Active and passive eavesdropper threats within public and private civilian wireless networks - existing and potential future countermeasures

SDR'13 Winncomm, session 1, München, 11 June 2013

<u>François Delaveau</u>

Thales Communications & Security; Gennevilliers, France; francois.delaveau@thalesgroup.com;

Antti Evesti ; Jani Suomalainen; Reijo Savola

VTT Technical Research Centre; Oulu, Finland; Antti.Evesti@vtt.fi; Jani Suomalainen@vtt.fi; Reijo.Savola@vtt.fi;

Nir Shapira

Celeno Comnunications Ltd; Ra'anana, Israël; Nir.Shapira@celeno.com.

Supported by PHYLAWS project FP7 ICT Id 317562

SUMMARY

Supported by PHYLAWS project FP7 ICT Id 317562

- **This work is supported by the Phylaws project and it introduces its content.**

- **Context of the Phylaws project**
  - ICT call 8, (17/1/2012) thema 1.1. et 1.4
    - **« Future networks »**
    - **« Trustworthy ICT »**
  - 4 Partners:
    - Institut Mines Telecom - Telecom Paris Tech (TPT)
    - Imperial College London (ICL)
    - VTT Technical Research Centre (VTT)
    - CELENO Communications LTD (CEL)
    - Thales communciation and Security (TCS)
  - Synthesis of the project :

    => see www.phylaws-ict.org

PHYLAWS

PHYsical LAyer Wireless Security

Project Coordinator

François Delaveau
Thales Communications and Security
Tel: +33 (0)1 46 13 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 Paris Tech (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*

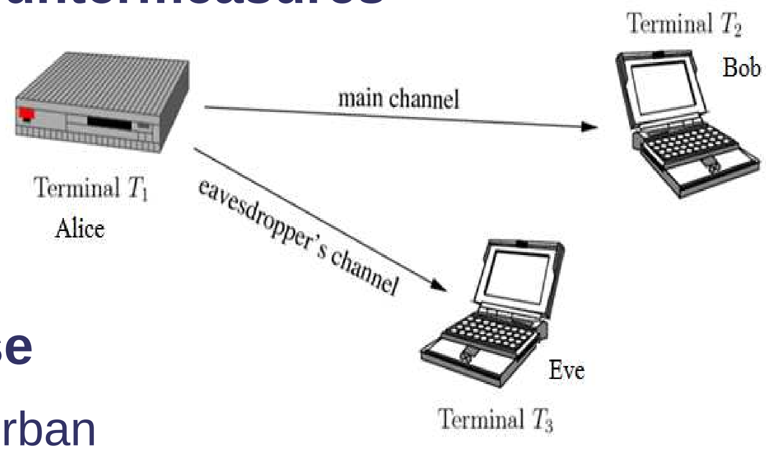
Contract Number: CNECT-ICT-317562

Supported by PHYLAWS project FP7 ICT Id 317562

PHYLAWS intends to design, prove efficiency and demonstrate realistic implantations of new privacy concepts for wireless networks that exploit radio-propagation phenomena.

⇒ **Application scenarios are eavesdropper and intrusion attempts inside public network, and physec countermeasures**

- at transmitted signals
- at network signalling data (databases)
- at subscriber private data (identifiers, etc.)
- at users data (msg content…)



=> Propagation environments are diverse

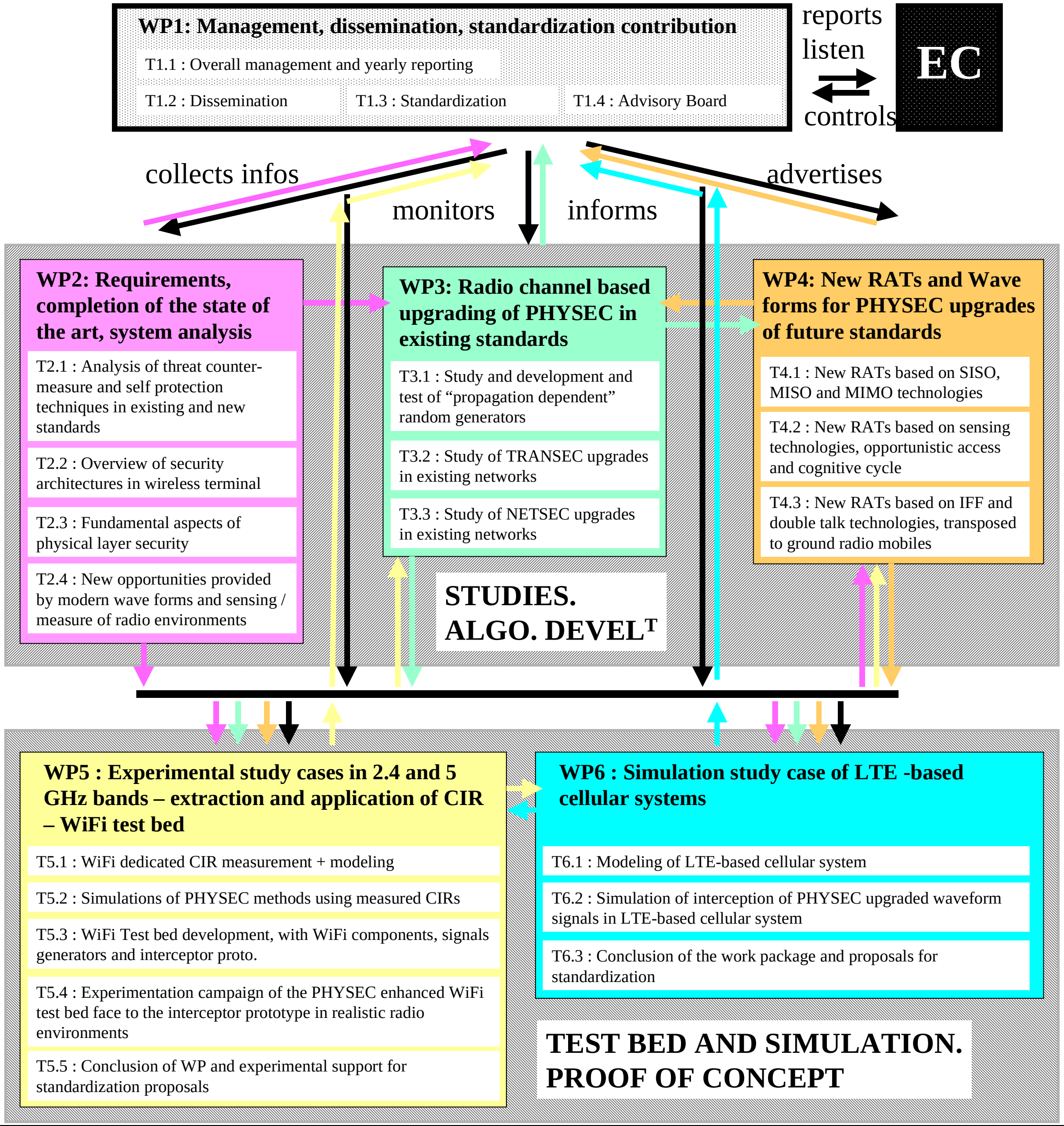
- Outdoor environment, from rural to dense urban
- Indoor environment

=> Any kind of public wireless (radio-cells, WLAN, PMR, SRC, BH)

- Special focus on Wifi: experiments of a Network + eavesdropper test bed
- Special focus on LTE: simulation.

Supported by PHYLAWS project FP7 ICT Id 317562

About the Phylaws project
Organization and contents



Overview of existing public radio access technologies

System	Uplink frequency plan (MHz)	Downlink Frequency plan (MHz)	Channel spacing	Modulation UL - DL	Radio Access Technlogy	Access mode	Range of Terminal Power	Typical propag. Range	ref standard
GSM 900	890 - 915	935 - 960	200 kHz	GMSK + variants	TDMA/FDMA	Aloha	2 W	100 m to 3 km	ETSI
DCS 1800	1710 - 1785	1805 - 1880							
PCS 1900	1850 - 1890	1930 - 1970							
UMTS	890 - 915	935 - 960	5 MHz	(OC) QPSK	DSSS/CDMA FDD and TDD, MISO	Aloha	0,25 W	10 m to 3 km	3GPP
	1920 - 1980	2110 - 2170							
LTE	890 - 915	935 - 960	1,4 - 5 MHz	OFDMA and SC-FDMA	FDD and TDD, MIMO	Aloha	0,25 W	10 m to 3 km	3GPP
	2500 - 2570	2620 - 2690							
IS-95 A/B	824-844 1850 - 1890 other	869-889 1930 - 1970 other	1,25 MHz	OQPSK - QPSK	DSSS/CDMA	Aloha	2 W	100 m to 3 km	3GPP2
CDMA2000 SR1/3GPP2			5 MHz						
CDMA2000 SR3/3GPP2			5 MHz						
WIMAX	2402 - 2480		10 MHz	OFDM and QPSK/CDMA	TDD, SC-OFDMA, MIMO	CSMA/CA	0,25 W	1 to 15 km	IEEE 802.16xxx
	3400 - 3600								
	5150 - 5850								
WIFI L band	2402 - 2480		20 MHz	OFDM and QPSK/MC-CDMA	TDD, MIMO	CSMA/CA	0,1 W	indoor	IEEE 802.11xxx
WIFI C band	5150 - 5850		20 - 80 MHz						
Bluetooth	2402 - 2480		157 kHz	0,5 BT GFSK	TDMA/TDD	CSMA/CA	0,01 W	indoor	IEEE 802.15.1
Zigbee	868 - 868.6		2 et 5 MHz	ASK, BPSK, O-QPSK, MSK	CDMA/TDMA	CSMA/CA	0,01 W	indoor outdoor < 50 m	IEEE 802.15.4
	902 - 928								
	2400-2483.5								
DVB-T		470-862	8 MHz	COFDM	FDD, MISO		20 - 200 kW	>> 10 km	ETSI

