Towards a key-free radio protocol for authentication and security of nodes and terminals in advanced waveforms

SDR'15 Winncomm, session 1, San Diego, 26 March 2015

Eric Nicollet

François Delaveau, Renaud Molière, Christiane Kameni Ngassa, Claude Lemenager

Thales Communications & Security; Gennevilliers, France

Taghrid Mazloum, Alain Sibille

Telecom ParisTech; Paris, France

Contacts: francois.delaveau@thalesgroup.com

Supported by PHYLAWS project FP7 ICT Id-317562

THALES Celeno TELECOM ParisTech PHYLAWS Imperial College London VTT

Summary

- Security lacks of networks' radio interface: the harsh reality
- Help of Physical Layer Security (PHYSEC)
- Tag Signals and Key-free authentication protocol
- Experimental measurements: first results
- Conclusion

Note: This paper is a follow up of Winncomm Munich 2013 papers

"Active and passive eavesdropper threats within public and private civilian networks – Existing and potential future countermeasures – An overview"

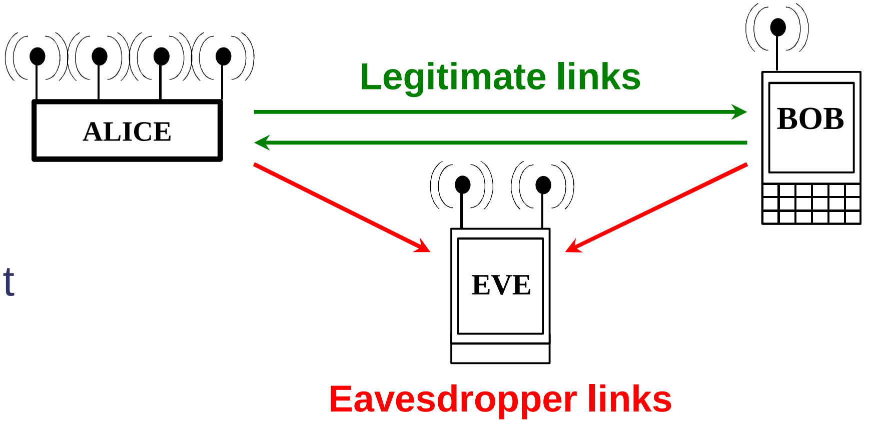
"PHYSEC concepts for wireless public networks – introduction, state of the art and perspectives"

Supported by PHYLAWS project FP7 ICT Id-317562

About security lacks of networks' radio interface: the harsh reality

Basic definitions

- **LEGITIMATE links are Alice to/from Bob**
- **EAVESDROPPER links are Alice to Eve and Bob to Eve**
- **Usual "Academic" hypothesis are:**
  - complete information of Eve about legitimate RATs/waveforms
  - no Information of Eve about legitimate Keys (e.g. Ki Keys on SIM cards)



- **TRANSEC (Transmission Security) is the waveform protection of the legitimate link face to interception of the transmitted radio signal, to intrusion attempts of the user receiver (and even jamming and direction finding)**
- **NETSEC (Network Transmission Security) is the protection of the signalling of the network of the legitimate link (usual solutions are authentication and integrity control, sometimes ciphering of signalling in military networks)**
- **COMSEC (Communication Security) is the protection of the content of user messages (voice, data). Most of solutions are based on ciphering + integrity control schemes**

Supported by PHYLAWS project FP7 ICT Id-317562

About security lacks of networks' radio interface: the harsh reality

The end of illusions

Usual assumptions of security are no more valid in wireless public networks, whatever the waveform is

- **Eve's knowledge about legitimate key is now usual**

Using failures of the SS7 and international roaming protocols to get Ki keys

  - Monitoring of Angela Merkel's smartphone during years
  - Security of subscribers is decreased by networks protocol failures and by operators' practices

SIM card providers may be hacked (to obtain Ki keys)

  - Revelations on hacking of SIM manufacturers by security agencies
  - Subscribers' keys may not be really secret in practice

- **Reveals especially that**
  - Subscribers' secret is not efficiently kept within public networks
  - Subscriber authentication, identification and roaming remain weak in 2G/3G/4G etc

Supported by PHYLAWS project FP7 ICT Id-317562

About security lacks of networks' radio interface: the harsh reality

Fall of usual assumptions

Usual assumptions of security are no more valid in wireless networks, whatever the RAT is:

- **Keys cannot be pre-distributed nor pre-computed by the legitimate users in wireless public networks**
- **Eve can intercept (and eventually disturb) early negotiation messages between Alice and Bob such as…**
  - Broadcast signalling
  - Channel State Information
  - Geolocated Sensing messages
  - Authentication of Bob and Alice
  - Ciphering key computation

… in order to

- Get information about Alice and Bob
- Impersonate Alice or Bob
- Overcome further protections (Ciphering negotiation, etc.)

