SPECTRUM INTELLIGENCE FOR INTERFERENCE MITIGATION FOR COGNITIVE RADIO TERMINALS

K. Dabcevic, M.O. Mughal, L. Marcenaro and C.S. Regazzoni

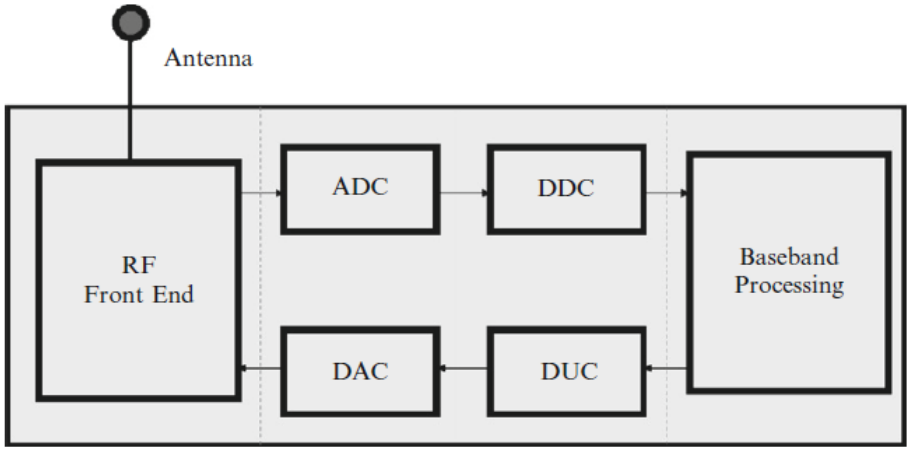
Department of Electrical, Electronics, Telecommunications Engineering and Naval Architecture – DITEN
University of Genoa

Presentation outline

1. Software Defined Radios and Cognitive Radios
2. Assembled SDR/CR test bed architecture
3. Communications electronic warfare
4. Spectrum Intelligence for interference mitigation
5. Experimental validation
6. Conclusions and future work

SDR and CR

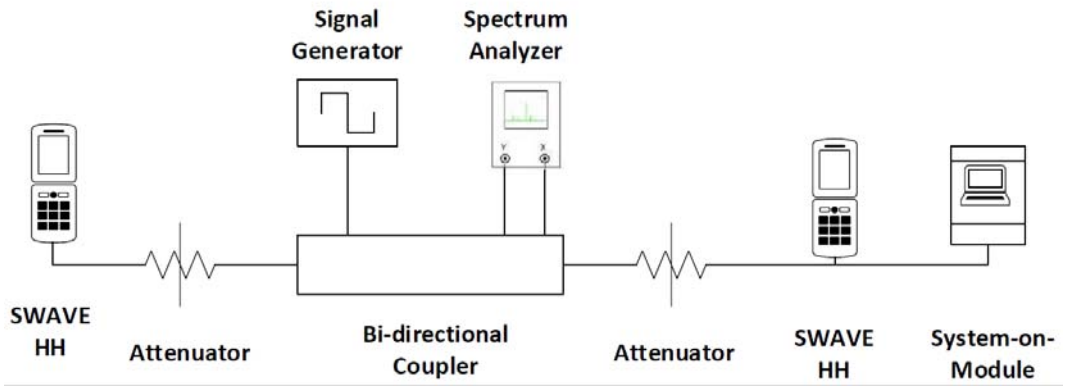
- Conventional digital radio
- Software Defined Radio (SDR)
  - Baseband processing entirely done in software
- Cognitive Radio (CR)
  - „A really smart radio”
  - Interoperability
  - Opportunistic Spectrum Access

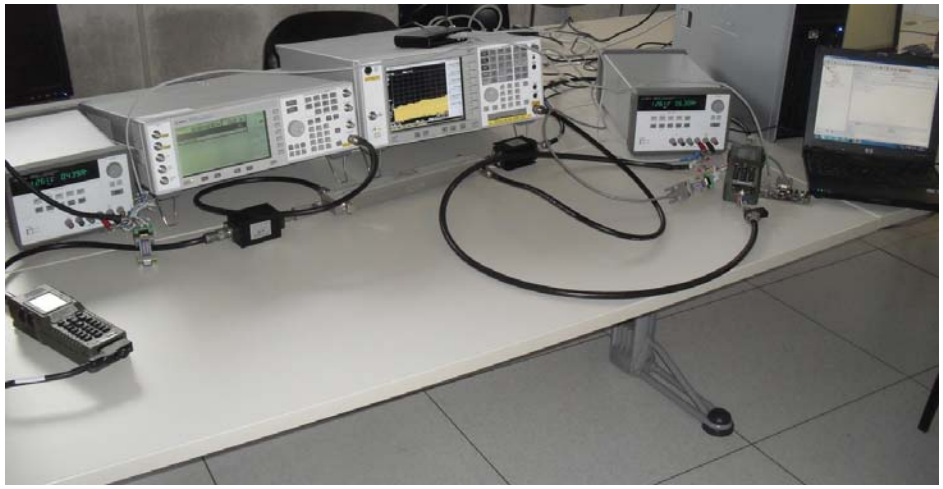


Schematic block diagram of a digital radio [1]

[1] M. Nekovee, “Dynamic spectrum access — concepts and future architectures,” *BT Technology Journal*, vol. 24, pp. 111–116, May 2006.

