EUROPEAN COMMISSION

Community Research

PHYLAWS

SEVENTH FRAMEWORK PROGRAMME

ICT Call 8

PHYLAWS

PHYsical LAyer Wireless Security

Advisory Board - Year 1 Meeting - Parts A-D

Telecom Paris Tech, room B603, 46 rue Barrault, 75013 Paris, 2 october 2013

Contacts : F. Delaveau : François.Delaveau@thalesgroup.com tel : 01 46 13 31 32 ; mob : 06 73 28 25 89

A. Sibille : alain.sibille@telecom-paristech.fr tel : 01 45 81 70 60

A/
Starting time 10h00:
Welcome (TPT + TCS) – Agenda proposal

A/ Starting time 10h00: Welcome (TPT + TCS) – Agenda proposal

B/ Brief presentation of each participant (All)

C/ Recall of the Phylaws project – scope of the project – answers to questions: (TCS + partners)

D/ Synthesis of the past and current work – year 2013 (TCS + VTT)
Interactive discussion of partners with Advisory Board members

E/ Submission of theoretical items to be followed on (TPT ICL VTT)
Interactive discussion of partners with Advisory Board Members

LUNCH AT TPT RESTAURANT

F/ Submission of development items to be followed on (CEL + TCS):
Interactive discussion of partners with Advisory Board Members

G/ Submission of simulation items to be followed on (VTT + TCS)
Interactive discussion of partners with Advisory Board Members

H/ Submission of dissemination initiatives (TPT + partners)
Interactive discussion of partners with Advisory Board Members

I/ Submission of standardization initiatives (TCS + partners)
Interactive discussion of partners with Advisory Board Members

J/ Conclusion – Thanks (TCS + all). Closing time 17h00

B/
Brief presentation of each participant
(All)

Brief presentation of each participant (All)

	Mail	Phone	PostaleAddress	Company Role
Dr Scott Cadzow	scott@cadzow.com	+447720290827	10 Yewlands, Sawbridgeworth, Hertfordshire CM219NP UK	Company director, Chief Engineering Officer
Pr Srdjan Capkun	srdjan.capkun@inf.ethz.ch	+41 (0)44 632 7190	ETH Zurich, CNB F 102.2 Universitätsstrasse 6 8092 Zurich SWITZERLAND	Professor, Doctor.
Dr Joseph Mitola III	joe.mitola@comcast.net jmitola@ieee.org	+001-703-314-5709 +001-703-346-8473	4985 Atlantic View Saint Augustine Florida 32080 USA	US Advisor Regarding Trustable Cognitive Systems
Pr Peter Mueller	pmu@zurich.ibm.com	+41 (0)44 724 8111	IBM reasearch GmBH, Zürich Research Laboratory, Säumerstrasse 4 CH-8833 Rüschlikon Switzerland	Doctor IBM Research Laboratory GmBH, Zurich
Pr Lee Pucker	Lee.Pucker@WirelessInnovation.org	+1-604-828-9846	12572 17A Ave Surrey, BC V4A 9H9 Canada	Chief Executive Officer Wireless Innovation Forum
Pr Philippe Aubineau	Philippe.Aubineau@itu.int	+41 (0)22 73 05 992	International Telecommunication Union Place des Nations Genève	Counsellor, ITU-R Study Group 1, CPM and SC Study Group Department Radiocommunication Bureau
P.O. Manuel Carvalhosa	Manuel.CARVALHOSA@ec.europa.eu	+32 (0)2 298 56 02	European Commission Avenue de Beaulieu 25 Brussels Belgium	EC Directorate General for Communications Networks, Content and Technology Technology Network Technologies unit Network Project Officer

Alain SIBILLE	France	Telecom Paris Tech	Professor	Alain.Sibille@telecom-paristech.Fr
Jean-Claude BELFIORE	France	Telecom Paris Tech	Professor	Belfiore@enst.Fr
Cong LING	China	Imperial College London	Professor	C.Ling@imperial.Ac.Uk
Changick SONG	Korea	Imperial College London	Doctor	Changick.Song@imperial.Ac.Uk
Mika LASANEN	Finland	VTT	Engineer	Mika.Lasanen@vtt.Fi
Jani SUOMALAINIEN	Finland	VTT	Engineer	Jani.Suomalainen@vtt.Fi
Nir SHAPIRA	Israël	Celeno	Technical director	Nir.Shapira@celeno.Com
Francois DELAVEAU	France	Thales C&S	Engineer	Francois.Delaveau@thalesgroup.Com

C/
Recall of the Phylaws project Scope - answers to questions

François Delaveau, Thales Communications and Security

francois.delaveau@thalesgroup.com

Wireless communications have become dominant to access information for citizen, for economical actors, for administrations, etc.

