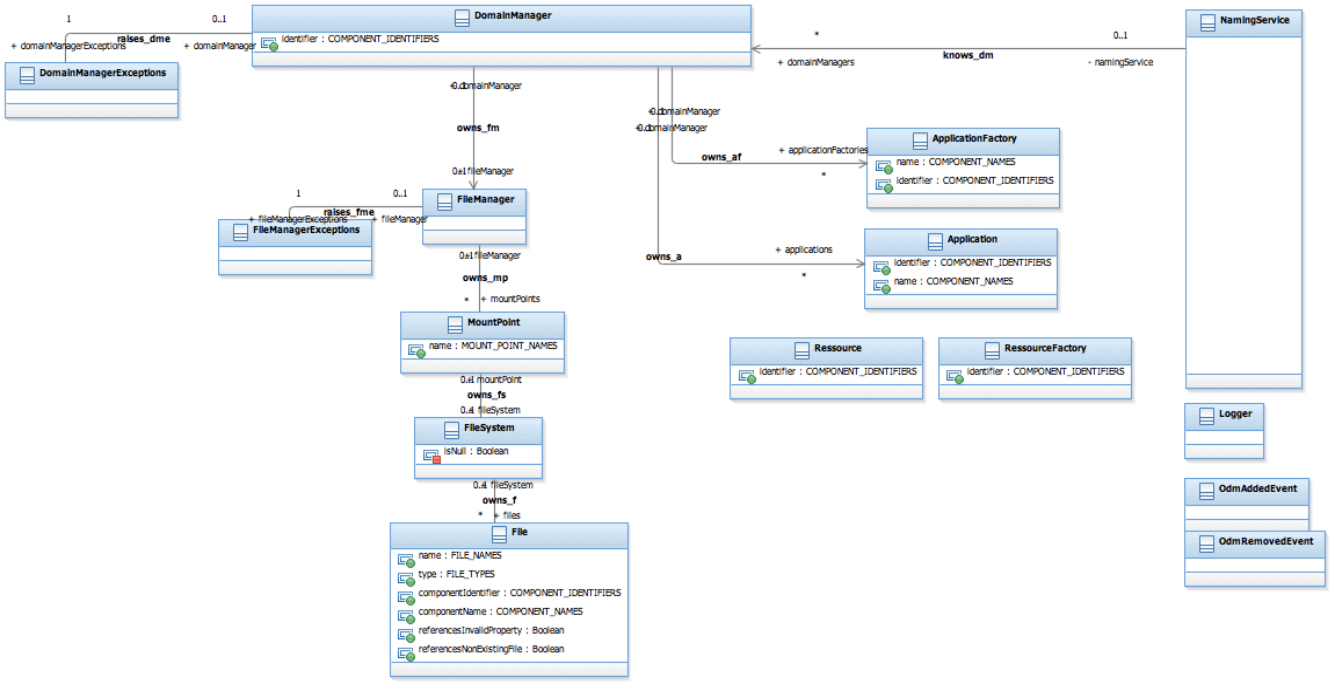


Figure 7: Class Diagram of the SCA Model

*Main *DiagrammeObjet1 mount

```
self.resetExceptions() and
let invalidFileName : Boolean = (mountPointName = MOUNT_POINT_NAMES::INVALID_NAME) in
let mountPointAlreadyExists : Boolean = (self.mountPoints->exists(mp|mp.name=mountPointName)) in
let invalidFileSystem : Boolean = fileSystem.isNull in

---@REQ: 3.1.3.4.3.5.1
if (not(invalidFileName) and not(mountPointAlreadyExists) and not(invalidFileSystem)) = true
then
    ---@AIM: MOUNT_OK
    let newMountPoint:MountPoint = MountPoint.allInstances()->any(mp|mp.name=MOUNT_POINT_NAMES::UNDEFINED_NAME) in

    newMountPoint.name = mountPointName and
    newMountPoint.fileSystem = fileSystem and
    self.mountPoints->includes(newMountPoint)
else
    ---@AIM: MOUNT_KO
    if (invalidFileName)
    then
        ---@AIM: INVALID_FILE_NAME
        self.raiseInvalidFileNameException()
    else
        if (mountPointAlreadyExists)
        then
            ---@AIM: MOUNT_POINT_ALREADY_EXISTS
            self.raiseMountPointAlreadyExistsException()
        else
            true
        endif
    endif

    and if (invalidFileSystem)
    then
        ---@AIM: INVALID_FILE_SYSTEM
        self.raiseInvalidFileSystemException()
    else
        true
    endif
endif
```

Figure 8: OCL Constraints of the Operation *mount()*

3.1.2. OCL constraints

The expected behavior of each specified operations is described by an OCL constraint to determine its effects. It allows the Smartesting *CertifyIt* tool to predict them in an automated manner. For instance, Figure 8 introduces the constraints of the operation *mount()*.

Requirements traceability is managed by tagging these OCL effects. More precisely, these ad-hoc comment symbols are used in the OCL annotations to associate the requirement identifiers with an OCL statement. When a test case covers this statement, this test case is referenced as covering the requirement defined by the annotated comment symbols. As an example, in Figure 8, the green expressions (specific line comment) starting with the keywords REQ (for high level requirement) or AIM (for sublevel requirement) associate the OCL code with the functional requirement identifiers that the OCL statement precisely covers.

This tagging mechanism makes it very easy to link initial functional requirements with the corresponding model behavior. They allow to automatically produce a traceability matrix at the same time as the generated test cases: when a test case executes the annotated statement, this test case is referenced as covering the annotated requirement(s).

3.1.3. Object diagram

Finally, the class diagram is instantiated using an object diagram that allows to determine the initial state of the system to be tested. Several object diagram can be created to cover various scenarios and/or various configurations depending of the testing objectives. Usually, one such diagram is created for each test suite to address the specific testing goals and functional features of them. Figure 9 introduces an excerpt of such model.

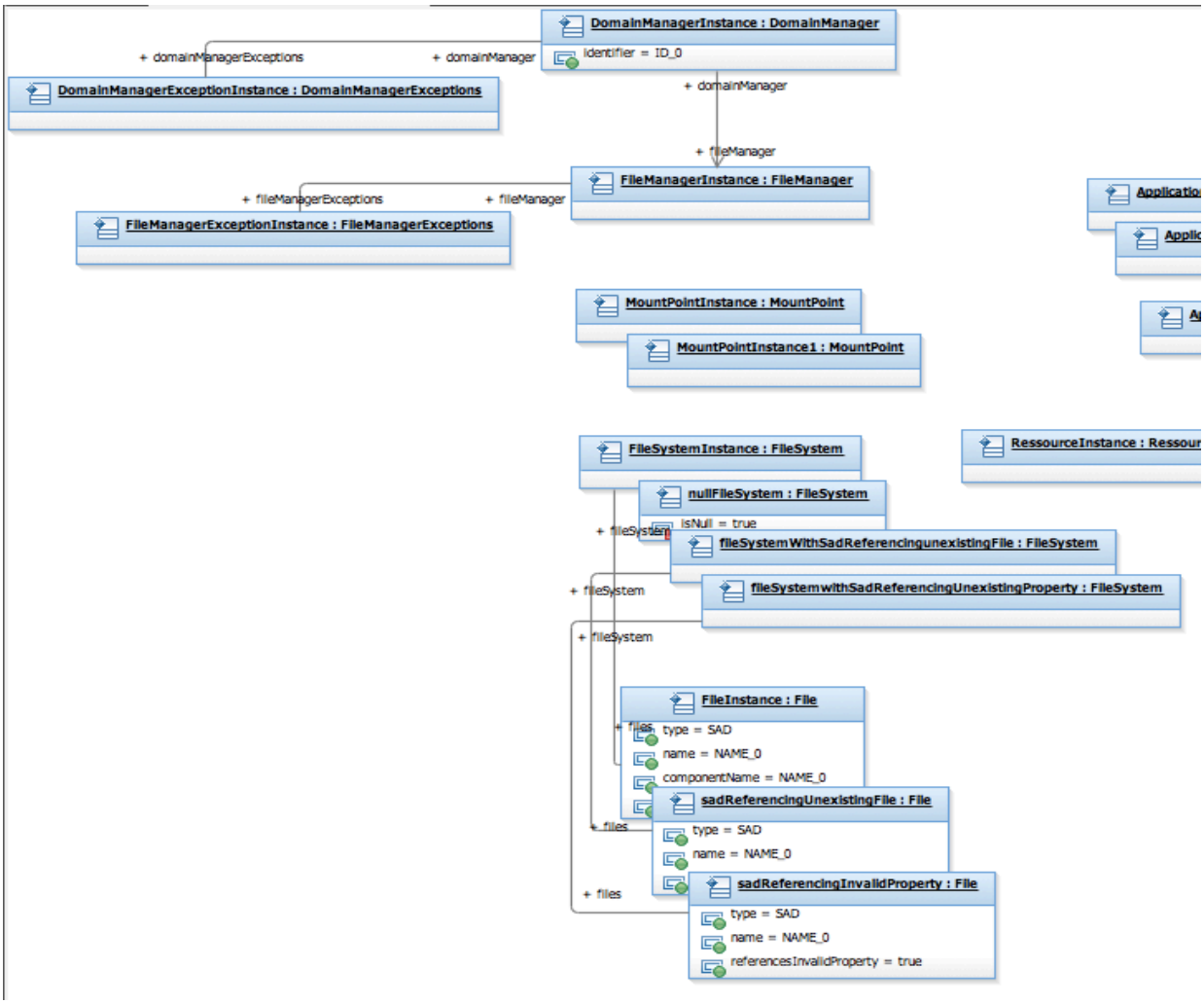


Figure 9: Excerpt of one Object Diagram

3.2. Test generation from the MBT model

Such UML4MBT models have a precise and unambiguous meaning, so that the behavior of those models can be automatically understood and manipulated by the Smartesting *CertifyIt* test generation engine. This precise meaning makes it possible to simulate the execution of the model, to use it as an oracle by predicting the expected output of the system under test, and finally to provide traceability matrix that gives a clear functional coverage metrics from the requirements point of view. Basically, the test generation algorithm carries out a systematic coverage of all the behaviors of the test model, which are tagged with a requirement identifier as shown in previous subsection. Each test corresponds to a sequence of operations taking the form of a 3-part structure: a first subsequence places the system in a specific context (preamble) to exercise a given behavior annotated by a requirement, a second subsequence invokes this behavior, and finally a last subsequence allows returning to the initial state so that test cases can be executed automatically in one single sequence. It should be noted that this 3-part structure can be completed by one or more observation function calls, which allow observing the system state at any time during the test execution to make the verdict assignment more relevant.

After test generation procedure is computed, a dedicated window of the test generator (see Figure 10) shows the set of generated test cases (at the left), and the sequence of called operations (at the top right) with the list of covered requirement identifiers (at the bottom right).

3.3. Test automation and execution

The generated test cases, which therefore include stimuli and expected outputs, can be exported to a large variety of format including customizable HTML or XML files, or directly to a scripted executable format computable in any testing framework (simulated system or real test bench). Within SCA case-study, the generated test cases are published as executable JUnit files.

Automation relies on the implementation of keywords, which are defined by the operations of the UML model, and the test data, which are define by the abstract attributes and values in this model. Finally, to ensure a fully automation, an adaptation layer (that is manually designed) concretizes the abstract test data of the model (operation names, inputs, outputs…) into concrete API calls and values. This layer can be seen as a table mapping the abstract data of the UML model to the concrete ones of the system to be tested. Thus, test publisher and adaptation layer make it possible to automatically derive executable test cases and offers the benefit of providing a structured and repeatable process. Such executable test suites can indeed be delivered to SDR manufacturers and platform providers in order to check, at a early stage of their development process, the compliance of their products. Moreover, automating test execution is a key aspect of regression testing (i.e. re-running test cases from existing test suites to build confidence that software changes have no unintended side-effects). Without test automation, testers have to execute the tests manually for each release of the application: a costly and time-consuming process.