SDR/CR test bed architecture





- Coaxial test bed architecture
  - 2 SWAVE HandHelds
  - System-on-Module (OMBRA v2)
  - Vector signal generator
  - Spectrum analyzer
  - Auxiliaries

SDR/CR test bed architecture - SWAVE HH

- SWAVE HH – some technical specs:
  - Maximum transmit power: 5W
  - 12-bit 250 MHz A/D converters
    - VHF: direct conversion
    - UHF: superheterodyne conversion
  - FPGA:
    - DDC
    - Matched filtering
    - Demodulation
  - Hypertach expansion
    - 10/100 Ethernet
    - USB 2.0
    - RS-485 serial
    - DC power interface

SDR/CR test bed architecture - SoM

- OMBRA v2 System-on-Module – some technical specs:
  - ARM A8 processor @1GHz
  - Xilinx Spartan 6 FPGA + TMS320C64+ DSP
  - Several external interfaces:
    - 10/100 Ethernet
    - USB 2.0
    - RS-232 serial
    - DC power interface
  - Connection HH<->SOM:
    - Serial port – spectrum data
    - Ethernet – remote control of the radio

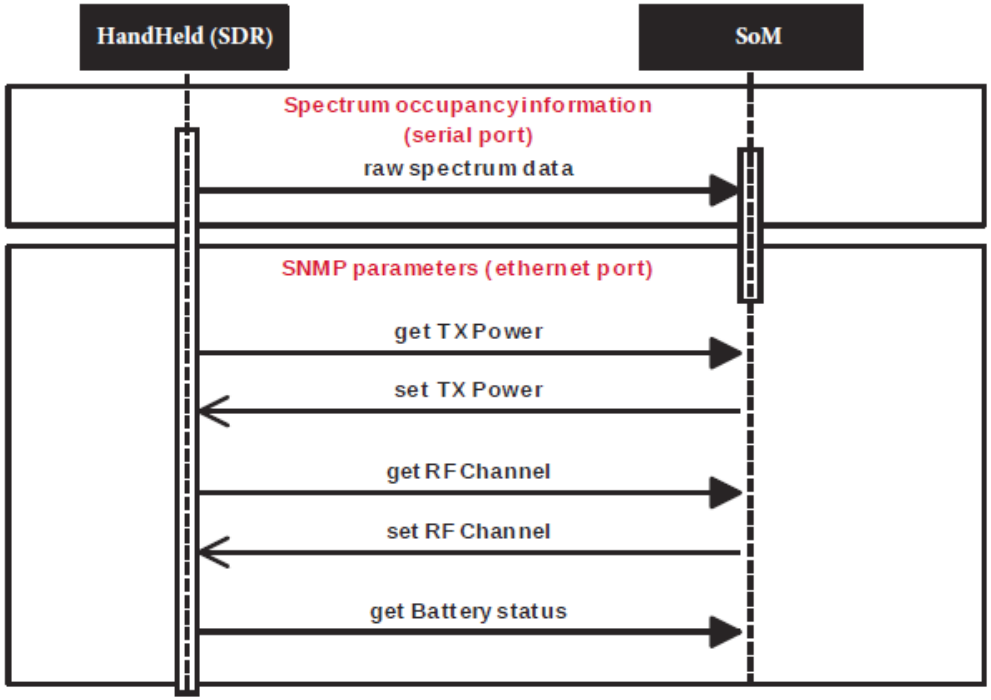
SDR/CR test bed architecture – remote control of HH

Parameter	Type	SNMP commands
File Transfer Activation	string	SET/GET
File Transfer Type	string	SET/GET
FTP User Name	string	SET/GET
FTP Password	string	SET/GET
FTP Address	string	SET/GET
Login Username	string	SET/GET
Login Password	string	SET/GET
Transmit Power	integer	SET/GET
Transmitter On/Off	integer	SET/GET
Currently Installed Waveform	string seq	GET
Waveform's MIB Root	string	GET
Waveform Status [ON/OFF]	integer	SET/GET
Audio Message ID	string	SET/GET
Create New Waveform	string	SET/GET
Activate Preset	string	SET/GET
Activate Mission File	string	SET/GET
Audio Output Gain	float	SET/GET
Battery Charge Percentage	integer	GET
File Download Status	integer	GET
Trap Receiver's IP Address	string	SET/GET
Zeroize All Crypto Keys	integer	SET/GET
Crypto Key Loaded	integer	GET
System End Boot [failed/ succeeded/ in progress]	integer	GET

- Simple Network Management Protocol (SNMP) v3
  - GET
  - SET
  - TRAP
- Parameters stored in Management Information Base (MIB)
  - Definitions of properties of the controllable parameters - OID