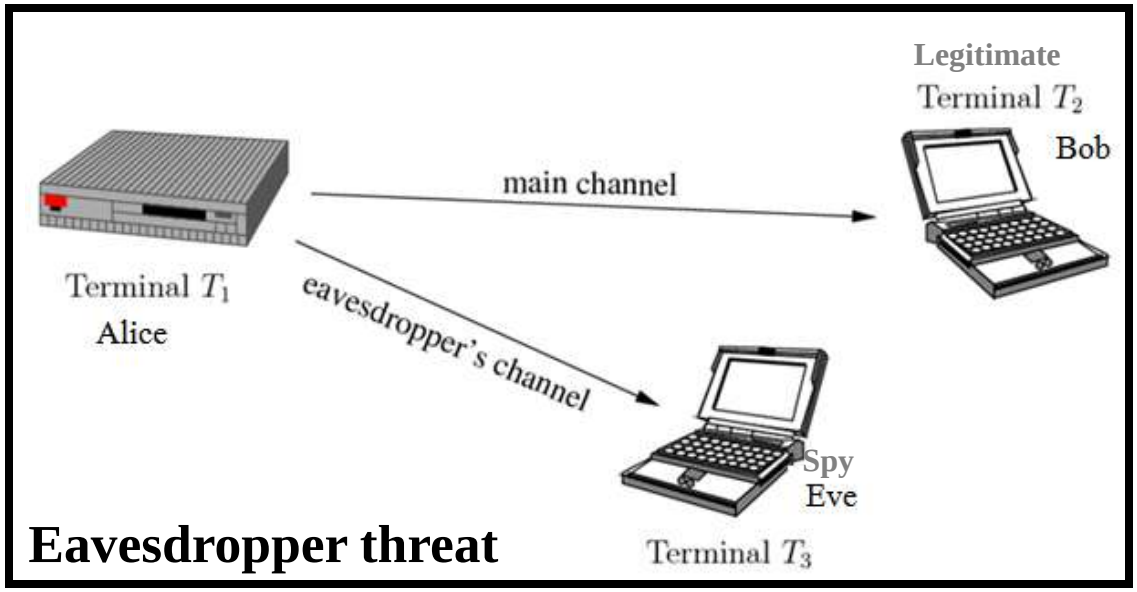
Protection leaks and non-suffisant security technologies of the current civilian wireless networks also **induce major risks to society**

Dedicated Authentification procedures and crypto. techniques exist but

- They reduce spectrum efficiency, increase computations latencies and complexity
- They induce added costs
- They are often not sufficiently secure, especially for worldwide public wireless systems.

PHYLAWS is needed to counter these difficulties in order to sustain the progress of the digital society and wide band internet for

- Future networks
- Trustworthy ICT



Eavesdropper threat

Enhance the security of wireless communications in an affordable, flexible and efficient manner : apply fundamentals of security and information theory in order to upgrade and design suitable radio architectures, wave forms and protocol stacks

Elaborate, study and demonstrate of TRANSEC and NETSEC upgrades :

- add PHYSEC concepts to existing authentification and cyphering procedures
- exploit the characteristics of the wireless radio channel, especially when dispersive
- enhance wave forms and radio access protocol of digital radio networks.
- search for easily developed and easily validated algorithms,
- consume less resources : less energy of the terminal level, reduced data consumption overhead (i.e. upgrade the spectral efficiency).
- reduce security management costs in wireless networks.

Facilitate the penetration of wireless technologies in the personal and professional sphere, guarantee a more efficient and safe access to the digital world through the future internet. Target a wide set of existing and future uses.

Disseminate PHYSEC solutions, propose upgrades to existing and influence new standards.

Review theorical and practical constraints of eavesdroppers:

Remain reasonable: no angelic but no paranoia. Physical constraints apply to Eve too.
Distinguish legal/administrative interceptions and radio non legal/pirates/hackers threats.

Target a wide set of existing and future wireless networks:

Focus on worldwide spread local loop : WiFi - experimental proof of concepts.
Focus on worldwide 4G radiocells : LTE - proofs of concepts based on simulation.

Upgrade existing and imagine new security concepts with PHYSEC:

- Secrecy coding
- Enhanced artificial / Cooperative Jamming
- Combination of PHYSEC and advanced RATs.

Add of physical dependant random at the transmitted signal and combine PHYSEC capabilities with other security procedures.

Upgrade the security of wireless networks and reduce its cost. Identify the relevant services / economical / industrial applications

Disseminated the most promising PHYSEC outputs, maximize their impact, take into account legal and administrative implications.

Basic definitions of security concepts

Term	Definition
COMSEC	Communication Security: is relevant to the protection of the content of the user messages (voice, data). Comsec applies either at the radio interface or at upper layer. Comsec techniques involve ciphering, authentication and integrity control of signalling and users' data at several protocol layer and interfaces (examples are point to point ciphering of each user data flux, ciphering of IP packets, ciphering of artery, etc.).
INFOSEC/ CSS	Information security Module/Cryptographic Sub-System: The Infosec/CSS module manages the generation of pseudo-random data that are used for TRANSEC NETSEC or COMSEC protection
NETSEC	Network Transmission Security: Netsec is relevant to the protection of the signalling of the network. Netsec applies mainly at the radio interface and at the medium access protocol layer, with request to upper protocol layers. Netsec techniques involve mainly transmitter authentication protocols, integrity control and ciphering of signalling data.
PHYSEC	Physical Layer Security is generic term that will be used in this project to design all kind of protection techniques that are based on the use of the physical layer sensing and/or measurement.
SECRECY CODES	Secrecy codes are modified channel codes that achieve null, asymptotically null, or low information leakage of a legitimate link (Alice to Bob) when facing and Eavesdropper Eve. Existence of secret codes is proven when a transmission advantage occurs for the legitimate link. Such as transmission advantage should be achieved over the radio interface by combining intentional jamming and advanced transmission and reception scheme such as MISO and MIMO transmissions.
TRANSEC	Transmission Security: Transec is relevant to the protection of the wave form face to interception/direction Finding of the transmitted radio signal, to jamming of the user receiver, and to intrusion attempts into the radio-communication access protocol. Transec applies mainly at the radio interface.
Trustworthy	Secure, reliable and resilient to attacks and operational failures; guaranteeing quality of service; protecting user data; ensuring privacy and providing usable and trusted tools to support the user in his security management.