Supported by PHYLAWS project FP7 ICT Id-317562

Help of Physical Layer Security (PHYSEC)

Principle and definition

What is PHYSEC (Physical Layer Security) ?

- **Key-less security technique exploiting propagation randomness to establish secret**
- **Theory is OK, practical applications in realistic radio-environment are in progress**

2 approaches for PHYSEC:

- **Secrecy codes: channel codes (FEC) are augmented with secrecy capabilities**
    - Require better radio link (SNR) between Alice and Bob than Alice and Eve
    - Approach Shannon capacity for legitimate link
    - Mitigate information at “any” other location

Theoretical feasibility is established but explicit design remains an active research domain

See Bloch and Barros,“Physical Layer security” ,Cambridge University Press, 2011

- **Secret Key Generation (SKG): keys are computed from propagation randomness**
    - Channels between legitimate nodes are reciprocal and uncorrelated elsewhere
    - Bits of the secret key are computed from channel measurements

Channel quantization algorithms target low mismatches between legitimate links
Existing SKG strategies ensure few information leakage to third parties

See Y. El Hajj et al., "Towards robust key extraction from multipath wireless channels“,
IEEE Journal of Comm. and Net., vol. 14, no. 4, Aug 2012

Supported by PHYLAWS project FP7 ICT Id-317562

Help of Physical Layer Security (PHYSEC)

Need for early and key-free secured authentication

- **Main advantages of PHYSEC**
  - PHYSEC avoids the use of ciphering keys, thus is resilient to any attack
    - Whatever the knowledge of Eve is
    - Whatever Eve's computing capabilities are (even with quantum computing)

  - Low impact at upper layers (MAC, software)

- **Remaining gaps of PHYSEC**
  - All PHYSEC schemes need authenticated Channel State Information
    - The channel estimate must be exclusively known by Bob
    - Without exclusivity, no security

  - PHYSEC scheme cannot rely on pre-distributed keys
    - Eve can also know the key

  - For some PHYSEC schemes, a better SNR is require for the legitimate links than for eavesdropper links

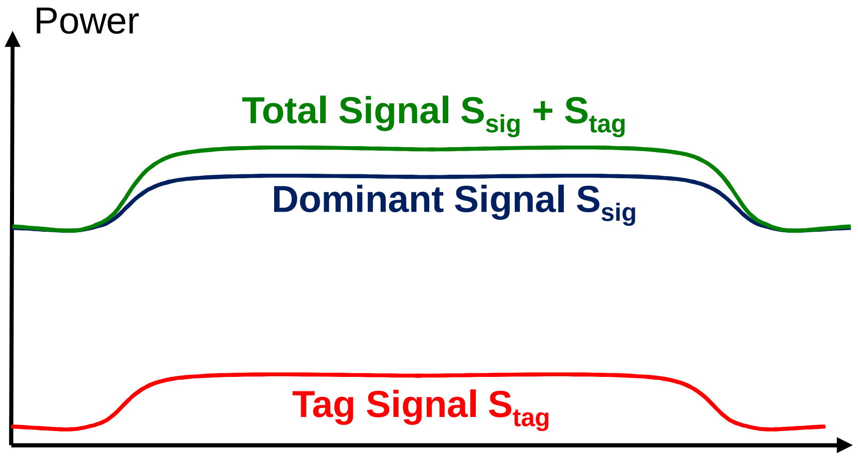
- **Proposed solution consists in using a new authentication protocol**
  - Without prior key distribution
  - Based on the generation of steath and adaptative signals, called Tag Signals
  - Able to provide suitable conditions for the implementation of PHYSEC schemes

Supported by PHYLAWS project FP7 ICT Id-317562

Tag Signals and Key-free authentication protocol

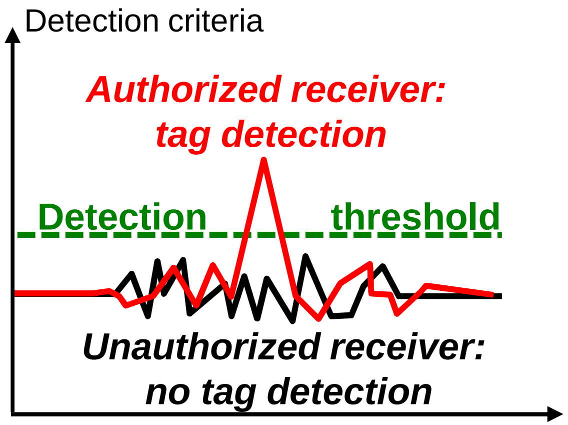
Principle

Tag signal: Low power superimposed signal, transmitted at the same time and on the same carrier than useful signal, with identification information