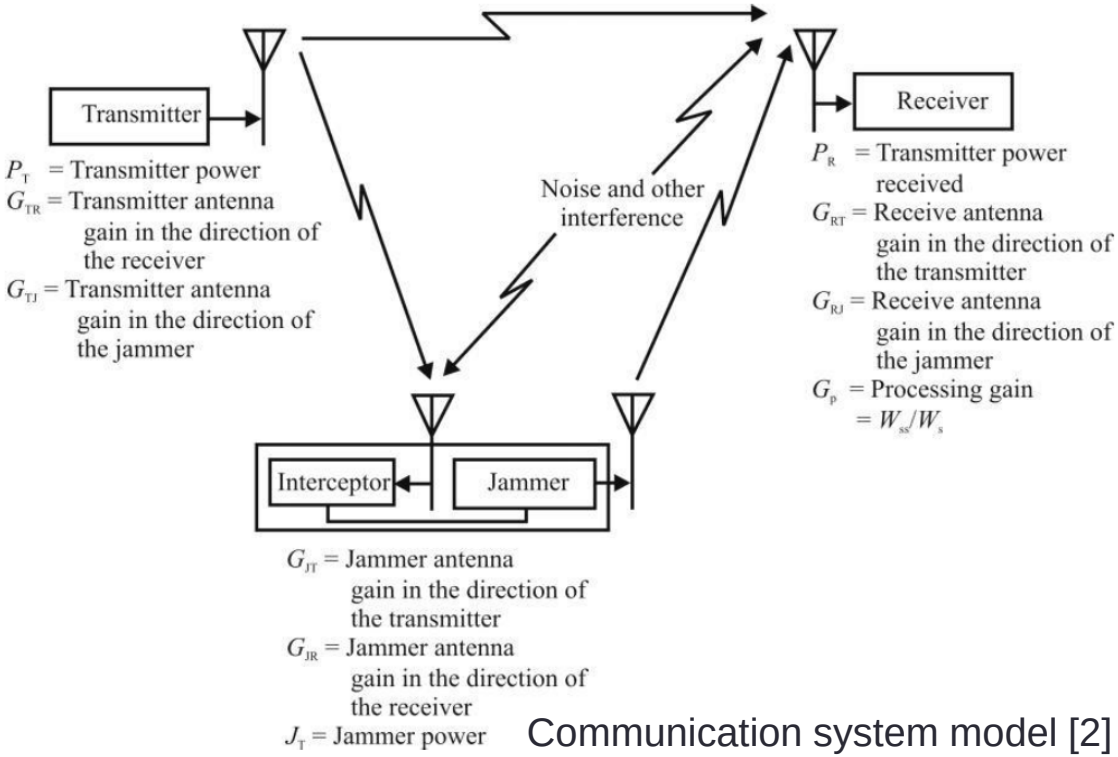
SDR/CR test bed architecture – spectrum sensing

- 14-bit ADC performs sampling at 250 Msamples/s
  - Every 3 seconds, a burst of 8192 consecutive samples buffered and outputted at 115200 bauds over serial port
  - All signal processing done on the SoM



Communication Electronic Warfare (CEW)

- Electronic attack
  - Intercepting or denying the communication on the target systems
  - Passive attacks (eavesdropping) and active attacks (RF jamming)
- Electronic defense
  - Preventing the electronic attacks from successfully occuring
- CEW and CRs
  - Self-reconfigurability + learning mechanisms = advanced CEW tactics



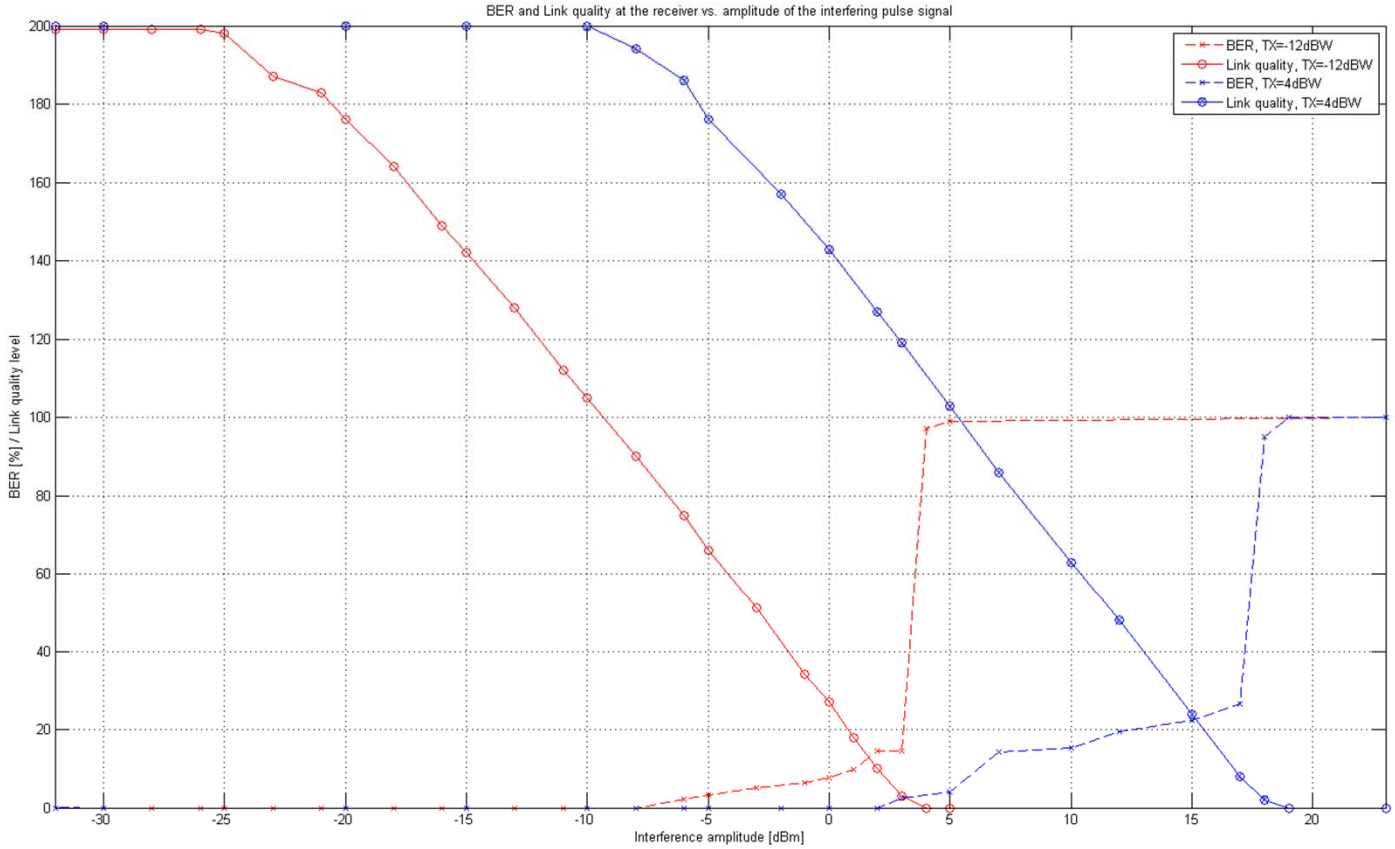
Communication system model [2]