[1] According to the European Commission Work Programme 2011-2012 for ICT

PHYLAWS intends to **design, prove efficiency and demonstrate realistic implantations of new privacy concepts for wireless networks that exploit radio-propagation phenomena,** with a merged approach: PHYLAWS merges academic and industrial skills in order to provide enhanced-secure RATs into existing and future public wireless standards.

PHYLAWS concentrates on physical layer security, secrecy coding and intentional (cooperative) jamming

PHYLAWS deals with both theoretical and practical items of physec.

1/ Taking into account the following constraints relevant to the Radio Access Technology (RAT) : Finite messages lengths, user data rate and data overhead for coding, integrity control and ciphering, Quality of service etc.

2/ Taking into account the attacker dependency of the radio conditions (over the complete radio access protocol and during the data transmission) when communities of crypto-analysis and of physical layer security usually consider “maximal” attack risk and ideal attack situations: complete a-priori knowledge of the legitimate link, negligible demodulation errors and infinite message lengths.

Organization of the PHYLAWS project

WP1: Management Dissemination Standarization Advisory Board

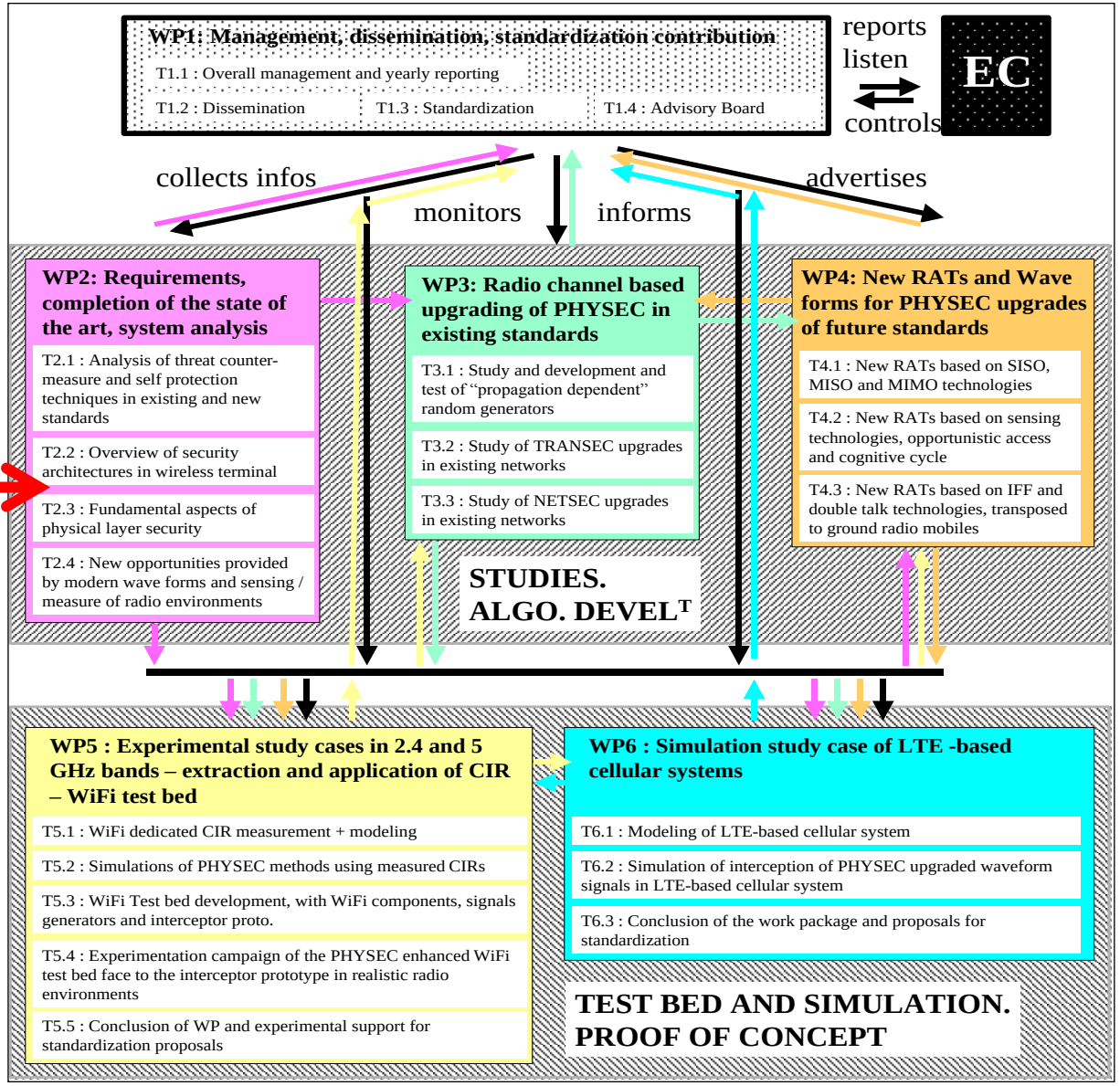
WP2 : State of the Art

WP3: Studies relevant to physec-driven solutions for existing standards

WP4: studies relevant to physec-driven solutions for new standards

WP5: Experiments of physec-driven solutions for WiFi

WP6: Simulations of physec-driven solutions LTE



Questions ?