- **Low power of emission to hide tag signal under dominant signaling**
- **Use of Direct Spread Spectrum Sequences (DSSS) to spread the tag signal over the carrier bandwidth.**
- **Provides the potential radio advantage required by PHYSEC schemes**

- **Detection of the tag signal requires to know the DSSS**



- **Innovative authentication approach**
    - First, DSSS of tag signals are «public»
    - Last, DSSS of tag signals are «private» taking advantage of the legitimate channel randomness

Supported by PHYLAWS project FP7 ICT Id-317562

Tag Signals and Key-free authentication protocol

Identification of threats

Different kinds of threat for Eve monitoring

- **Eve is passive**
  - Eve records and decodes exchanged messages between Alice and Bob
  - Eve does not emit any signal
  - No real-time constraints of any kind

- **Eve is Man-In-The-Middle (MITM)**
  - Eve intercepts and real time processes exchanged messages between Alice and Bob
  - Eve sends falsified signals to impersonate either Alice or Bob

- **Eve attacks the authentication protocol (“Intelligent Jamming” / IJ)**
  - Eve detects authentication messages and jams them with dedicated signals
  - Eve aims at forcing the use of a less secure protocol between Alice and Bob

Main countermeasures included in the protocol

- **Authentication through tag signals and channel measurements**
  - Alice and Bob exchange tag signals to authentify themselves
  - Those tag signals are **computed from channel measurements**
  - Thus, Eve cannot predict nor follow the tag signals exchanges (at more than $\lambda/2$)

- **Authentication through accuracy of time of arrival of tag signals**
  - Fast exchanges of tag signals between the legitimate users
  - Imposing extremely high reactivity requirements for any MITM or IJ Eve

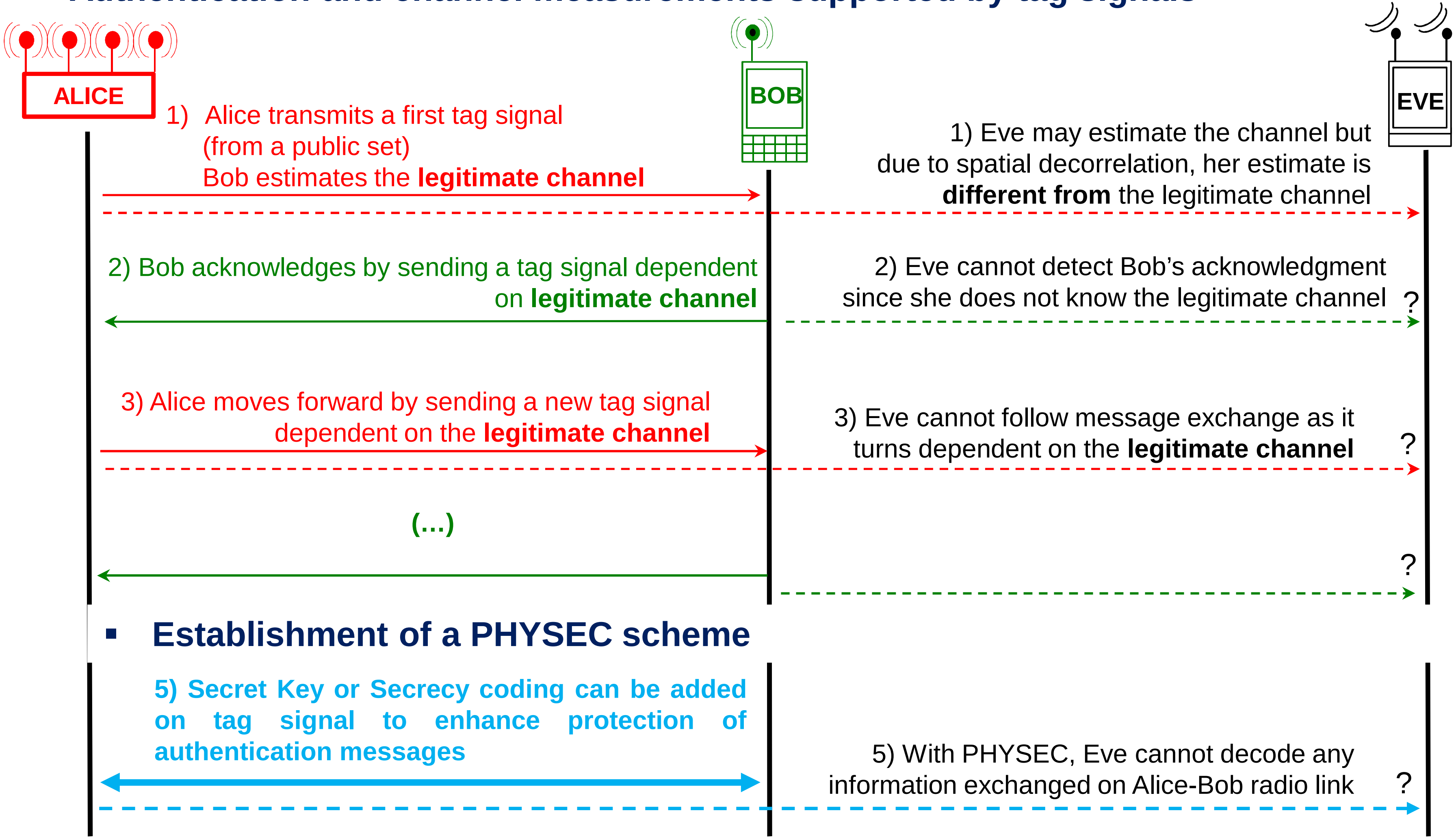
Supported by PHYLAWS project FP7 ICT Id-317562