[2] R. Poisel, „Moder communication jamming principles and techniques, 2nd ed., 2011”

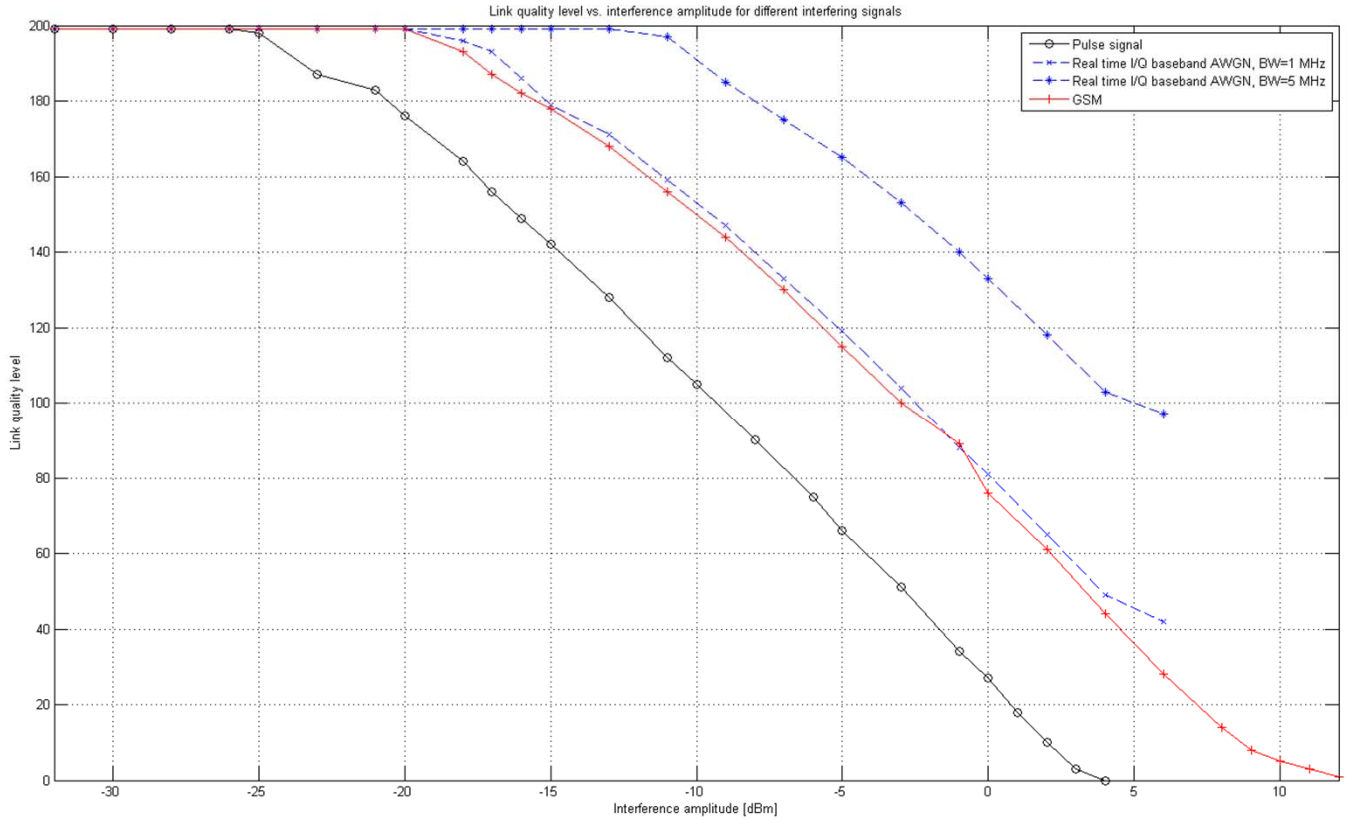
RF jamming

- Successful jamming depends, among other, on:
  - Channel conditions
  - Type of modulation;
  - Coding techniques;
  - Type of detector (coherent/non-coherent)
- Jamming in analog voice communication
  - >30% of communication unintelligible
- Jamming in digital data communication
  - >10% BER