See deliverable D.1.12
"Advisory Board Year 1 Meeting Report"

D/
Synthesis of the past and current work – year 2013 (TCS + VTT)

François Delaveau, Thales Communications and Security

francois.delaveau@thalesgroup.com

- Workpackage 1:

Management plan etc. (WP.1.1.),

Dissemination plan and first dissemination actions (WP.1.2),

=> Two papers at the Winncomm' Forum 2013 Munich

=> One special session at PIMRC London Sept 2013

Standardization plan (WP.1.3)

+ Advisory board organisation (WP.1.4)

- Workpackage 2:

Analysis of threats,

=> has led to deliverable D.2.1. (June 2013)

Analysis of secure architectures in wireless networks,

=> has led to deliverable D.2.2. (October 2013)

- Workpackage 3 and 4: "inventions" of physec-driven security solutions are initiated in first deliverables and papers

=> developed in the following

- Workpackage 5 and 6: Initialisation < end 2013

Deliverable D2.1 "Analysis of threats, countermeasures and self-protection techniques" + Paper "Active and passive eavesdropper threats within public and private civilian wireless networks - existing and potential future countermeasures – an overview

I/ A classification of radio attacks

II/ A classification of the attackers

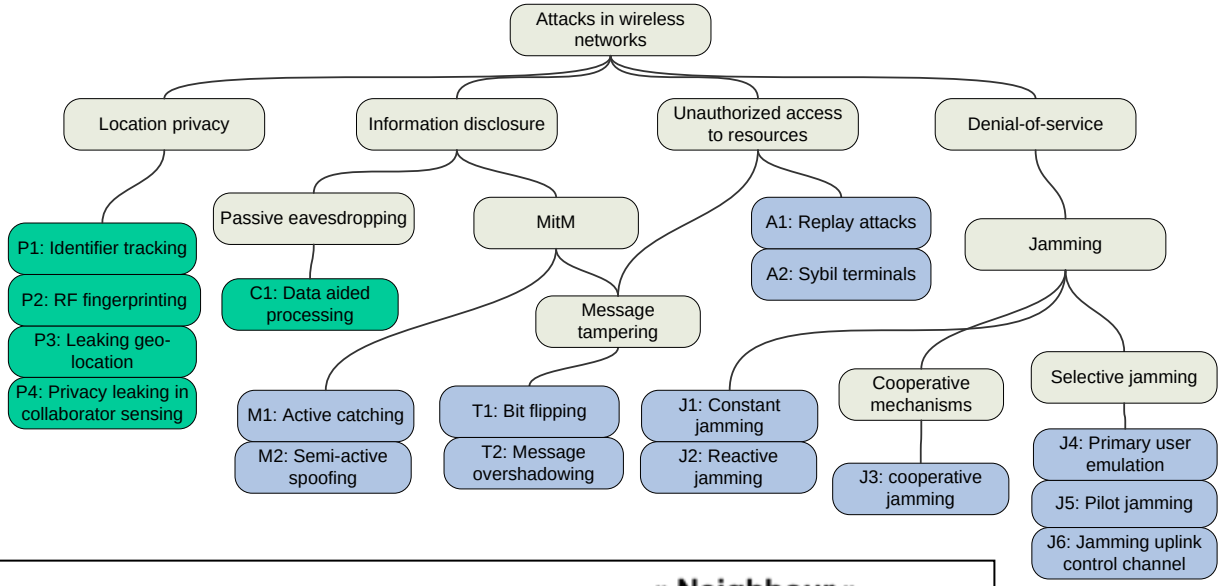
Practical threats and attacks were described for

- Radio-cell standards (focus on GSM, UMTS, LTE)
- Wireless Local Area Networks (focus on WiFi)
- Short range communications (Bluetooth, Zigbee)