Tag Signals and Key-free authentication protocol

Case of passive Eve

Protocol and resilience to passive Eve

- **Authentication and channel measurements supported by tag signals**



1) Alice transmits a first tag signal (from a public set)
Bob estimates the **legitimate channel**

1) Eve may estimate the channel but due to spatial decorrelation, her estimate is **different from** the legitimate channel

2) Bob acknowledges by sending a tag signal dependent on **legitimate channel**

2) Eve cannot detect Bob's acknowledgment since she does not know the legitimate channel

3) Alice moves forward by sending a new tag signal dependent on the **legitimate channel**

3) Eve cannot follow message exchange as it turns dependent on the **legitimate channel**

(…)

- **Establishment of a PHYSEC scheme**

5) Secret Key or Secrecy coding can be added on tag signal to enhance protection of authentication messages

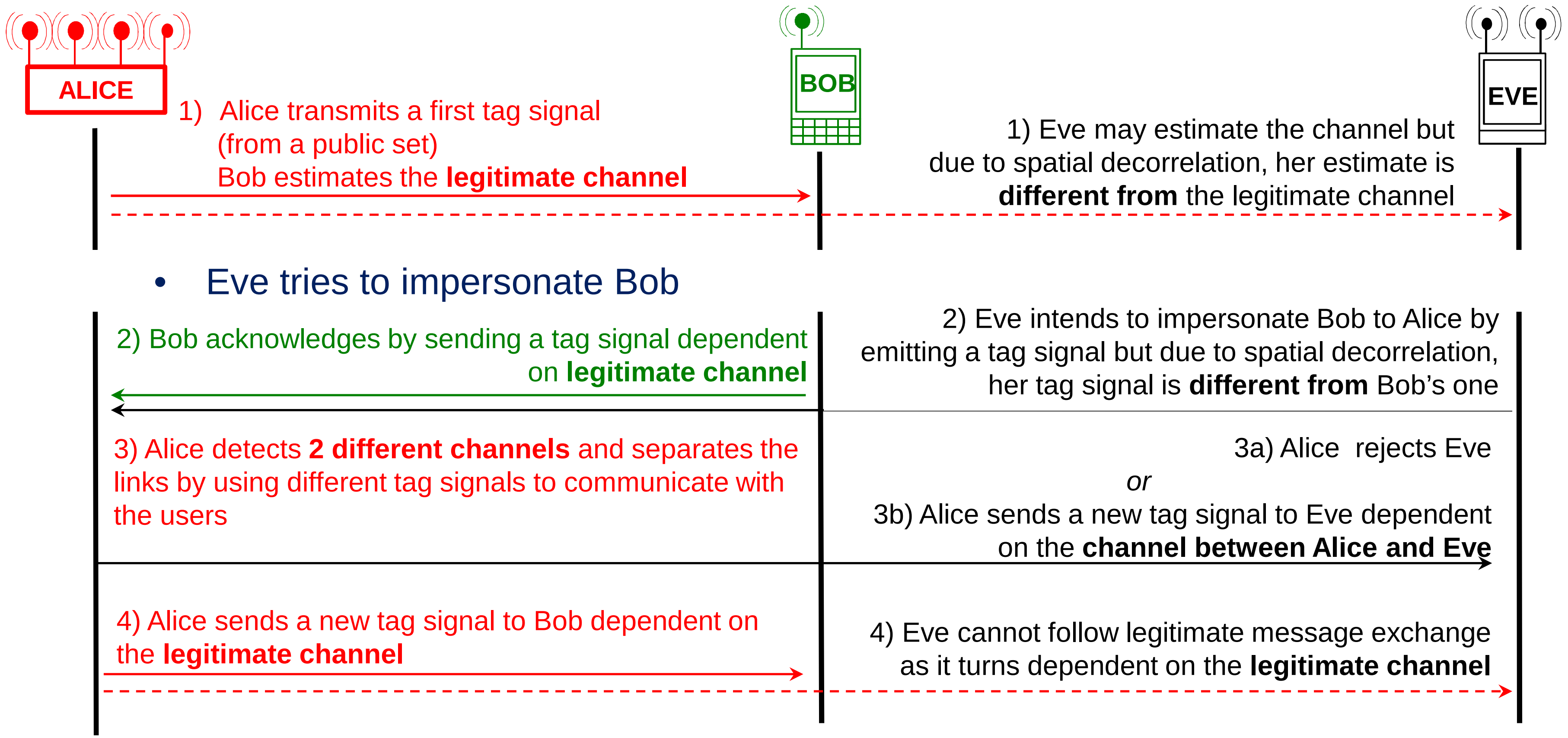
5) With PHYSEC, Eve cannot decode any information exchanged on Alice-Bob radio link