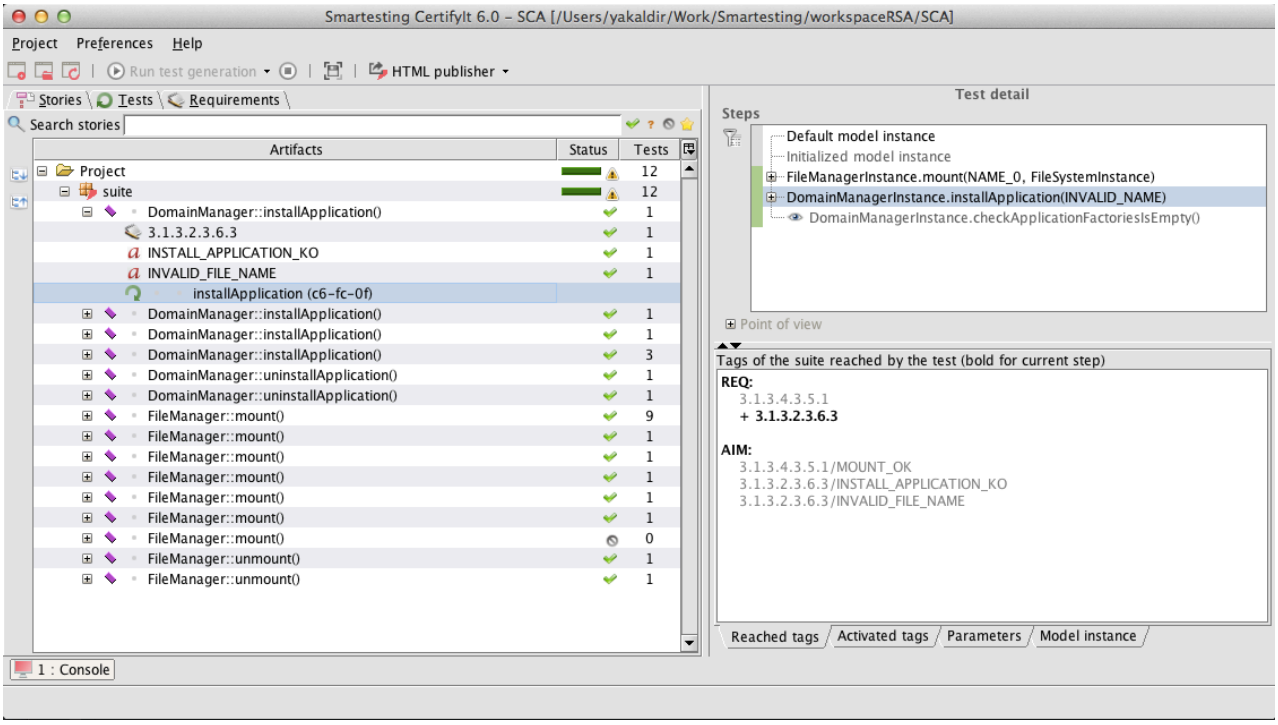


Figure 10: Smartesting CertifyIt GUI with Generated Test Cases

Figure 11 and Figure 12 respectively depict an example of generated JUnit file and the corresponding Java library that declares the UML keywords that have to be implemented. These files are automatically generated by the Smartesting *CertifyIt* testing tool. Hence, the Java keyword library specification is automatically generated from the UML model, but has to be manually documented. To achieve that, for each keyword (representing the UML operations of the model), the implementation activity consists to complete its definition by implementing the stub (see TODO comments) with the corresponding concrete code instructions.

Therefore, this file is manually designed since it directly depends on the implementation to be tested. To perform this task, as shown in Figure 13, the generated files allow the user to document the commands as well as the concrete data to be used in order to concretize and execute the generated test suite. Once this automation design is completed, the generated test cases can be executed using a JUnit engine and the related test execution report can be computed and delivered. Figure 14 shows an example of execution status given by the Eclipse interface.

```
package Smartesting.SCA.suite;

import junit.framework.TestCase;
/*
REQUIREMENTS:
    3.1.3.2.3.6.3
    3.1.3.4.3.5.1
*/
public class InstallApplication__c6_a4_38_ extends TestCase {

    private AdapterImplementation adapter;

    public void setUp() throws Exception {
        adapter = new AdapterImplementation(new TypesAdapterImplementation());
    }

    public void testInstallApplication__c6_a4_38_() throws Exception {
        adapter.componentsFrameworkServicesInterfacesFileManagermount(FileManager.FileManagerInstance, MOUNT_POINT_NAMES.NAME_0, FileSystem.FileSystemInstance);
        adapter.componentsFrameworkControlInterfacesDomainManagerinstallApplication(DomainManager.DomainManagerInstance, FILE_NAMES.INVALID_NAME);
        adapter.componentsFrameworkControlInterfacesDomainManagercheckApplicationFactoriesIsEmpty(DomainManager.DomainManagerInstance);
    }

    public void tearDown() throws Exception {
        adapter.closeAdapter();
    }
}
```

Figure 11: Example of Generated JUnit Test File

```
package Smartesting.SCA;

import Smartesting.SCA.TypesDeclaration.ApplicationFactory;

public class AdapterImplementation implements AdapterInterface {
    private TypesAdapterInterface typesAdapter;

    public AdapterImplementation(TypesAdapterInterface typesAdapter){
        this.typesAdapter = typesAdapter;
    }

    @Override
    public void componentsFrameworkServicesInterfacesFileManagermount(
            FileManager receiverInstance, MOUNT_POINT_NAMES mountPointName,
            FileSystem fileSystem) throws Exception {
        // TODO Auto-generated method stub

    }

    @Override
    public void componentsFrameworkControlInterfacesDomainManagercheckApplicationFactoriesIsEmpty(
            DomainManager receiverInstance) throws Exception {
        // TODO Auto-generated method stub

    }
```

Figure 12: Generated Java Keyword Library

```
import SCA.TypesDeclaration.COMPONENT_NAMES;
import SCA.TypesDeclaration.FILE_NAMES;
import SCA.TypesDeclaration.MOUNT_POINT_NAMES;
import SCA.TypesDeclaration.OdmAddedEvent;
import SCA.TypesDeclaration.OdmRemovedEvent;
import SCA.TypesDeclaration.SOURCE_CATEGORY_TYPE;
import SCA.TypesDefinition.COMPONENT_IDENTIFIERS;
import SCA.TypesDefinition.FileSystem;

public class AdapterImplementation implements AdapterInterface {

    static String tab = "    ";
    PrintStream ps;
    int ok = 0;
    int ko = 0;
    private String fileLogs = "./fileLog.txt";
    private FileOutputStream fileLog;
    private PrintStream pfileLog;
    private int appFactorySeqLength = 0;

    @Override
    public void componentsFrameworkControlInterfacesDomainManagercheckApplicationFactories(
            SCA.TypesDefinition.DomainManager receiverInstance,
            SCA.TypesDefinition.ApplicationFactory applicationFactory,
            SCA.TypesDeclaration.COMPONENT_IDENTIFIERS out_identifier,
            COMPONENT_NAMES out_name) throws Exception {
        // TODO Auto-generated method stub

    }
    @Override
    public void componentsFrameworkServicesInterfacesFileManagerunmount(
            SCA.TypesDefinition.FileManager receiverInstance,
            MOUNT_POINT_NAMES mountPoint) throws Exception {
        final FileManager fm = TypesAdapter.getConcreteValue(receiverInstance);
        try {
            fm.unmount(mountPoint.toString());
            ps.println("OK : File System unmounted");
            ok++;
            listMountedFileSystems(fm);
        } catch (NonExistentMount e) {
            ps.println("KO : Non Existent Mount Exception : File System");
            ko++;
        }
    }

    private void listMountedFileSystems(FileManagerOperations fm) {
        ps.println(tab + "List of Mounted Types : " + fm.getMounts().toString());
        for (int i = 0; i < fm.getMounts().length; i++) {
            ps.println(tab + "Mount Point : " + fm.getMounts()[i].mountPoint
                    + " \n File System : " + fm.getMounts()[i].fs.toString());
        }
    }
```

Figure 13: Java Implementation of the Keyword Library

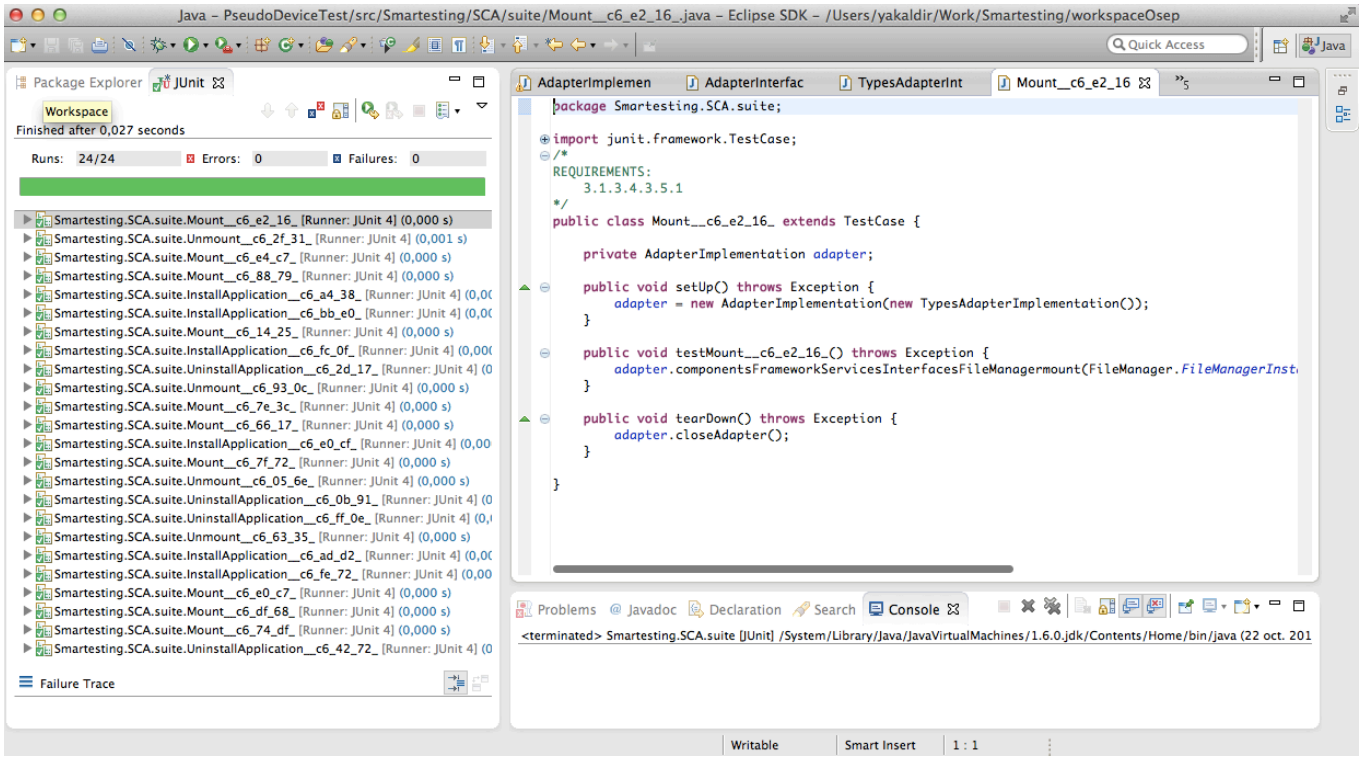


Figure 14: Example of Eclipse Test Execution Report

3.4. Lessons learnt from our experiments

The Model-Based Testing approach has been successfully applied on a subpart of the SCA 2.2.2 specifications, and this project enabled to implement a fully automated and suitable conformance testing approach for SCA standard. The main learned lessons from these experiments are:

1. The UML modeling style (the UML4MBT meta-model) is adequate to design such SCA MBT models. The interpretation of the specification was easy, and no specific issues appears during the modeling phase.
2. The annotation of the MBT model by SCA requirements (at the level of OCL constraints) is a good mean to ensure an appropriate and relevant coverage of the SCA specification during automated test generation.
3. Finally, due to a good mapping between the modeled operation and the SCA APIs of the SDR platform, automated test execution was straightforward managed.