Main Source :
A Kaiser,
GDR Soc Sip
Paris tech
10 Mai 2011

Supported by PHYLAWS project FP7 ICT Id 317562

Overview of existing public radio access technologies
Details on FDMA TDMA

FDMA (Frequency Division Multiple Access)

- **signal repartition over frequency**
- **examples are 1G public standards:**
  - **NMT,**
  - **AMPS.**
  - **…**
- **propagation equalization is required in receivers**
- **hopped frequency and opportunistic frequency variants**
  - ⇒ **Military,**
  - ⇒ **Automatic Link Establishment (HF modem, ancestry of C.R.)**

TDMA (Time Division Multiple Access)

- **signal repartition over time slot**
- **mixt TFDMA/FDMA variant with hopped frequency**
- **propagation equalization is required in receivers**
- **examples are**
  - **2G public standards (GSM, D-AMPS IS 54/136)**
  - **short range radios : Bluetooth, Zigbee, DECT,**
  - **numerous tactical VHF Military ad hoc radios (PR4G, Sincgars)**

Supported by PHYLAWS project FP7 ICT Id 317562

Overview of existing public radio access technologies

Details on CDMA OFDM

CDMA (Code Division Multiple Access)

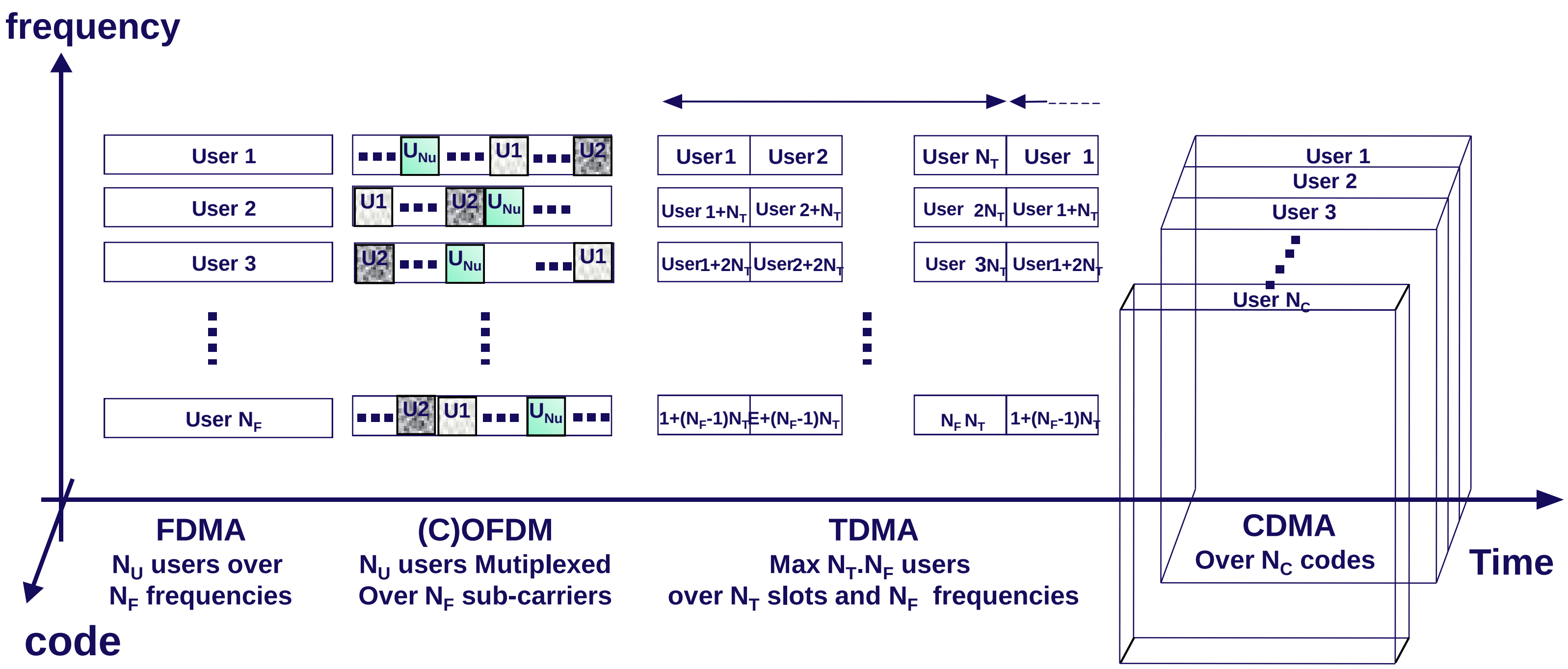
- **signal repartition over scrambling codes + spreading codes**
- **receiver Rake processing**
- **mixt CDMA/FDMA/TDMA variants with hopped frequency / slots**
- **examples are**
  - **3G public standards (3GPP, 3GPP2),**
  - **WLAN (802.11a)**
  - **several UHF and SHF Military ad hoc networks (ex: MIDS).**

OFDM (Orthogonal frequency Division Multiplex)

- **signal multiplexing over frequency**
- **simplified equalization in receivers (when facing frequency selective fading)**
- **numerous examples:**
  - **Digital broadcast: DAB DVBT/H, DRM,**
  - **Numerous WLAN: Wifi, Wimax**
  - **4G radiocells : LTE**
- **specific planning capabilities (Single Frequency Network, MISO, MIMO)**
- **numerous variants and derived RATs : COFDM, O-FDMA, SC-FDMA, SC-FDE**

Supported by PHYLAWS project FP7 ICT Id 317562

Overview of existing public radio access technologies
Illustration of FDMA TDMA CDMA OFDM



Overview of existing public radio access technologies
Initial radio exchanges of the radio access protocol