Supported by PHYLAWS project FP7 ICT Id-317562

Tag Signals and Key-free authentication protocol

Case of Man-In-The-Middle attack

Protocol and resilience to Man-In-The-Middle attack: one scenario among others



1) Alice transmits a first tag signal (from a public set)
Bob estimates the **legitimate channel**

1) Eve may estimate the channel but due to spatial decorrelation, her estimate is **different from** the legitimate channel

- Eve tries to impersonate Bob

2) Bob acknowledges by sending a tag signal dependent on **legitimate channel**

2) Eve intends to impersonate Bob to Alice by emitting a tag signal but due to spatial decorrelation, her tag signal is **different from** Bob's one

3) Alice detects **2 different channels** and separates the links by using different tag signals to communicate with the users

3a) Alice rejects Eve

or

3b) Alice sends a new tag signal to Eve dependent on the **channel between Alice and Eve**

4) Alice sends a new tag signal to Bob dependent on the **legitimate channel**

4) Eve cannot follow legitimate message exchange as it turns dependent on the **legitimate channel**

- **The following of the protocol is similar to passive attack case**
- **Tag signal mismatch + late time of arrival of Eve's signals are discriminant**
- **Several protections can be added to make the transmission sequences and time of emission unpredictable for Eve (see following page).**

Supported by PHYLAWS project FP7 ICT Id-317562

Tag Signals and Key-free authentication protocol
Case of intelligent jamming attacker

How Intelligent jamming Eve is countered ?

- **Help of Un-coordinated Spread Spectrum (USS) scheme**
  - sequential emission of random tag signals chosen in a public set
  - only one code is dedicated to Bob
  - tag signal sequence is unpredictable for Eve
- **Help of TJ schemes**
  - randomness of the transmission time
  - transmission time is unpredictable for Eve

Apply also against MITM attack

- **As USS and Time Jitter randomize transmission of tag signals, intelligent jamming Eve has to spread her power over time, frequency and tag signals set**

Conclusion on the proposed protocol

- **Enables authentication without prior-key distribution**
- **Resilience to attacks are mainly based on**
  - Spatial diversity of channels which drives the building of tag signals
  - Rapidity of answer and accurate synchronization on tag signal (large bandwidth)
  - Added protection scheme : Uncoordinated Spread Spectrum and Time Jitter
- **Opens the implementation of PHYSEC scheme such as Secret Key Generation**