Some other benefits, directly inherited from well-known advantages of the MBT approaches [5] (and already demonstrated on software radio protocol during a previous experiment [15]) have also been noticed. For instance, this MBT approach for SCA compliance testing reduces test maintenance costs because only the test model has to be managed instead of the test cases. Moreover, conformance tests being based on the same model, they are generated for various implementations, releases, and versions of a single application, which ensures efficient regression testing and makes easier all maintenance and upgrade activities.

4. CONCLUSION AND PERSPECTIVES

Model-based Testing (MBT) has seen last 10 years an increasing interest in different industrial area of software and system testing. This is due to the fact that benefits of MBT, such as facilitation to define and automate specialized testing strategies, help to tackle the challenges of ever more complex software and systems. In the context of conformance testing, several deployments of MBT led by industrial consortium (GlobalPlatform for instance) show that this process and technologies may help standardization organization to better conduct and master their compliance program. In this paper, we report a small but successful technical proof of concept on applying MBT for SCA conformance testing. Modeling the functional part of SCA was easy, and automated test generation techniques provide the corresponding tests to be run on the SCA platform. Therefore, experimentation feedback using this automated conformance test generation process are very encouraging.

The perspective of this project is to continue to extend the coverage of SCA functional specifications by the MBT model, and therefore to extend the generated conformance test suite.

5. REFERENCES

[1] M. Utting, B. Legeard. “Practical Model-Based Testing – A Tools Approach”, Morgan & Kauffmann, 2007

[2] J. Rumbaugh, I. Jacobson and G. Booch. “The Unified Modeling Language Reference Manual”, Second Edition. Addison-Wesley, 2004. ISBN 0 321 24562 8

[3] JTNC Standards, Joint Tactical Networking Center, “JTRS/JPEO Software Communications Architecture Specification”, Final/15 May 2006 V.2.2.2, http://jtnc.mil/sca/Pages/default.aspx

[4] E. Bernard, F. Bouquet, A. Charbonnier, B. Legeard, F. Peureux, M. Utting, and E. Torreborre. “Model-based testing from UML models”. *Proceedings of the international workshop on Model-based Testing (MBT’2006)*, LNCS, vol. 94. pages 223–230. Dresden, Germany. October 2006.

[5] A. Dias-Neto and G. Travassos. “A Picture from the Model-Based Testing Area: Concepts, Techniques, and Challenges”. *Advances in Computers*, vol. 80, pp. 45–120, July 2010, iSSN:0065-2458.

[6] H. Zhu and F. Belli. “Advancing test automation technology to meet the challenges of model-based software testing,” *Journal of Information and Software Technology*, vol. 51, no. 11, pp. 1485–1486, 2009.

[7] “ETSI Conformance Testing Process – An introduction”, available on-line (last access June 2014) http://www.etsi.org/images/files/ETSITechnologyLeaflets/MethodsforTestingandSpecification.pdf

[8] G. Bernabeu, N. Lavabre. “Model-Based Testing for a world-wide Compliance Program”, *User Conference on Advanced Automated Testing (UCAAT 2013)*, Paris, October 2013. http://ucaat.etsi.org/2013/presentations/Keynote_MBT%20for%20a%20Compliance%20Program-GlobalPlatform-GilBernabeu.pdf

[9] J. Rumbaugh, I. Jacobson, G. Booch.: “The Unified Modeling Language Reference Manual”. 2nd edition. Addison-Wesley (2004) ISBN 0321245628.

[10] F. Bouquet, C. Grandpierre, B. Legeard, F. Peureux, N. Vacelet, and M. Utting. “A subset of precise UML for model-based testing”. *Proceedings of the 3rd international workshop on Advances in model-based testing (A-MOST'07)*, pages 95--104. ACM, July 2007.

[11] J. Warmer and A. Kleppe. “The Object Constraint Language: Precise Modeling with UML”. Addison-Wesley, 1996. ISBN 0 201 37940.

[12] F. Bouquet, C. Grandpierre, B. Legeard, and F. Peureux, “A test generation solution to automate software testing,”. *Proceedings of the 3rd international workshop on Automation of Software Test (AST’08)*. ACM Press, May 2008.

[13] H.Q. Nguyen, M. Hackett, and B.K. Whitlock. “Global Software Test Automation: A Discussion of Software Testing for Executives”, Happy About, 2006.

[14] G. Bernabeu, E. Jaffuel, B. Legeard, and F. Peureux. “MBT for GlobalPlatform Compliance Testing: Experience Report and Lessons Learned”. *Proceedings of the 25th International Symposium on Software Reliability Engineering (ISSRE’14)*, IEEE Computer Society Press, November 2014.

[15] S. Li, M. Bourdellès, A. Acebedo, J. Botella, and F. Peureux. “Experiment on Using Model-Based Testing for Automatic Tests Generation on a Software Radio Protocol”. *Proceedings of the 9th international workshop on Systems Testing and Validation (STV'12)*, October 2012.

SPECTRUM INTELLIGENCE FOR INTERFERENCE MITIGATION FOR COGNITIVE RADIO TERMINALS

Kresimir Dabcevic, Muhammad Ozair Mughal, Lucio Marcenaro, Carlo S. Regazzoni

(DITEN, University of Genova, Genoa, Italy)

ABSTRACT

Cognitive Radio (CR) is defined as a radio that is aware of its surroundings and adapts intelligently. While CR technology is mainly cited as the enabler for solving the spectrum scarcity problems by the means of Dynamic Spectrum Access (DSA), perspectives and potential applications of the CR technology far surpass the DSA alone. For example, cognitive capabilities and on-the-fly reconfiguration abilities of CRs constitute an important next step in the Communication Electronic Warfare (CEW). They may enable the jamming entities with the capabilities of devising and deploying advanced jamming tactics. Analogously, they may also aid the development of the advanced intelligent self-reconfigurable systems for jamming mitigation. This work outlines the development and implementation of the Spectrum Intelligence algorithm for Radio Frequency (RF) interference mitigation. The developed system is built upon the ideas of obtaining relevant spectrum-related data by using wideband energy detectors, performing narrowband waveform identification and extracting the waveforms' parameters. The recognized relevant spectrum activities are then continuously monitored and stored. Coupled with the self-reconfigurability of various transmission-related parameters, the Spectrum Intelligence is the facilitator for the advanced interference mitigation strategies. The implementation is done on the Cognitive Radio coaxial test bed architecture which consists of two Software Defined Radio terminals, each interconnected with the computationally powerful System-on-Module (SoM).

1. INTRODUCTION

As opposed to the legacy radio systems, where the functionalities are for the most part restricted by the deployed hardware components, Software Defined Radios (SDRs) provide reconfigurability of most of their parameters through software changes run on the programmable processors - Field Programmable Gate Arrays (FPGAs) or Digital Signal Processors (DSPs). Originally introduced by Mitola in 1991, SDR is nowadays becoming a dominant design architecture for wireless systems. Cognitive Radio (CR) is usually built on a SDR platform, and is further embodied with awareness and self-adapting capabilities. This, however, inherently brings along higher implementation complexity and the needs for even more powerful computational resources.

SDRs and CRs [1] have received particular interest from the wireless communication research community as potential solutions to spectrum underutilization problems. For these purposes, a variety of Dynamic Spectrum Access (DSA) techniques have been proposed and investigated. These may be categorized under the three models: Dynamic Exclusive Use, Open Sharing, and Hierarchical Access Models [2]. Opportunistic Spectrum Access (OSA) is a form of the Hierarchical Access Model, where unlicensed CRs (secondary users) are allowed to utilize the spectrum as long as licensed (primary) users' communication is protected. In order to access the spectrum opportunistically, secondary users need to be able to acquire the spectrum occupancy information. Three methods enabling the spectrum occupancy inference are generally adopted: spectrum sensing, geolocation/database and beacon signals. Among them, various spectrum sensing techniques such as energy detection [3, 4], feature detection [5] and matched filters [6] were given the most attention up to date.

However, the potentials of SDR and CR paradigms are not necessarily restricted to the application of DSA. Seamless transition between the existing communication solutions, higher interoperability between different standards and flexibility in waveform selection all impose themselves as the viable reasons for research and development of the SDR and CR concepts.

In this work, we focus on some of the impacts that the SDR/CR technology brings to the Communication Electronic Warfare (CEW) domain. CEW systems [7] focus on intercepting or denying the communication on the target systems (electronic attack) [8], or taking actions aimed at preventing the electronic attacks from successfully occurring (electronic defense). A multitude of ways with respect to how on-the-fly reconfiguration capabilities coupled with the learning and self-adaptive potentials of the CR technology may aid both the attacking and the defending side can be imagined [9]. Deploying energy detection spectrum sensing may embody the attacker with the ability to monitor the target transmitter's transmission frequency, estimate the target receiver's signal strength and calculate the signal strength necessary to efficiently jam the communication. Performing feature detection

spectrum sensing may allow the attacker to infer even more of the parameters of the target transmitter, such as deployed modulation type or coding mechanism. Subsequently, it may use these inferences to deploy jamming tactics with higher probability of success rate, e.g. by taking advantage of the fact that different modulation techniques are characterized by different levels of resilience to interference. Finally, the attacker may use learning techniques to observe and learn the transmitter's patterns, such as the deployed frequency hopping or power allocation schemes. Analogously, similar benefits may be provided to the defending side.

This work focuses on the electronic defense part of the CEW. It presents ideas, development and implementation aspects of the Spectrum Intelligence algorithm for Radio Frequency (RF) interference mitigation. The concept is built on the enabling technologies of spectrum sensing, waveform analysis, Temporal Frequency Maps[1], and self-reconfigurability potentials of the SDR/CR technology.

Along the way, we acknowledge and address some of the challenges faced when porting the algorithms to the real-life SDR/CR platform, and propose practical solutions for the identified problems.

The remainder of the paper is organized as follows: section 2 describes the enabling technologies and concepts for the Spectrum Intelligence algorithm, as well as the concepts and functionalities related to the algorithm itself. The SDR/CR platform used for porting the developed algorithms, along with the identified issues and proposed solutions is described in section 3. Performance of several crucial functionalities of the algorithm is evaluated in section 4, whereas conclusions and the roadmap are presented in section 5.

2. SPECTRUM INTELLIGENCE

The principal idea behind the Spectrum Intelligence algorithm consists of continuously monitoring relevant RF spectrum activities, identifying potential threats to the communication, and taking proactive measures to ensure communication robustness and secrecy. For doing so, the algorithm relies on the reliable spectrum sensing mechanism, correct identification and extraction of the relevant parameters, and secure software unsubjected to tampering. The functional process of the Spectrum Intelligence algorithm may be represented in the form of the Cognitive Cycle, as shown in Figure 1.

Sensing is performed periodically, either by taking a quiet or active approach, for the frequency band of interest.

Then, *data processing* takes place. Parsed data is time aligned if needed, and transformed into frequency domain by performing Fast Fourier Transform (FFT). Thresholding is then performed with the aim of discarding the background noise, and keeping only the FFT bins corresponding to actual

[1]We are intentionally creating a distinction between the Temporal Frequency Maps, and the similar but more advanced concept of Radio Environment Maps [10].