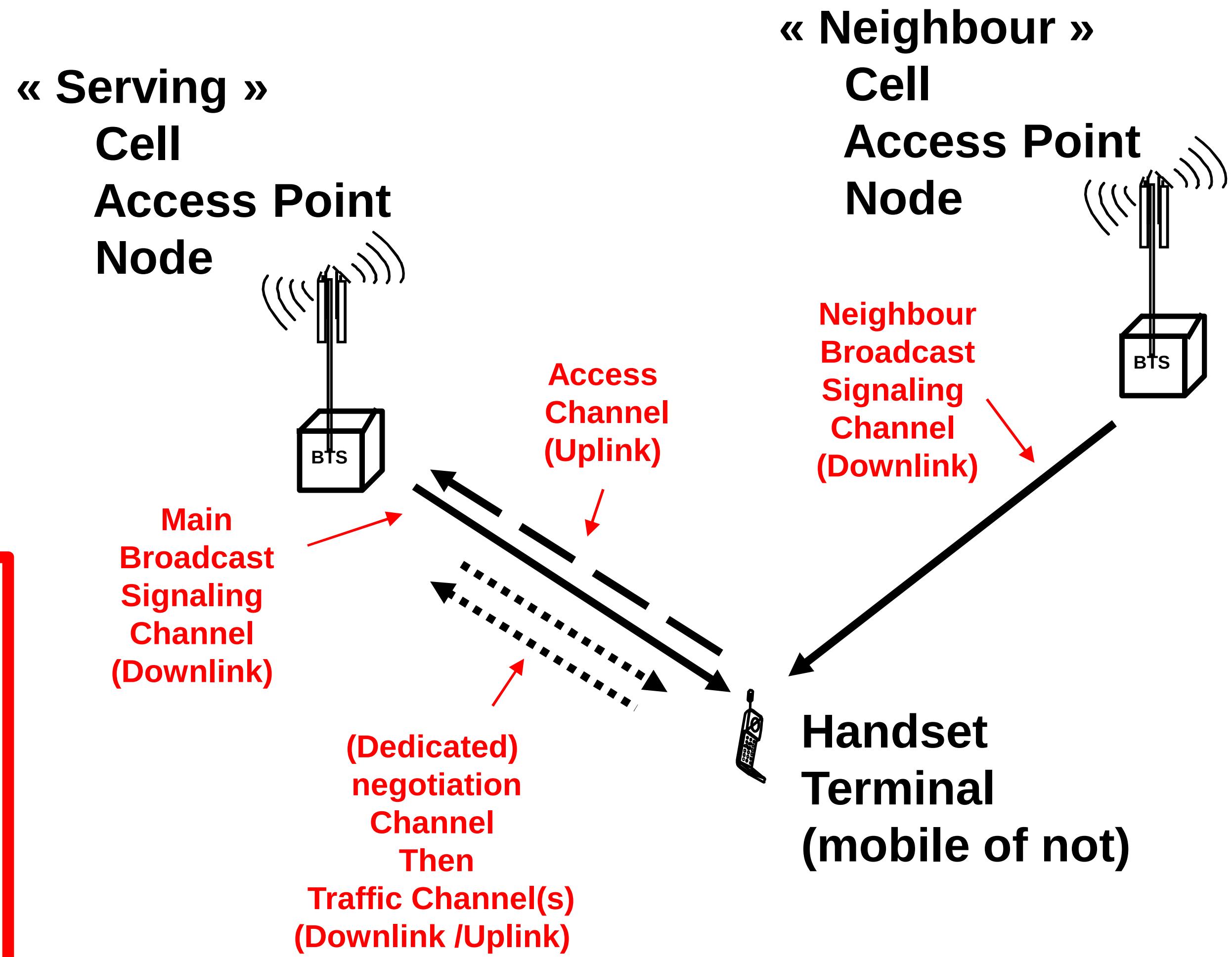
Radio-Cellular model

⇩

Applies roughly to any modern digital standard

⇩

First exchanges of radio access protocol are the weakest ones regarding privacy and security of public radio standards



Supported by PHYLAWS project FP7 ICT Id 317562

Security lacks of public network
Global overview

Some Native trends involve privacy lacks

When Standards address a worldwide mass market with numerous operators and industrials
=> difficult to share deep secret among millions of subscribers/terminals worldwide
=> signal received for early access attempts must be easy to detect/decode
=> signaling must be easy to interpret/understand
=> implies simplified early registration and authentication procedures
=> facilitates mimic attacks of legitimated nodes and mitm attacks thanks to a minimal checking of signaling and to recovery/recording of network planning + traffic load

When Standards address mobile service
=> location updating (roaming) and handover are necessary
=> large scale sharing of subscribers data bases
=> recurrent /repeated subscriber authentication
=> recurrent measurement of radio link and reporting + associated power control

When Standards address cognitive/opportunistic RAT
=> Geo-referenced database downloading
=> geo-referenced access attempts
=> (geo-referenced) sensing and reporting

When terminal are multi-Standards or muti-RATs
=> impeachment of one RAT often forces the use of the other available RATs, even when weaker.

When Backward Compatibility of Security mechanisms occur
=> example is EPS AKA in LTE compatible with previous GSM and UMTS
-> security information got on GSM or UMTS may be re-used within LTE network

Supported by PHYLAWS project FP7 ICT Id 317562

Security lacks of public network
Global overview – non exhaustive

Some standards have Intrinsic privacy failures

Channel State Information (CSI) negotiation
=> in Wifi and in many other MIMO RATs
=> most often in clear text

Subscriber/terminal dependent traffic channel allocation instead of full random allocation
=> in 3GPP2 RAT public modes.

Low combinatory pilot symbols in traffic channel
=> 3GPP and others

Clear text delivery of radio resource characteristics
=> frequency hopping sequences of intermediate channels (SDCCH GSM)
=> frequency hopping sequences of traffic channel (Bluetooth)
=> pilot codes of access paging channels and intermediate control channels (3GPP, 3GPP2)

Poor random generation and poor management of system time
=> conception defaults or random generators in Bluetooth
=> shared public GPS system time in 3GPP2/IS95/CDMA2000.

"Master management" of security concentrates weaknesses/attacks on one node (example Zigbee).

Conception defaults of Cipher / protection algorithms
=> weak WEP keys initially used in Wifi, uncrypted MAC header in Wifi Frames.
=> unprotected transmission of terminals' and nodes' cipher capabilities: GSM, Wifi, other…
=> weak cipher mode A5-2 of GSM
=> clear text SMS in many standards

Supported by PHYLAWS project FP7 ICT Id 317562

Security lacks of public network

Global overview – non exhaustive

In addition privacy risk may be improved in "real life"

Added geo-location services

=> imply more frequent location updating + transmission of relevant message
=> very frequent in Satellite mobiles (facilitate routing and billing) and in multi–RAT terminals
=> very often geo-location data are in clear text, especially at earliest RAT stages: PCS, 4G, CR…

Economic competition among standards, unexpected publications and hacker activities

=> publications that point out weaknesses of adverse standards
=> un expected publication of MoUs secrets; examples are A3/8 and A5 algorithm of GSM
=> web publication of subscribers' lists by hackers with relevant identifiers
may lead to (successful) attempts for cloning SIM cards, passive monitoring of voice/data services…

Sub-optimal radio-engineering practices

=> radio engineering is often facilitated when minimum security options are activated
=> "GSM atavism" of some network technicians/operators
=> a typical example is single sense AUTH in many UMTS networks,
even if 3GPP specifies dual sense AUTH procedure

Sub-optimal terminal conception: many terminals have pre-SIM cards inside (test in production chain
several have defaults in their protocol implantation.

Legal restrictions : best protection may be non-authorized in several countries or in specific location
(exterior to EU in general)

Security lacks of public network
GSM example

MAIN GSM ACCESS PROCEDURES

PROCESSING & CHANNEL	TERMINAL STATE	EXCHANGED PARAMETERS	BTS STATE
Idle. Monitors signalling and paging channels	Monitoring signalisation&paging	← Infos cells network & paging msg BCCH and PCH clear text	Emitting signalization and paging *Broadcast Signaling Channels, Paging channels*
Access demand ACH Paging response ALOHA fixed freq. signals No cipher	*Access Channels* **ACCESS DEMAND** **PAGING REPONSE** Request Number	ACH clear text →	**IMMEDIATE ASSIGNMENT** Time and freq. parameters Time Advance comp. Carrier, Slot Number, etc.
Location Updating Start of Authentication (SDCCH, Hopped Freq, No cipher)	**LOCATION UPDATING REQUEST** **(when : stop -> idle)** Temporary ID : **TMSI** Permanent ID : **IMSI** Electronic ID : IMEI	← 1st Msg chan. assignT : SDCCH clear text (HSN, MAIO, TS, FN) **Old TMSI** or **IMSI** or IMEI → SDCCH clear text	**AUTHENTICATION REQUEST** NRAND generation
Preliminary Identification SDCCH, Hopped Freq, No cipher	**AUTHENTICATION RESPONSE** comp. Of SRES=f (A3, NRAND) NOTA in GSM algo. A3 prop. Oper. A3	← **NRAND** SDCCH clear text **SRES** → SDCCH clear text	**AUTHENTICATION UPDATED** VLR/HLR check of SRES => IMSI & Ki are known
Authentication ack. Cipher key computation (SDCCH, Hopped Freq, No cipher)	**CIPHERING MODE COMPLETE** Cipher key Kc=f (Ki, A8, NRAND)	← **NRAND** SDCCH clear text Ack. →	**CIPHERING MODE COMMAND** Comp. Of key Kc =f (Ki, A8, NRAND) NOTA in GSM : algo A8 prop. operator A8
Traffic Channel allocation New TIMSI alocation (SDCCH, Hopped Freq, Ciphered)		← New TIMSI 2nd msg chan. assignT SDCCH/TCH cipher text (HSN, MAIO, TS, FN, TSC)	**LOCATION UPDATING ACCEPT** New identifiers in cipher text NOTA : Algo IMSI -> TMSI prop. operator
Communication + handover (TCH, Hopped Freq, Ciphered)	**MS → BS**	↔ **Ciphering = f (algo. A5-1, A5-2,...)** A5	**BS → MS**

Winncomm 2013 Europe Munchen, 11 June 2013 session 1 - paper 1 : privacy threats within civilian wireless networks

Supported by PHYLAWS project FP7 ICT Id 317562

THALES Celeno TELECOM ParisTech PHYLAWS Imperial College London VTT

Security lacks of public network
GSM example

Frequency hopping is an option (depending of operators choice).
Many of Channel assignments characteristics are stationary in practice (depending of operators choice

GSM Signaling is in clear text
=> easy recovery of cell synchronization
=> easy decoding of cell frequencies (CA list), esay recovery of network structure and planning (BA list)
=> easy decoding of First assignment message (SDCCH supporting AUTH and cipher procedures)

GSM Authentication procedure is poor
=> single sense only : BS authenticate MS but MS does not authenticate BS
=> MS spoofing is possible with a fake BS *(a typical example of a fake BS is a R&S mobile protocol tester such as the "old" CMD45)*
=> NRAND and SRES are in clear text
=> A3 should remain and operator's secret it is known that most operator uses the COMP128 algo. and the COMP128 algo was published in the late 90s
=> unexpected publications of subscriber lists including Keys Ki and identifier IMSI.