Threshold effect in RF jamming

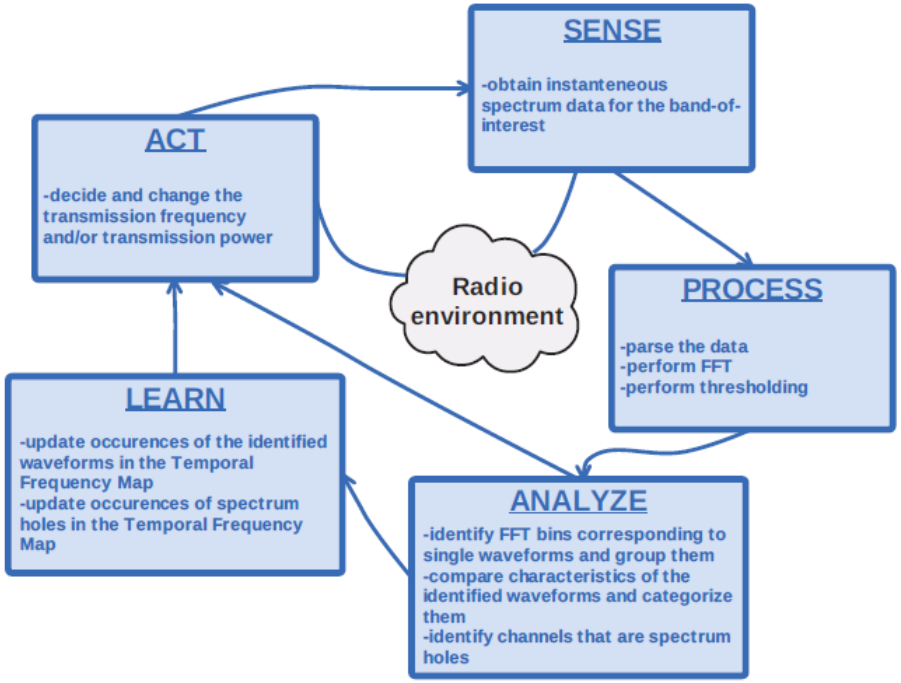


Influence of different jamming signals on the quality of communication



Spectrum Intelligence for interference mitigation

- Continuous monitoring of RF spectrum activities
- Identifying potential threats to communication
- Taking proactive electronic defense measures
- **Focus: practice before theory**!



Spectrum Intelligence for interference mitigation (2)

- Challenge: discriminating between „signal” and „noise”

$$Y(n) = \begin{cases} W(n) & H_0 \\ X(n) + W(n) & H_1 \end{cases}$$

received signal transmitted signal noise

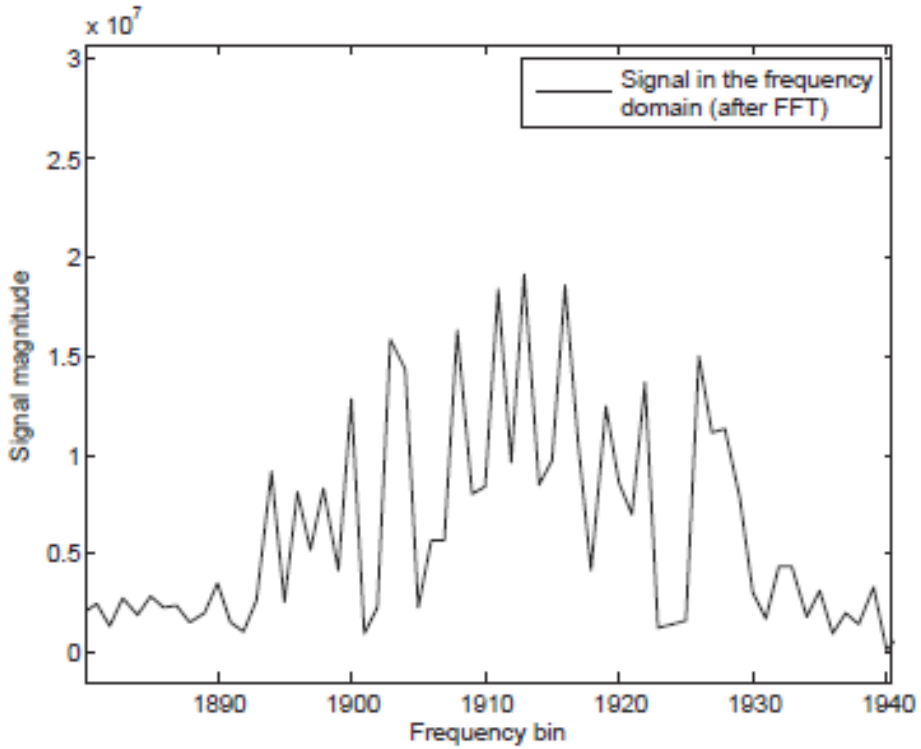
- Challenge: setting the appropriate threshold