Supported by PHYLAWS project FP7 ICT Id-317562

Experimental measurements: first results

Experimental test bed

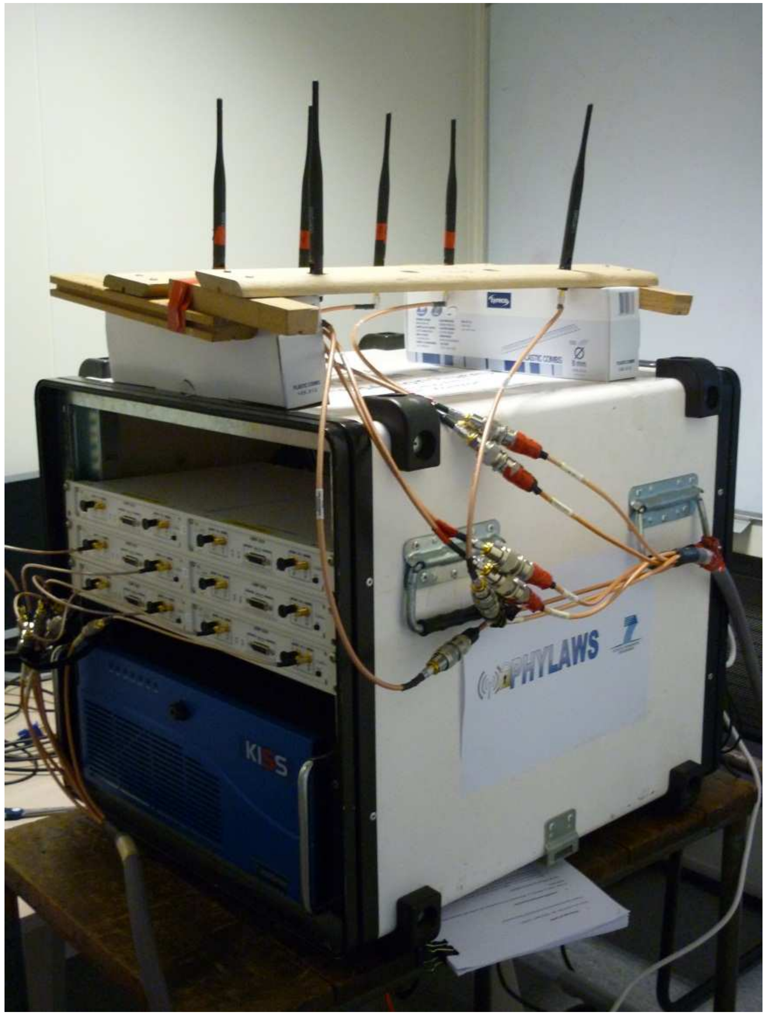
Purposes

- **Measuring real channels on Ultra High Frequency ranges (2/3/4G, Wifi)**
- **Studying channel diversity to implement PHYSEC schemes**
  - Secret Key Generation of good quality (> 128 bits, NIST criteria)
  - Secrecy Codes and associated metrics

Test-bed

- **Emission Equipment (Alice)**
  - Wifi AP 802.11a/n (f=2.46GHz, λ=12cm)
- **Acquisition Equipment (Bob and Eve)**
  - 6x USRPs (0.4 - 4.4 GHz) + Octoclock
  - Top grade PC (KISS 4U X9DR3)
  - 6 synchronized antennas
    - Bob: 2 antennas, spaced out by 33 cm
    - Eve: 4 antennas, spaced out by 11 cm
  - Bandwidth of 25 MHz

Hardware: NI/Ettus + Kontron
Software: Phylaws partners



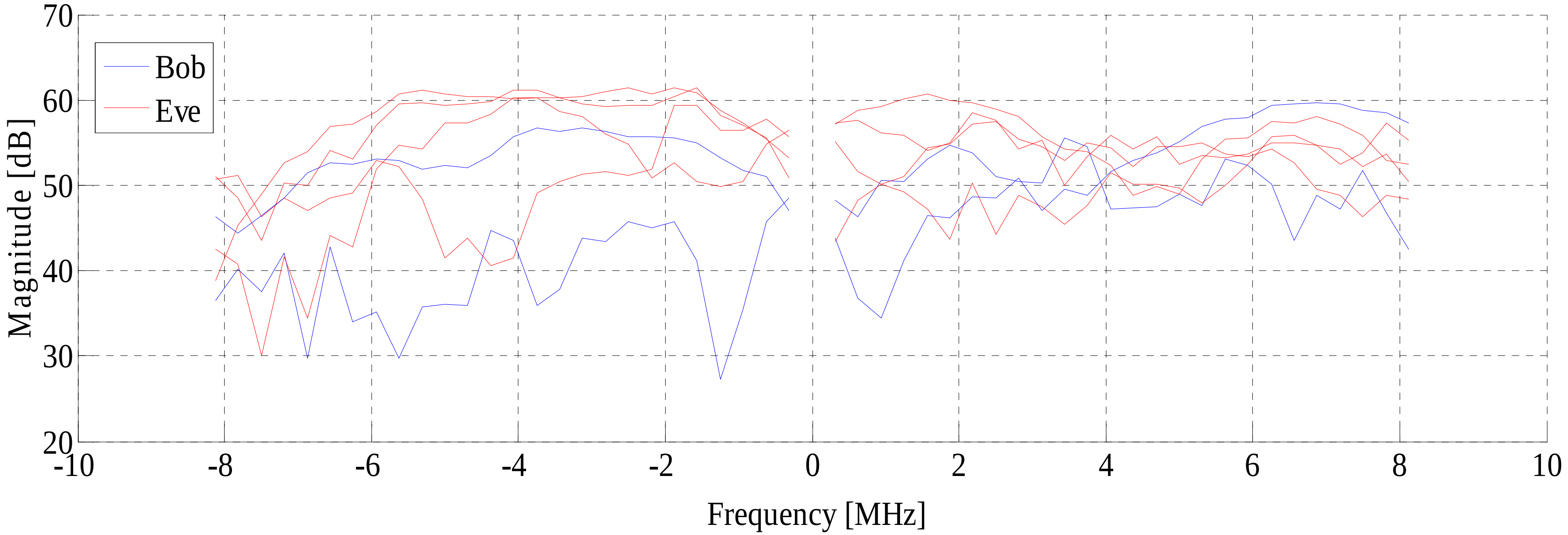
Supported by PHYLAWS project FP7 ICT Id-317562