GSM Identity management is weak
=> old TMSI is transmitted in clear text in the early stage of RAT
=> use of TMSI is not systematic (IMSI is frequent in border zones, airport, etc.)
=> change of TMSI is not systematic (operators' management)
=> many operator use COMP128 derived algo. (same as A3/A8) to compute TMSI from IMSI

GSM Cipher management is weak
=> ciphering capabilities of MS are transmitted in clear text without integrity control
=> A8 for most of operators is known to be COMP128 (published). A5 is not secret yet
=> change of Kc is not systematic at each new session (operators management)

Supported by PHYLAWS project FP7 ICT Id 317562

Sensing and downloading – protocol aspects

Source : E²R project, White Paper Nov 2007

0- Switch-on and initialization

Location determination

Detection of CPC

1- Exploitation of the DL "public advertiser"

Extraction of the information relevant to the mesh where the mobile is located

Local check and upgrade of the signal model data base

2- Sensing and Measurement of radio link

Priority to "oriented analyses"

with the help of upgraded data-bases

Shortcut with data-aided processing when suitable

Back-up stand-alone analyses for failure cases

+ recording of signal samples for further deeper analysis

3- Reporting through dedicated radio-links

Sensing : radio measurements

→ cognitive manager / network

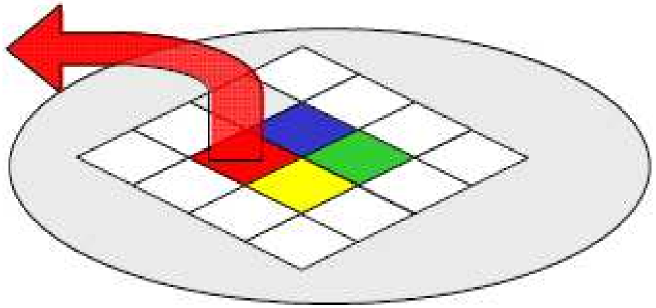
SM : radio measurements + signal samples

→ towards SM centers

CPC information

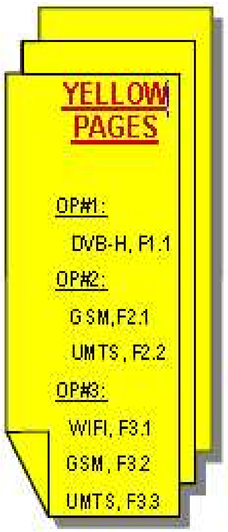
- **mesh dependant**
- **contains relevant updated data describing the way spectrum is locally used in mesh #i**

Mesh #i Geographic area

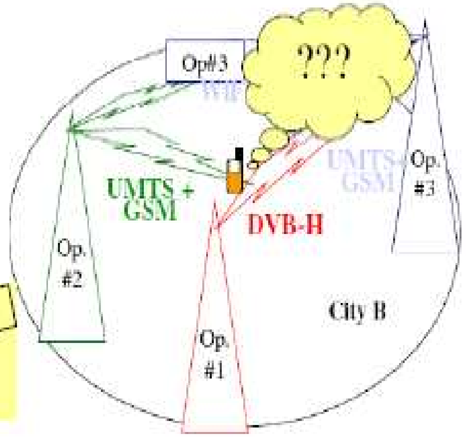


CPC mesh organization

CPC DL "public advertiser" concept



At switch on:
The terminal does not know the "current" configurations of the various networks, neither the frequency bands allocated to the Radio Access Technologies (RAT)



Security lacks of public network
Special Focus on SDR and CR

. **Geo-referenced database downloading** will inform about
=> the available radio-networks
=> the relevant radio-access parameters.

. **Terminal will perform sensing and report to nodes** about the local radio spectrum.

. **Terminals should perform geo-referenced access attempts**
=> systematic transmission of subscribers' locations in the early stages of the negotiation protocols

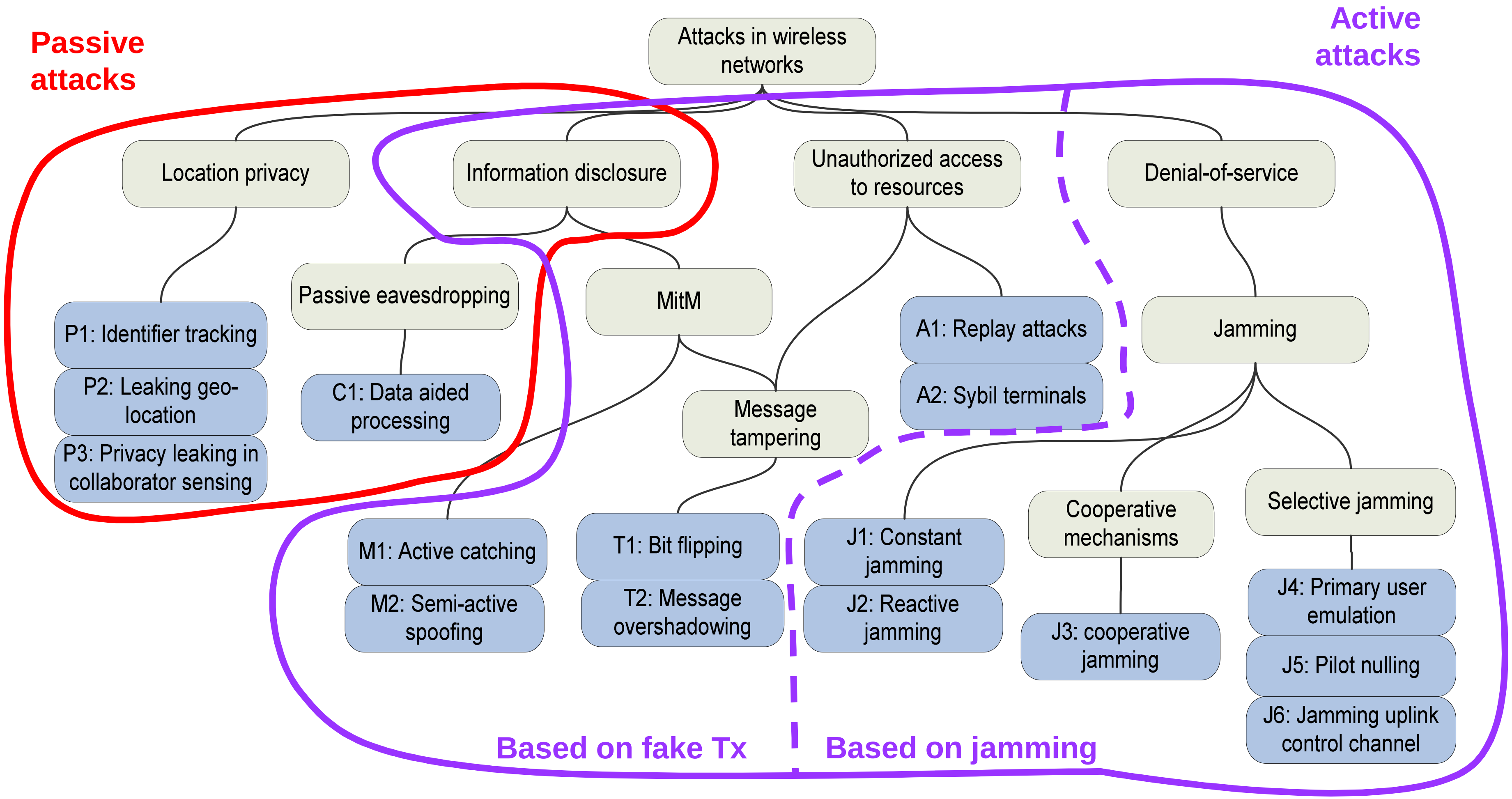
. **Dedicated "beacon" signals such as DL/UL-CPC** (Down Link and Up Link Cognitive Pilot Channel)
=> broadcasted in order to support terminal and nodes
- downloading and sensing
- channel sounding procedures
=> Network downloading and terminal embedded sensing should be based on a DL-CPC.
=> Sensing information reporting and BS/node sensing should be based on the use of a UL-CPC signal.

. **Simplification of early procedures**,
=> both DL-CPC and UL-CPC should be designed for fast recognition
+ accurate measurements
+ easy decoding.