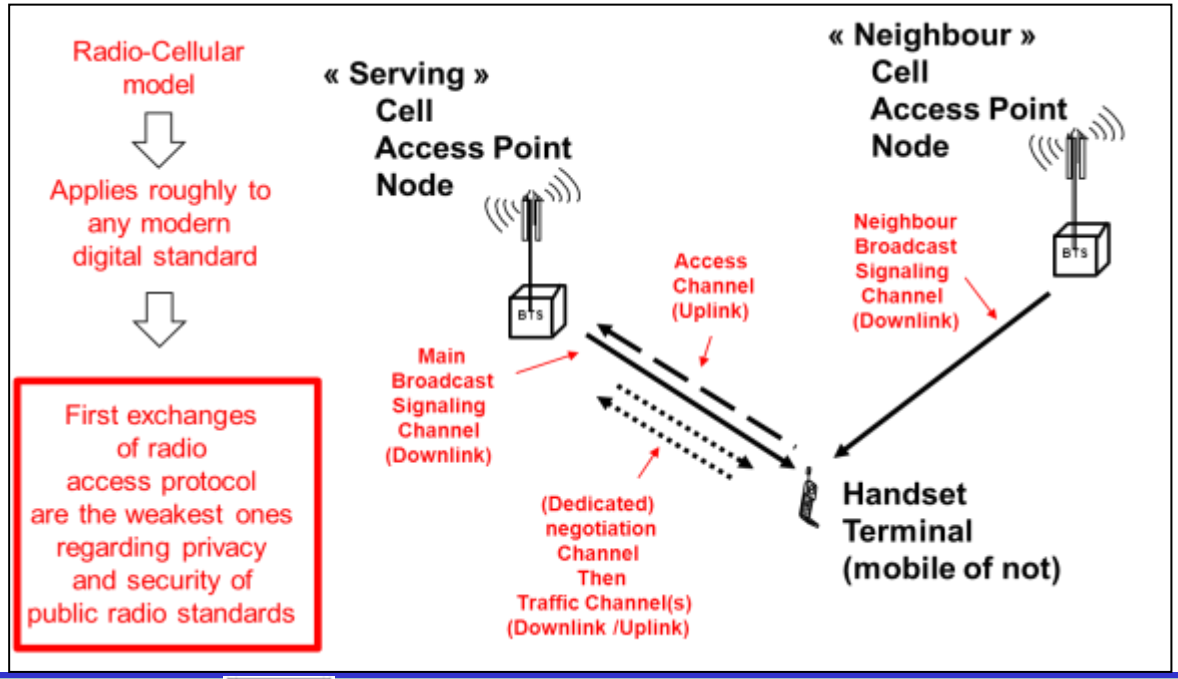
III/ A special focus of the analyses applied to first negotiation stages of the radio access protocol (see figure below): signaling, access attempts, auth. and subscriber identif. cipher key establishment

Roughly, it is considered in the Phylaws project that the worldwide nature of modern public digital standards induces intrinsic privacy lacks of the early negotiation protocol.

Classification of radio attacks



First negotiation stages of the radio access protocol



IV/ Practical considerations are considered in the description of threats

IV-a/ Difference of point of view that may occur among communities:

1/ Taking into account the following constraints relevant to the Radio Access Technology (RAT) : Finite messages lengths, user data rate and data overhead for coding, integrity control and ciphering, QoS etc.

2/ Taking into account the attacker dependency of the radio conditions when communities of crypto-analysis and of physical layer security usually consider "maximal" attack risk and ideal attack situations: complete a-priori knowledge of the legitimate link, negligible demodulation errors and infinite message lengths.
on phases of the RATs

III-b/ Radio access technology constraints apply to expected protections

Limited periods of coding and interleaving schemes are limited
Constraints at terminals' embedding should be considered for perspectives of physec upgraded protections

Limitation of radio and CPU capabilities
Limitation of the complexity of channel coding (including secret codes complexity),
Limitation of embedded memory and especially of fast memory,
Control of latencies, etc.

Deliverable D2.2 "Security architectures in wireless terminals"
+ Paper "Active and passive eavesdropper threats within public and private civilian wireless networks - existing and potential future countermeasures – an overview
+ paper "PHYSEC concepts for wireless public networks – introduction, state of the art and perspectives"

I/ Analyses of protections that exist in public wireless networks
- considerations on network architecture
- implantation trends of security components and of secure procedures in wireless terminals

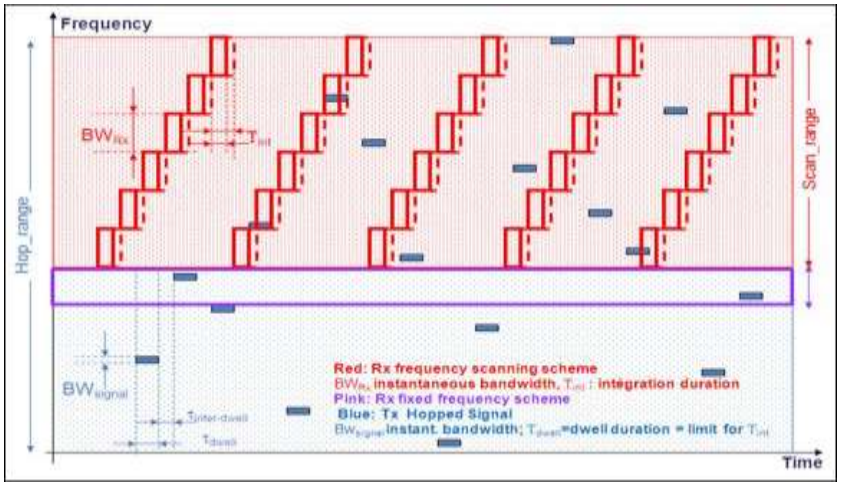
II/ protections within military network special focus on on ad-doc tactical radios
- very specific architecture
- existing practices relevant to transec netsec and comsec in military radios