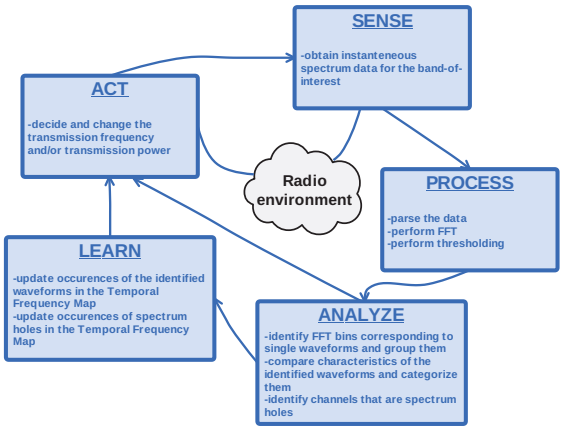


Fig. 1: Cognitive cycle representing the Spectrum Intelligence algorithm

signals. This corresponds to solving the decision problem between the following two hypotheses [11]:

$$Y(n) = \begin{cases} W(n) & H_0 \\ X(n) + W(n) & H_1 \end{cases} \quad (1)$$

where $Y(n)$, $X(n)$ and $W(n)$ are the received signals, transmitted signals and noise samples, respectively, H_0 is the hypothesis corresponding to the absence of the signal, and H_1 is the hypothesis corresponding to the presence of the signal.

Finding the appropriate threshold is the principal challenge of any energy detection scheme. The most common approaches are the Constant Detection Rate (CDR) and Constant False Alarm Rate (CFAR) detectors, where threshold is set adaptively depending on the SNR regime and the characteristics of the sensed wideband signal. However, it should be noted that even in adaptive thresholding, presence of interference may confuse the energy detector [12].

In CEW domain, it is reasonable to assume relatively low spectrum utilization - namely, more often than not there will only be a limited number of actual narrowband signals (either "friendly" or "potentially malicious") in the scanned wideband signal at any time instance. For this purpose, it is sufficient to implement a suboptimal thresholding algorithm, where CFAR or CDR performance is not necessarily achieved. Namely, practical experience has shown that threshold $\hat{\lambda}$ may be adaptively set based only on the mean value of the magnitudes of the scanned wideband signal, as:

$$\hat{\lambda} = 2 \cdot \frac{1}{n} \sum |Y(n)| \quad (2)$$

This step concludes the energy detection.

Let us assume that as a result of the thresholding process, N frequency bins are identified. For a system where M actual signals ($N > M$) are present, $N - M$ frequency bins would

incorrectly be classified as signals. Then, simple thresholding would result in the false alarm rate of $\frac{N-M}{N}$.

For this reason, frequency bins corresponding to the same signal need to be grouped together. For the ideal case (generic signals in high-SNR environments), the simplest approach consists of grouping consecutive samples together and classifying them as single waveforms. However, in most practical situations, some frequency bins may have erroneous magnitude values as a result of imperfect sampling and would thus be discarded during the thresholding phase. For this purpose, maximum acceptable distance (in Hz) between the two samples belonging to the same waveform is defined, and is a function of the frequency resolution of the FFT as given by:

$$d_{MAX} = K \cdot d_f. \tag{3}$$

Here, K is the estimate of a number of consecutive samples that could be erroneously disregarded, and d_f is the frequency resolution of the FFT, defined as:

$$d_f = \frac{2 \cdot f_{max}}{N_S}, \tag{4}$$

where f_{max} is the maximum resolvable frequency (which in case of Nyquist sampling equals to half of the sampling frequency), and N_S is the number of samples acquired during the sampling process.

Figure 2 illustrates the difference between the original transmitted signal (2(a)), sensed FFT bins (2(b)), and estimated signal after performing thresholding/bin grouping (2(c)).

Next, the *waveform analysis* is performed, i.e. for each of the identified narrowband waveforms, relevant parameters are extracted. These parameters include waveforms' respective center frequencies, bandwidths and maximum values of their magnitudes. It is assumed that the algorithm has an access to a database containing pre-defined parameters of the "friendly" and/or "potentially malicious" waveforms in the system. Then, parameters of the identified waveforms in the system are compared to the parameters from the database, eventually resulting in classification of each waveform as either "friendly" or "potentially malicious".

The considered method for waveform analysis is computationally inexpensive, and is suitable for analysis in systems with low frequency resolution. However, there is a tradeoff between the lightweight nature of the algorithm and the limitations it imposes, which are as follows:

1. Relatively high probability of misclassification / misdetection compared to more advanced waveform analysis methods in systems with higher frequency resolution, as a result of a limited number of analyzed parameters.

2. The need for a-priori knowledge of the expected maximum values of the magnitudes, which in real-life situations may not always be feasible.

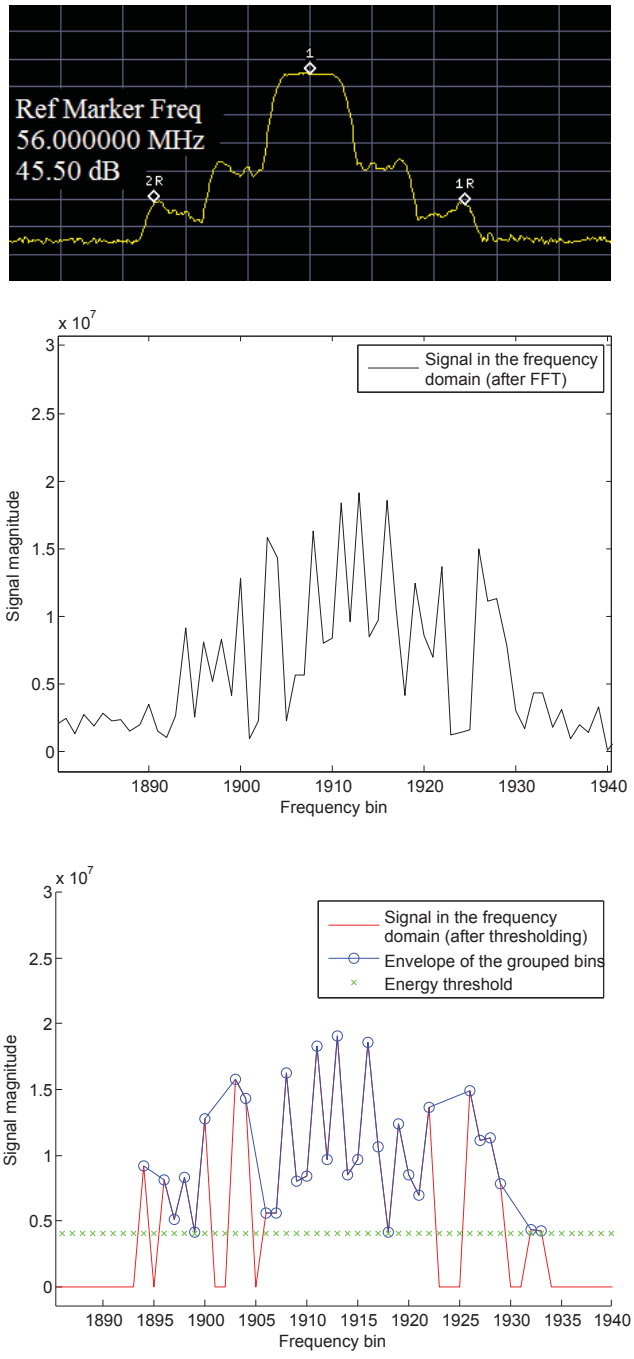


Fig. 2: Signal: transmitted - maximum hold (a), sensed (b), after thresholding and bin grouping (c)

3. Vulnerability against adversaries able to refine their transmission-related parameters in order to mimick "friendly" users (the so-called User Emulation Attackers [13]).

Alternative, computationally more expensive waveform analysis techniques include cross-correlation in time domain; more comprehensive Statistical Signal Characterization (SSC) methods [14]; modulation classification methods [15]; and cyclostationary detectors [5]. These are not analyzed within this work, however they all impose themselves as viable future research topics.

Besides waveform identification and classification, the system also recognizes instantaneous spectrum holes. We define a spectrum hole as the channel where the magnitudes of all of the corresponding FFT bins are below the energy threshold.

The algorithm next accesses the Temporal Frequency Map, where previous occurrences of spectrum activities are stored. The Temporal Frequency Map is a $n \times 3$ matrix that keeps track of the number of occurrences of "friendly" waveforms, "potentially malicious" waveforms and spectrum holes for each of the n channels-of-interest, as illustrated in Table 1.

Table 1: Temporal Frequency Map

Spectrum activity/CHANNEL	1	2	...	n
Friendly	$m_{F/1}$	$m_{F/2}$		$m_{F/n}$
Potentially malicious	$m_{PM/1}$	$m_{PM/2}$		$m_{PM/n}$
Spectrum hole	$m_{SH/1}$	$m_{SH/2}$		$m_{SH/n}$

In each cycle, previous values are updated with the newly acquired and processed information. This corresponds to the *learning* phase of the Cognitive cycle. Temporal forgiveness is implemented within the algorithm, i.e. spectrum activities corresponding only to the last k spectrum readouts are taken into account while making future decisions. This reduces the probability of data becoming obsolete, at the expense of the lower amount of accessible information.

Finally, based on the processed spectrum information, current transmission parameters (channel and power) and the history obtained from the Temporal Frequency Map, the CR may decide to *act* in order to improve its chances of reliable transmission. The actions constitute of proactively changing the transmission frequency (channel surfing), or the transmission power whenever a threat has been detected. A system is considered "under threat" when a "potentially malicious" waveform has been identified on the channel close to the channel currently used for transmission. The new channel for the transmission is then chosen according to (5).

$$c_{t+1} \in (c_t = SH \mid (X(c_t) = min). \tag{5}$$

This means that the new channel c_{t+1} is selected among all the channels c_t that are currently spectrum holes, such that the $X(c_t)$ is minimum. $X(c_t)$ represents the expected channel reliability, defined as (6).

$$X(c_t) = k^2 \cdot m_{PM/c_t} + (k+1) \cdot m_{F/c_t} - m_{SH/c_t}, \tag{6}$$

where m_{PM/c_t}, m_{F/c_t} and m_{SH/c_t} represent the numbers of occurrences of the "potentially malicious" waveforms, "friendly" waveforms and spectrum holes on the channel c_t over the last k steps, respectively. The coefficients k^2 and $(k+1)$ are assigned in order to give highest priority of action to avoiding channels with history of occurrences of "potentially malicious" waveforms, followed by the channels with history of occurrences of "friendly" waveforms.

The new transmission power is chosen according to (7).

$$P_{t+1} \in P \mid P_R > 10log_{10}\hat{\lambda} + 3dB. \tag{7}$$

Algorithm 1 provides the pseudocode demonstrating processes related to the Spectrum Intelligence algorithm.

Algorithm 1 Spectrum Intelligence pseudocode

```
function SPECTRUM INTELLIGENCE
    Initialize all channel states to "free"
    Sample the wideband signal → N_S amplitude values
    Data parsing → N_S = 2^x amplitude values
    Perform FFT → N_S/2 frequency bins with magnitudes M
    Calculate mean value of M → M_mean
    Based on M_mean, set the energy threshold → λ̂
    for i = 1 to n_S/2 do (For each frequency bin)
        if M(i) > λ̂ then
            Bin i belongs to the signal
            Change channel state of bin i to "occupied"
            if any of M(i−K):M(i−1) > M_T then
                Group these bins as a single waveform
            end if
        end if
    end for
    Extract parameters of identified waveforms → bandwidth, center frequency, maximum M
    Compare parameters to the database → waveform is either "friendly" or "potentially malicious"
    Update Radio Frequency Map
    If "potentially malicious" waveforms are near the current operating channel, choose new TX frequency/power
end function
```

3. IMPLEMENTATION ON THE CR TEST BED

The proposed algorithm was implemented on the SDR/CR coaxial test bed architecture. Compared to the over-the-air

implementation, coaxial test bed exhibits several important advantages:

- Possibility to set accurate and stable RF levels,
- Repeatability of the experiments without the uncertainties characteristic to wireless transmission,
- Possibility to connect test instruments and generators to one or more branches,
- Avoiding regulatory issues related to transmitting outside of the Industrial, Scientific and Medical (ISM) frequency bands.