. **Strong security risks:**
=> massive accurate information is broadcasted every time everywhere about neighbor network and MS
=> DL-CPC and UL-CPC are perfect targets for eavesdropper and radio hacker systems

Supported by PHYLAWS project FP7 ICT Id 317562

Security lacks of public network
An attempt for threat classification



Supported by PHYLAWS project FP7 ICT Id 317562

Data aided signal processing achieve good eavesdroppers' performances
Smart antennas achieve very good eavesdroppers' performances

"Direct" Inter-correlation

- Early detection and recognition
- Protocol structure recovery

Direct identification

- Modulation parameters
- Radio access protocol
- Set of coding schemes

Comparative advantages

> When Low combinatory

and low Doppler domain

=> reduced complexity

=> real Time OK

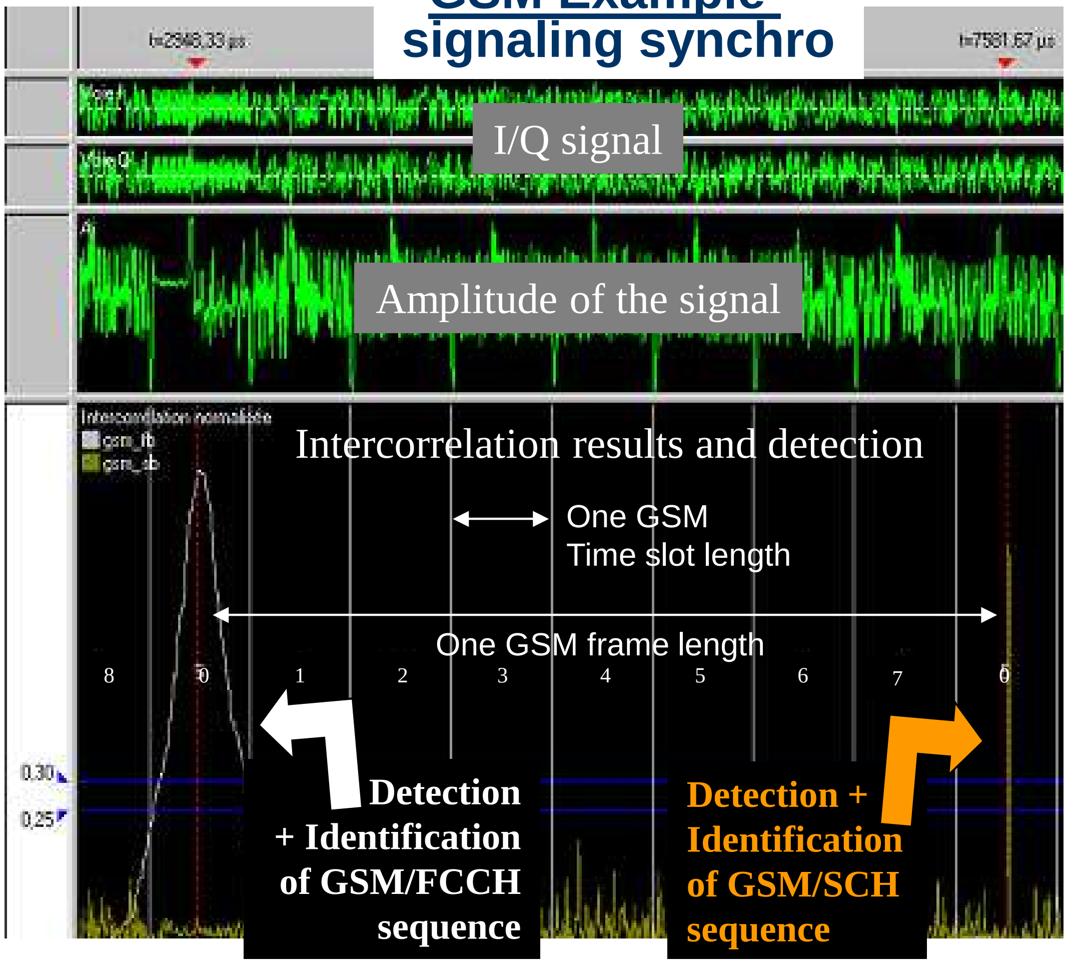
> Processes low powers signals

SISO eavesdropper : SINR > 6 dB

SIMO eavesdropper : SINR > -10 dB

is usal

GSM Example – signaling synchro



Supported by PHYLAWS project FP7 ICT Id 317562

Data aided signal processing achieved good eavesdroppers' performances
Smart antennas achieve very good eavesdroppers' performances

<u>GSM real filed Example</u> : measurement and decoding of broadcast signaling

Radio parameters | **Network parameters**

	FU	Level(dBm)	C/I(dB)	CI	LAC	MNC	BSIC	FN
BTS1	70	-99.2	-13.1	39911	33391	1	50	69932
BTS2	70	-94.4	-7.9	35562	240	20	40	1251388
BTS3	70	-89.0	-0.6	2581	21235	1	2	1119767

	List of Cell Allocated frequencies	List of Border Cell beacon frequencies
BTS1	70	98 99 100 102 103 104 107 108 111
BTS2	70 101	90 94 100 104 110 116 118 124 675 681 689 697 705
BTS3	70 113 114 115 116 117 118 119 120	101 103 110

Supported by PHYLAWS project FP7 ICT Id 317562

Data aided signal processing achieved good eavesdroppers' performances
Smart antennas achieve very good eavesdroppers' performances

GSM Example: decoding of dedicated signaling (PCH, SDCCH etc.)

Access to protocol parameters : below are authentication result
Then demodulation of ciphered messages => ready for cipher attack

Layer 3 messages

Sense		Message	Frame ID	length	Frame Number		
DL	OM	Sync Channel Info	0x013819	4	31	28	25
DL	RR	System Info Type 6	0x013824	9	42	28	10
DL	OM	Sync Channel Info	0x013823	4	41	[illegible]	09
UL	MM	Authentication Response	0x013822	4	40	28	08

Message content

Offs.	Bytes (hex)	Mask	Fields
-2	05	00001111	Protocol Discriminator = Mobile Management
-2	05	11110000	Skip Indicator = 0
-1	54	00111111	Message Type = Authentication Response
			Message Content:
			Authentication Parameter
0	4E 5A B3 58		SRES = 4E 5A B3 58

APPLIES TO INITIAL ASSIGNMENT PARAMETERS,
OLD TMSI,
NRAND&SRES,
MOBILE CIPHERING MESSAGE, ETC.
UP TO CIPHERING IS ESTABLISHED

Supported by PHYLAWS project FP7 ICT Id 317562

Data aided signal processing achieved good eavesdroppers' performances
Smart antennas achieve very good eavesdroppers' performances

A => Complete identification of 3GPP/WCDMA Node-Bs

I- Smart antenna techniques for source separation (Matched Spatial Filter)

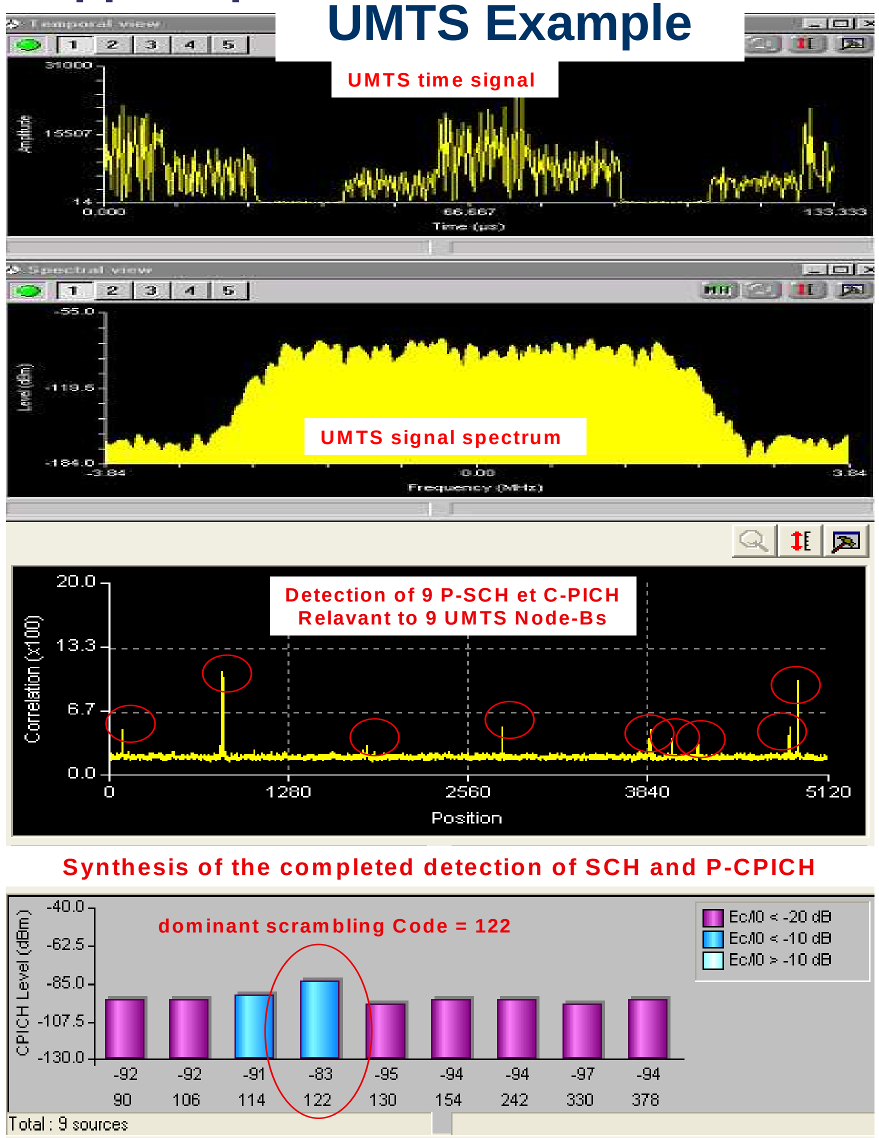
II- Three stages processing
- a) slot synchronization
- b) CPICH descrambling
- c) CCPCH demodulation and decoding