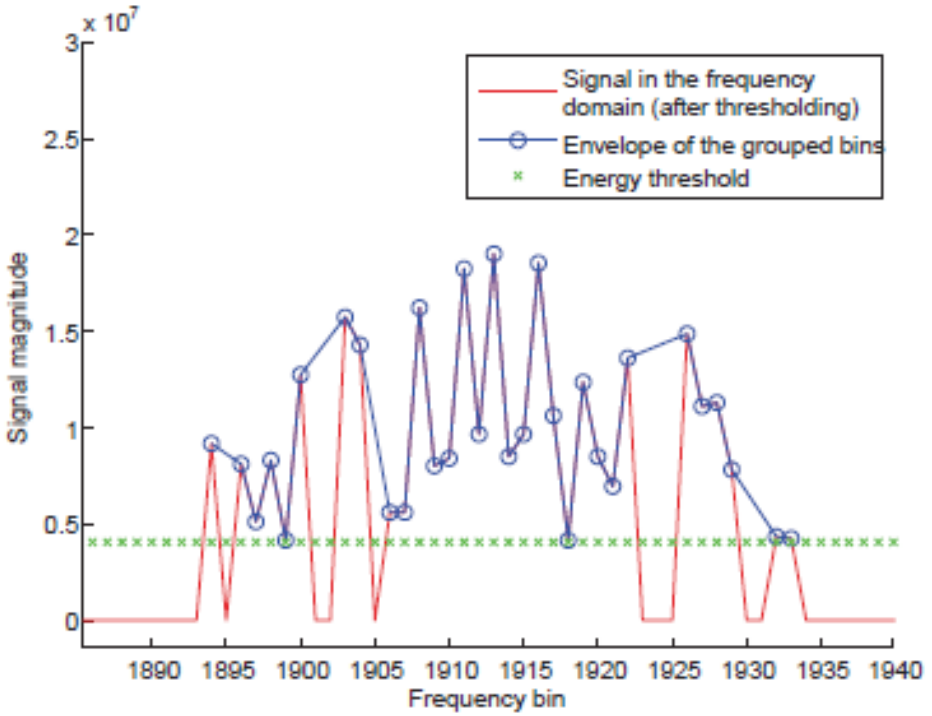
$$\hat{\lambda} = 2 \cdot \frac{1}{n} \sum |Y(n)|$$

- Challenge: grouping frequency bins corresponding to the same signal

$$d_{MAX} = K \cdot d_f \qquad d_f = \frac{2 \cdot f_{max}}{N_S}$$

Spectrum Intelligence for interference mitigation (3)





Spectrum Intelligence for interference mitigation (4)

- Next, parameter extraction is performed:
  - Center frequency
  - Bandwidth / 3dB bandwidth
  - Maximum value of the magnitude
- Waveform classification:
  - „friendly”
  - „potentially malicious”
- Spectrum holes are recognized
- Then, Temporal Frequency Map is assessed and updated
  - Temporal forgiveness over the last *k* steps

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	$m_{SH/1}$	$m_{SH/2}$		$m_{SH/n}$

Spectrum Intelligence for interference mitigation (5)

- Finally, the Spectrum Intelligence may decide to *act*
  - Proactively changing the transmission frequency

$$c_{t+1} \in (c_t = SH \mid (X(c_t) = min)$$

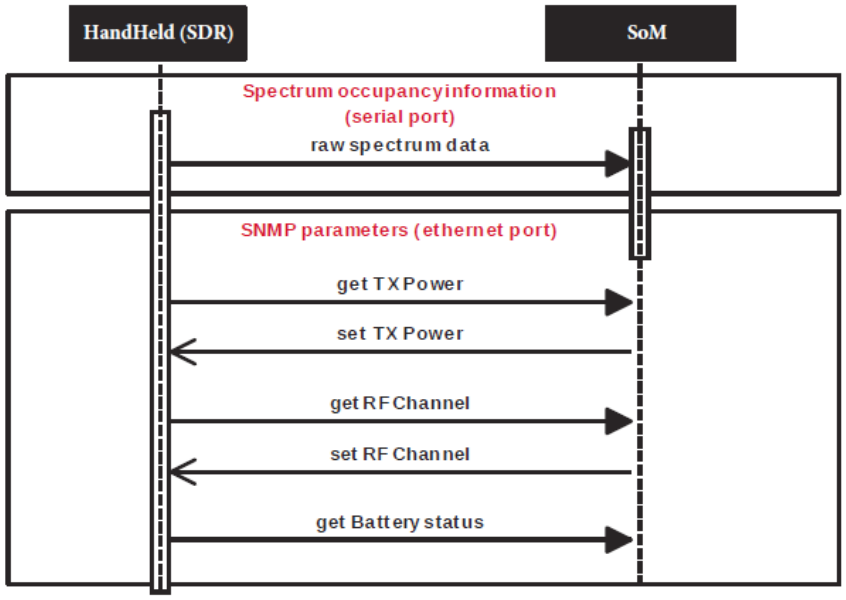
$$X(c_t) = k^2 \cdot m_{PM/c_t} + (k+1) \cdot m_{F/c_t} - m_{SH/c_t}$$