Test bed consists of two Software Defined Radio (SDR) SWAVE HandHeld (HH) terminals [16], each interconnected with the computationally powerful System-on-Module (SoM) embodied with a Digital Signal Processor (DSP) and a Field Programmable Gate Array (FPGA). Inbetween, a dual directional coupler is placed. Vector signal generator allows for injecting noise/interference to the system, whereas spectrum analyzer provides reliable monitoring of the relevant RF activities in real-time. Block diagram of the test bed architecture is provided in Figure 3.

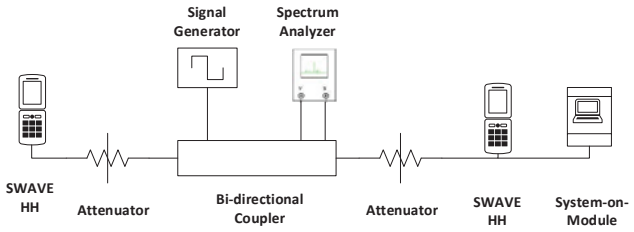


Fig. 3: CR test bed block diagram

SWAVE HH is a fully functional SDR terminal operable in Very High Frequency (VHF) and Ultra High Frequency (UHF) bands, capable of hosting a multitude of both legacy and new waveforms. Additionally, it provides support for remote control of its transmit and receive parameters via the Simple Network Management Protocol (SNMP). All of the signal processing is delegated to the SoM. Connection between the HH and SoM is achieved through Ethernet and serial ports. Ethernet is used for the remote control of the HH's parameters, using SNMP v3. For the purposes of the Spectrum Intelligence algorithm, relevant remotely controllable parameters are operating channel and transmission power. Serial port is used to transfer raw spectrum data from the HH to SoM. The interfaces are illustrated in Figure 4, and the actual implementation in Figure 5. Full details on the test bed architecture may be found in [17].

Here follows a description of the spectrum sensing process based on the HH's wideband front end architecture (Figure 6). HH's 14-bit Analog-to-Digital-Converter (ADC) performs sampling at 250 Msamples/s. Every 3 seconds, a burst

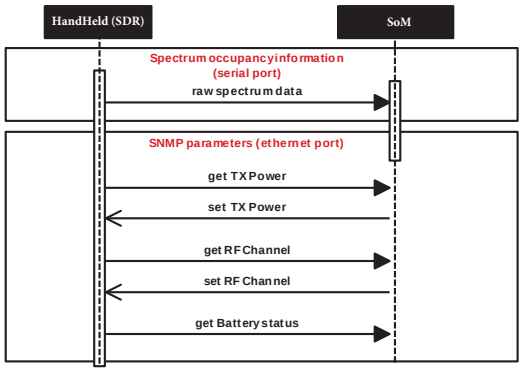


Fig. 4: Interfaces HandHeld-SoM

Fig. 5: Implementations of HandHeld and SoM

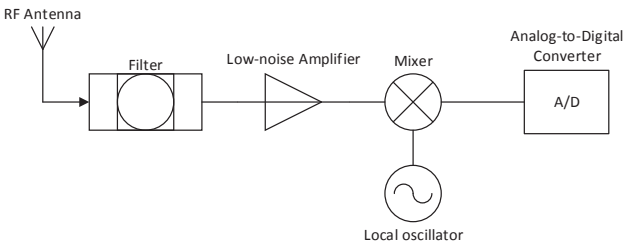


Fig. 6: HandHeld's wideband RF front end architecture

of 8192 consecutive samples is buffered, and then outputted over the serial port at 115200 bauds to the SoM. There, the samples, corresponding to 120 MHz around the center carrier frequency of the radio, are parsed, transformed into the frequency domain using the Fast Fourier Transform (FFT), and subsequently analyzed by the implemented energy detector. Alternatively, in order to increase the frequency resolution of the FFT bins, several consecutive spectrum bursts may be FFT-ed, averaged and analyzed together. The spectrum sensing and the Spectrum Intelligence as a whole is a quite process, i.e. throughout the process, HH is able to transmit/receive data. Controlled environment achieved by the coaxial implementation allows us to assume high coherence time of the analyzed frequency band, i.e. while performing the averaging of consecutive spectrum readouts, temporal variability of the channel may be disregarded. We acknowledge, however, that in case of the over-the-air transmission, nature of the wireless medium would not allow us to make such assumption. In order to obtain higher FFT frequency resolutions, necessary modifications to the equipment would include increasing the buffer size on the HH, and finding ways to transfer spectrum data at higher baud rate than is currently supported. Alternatively, appropriate techniques that estimate the temporal variability of the channel would need to be deployed.

The FFT-ed data is then further analyzed by the Spectrum Intelligence algorithm, as explained in Section 2. The output of the algorithm is the transmission frequency and transmission power to be deployed in the next cycle. These values are written to the .xml file at the end of the Spectrum Intelligence cycle.

As previously mentioned, HH provides support for reconfigurability of its transceiving parameters by the means of the SNMP v3. The implementation is done in the following way: whenever a new value is written into the .xml file representing the new transmission frequency/power, the algorithm running on the SoM intreprets it as the SNMP command that needs to be invoked. Each SNMP command (`SET_RFchannel` or `SET_TXpower`) is characterized by the corresponding unique Object IDentifier (OID) and the new value of the parameter. OIDs and the respective values that each object can take are stored in the Management Information Base (MIB) on the HH. Once that the HH receives the SET request, it accesses the MIB, checks whether the requested value of the object is defined in MIB and, if so, changes the corresponding parameter. This finishes one cycle of the Spectrum Intelligence algorithm. Change of the transmission parameters occurs in every cycle in which the "under threat" alarm has been triggered.

4. EXPERIMENTAL VALIDATION

Performance of the overall algorithm depends mainly on the accuracy of the energy detection and waveform classification phases. In order to evaluate the performance of these functionalities, a set of experiments is performed using the test bed architecture.

SelfNET Soldier Broadband Waveform (SBW) [16], representing the "potentially malicious" waveform, is continuously transmitted on the fixed carrier frequency. SBW is a digital waveform with 1.25 MHz bandwidth, operable in VHF (30 MHz-88 MHz) and UHF (256 MHz-512 MHz) frequency bands. When operating in VHF, direct conversion principle is utilized, and the frequency band scanned is always 0-120 MHz. When operating in UHF, superheterodyne principle is used, and the frequency band scanned depends on the center carrier frequency f_c of the radio - namely, analyzed band is $[f_c - 35, f_c + 85]$ MHz. Vector signal generator is used to create and inject the "friendly" waveforms into the channel, emulating friendly communication. In addition, for the ease of analysis, all other sensed recognized signals that are not classified as "potentially malicious" are classified as "friendly". Hence, the database contains only the parameters of the "potentially malicious waveform" - i.e. its bandwidth and expected maximum magnitude.

For the experiments, we utilize the VHF transmission band where the radios are operable, meaning that the spectrum sensing is performed for the frequency band of 0-120 MHz. SBW signal representing the "potentially malicious" waveform is transmitted at the center carrier frequency of 61 MHz (first 100 spectrum bursts) and 71 MHz (second 100 spectrum bursts), always with the constant transmission power. These results are then aggregated and analyzed. Besides the SBW signal, a number of other signals from the environment are successfully sampled, e.g. FM radio transmission in the frequency band of 88-108 MHz. Figure 7(a) shows an example of the scanned wideband signal for 1 sensing burst (29.3 kHz frequency resolution). Figures 7(b) and 7(c) show the difference in frequency resolution between 1 burst and 5 consecutive averaged bursts (5.86 kHz frequency resolution).

Ideally, waveform analysis should classify only the SBW waveform as the "potentially malicious" waveform in every analysis cycle (true positives). However, the analysis procedure will occasionally erroneously classify other waveforms as "potentially malicious" (false positives).

These classification results are directly dependent on the following factors:

- Energy detection threshold, $\hat{\lambda}$ - inappropriately low threshold may result in grouping together many adjacent bins (some of which actually corresponding to noise) as single waveforms, consequently increasing the estimated bandwidths of these waveforms.

- Estimated number of consecutive samples that could be erroneously disregarded, K - overly low K may result in single waveforms being erroneously recognized as different waveforms on adjacent frequencies; overly high

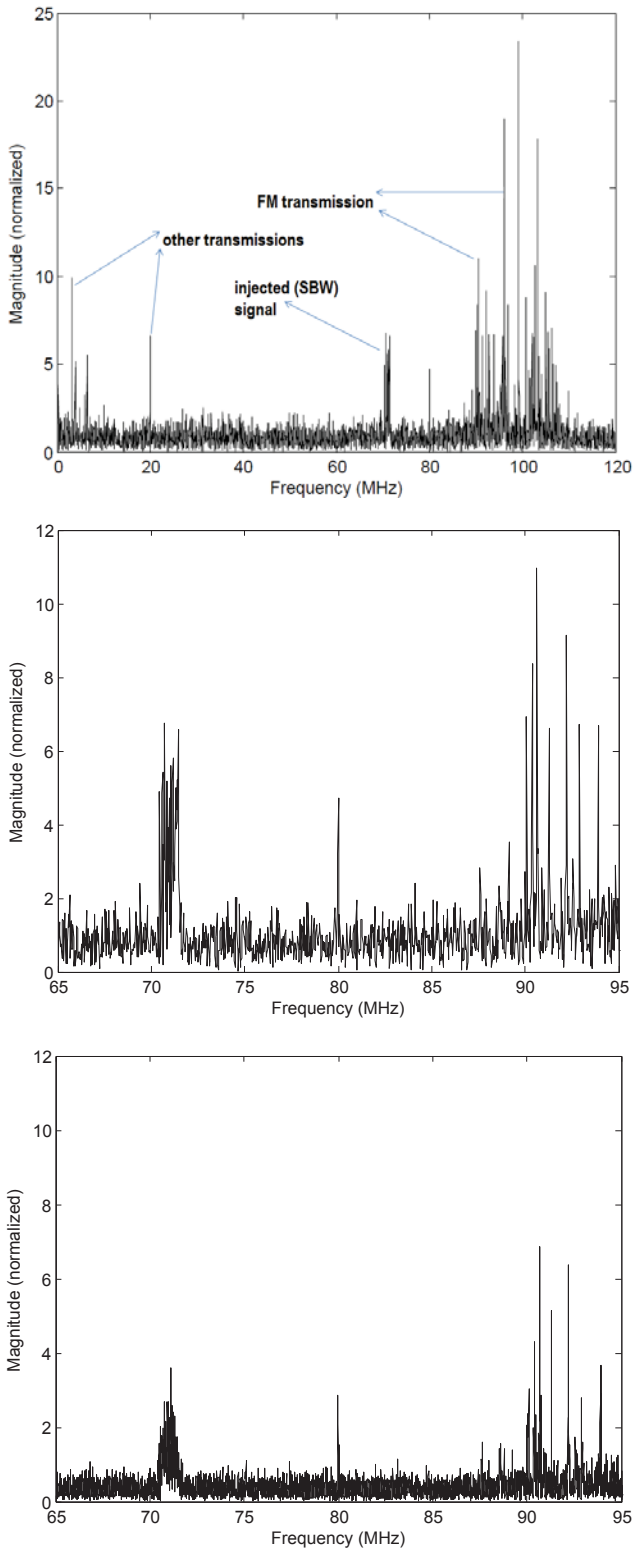


Fig. 7: Signal: wideband sensed - 1 analyzed burst (a), zoomed in - 1 analyzed burst (b), zoomed in - 5 analyzed bursts (c)

K may result in waveforms on adjacent frequencies being erroneously grouped as single waveforms.