Experimental measurements: first results

Spatial diversity of the channel responses

Channel Frequency Response (CFR) estimation of Wifi AP signals

- **Evolution of the channel response for the different antennas at the same time**



  - Decorrelation between channel observations over the different antennas
  - Confirmation of previous experiments
    - W.C. Jakes Jr., « Microwave Mobile Communiations ». Piscataway, NJ: Wiley-IEEE Press
    - J.Wallace and R.Sharma, "Automatic secret keys from reciprocal MIMO Wireless channels: measurement and analysis," IEEE Trans. on info. for. and sec., September 2010

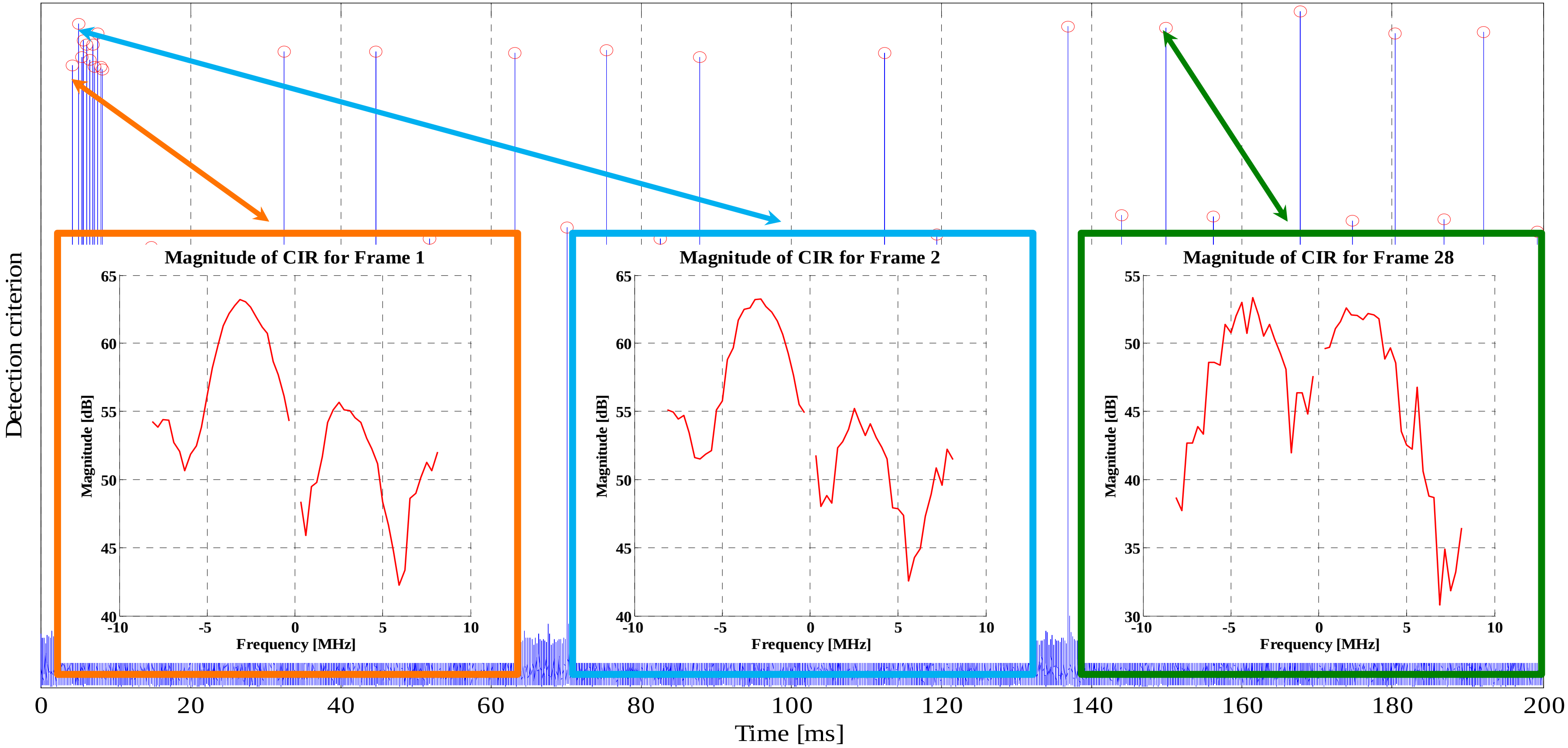
- **High <u>spatial</u> diversity enables computation of good secret keys (length, randomness), evaluated later by using NIST criteria**

Supported by PHYLAWS project FP7 ICT Id-317562

Experimental measurements: first results

Time diversity of the channel responses

- **Evolution of Channel Frequency Response of the same antenna over 200 ms**



- Channel evolves over time
- Need to regenerate the secret-keys after 100 ms (indoor case)