Cf. Antium FP7 project (2003)

B => Complete de-spreading and demodulation of DL traffic

SISO Eve: usual SINR are
- SINR down to – 18 dB with P-SCH
- SINR down to – 30 dB with P-CPICH

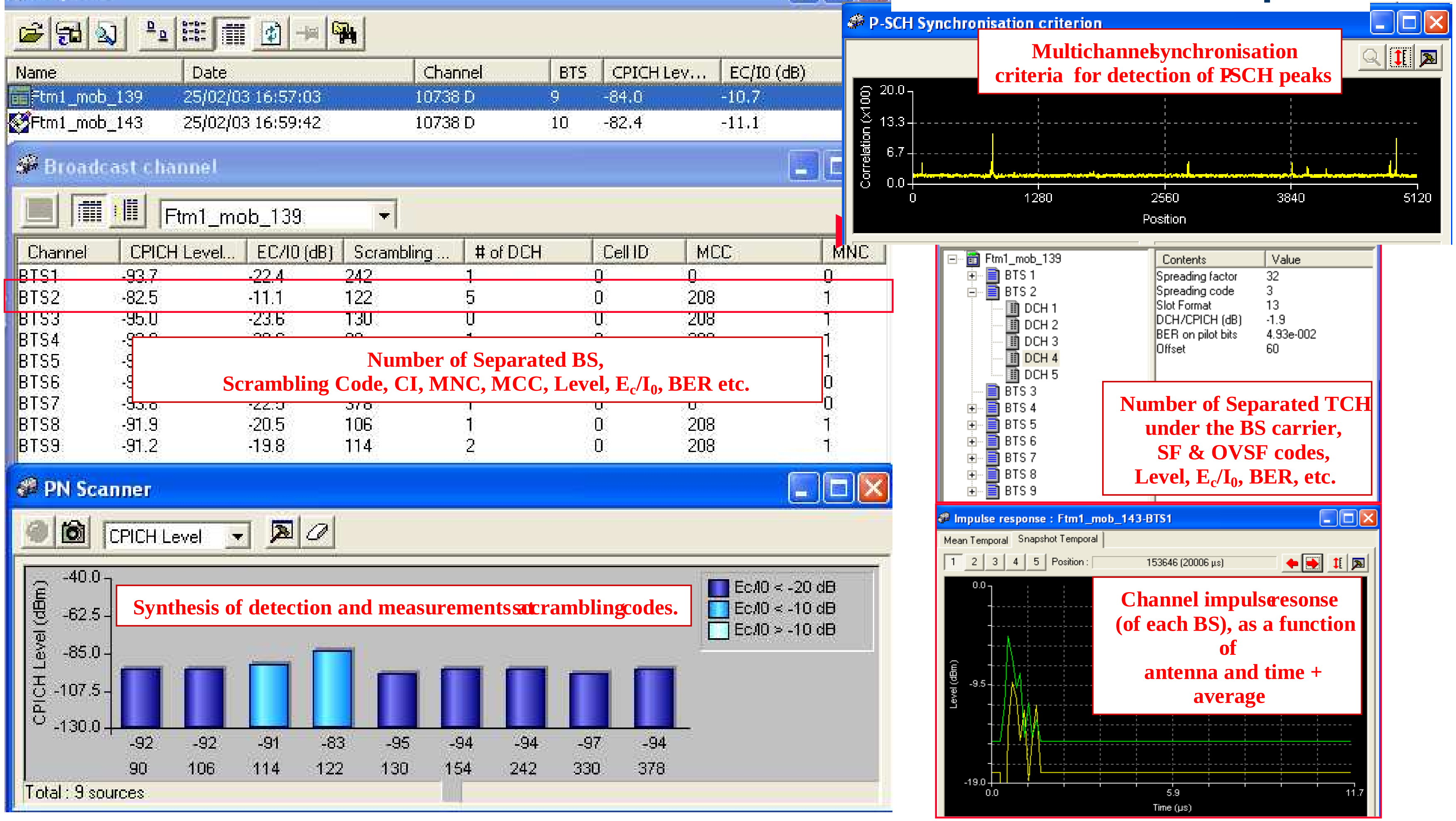
SIMO Eve: achievable SINR are :
- SINR down to – 30 dB with P-SCH
- SINR down to – 50 dB with P-CPICH



About passive threats
Cooperative processing

Data aided signal processing achieved good eavesdroppers' performances
Smart antennas achieve very good eavesdroppers' performances

UMTS Example

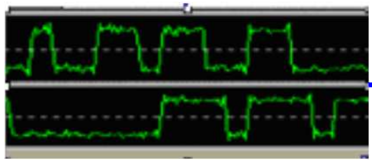


Supported by PHYLAWS project FP7 ICT Id 317562

THALES Celeno TELECOM ParisTech PHYLAWS Imperial College London VTT

About passive threats
Semi-Cooperative processing

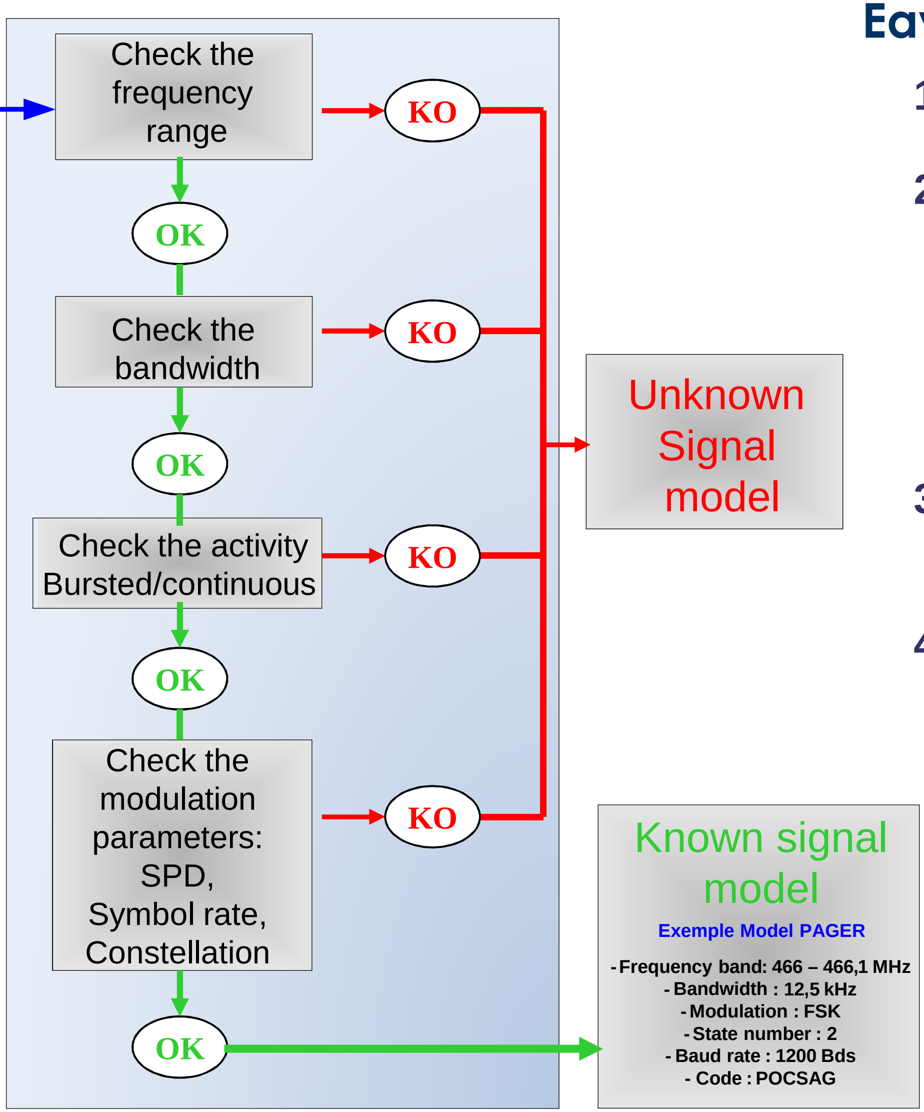
Even non standard civilian signal may be weak when facing oriented Eavesdropper processing