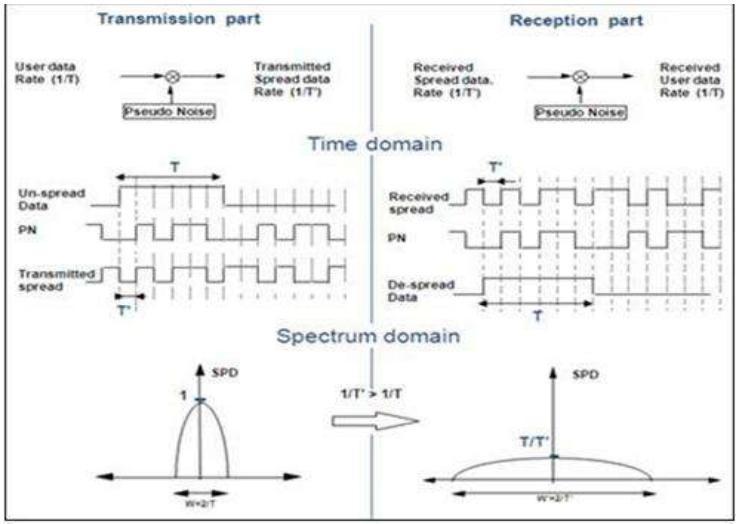
III/ Initiation of Software-based architectures for physec-driven security solutions

See following pages

Transec perspectives: make signals more furtive and RAT structure more confusing.

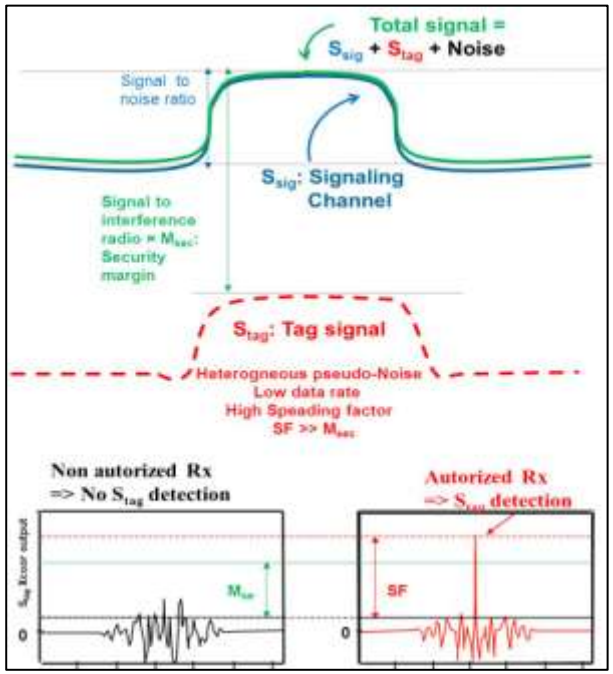
- mixt frequency hopping and time hopping
- Introduce Un-coordinated spectrum spreading (USS) schemes for direct spread spectrum RATs, for time and frequency hopping of TDMA RATs
- Introduce dummy signals in order to upgrade Eve's confusion + full Duplex techniques in the processing of dummy signals.
- Imbricate cipher establishment and traffic channel allocation for subscriber's transmission (cf. GSM)
- Take advantage of opportunistic RATS (Frequency White Space, Cognitive Radios) for improving Eve's confusion
- Input physical random into any transec protection: examples of such input are outputs of equalization/rake processing)

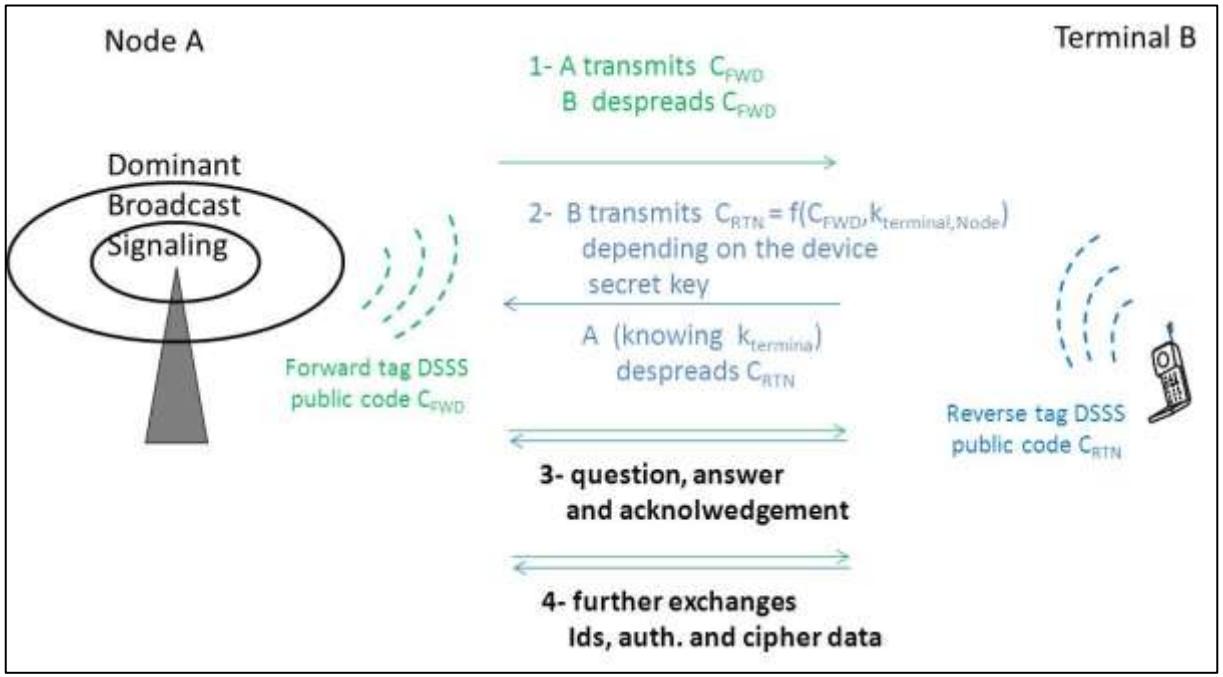




Netsec perspectives: make signalling more protected and better authenticated.