- Similarity in the parameters between the analyzed waveform and other scanned waveforms present in the communication system.
- Level of tolerance on the analyzed parameters (e.g. 20% tolerance on bandwidth means that for SBW, whose bandwidth is 1.35 MHz, all scanned waveforms whose bandwidth falls between [1.08,1.62] MHz will be classified as the SBW waveform) - higher tolerance will increase the probability of both true and false positives.
- Frequency resolution, directly stemming from the number of averaged consecutive bursts.

The first two points are defined according to (2) and (3) respectively, with $K = 3$. In the analyzed system, all scanned signals have significantly narrower bandwidths than the analyzed (SBW) signal, as can be seen from Figure 7(b). Hence, we focus our analysis on the influence of the last two points.

First, waveform analysis is performed using only the estimated bandwidths of the scanned waveforms. Level of tolerance varies between 10% and 30%, and number of consecutive analyzed bursts varies from 1 to 10. Results are summarized in the form of the confusion matrix in Table 2.

Here, "true positives" refer to the correctly classified instances of the "potentially malicious" (SBW) waveform. "False positives" are all other ("friendly") waveforms erroneously classified as "potentially malicious". Whereas it could have been foreseen that the rate of true positives increases significantly with frequency resolution (number of averaged bursts), the rate of increase of false positives may

Table 2: Confusion matrix when only the estimated bandwidths are used

		Parameter tolerance (%)		
No. of bursts		*10*	*20*	*30*
1	*True positives (200 runs)*	*55*	*92*	*130*
	False negatives (200 runs)	*145*	*108*	*70*
	False positives (200 runs)	*0*	*4*	*9*
3	*True positives (66 runs)*	*48*	*59*	*61*
	False negatives (66 runs)	*18*	*7*	*5*
	False positives (66 runs)	*14*	*20*	*27*
5	*True positives (40 runs)*	*36*	*40*	*40*
	False negatives (40 runs)	*1*	*0*	*0*
	False positives (40 runs)	*20*	*26*	*34*
10	*True positives (20 runs)*	*18*	*20*	*20*
	False negatives (20 runs)	*2*	*0*	*0*
	False positives (20 runs)	*16*	*23*	*52*

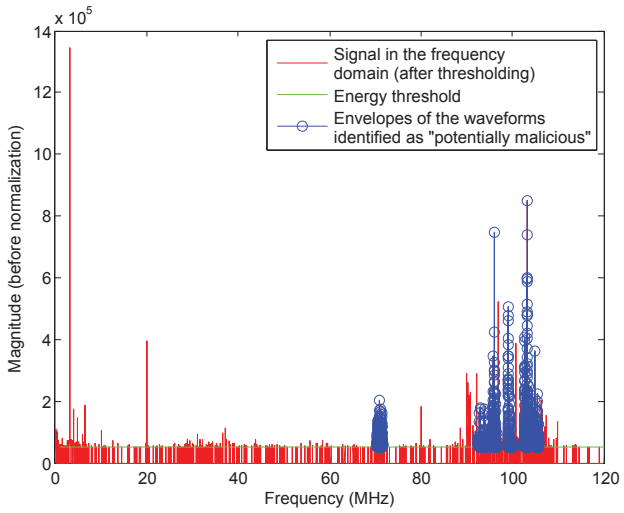


Fig. 8: Occurrences of false positives - 10 consecutive analyzed bursts, parameter tolerance 30%

come as a surprise. Figure 8 proffers a good explanation for this occurrence:

Here, instances of both the correct detection (waveform at 71 MHz) and of five false detections (waveforms at approximately 94, 96, 99, 103 and 105 MHz) are present. False detections are caused by several factors: imperfect sampling and low sampling time throughout analyzed sampling windows cause that the FFT bins appear at slightly different frequencies (especially for the narrowband FM radio signals). Some of these values then superimpose, making their respective magnitudes satisfy the threshold $\hat{\lambda}$. Adjacent ($K = 3$) frequency bins that are over the threshold are grouped together and analyzed as single waveforms. Occasionally, these "waveforms" will have estimated bandwidth that falls within the tolerance of the analyzed (SBW) waveform, in turn triggering the false detection.

This may partially be solved by imposing higher constraint on $\hat{\lambda}$ or lower constraints on K. Alternatively, analyzing other waveform parameters (when available) may provide even better analysis results. In the second step, waveform analysis is performed using both the information of the estimated bandwidth and the maximum magnitude for the scanned waveforms. Table 3 shows the improvements with respect to the reduced number of false positives, at the expense of the reduced number of identified true positives.

We acknowledge that, whereas information on the adversaries' transmission powers may often not be known a-priori in real-life scenarios, they might be known for some "friendly" signal. Then, with the appropriate channel estimation techniques and the information on the "friendly" waveforms' geographical positions, expected scanned power or magnitude may be predicted (with a certain tolerance).

Table 3: Confusion matrix when both the estimated bandwidths and the estimated magnitudes are used

		Parameter tolerance (%)		
No. of bursts		*10*	*20*	*30*
1	*True positives (200 runs)*	*32*	*85*	*123*
	False negatives (200 runs)	*168*	*115*	*77*
	False positives (200 runs)	*0*	*0*	*0*
3	*True positives (66 runs)*	*35*	*44*	*54*
	False negatives (66 runs)	*31*	*22*	*12*
	False positives (66 runs)	*0*	*0*	*0*
5	*True positives (40 runs)*	*34*	*36*	*37*
	False negatives (40 runs)	*6*	*4*	*3*
	False positives (40 runs)	*0*	*0*	*0*
10	*True positives (20 runs)*	*17*	*20*	*20*
	False negatives (20 runs)	*3*	*0*	*0*
	False positives (20 runs)	*0*	*0*	*0*

Finally, we measure the execution time of the Spectrum Intelligence algorithm for varying numbers of analyzed bursts. The results are shown in Figure 9.

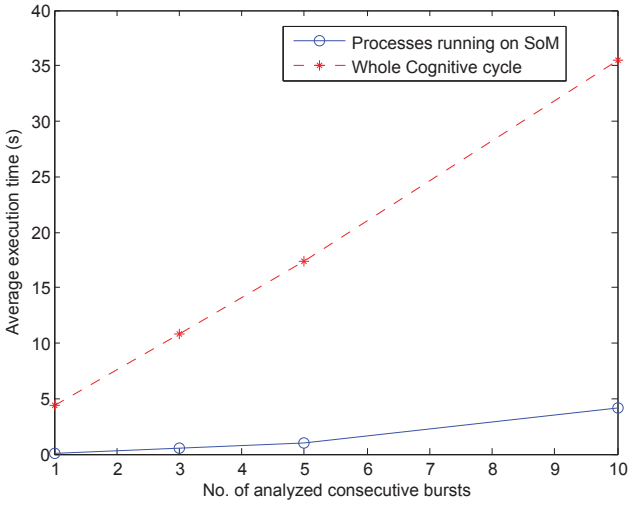


Fig. 9: Average execution times of the Spectrum Intelligence algorithm

Full blue line shows the computational time of the Process-Analyze-Learn-Decide phase of the Spectrum Intelligence, corresponding to all the processes that are running on the SoM. Computational times of the whole cognitive cycle, including the sensing time and the time needed to deploy the appropriate SNMP command on the radio are represented by the dashed red line. Sensing time takes approximately 3 seconds per burst, whereas invoking and executing the SNMP command takes approximately 1.3 seconds. In case of channel surfing, additional frequency settling time of the HH is

negligible, and corresponds to 40 microseconds.

The performance of the Spectrum Intelligence algorithm as a whole depends primarily on the jamming tactics deployed by the adversaries, as well as on the system parameters such as number of available channels for frequency hopping, and successful classification of these channels as spectrum holes depending on the occurrences of "friendly"/other waveforms in the system. Against naive narrowband jamming entities that change their transmission frequency slowly, Spectrum Intelligence proffers next to a foolproof strategy for jamming evasion. However, against more advanced opponents that are able to adapt their tactics as fast as the Spectrum Intelligence algorithm, the performance is yet to be evaluated.

5. CONCLUSIONS AND FUTURE WORK

In the paper, we have presented the ideas, development and implementation aspects of the Spectrum Intelligence algorithm for Interference Mitigation. The algorithm is based on the learning capabilities and the on-the-fly reconfiguration of the transmission-related parameters characteristic to Cognitive Radio technology. Implementation of the algorithm was done on the SWAVE HandHeld - a military Software Defined Radio - interconnected with the computationally powerful System-on-Module. Performance of several crucial functionalities of the algorithm was evaluated and presented. Main identified challenges included: finding optimal algorithm for adaptive energy detection thresholding; optimal set of features for waveform comparison and classification, and reasonable execution time.

Future work will involve further work on the optimal adaptive thresholding, as well as the more advanced waveform classification techniques. Testing of all of the implemented functionalities will be done against emulated Cognitive Radio jammers able to deploy advanced jamming tactics.

Acknowledgements

This work was partially developed within the nSHIELD project (http://www.newshield.eu) co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-programme SP6) focused on the research of SPD (Security, Privacy, Dependability) in the context of Embedded Systems.

The authors would like to thank Selex ES and Sistemi Intelligenti Integrati Tecnologie (SIIT) for providing the equipment for the test bed, and the laboratory premises for the test bed assembly. Particular acknowledgments go to Virgilio Esposto of Selex ES and to Gabriele Dura of University of Genova, for providing expertise and technical assistance.

6. REFERENCES

[1] J. Mitola and Jr. Maguire, G.Q., "Cognitive radio: making software radios more personal," *Personal Communications, IEEE*, vol. 6, no. 4, pp. 13–18, 1999.

[2] Qing Zhao and B.M. Sadler, "A survey of dynamic spectrum access," *Signal Processing Magazine, IEEE*, vol. 24, no. 3, pp. 79–89, May 2007.

[3] M. O. Mughal, L. Marcenaro, and C. S. Regazzoni, "Energy detection in multihop cooperative diversity networks: An analytical study," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[4] G. Bartoli, D. Marabissi, R. Fantacci, L. Micciullo, C. Armani, and R. Merlo, "Performance evaluation of a spectrum-sensing technique for ldacs and jtids coexistence in l-band," in *Proceedings of SDR'12 - WinnComm-Europe*, June 2012, pp. 17–23.

[5] A. Tkachenko, D. Cabric, and R.W. Brodersen, "Cyclostationary feature detector experiments using reconfigurable bee2," in *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, April 2007, pp. 216–219.

[6] S. Kapoor, S.V.R.K. Rao, and G. Singh, "Opportunistic spectrum sensing by employing matched filter in cognitive radio network," in *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, June 2011, pp. 580–583.

[7] R. Poisel, *Introduction to Communication Electronic Warfare Systems*, Artech House, Inc., Norwood, MA, USA, 2 edition, 2008.

[8] F. Delaveau, A. Evesti, J. Suomalainen, and N. Shapira, "Active and passive eavesdropper threats within public and private civilian wireless-networks - existing and potential future countermeasures - a brief overview," in *Proceedings of SDR'13 -WinnComm-Europe*, June 2013, pp. 11–20.

[9] K. Dabcevic, A. Betancourt, C.S. Regazzoni, and L. Marcenaro, "A fictitious play-based game-theoretical approach to alleviating jamming attacks for cognitive radios," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, 2014, pp. 8208–8212.

[10] H.B. Yilmaz, T. Tugcu, F. Alagoz, and S. Bayhan, "Radio environment map as enabler for practical cognitive radio networks," *Communications Magazine, IEEE*, vol. 51, no. 12, pp. 162–169, December 2013.