Example of Input Signal

Model 1: PAGER
- Frequency band: 466 – 466,1 MHz
- Bandwidth : 12,5 kHz
- Modulation : FSK
- State number : 2
- Baud rate : 1200 Bds
- Code : POCSAG

Example of semantic model from data base



⇒ **Step by step oriented analyses + checking of semantic characteristics**

⇒ **Very efficient when dealing with digital modulations**

1/ «expert system» type

2/ progressive estimators
- signal enveloppe,
- modulation parameters
- code parameters

3/ from general to dedicated

4/ model comparison at each step

=> leads the following processing

=> reduces combinatory

See annex

Supported by PHYLAWS project FP7 ICT Id 317562

Main advantages of passive attacks

- ⇒ **Discrete and anonymous**
- ⇒ **May be selective on the targeted victim**
- ⇒ **Usually more efficient in DL sense (power budget, more stationary propagation)**
- ⇒ **May be re-enforced with directive antennas, and with smart-antennas**
- ⇒ **May be implanted with massive recording + off line processing**

Main drawbacks / difficulties of passive attacks

- ⇒ **Very sensitive to radio environment (see examples in annex)**
  - ⇒ Spectrum occupation
  - ⇒ Propagation losses (especially in UL sense)
  - ⇒ Interferences
  - ⇒ Disturbed by the power control of the legitimate link

Main principles for counter-measure of passive attacks

- ⇒ **Reduced DSP of signals**

  Direct spread spectrum;

  Tag signal under main signals
- ⇒ **Furtive signals** (frequency hopping, low duty cycle and time hopping)

=> Earlier protections (ideal would be protected of signalling and paging – see paper 2)

=> Advanced coding + ciphering, secrecy codes

Supported by PHYLAWS project FP7 ICT Id 317562

Radio Hacker System (RHS) Application example to GSM

RHS exploit:

Network signaling

+

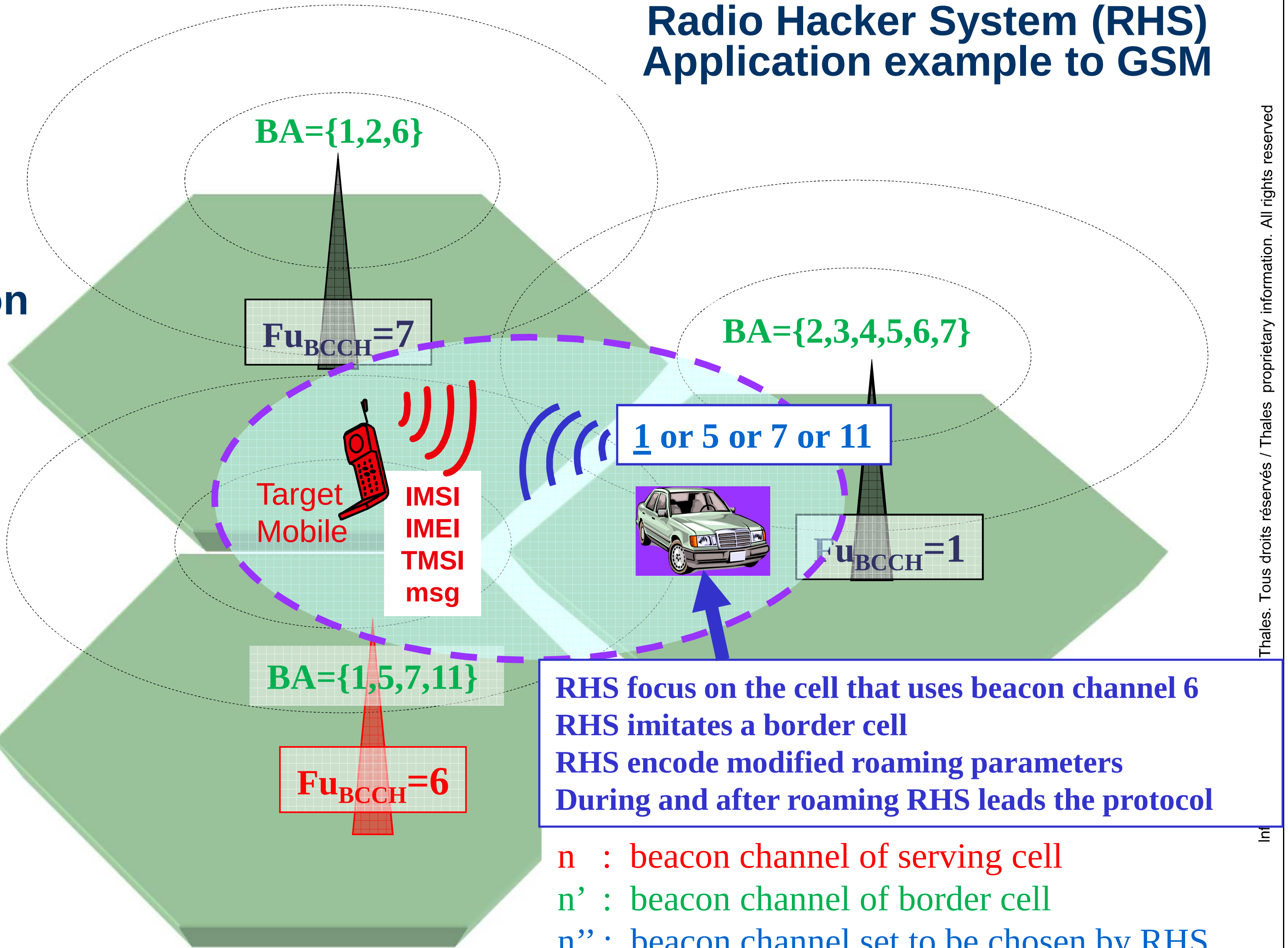
Authentication Defaults

+

Forcing of Location updating procedure

+

added jamming



n : beacon channel of serving cell
n' : beacon channel of border cell
n'' : beacon channel set to be chosen by RHS

Supported by PHYLAWS project FP7 ICT Id 317562

Radio Hacker System (RHS)
Application example to GSM

Beacon channels

Same Identifiers are cloned
Except roaming LAC

different synchronization Parameters

Power différence is significant

BCCH	FU	CI	LAC	MCC	BSIC	FN	Level (dBm)	C/I (dB)	
BCCH1	22	19607	24576	208	33	43572	<-98.3	<-20.0	Real BTS (Neighbor)
BCCH2	22	19607	00001	208	33	1972	-60.7	14.6	RHS Transmitter (programmable MS protocol tester)

Note : **This example is a <u>real field</u> record**
Measurement and diagnosis are performed with a dedicated system

GSM/UMTS interference analyser - Smart antenna technology
Direct scanning of GSM band + carrier measurement,
No a priori knowledge for detection,
A posteriori validation (consultation of network database)

Supported by PHYLAWS project FP7 ICT Id 317562

Main advantages of active attack

=> The RHS controls the protocol (such as a real BTS) => Many capabilities :

forcing location updating IMSI attach/detach of MS targets

catching IMSI and IMEI instead of TMSI

forcing a non/ligher-encryption mode for easy monitoring,

possible coupling with a Direction Finder (filters target) and smart antennas (improves range)

blocking the MS target communications

Main drawbacks / difficulties of active attacks

⇒ **The RHS has to overhead the real network and the cell re-selection criteria**

- power disadvantage especially when facing urban BS,
- usually low effect range

⇒ **"Basic" RHS are very indiscrete, thus easily detectable**

with a tracking mobile at low range, with a SM System at large range (see page above)

⇒ **"Basic" RHS turn the mobile off the network (MS is not reachable yet)**

⇒ **RHS are "real time" only**

⇒ **"Basic" RHS disturb many mobiles in the neighborhood.**

saturation risk of the RHS because of multiple roaming/detach of non-targeted terminals.

Note that there exist more advanced RHS concepts :

active and more discrete, semi-active, re-enforced with selective jammer, etc.