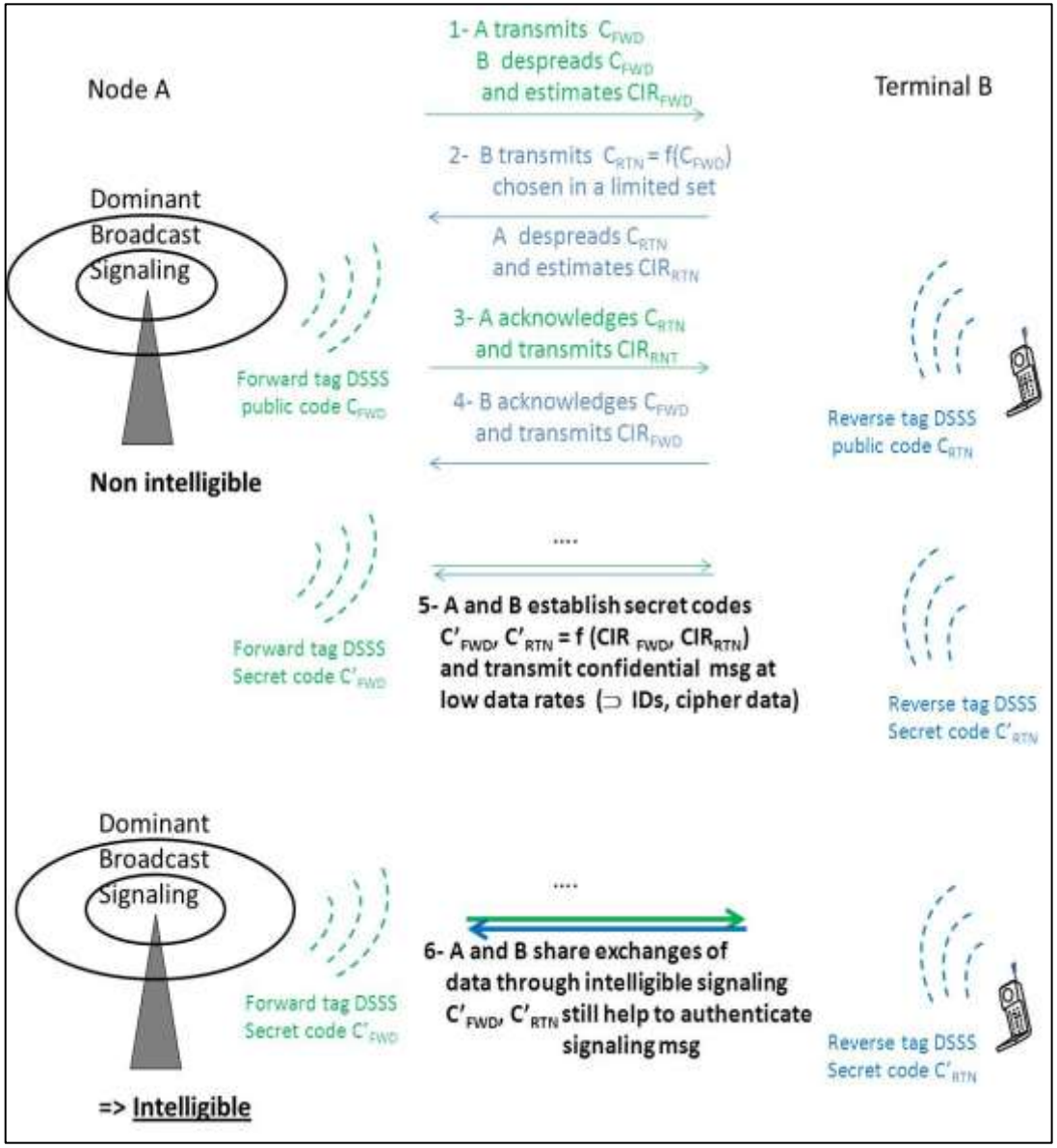
- Introduce Tag signal under signalling carriers
- Combine tag signals processing and full Duplex techniques
- Combine tag signals with radio advantages in order to build secret codes applied to “tag channels”
- Introduce pre-identification exchanges based on tag signals/channels before further authentication and subscriber’s identification
- Introduce Finger printing and water marking in signalling messages
- Combine Finger print and water mark with secret codes