[11] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Trans. on Commun.*, vol. 55, no. 1, pp. 21–25, 2007.

[12] D. Cabric, S.M. Mishra, and R.W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, Nov 2004, vol. 1, pp. 772–776 Vol.1.

[13] N.T. Nguyen, Rong Zheng, and Zhu Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric bayesian classification," *Signal Processing, IEEE Transactions on*, vol. 60, no. 3, pp. 1432–1445, 2012.

[14] H.L. Hirsch, "Statistical signal characterization - new help for real-time processing," in *Aerospace and Electronics Conference, 1992. NAECON 1992., Proceedings of the IEEE 1992 National*, May 1992, pp. 121–127 vol.1.

[15] W. M. Meleis, *Signal detection and digital modulation classification-based spectrum sensing for cognitive radio*, Ph.D. thesis, Northeastern University, Boston, Massachusetts, 2013.

[16] SelexES, "Swave hh specifications," 2013.

[17] K. Dabcevic, L. Marcenaro, and C. S. Regazzoni, "Spd-driven smart transmission layer based on a software defined radio test bed architecture," in *Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems*, 2014, pp. 219–230.

Experimental Study of Spectrum Estimation and Reconstruction based on Compressive Sampling for Cognitive Radios

M. O. Mughal*, K. Dabcevic, G. Dura, L. Marcenaro and C. S. Regazzoni
Department of Electrical, Electronic, Telecommunications Engineering and Naval Architecture - DITEN
University of Genova, Genova, Italy.
*Email: ozairmughal@ginevra.dibe.unige.it

***Abstract*—This paper addresses the experimental study of the wide band signal estimation and reconstruction using the established compressive sampling (CS) methods. For this purpose, a hardware test bed was setup inter-connecting a wide band SDR based hand held military radio (SWAVE HH or HH), vector signal generator, bi-directional coupler, attenuators, PC and other auxiliaries. Real-world communication signals were created by the signal generator and SWAVE HH was used to scan these signals. The discrete samples from the HH were collected on PC for reconstruction and application of CS. It was shown that good reconstruction of the acquired wide band signal is possible with sub-Nyquist rate sampling by means of signal reconstruction under CS framework. In the end, mean squared error (MSE) performance is shown to indicate better estimation and reconstruction of the signal with higher compression rate and higher sparsity.**

I. Introduction

Software Defined Radio (SDR) is a communication device in which some or all of the physical layer functions are defined in software. Traditionally, Cognitive Radio (CR) is assembled upon SDR [1], [2]. CR is a technology that allows unlicensed users to access the licensed frequency bands opportunistically. Hence, spectrum awareness is of prime importance for CR terminals. Spectrum awareness, in addition to open database (as in IEEE 802.22), typically comes from spectrum sensing which can be achieved by means of different methods, for example, matched filter detection, cyclo-stationary detection or energy detection [3]. Matched filter is a coherent detector and requires a priori information of the licensed users' signals thus increasing the CR complexity. Cyclo-stationary detector make use of some of the inherent properties of the licensed users' signals and uses computationally complex algorithms to identify the spectrum holes. Energy detector is a non-coherent or blind detector which only measures the energy of the received signal, and takes decision on spectrum availability after comparing the measured energy with a predefined threshold. Each of these methods has its own pros and cons, however, energy detection appears as a preferred choice for CRs with limited computational power, due to their low implementation complexity.

Lately, there has been much interest shown by researchers on the analysis of energy detectors both in narrowband [4], [5] and wideband regimes [6], [7]. Nevertheless, the task of spectrum sensing becomes increasingly difficult for wideband signals. It is because the receiver requires to sample the wideband signals at or above Nyquist rates. This, in turn, requires very high-rate analog-to-digital converters (ADC) which increases the cost of the CR terminals. To overcome this shortcoming, compressive sampling (CS) [8] has stormed into the signal processing research for the purpose of spectrum estimation and reconstruction. Literature on CS shows that a sparse signal can be recovered from random or random like samples taken at sub-Nyquist rates. Due to low spectrum occupancy by licensed users, the signals in CR networks are typically sparse in the frequency domain. Recovery using CS requires intense, non-linear optimization to find the sparsest solution. One solution to this is by means of Convex Programming as in Basis Pursuit (BP) method [9]. BP is a technique for decomposing a signal into an optimal superposition of dictionary elements and the optimization criterion is the l_1-norm of coefficients. The other solution is the usage of Greedy Algorithms, such as Matching Pursuit (MP) and Orthogonal MP (OMP) [10], [11]. For instance, MP iteratively incorporates into the reconstructed signal the component from the measurement set that explains the largest portion of the residual from the previous iteration. OMP additionally orthogonalizes the residual against all measurement vectors selected in previous iterations.

This work addresses the applicability of CS approach to spectrum estimation and reconstruction to real world communication data acquired from a wide band SDR based hand held military radio (SWAVE HH or HH) [12]. For these purposes, a test bed was assembled for a frequency range of interest, consisting of a HH interconnected with the PC; vector signal generator; and the corresponding auxiliaries. For the demonstration purpose, we choose to implement a conventional CS approach, i.e., BP. To find the sparsest solution, BP requires to solve the complex optimization problem for an underdetermined system of equations. The Primal-Dual (PD) interior-point method solves this convex optimization by using the classical Newton Method. Performance of the scheme was evaluated for different values of compression rates. It was shown that through application of CS, sub-Nyquist rate sampling can achieve good signal reconstruction. This is particularly useful because it can reduce the cost incurred by high rate ADCs. In the end, performance is also shown

in terms of Mean squared error (MSE) of the reconstructed waveform under different compression ratios.

The rest of the paper is organized as follows. Section II describes the system model and CS preliminaries. Section III outlines the test bed architecture while experimental results are presented in Section IV. Finally, the paper is concluded in Section V along with some future directions.

II. System Model and CS Preliminaries

Herein, we explain our system model along with the preliminaries of compressive sampling along the lines of [6]. The received time-domain wideband signal at the HH can be expressed as,

$$r(t) = h(t) * s(t) + w(t) \tag{1}$$

where $h(t)$ is the channel coefficient between transmitter and HH, $s(t)$ denotes the transmitted signal, $*$ denotes the convolution operation and $w(t)$ is the additive white gaussian noise (AWGN) with zero mean and power spectral density σ_w^2.

In order to observe the frequency response of the received signal, an N-point discrete fourier transform (DFT) is taken on $r(t)$. Collecting the frequency-domain samples into an $N \times 1$ vector r_f, we have

$$\mathbf{r}_f = \mathbf{D}_h \mathbf{s}_f + \mathbf{w}_f \tag{2}$$

where $\mathbf{D}_h = diag(\mathbf{h}_f)$ is an $N \times N$ diagonal channel matrix, and $\mathbf{h}_f$, $\mathbf{s}_f$ and $\mathbf{w}_f$ are the discrete frequency-domain samples of $h(t)$, $s(t)$ and $w(t)$, respectively. In general form, this signal model can be written as,

$$\mathbf{r}_f = \mathbf{H}_f \overline{\mathbf{s}}_f + \mathbf{w}_f \tag{3}$$

Given the above expression, the spectrum sensing task boils down to estimating $\overline{\mathbf{s}}_f$ in (3) provided we have $\mathbf{H}_f$ and $r(t)$. However, since we have a wideband signal at our disposal, it will be beneficial to apply CS framework to relieve high sampling rate (Nyquist rate) ADC requirements. Recent advances in CS have demonstrated reliable signal reconstruction at sub-Nyquist rate sampling via computationally feasible algorithms, such as BP, MP or OMP.

At first, the compressed time-domain samples are collected at the receiver. For this, a compressive sampling matrix $\mathbf{S}_c$ is adopted to collect a $K \times 1$ sample vector $\mathbf{x}_t$ from $r(t)$ as follows:

$$\mathbf{x}_t = \mathbf{S}_c \mathbf{r}_t \tag{4}$$

where $\mathbf{r}_t$ is the $N \times 1$ vector of discrete-time representations of $r(t)$ at the Nyquist rate with $K \leq N$, and $\mathbf{S}_c$ is the $K \times N$ projection matrix. There are various designs introduced in literature for compressive sampler such as non-uniform sampler [13] and random sampler [14], [15].

With the K compressed measurements, the frequency response $\overline{\mathbf{s}}_f$ can now be estimated in (3). Noting that $\mathbf{r}_t = \mathbf{F}_M^{-1} \mathbf{r}_f$, we can write

$$\mathbf{x}_t = \mathbf{S}_c^T \mathbf{F}_M^{-1} \mathbf{H}_f \overline{\mathbf{s}}_f + \tilde{\mathbf{w}}_f \tag{5}$$

where $\tilde{\mathbf{w}}_f = \mathbf{S}_c^T \mathbf{F}_M^{-1} \mathbf{w}_f$ is the noise sample vector which is white gaussian. In CR networks, the spectrum occupancy by the licensed users is typically low. Thus the signal vector $\mathbf{s}_f$ is sparse in frequency domain with few non-zero entries. The sparsity is measured by p-norm $||\overline{\mathbf{s}}_f||_p$, $p \in [0, 2)$, where $p = 0$ indicates exact sparsity.

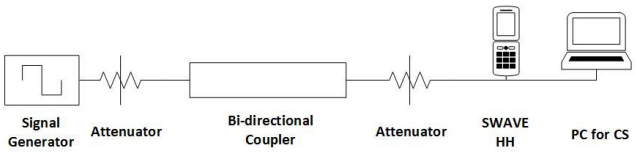


Fig. 1. Simplified block diagram of the assembled test-bed.

Thus, equation (5) is a linear regression problem with signal $\overline{\mathbf{s}}_f$ being sparse. This signal $\overline{\mathbf{s}}_f$ can be reconstructed by solving the following linear convex optimization problem:

$$\min_{\overline{\mathbf{s}}_f} ||\overline{\mathbf{s}}_f||_1, \quad s.t. \quad \mathbf{x}_t = \mathbf{S}_c^T \mathbf{F}_M^{-1} \mathbf{H}_f \overline{\mathbf{s}}_f \tag{6}$$

There are different methods to solve this optimization problem, for example, by means of Convex Programming as in BP method or by usage of Greedy Algorithms such as MP or OMP.

III. SDR Test-bed Setup

In this section, we will briefly outline the SDR test-bed setup which we used to obtain our required real world experimental data. More details about the test bed assembly can be found in [16].

A test bed was assembled for a frequency range of interest, consisting of a HH interconnected with the PC, vector signal generator and the corresponding auxiliaries. A simplified block diagram is shown in Fig. 1. Agilent E4438C signal generator is used to generate various real-world, as well as custom, wideband and narrowband signals. The signal generator is connected to Agilent 778D 100MHz - 2GHz dual directional coupler with 20 dB nominal coupling, by means of a coaxial RF cable. Use of coaxial cable allows us to repeat the experiment under same conditions, eliminating uncertainties of wireless transmission. On each end of the coupler, two programmable attenuators of 30 dB attenuation value were connected. HH was then connected to the attenuator by means of RF cable and was also connected to the PC through serial port. HH is a fully operational SDR transceiver capable of processing various wideband and narrowband waveforms. Currently, two functional waveforms are installed on the radio: SelfNET Soldier Broadband Waveform (SBW) and VHF/UHF Line Of Sight (VULOS), as well as the waveform providing support for the Internet Protocol (IP) communication in accordance with MIL-STD-188-220C specification [17]. HH has 12-bit analog-to-digital converter (ADC) which performs the sampling of incoming signals at very high rates of 250 Msamples/sec, and it is capable of scanning 120 MHz of wideband. The digitized signal is then issued to the FPGA, where it undergoes down conversion, matched filtering and demodulation. Being a military technology, several technical characteristics of SWAVE HH , i.e., processor specifications and more in-depth operational details are inclosable.