  - Increasing the transmission power

$$P_{t+1} \in P \mid P_R > 10log_{10}\hat{\lambda} + 3dB$$

Implementation on the SDR/CR test bed

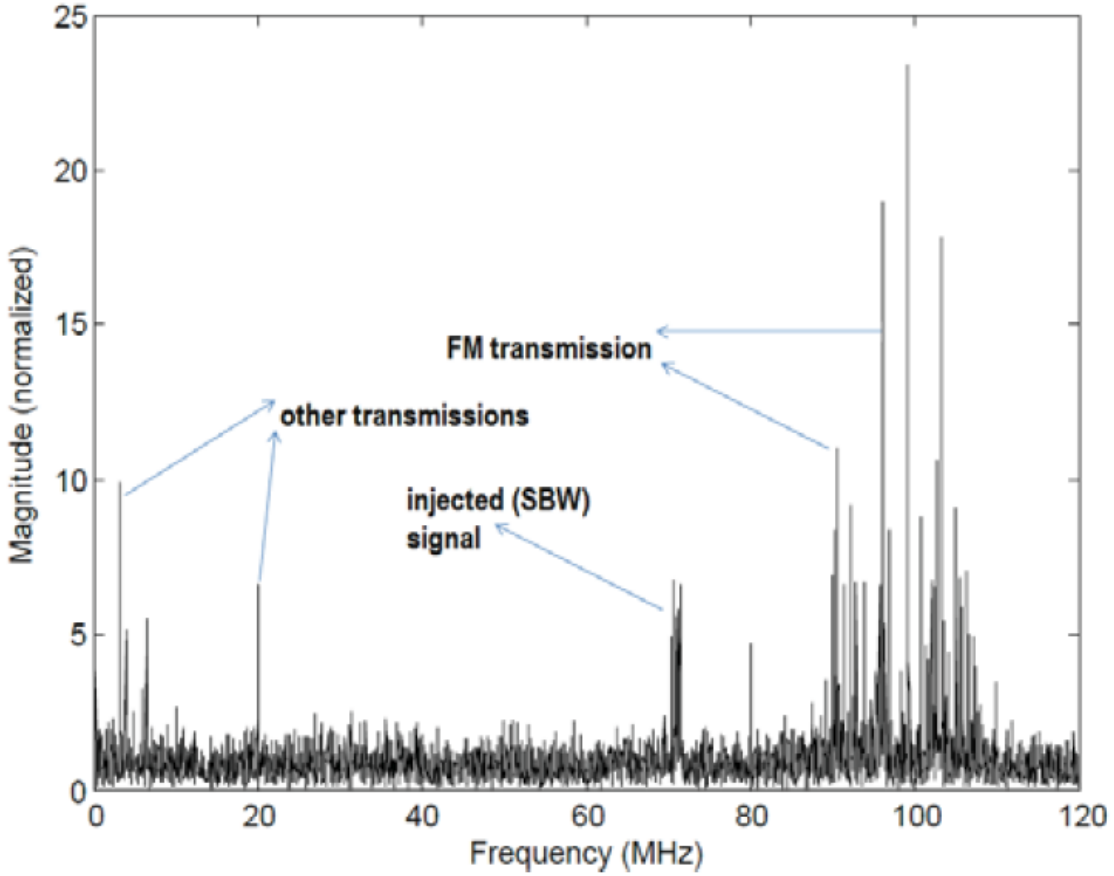
- Arbitrary (1-10) no. of consecutive bursts may be averaged and analyzed together
  - Assumption: high coherence time of the whole analyzed frequency band
- *Act* part of the Cognitive cycle is enabled by the SNMP v3 (GET/SET)
  - Occurs whenever the „under threat” alarm is triggered by the SI algorithm



Experiments

- Critical features: energy detection and waveform classification
- Experimental waveform – Soldier Broadband Waveform (SBW)
  - Digital waveform
  - 1.25 MHz bandwidth
  - Operable in VHF and UHF
- Critical parameters:
  - Energy detection threshold, $\hat{\lambda}$
  - Estimated no. of potentially erroneous consecutive samples, *K*
  - Similarity in the parameters of the waveforms
  - Level of tolerance on the analyzed parameters
  - Frequency resolution