- **High <u>time</u> diversity enables computation of good secret keys (length, randomness), evaluated later by using NIST criteria**

Supported by PHYLAWS project FP7 ICT Id-317562

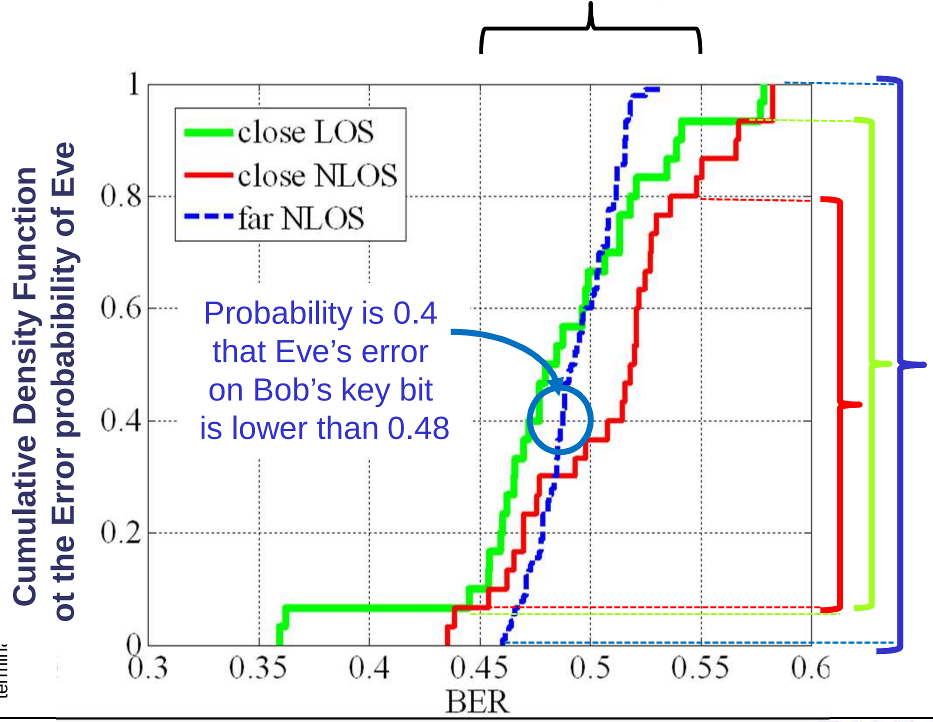
Experimental measurements: first results

Performance evaluation of SKG scheme

Protection of Bob's secret-keys

- **Criterion is the Bit Error rate (BER) of Eve**
- **BER close to 0.5 means Eve unable to recover Bob's secret key**

Around 0.5 is the best security region



Probability is 0.4 that Eve's error on Bob's key bit is lower than 0.48

Quality of Bob's secret-keys

- **Criterias are defined by the National Institute of Standards and Technologies (NIST)**
- **Evaluate the probability distribution and the entropy of Bob's key bits**
- **60 + 22 keys of 242 bits computed from channel measurements**

NIST Test		Propagation scenario	
		Line of Sight	Non Line of Sight
1	Frequency (bit)	60/60	22/22
2	Frequency (block)	59/60	22/22
3	Runs	56/60	21/22
4	Entropy	55/60	22/22

Conclusion

Our new authentication protocol offers practical perspectives for improving wireless security

- **No prior key distribution**
- **Secure device authentication protocol for the first messages**
  - Based on exchanges of stealth tag signals
  - Counter any Eve: passive, man in the middle, intelligent jamming
  - Re-enforce integrity control of further negotiation messages
- **Authenticated estimation of the legitimate channel at the earliest stage**
- **Including of versatile transmitting techniques such as:**
  - Un-coordinated Spread Spectrum
  - Time Jitter
- **Large opportunities for enhanced PHYSEC implementation**
  - Authenticated CSI
  - Secret Key Generation
  - Secrecy Coding
  - Other schemes (Artificial Noise)
- **Further work: implement secrecy codes**

Supported by PHYLAWS project FP7 ICT Id-317562

CONCLUSION

Thank you for your attention

This work is supported by Phylaws project

see www.phylaws-ict.org

PHYLAWS

PHYsical Layer Wireless Security

Project Coordinator: François Delaveau
Thales Communications and Security
Tel: +33 (0)1 46 43 31 32
Fax: +33 (0)1 46 13 25 55
Email: francois.delaveau@thalesgroup.com
Project website: www.phylaws-ict.org

Partners: Institut Mines-Telecom ParisTech (FR), Imperial College of Science, Technology and Medicine (UK), Teknologian tutkimuskeskus VTT (FI), Celeno Communications Israel Ldt (IS).

Duration: November, 2012 – October, 2015
Funding scheme: STREP

Contract Number: CNECT-ICT-317562