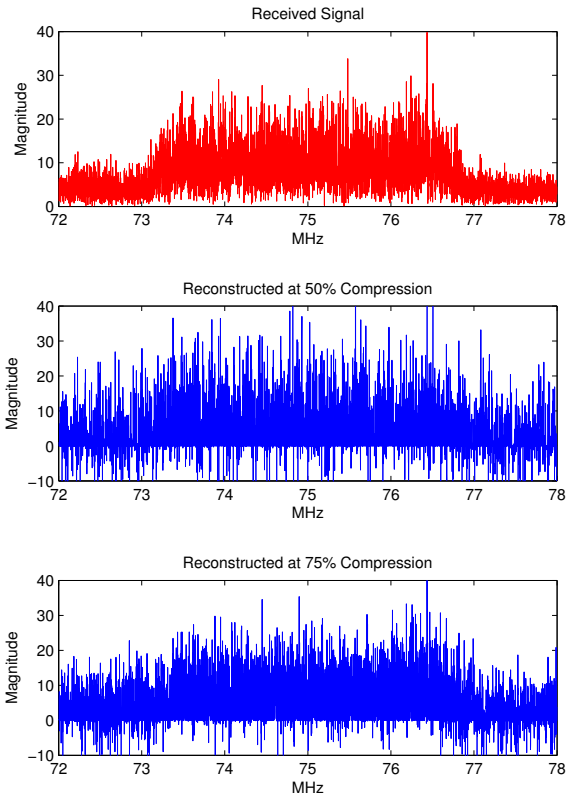


Fig. 2. (a) Received 3 MHz wide band gaussian waveform; (b) reconstruction at 50% compression ratio; (c) reconstruction at 75% compression ratio.

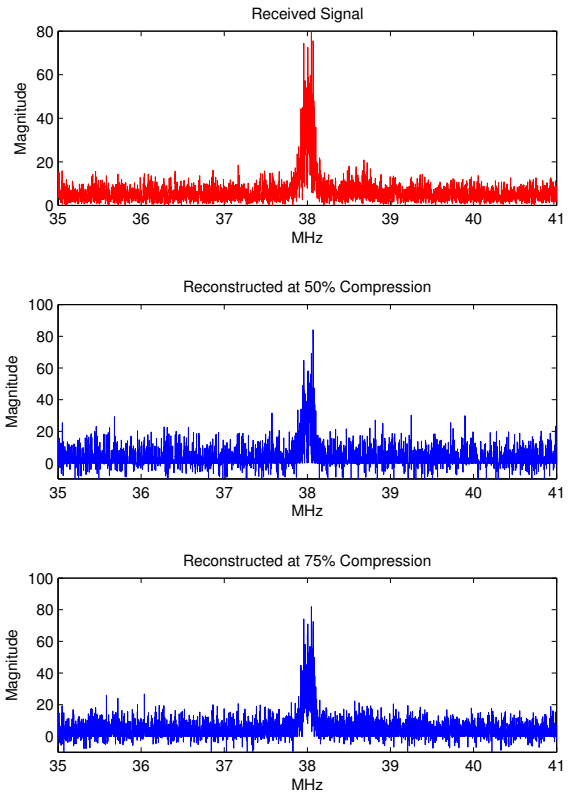


Fig. 3. (a) Received 250 KHz narrow band GSM waveform; (b) reconstruction at 50% compression ratio; (c) reconstruction at 75% compression ratio.

Several interfaces are available on the HH, namely, 10/100 Ethernet, USB 2.0, RS-485 serial, DC power interface and PTT. Ethernet connection on the SWAVE HH is used for the remote control of the HH, using Simple Network Management Protocol (SNMP) while serial connection is used for transferring the spectrum snapshots from HH to PC. Since the data transfer rate of the serial port is low, i.e., 115200 bits/s, therefore, real time transfer of samples is not possible from the ADC of HH. Because of this, 8192 samples are transmitted from the ADC over the RS-485 serial port every 1.3 seconds. It is a functionality hard-coded in the HH's FPGA. Specifically speaking, the output of ADC contains discrete samples of the wideband signal. These samples are stored in an internal buffer of the FPGA and output through HH's serial port to the PC, where they can be processed. Because 8192 samples make the waveform analysis a difficult task due to the low frequency resolution, multiple snapshots of the spectrum are taken and analyzed at once. Once that the satisfying number of samples is collected and transferred to the PC, CS may be performed.

IV. Experimental Results

For our experiments, we generated two different kinds of waveforms from the Agilent E4438C vector signal generator, namely;

1) 3 MHz wide band gaussian waveform, and
2) 250 KHz narrow band GSM waveform.

These two waveforms were centered at 75 MHz and 38 MHz carrier frequencies before transmission. At the receiver side, SWAVE HH scanned the entire 120 MHz of bandwidth to locate these waveforms. The HH outputs 8192 digitized samples every 3 seconds from its serial port. Because 8192 samples are not sufficient to observe a meaningful waveform, we capture multiple bursts, i.e., 8192×10 samples to construct meaningful waveforms. These samples are then gathered on a PC through the serial port for the application of CS.

Reconstruction: In Fig. 2, we show the received wide band 3 MHz gaussian signal in frequency-domain and its reconstructed versions with 50% and 75% of compression ratios. It can be seen that reconstruction at $K/N = 0.75$ appears better than the reconstruction at $K/N = 0.5$. The same trend is observable in Fig. 3 where we plot the 250 KHz GSM waveform with its reconstructed versions with compressed samples. However, the reconstruction of GSM signal appears better even with low K/N ratio of 0.5. It is because the GSM signal has more sparsity (or zero elements)

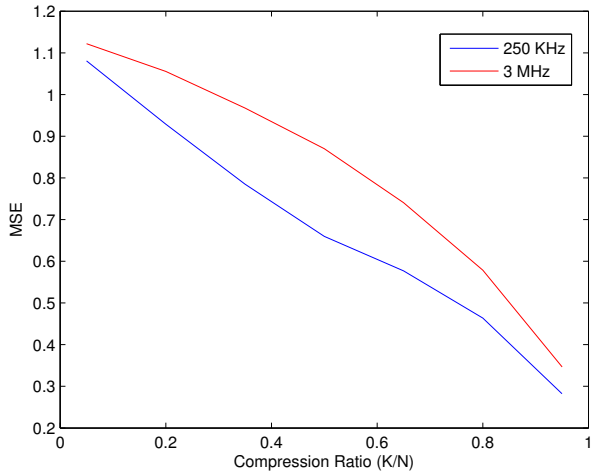


Fig. 4. MSE performance of 250 KHz GSM waveform compared with 3 MHz gaussian waveform at different compression rates.

compared to the 3 MHZ wide band signal, permitting for better reconstruction even with low compression ratios.

MSE Performance: We compare the normalized MSE of the reconstructed 3 MHZ signal with that of 250 KHz signal, at varying compression rates in Fig. 4. The normalized MSE is defined as

$$MSE = E\left\{\frac{||\hat{\mathbf{s}} - \mathbf{s}||_2^2}{||\mathbf{s}||_2^2}\right\} \quad (7)$$

where $\mathbf{s}$ is the signal vector sampled at Nyquist rate (or in our case at 8.192×10^4 samples) while $\hat{\mathbf{s}}$ is the estimated signal vector with compressed samples. We can see that MSE decreases with increasing K/N ratio. Furthermore, MSE performance of 250 KHz signal is better than the 3 MHz signal due to higher sparsity.

V. Conclusion and Future Work

In this work, we conducted an experimental study of the compressive sampling based wide band signal estimation and reconstruction. To gather real-world communication data, a hardware test bed was setup consisting of an SDR based radio, signal generator, PC and corresponding auxiliaries. Different real-world signals were captured by the HH and studied under CS framework. It was shown that reconstruction was successfully achieved with fewer than the Nyquist rate samples on real-world communication data. MSE performance was also shown to improve with higher sparsity in the data and higher compression ratios.

In future, we plan to connect two more SWAVE HH at the input port and scan various pre-installed waveforms from these HHs by means of a third HH. We also plan to study and implement various collaborative spectrum sensing algorithms based on the CS framework, which allows for more reliable spectrum holes detection in wide band regime and improves the overall spectrum utilization.

Acknowledgements

This work was developed within nSHIELD project (http://www.newshield.eu) co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-programme SP6) focused on the research of SPD (Security, Privacy, Dependability) in the context of Embedded Systems.

The authors would like to thank Selex ES and Sistemi Intelligenti Integrati Tecnologie (SIIT) for providing the equipment for the test bed, and the laboratory premises for the test bed assembly. Particular acknowledgment goes to Virgilio Esposto of Selex ES, for providing expertise and technical assistance.

References

[1] J. Mitola and G. Q. Maguire Jr. Cognitive radio: Making software radios more personal. *IEEE Personal Commun.*, 6(4):13–18, Aug. 1999.

[2] S. Haykin. Cognitive radio: Brain-empowered wireless communication. *IEEE Journal on Selected Areas in Communications*, 23(2):201–220, Feb. 2005.

[3] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks*, 50:2127–2159, 2006.

[4] F. F. Digham, M.-S. Alouini, and M. K. Simon. On the energy detection of unknown signals over fading channels. *IEEE Trans. on Commun.*, 55(1):21–25, 2007.

[5] M. O. Mughal, L. Marcenaro, and C. S. Regazzoni. Energy detection in multihop cooperative diversity networks: An analytical study. *International Journal of Distributed Sensor Networks*, 2014:9 pages, 2014.

[6] F. Zheng, C. Li, and Z. Tian. Distributed compressive spectrum sensing in cooperative multihop cognitive networks. *IEEE Journal of Selected Topics in Signal Processing*, 5(1):37–48, Feb. 2011.

[7] J. Haupt and R. Nowak. Compressive sampling for signal detection. In *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, pages 1509–1512, 2007.

[8] D. L. Donoho. Compressed sensing. *IEEE Trans. on Information Theory*, 52(4):1289–1306, April 2006.

[9] S. Chen, D. L. Donoho, and M. A. Saunders. Atomic decomposition by basis pursuit. *SIAM J. Sci. Comp.*, 20(1):33–61, 1999.

[10] M. F. Duarte, M.B. Wakin, and R.G. Baraniuk. Fast reconstruction of piecewise smooth signals from random projections. In *SPARS*, 2005.

[11] J. A. Tropp and A. C. Gilbert. Signal recovery from random measurements via ofthogonal matching pursuit. *IEEE Trans. on Information Theory*, 53(12):4655–4666, 2007.

[12] *SWAVE HH specifications, http://www.selexelsag.com/ internet/localization/IPC/media/docs/ SWave-Handheld-Radio-v1-2012Selex.pdf.*

[13] P. Feng and Y. Bresler. Spectrum-blind minimum-rate sampling and reconstruction of multiband signals. In *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, volume 3, pages 1685–1691, May 1996.

[14] Z. Yu, S. Hoyos, and M. Sadler. Mixed-signal parallel compressed sensing and reception for cognitive radio. In *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, pages 3861–3864, 2008.

[15] J. Laska, S. Kirolos, Y. Massoud, R. Baraniuk, A. Gilbert, M. Iwen, and M. Strauss. Random sampling for analog-to-information conversion of wideband signals. In *Proc. IEEE Dallas/CAS Workshop on Design, Applications, Integration and Software*, pages 119–122, 2006.

[16] K. Dabcevic, L. Marcenaro, and C. S. Regazzoni. Spd-driven smart transmission layer based on a software defined radio test bed architecture. In *Proc. of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems*, pages 219–230, Jan. 2014.

[17] H. Li, P. D. Amer, and S. C. Chamberlain. Estelle specification of mil-std 188-220 datalink layer - interoperability standard for digital message transfer device subsystems. In *Proceedings of MILCOM*, 1995.