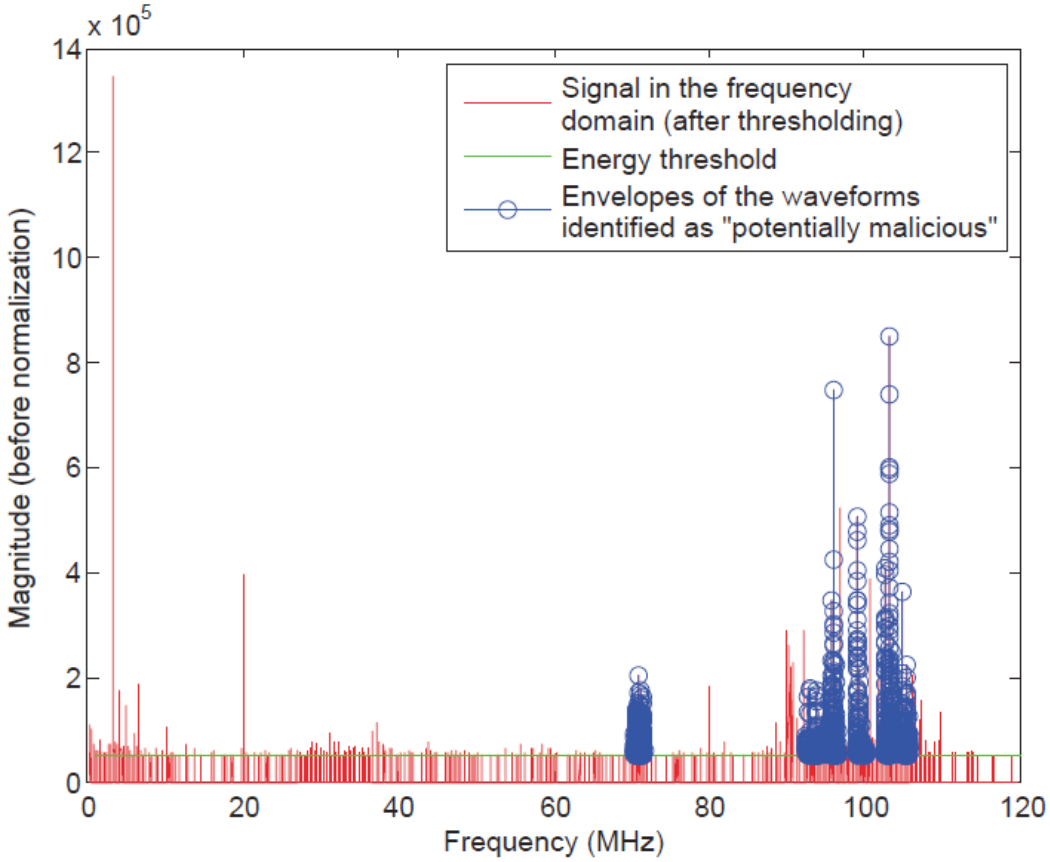
Experiments (2)



Experiments (3)

No. of bursts		Parameter tolerance (%) 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

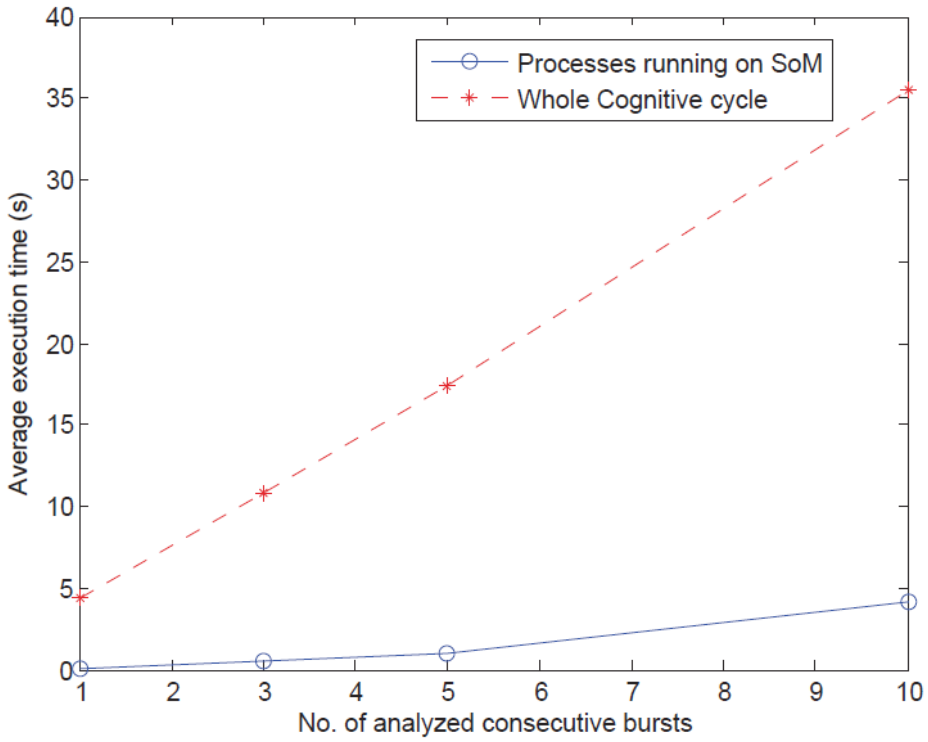
Only estimated bandwidths



Experiments (4)

No. of bursts		Parameter tolerance (%) 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

Estimated bandwidths & max magnitude



Average execution time

Future work

- Optimal adaptive thresholding
- More advanced waveform classification techniques
  - Statistical Signal Characterization
- Testing against advanced jammers

Acknowledgements

- This work was developed within nSHIELD project 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 (http://www.newshield.eu/)

- Selex ES (http://www.selex-es.com/)

- SIIT-Sistemi Intelligenti Integrati Tecnologie (http://www.siitscpa.it/)

Thank you

Q & A