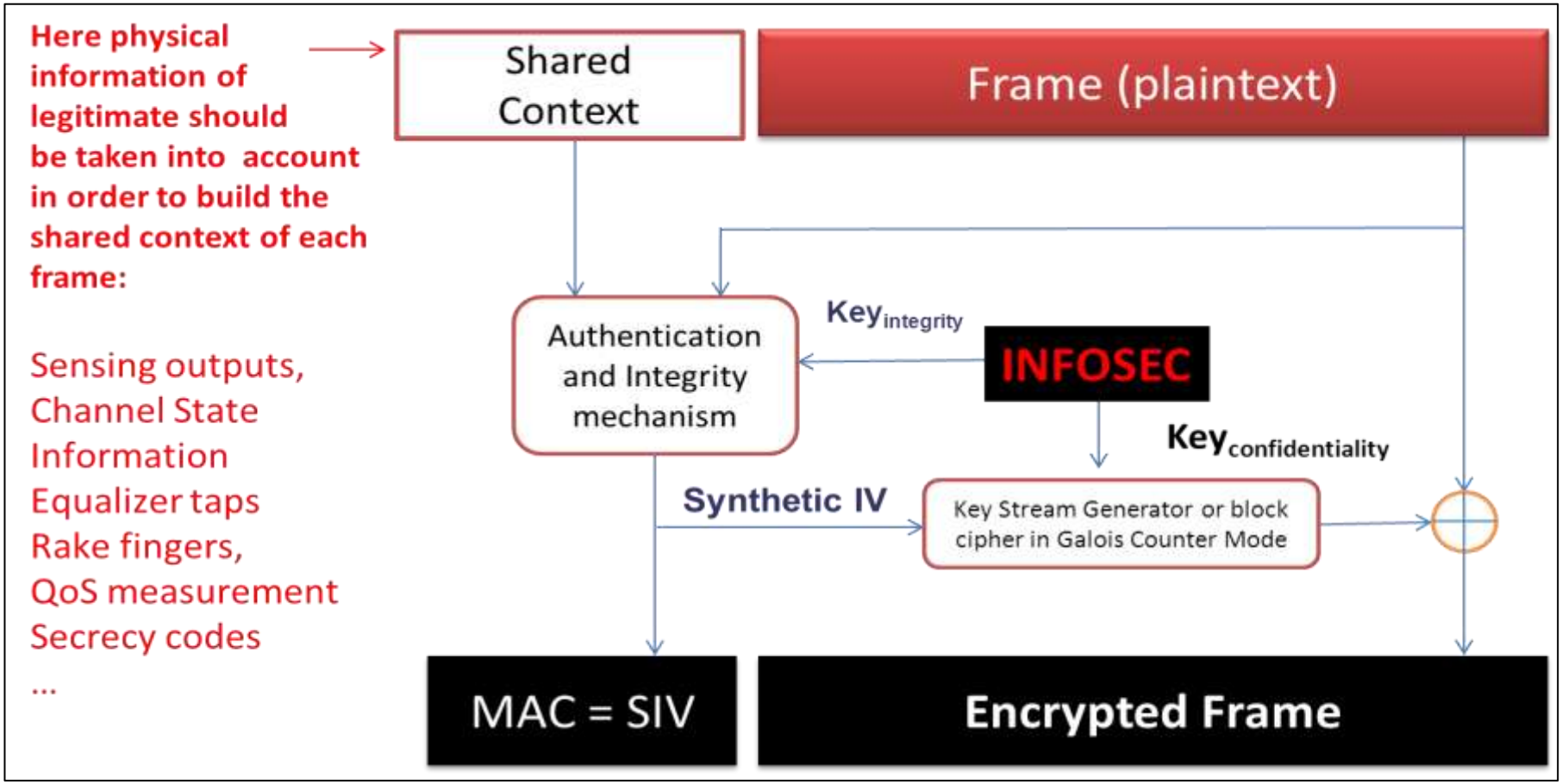
Re-enforced use of dual sense tag signals with

- CIR measurements
- secret codes establishment



Comsec perspectives: adapt physec-driven concepts to advanced Cipher schemes

- Introduce physical random in cipher schemes
- Combine computation of Synthetic Initiation Vector in advanced Authentication Encryption schemes and propagation-dependent random issued from receiver processing (equalization, rake etc.)



Intentions of Deliverable 2.3. "Fundamental aspects of physical layer security"

- Theoretic considerations and current state of the art of physec domain
- Progress toward the construction of secret codes
  - . Gaussian channel
  - . Fading channels

- We keep in mind that in future works we deal with
  - => realistic propagation channels
  - => realistic codes with finite lengths

  - => Evaluation of the complexity of secret codes decoding,
  - => sub-optimal codes that are expected to approach secrecy capacity in realistic channels

⇒ **Practical perspectives for computation of secret codes in existing and next RATs and in future terminals.**

⇒ **initialization of WP3**

Intentions of Deliverable 2.4 "New opportunities provided by modern wave forms and sensing/measure of radio environments"

- Exploitation capabilities of advanced RATs that are in progress for 4G and 5G networks in SDRs CRs
  - Privacy vulnerabilities relevant to geo-referenced sensing, to data base downloading and to other advanced procedure of the opportunistic RAT
  - How could netsec improve privacy and integrity of geo-referenced sensing, and of data base downloading (privacy being relevant here to both subscriber and operator)?
  - How secret codes should be combined with tag signal and finger print techniques?
  - How to take a radio advantage thanks of the sensing capabilities and of the versatile RAT, in order to enhance transec and netsec protections?

- Exploitation capabilities of Full Duplex radio Access technologies and relevant processing techniques, especially for dummy signals and for tag signals/channels.
  - How to introduce IFF-like modes before access attempt (based on tag signals and/or based on fingerprints/watermarks), before authentication, before subscriber identification or before key establishment?

⇒ Practical perspectives for physec in future advanced RATs.
⇒ initialization of WP4

Interactive discussion of partners with Advisory Board members

See deliverable D.1.12
"Advisory Board Year 1 Meeting Report"