Main principles for counter-measure of active attacks

=> Re-enforce cell-reselection criteria

⇒ **Re-enforce subscriber and network Authentication:**
   => at least dual sense

⇒ **Re-enforce signal integrity control and identification of received signals :**
   ⇒ More accurate check of dual sense synchronization
   ⇒ Radio-electric Tag with heterogeneous signal

⇒ **Re-enforce message integrity control**
   ⇒ When facing semi active attacks
   ⇒ When facing advanced RHS that achieve accurate synchronisation on legitimate links

Supported by PHYLAWS project FP7 ICT Id 317562

Existing countermeasures principles

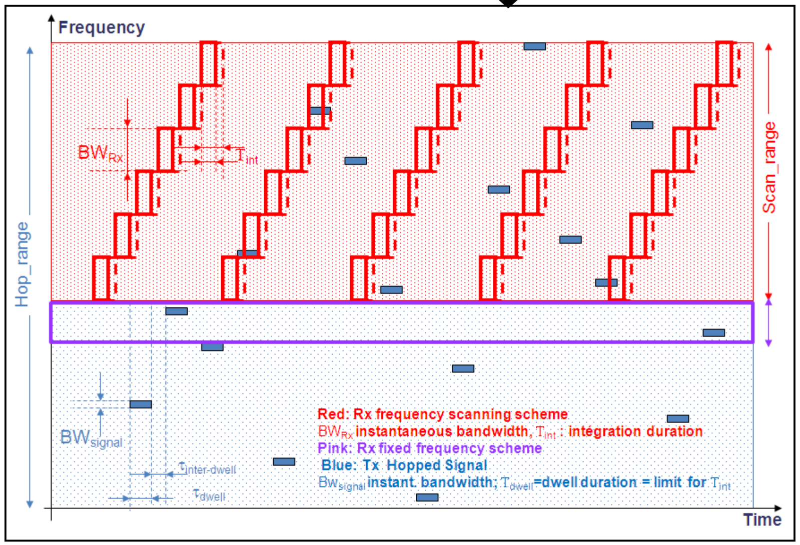
TRANSEC (Transmission Security):

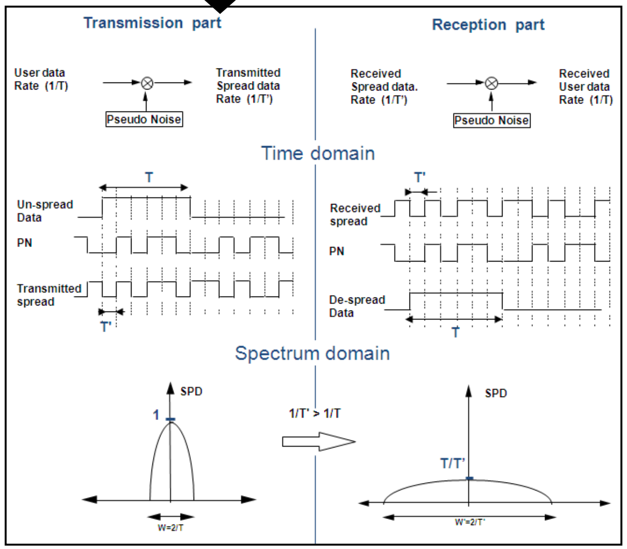
=> relevant to the protection of the wave form

- Face to interception/direction Finding
- Face to jamming of the user receiver,
- Face to intrusion attempts into the radio-communication access protocol.

Mainly at the radio interface.

Usually based on frequency hopping and spread spectrum technologies





An other innovative idea is intentional cooperative jamming at the legitimate Tx part associated with MISO or MIMO RATs (see next presentation)

Supported by PHYLAWS project FP7 ICT Id 317562

Existing countermeasures principles

NETSEC (Network Transmission Security)
=> relevant to the protection of the content of signalling

Either at the radio interface and Medium Access Control + request to upper layer.

Usually based on **<u>authentication and identification of transmitters</u>**
<u>integrity control of signalling data</u>
+ ciphering of signalling (military communications)

COMSEC (Communication Security):
=> relevant to the protection of the content of the user messages (voice,data).

Either at the radio interface and at upper layer (management).

At several protocol layers and interfaces (examples are point to point ciphering of each user data flux, ciphering of IP packets, ciphering of artery, etc.).

Usually based on **<u>ciphering,</u>**
<u>authentication and integrity control of signalling and users data</u>

Perspectives offered by physical layer security (PHYSEC)

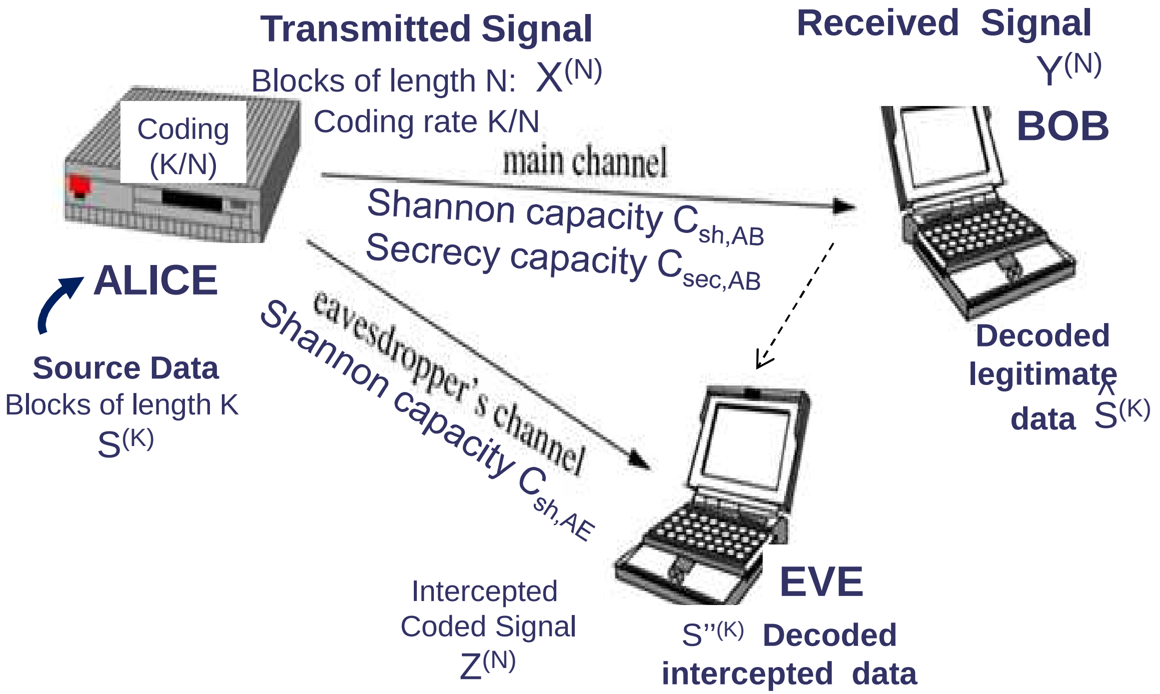
PHYSEC (PHYsical layer SECurity) :

=> generic

=> all kind of protection technique that is based on the use of the physical layer sensing and/or measurement.

Native physec is based on <u>secrecy codes,</u> i.e. modified channel codes

- So that legitimate information from Alice to Bob approaches Shannon capacity
- So that information from Alice to Eve is mitigated.



(see next presentation for further explanations)

Supported by PHYLAWS project FP7 ICT Id 317562

Perspectives offered by physical layer security (PHYSEC)

Impact of TRANSEC NETSEC COMSEC and PHYSEC to OSI layers:

PHYSEC ADRESSES

	OSI Layers
COMSEC (Communication Security) Content protection, i.e. voice data. Radio interface or upper layers. Authentication, confidentiality and integrity of signaling and user data.	Network layer Data link layer Physical layer
NETSEC (Network Security) Protection of signaling of the network. Radio interface or medium access control layer. Transmitter authentication, integrity control and confidentiality of signaling data.	Data link layer Physical layer
TRANSEC (Transmission Security) Protection of wave form from interception and direction. Radio interface. Transmitter finding, receiver jamming, access of radio communication.	Physical layer

Supported by PHYLAWS project FP7 ICT Id 317562

Perspectives offered by physical layer security

The (network) impact of phylaws' innovations is expected to remain limited

⇒ **Native secrecy coding & physec solutions apply mainly at the radio interface of handsets and communication nodes**
- at modulation and coding stacks
- at radio access protocol stacks
- no transec nor comsec key

=> expectations are "No impact at upper layer protocol"
"No impact at network architecture"

⇒ **Merged Physec + transec solutions could lightly impact the PHY layer and at the MAC layer**
- dedicated wave forms for
  initial access attempts (ACH phase, IFF modes)
  authentication procedures
- revised "channel sounding" procedures (MIMO, Wifi, LTE-A…)
- upgraded sensing procedures (cognitive radio)

=> expectation is "No more constraints at upper layers than existing"

Supported by PHYLAWS project FP7 ICT Id 317562

Perspectives offered by physical layer security

The (network) impact of phylaws' innovations is expected to remain limited (follow on)

⇒ **Merged physec + comsec solutions should simplify existing ciphering and integrity control schemes**

- **introduce "new random"** inside existing ciphering procedures (such as self-synchronized stream cipher)
  . that would be propagation dependant
  . that would take benefit of Alice-Bob and Alice-Eve un-correlated channel
  . That would use no added keys neither redundancy

- **limit redundancy** inside signalling and users' messages, thus increase effective data rates for users and spectrum efficiency

- **limit/avoid the use and the exchanges of ciphering keys**

⇒ The expectations are both enhancement, simplification, and redundancy reduction inside existing netsec/comsec procedures

Supported by PHYLAWS project FP7 ICT Id 317562

Conclusion

Existing wireless public standards are (very) weak regarding security and privacy at the radio interface

Physec should provide practical and significant enhancement perspectives for wireless security

A complementary presentation follows on PHYSEC concepts:

- Deeper explanations of physec concepts
- State of the art
- Perspectives for transec, netsec and comsec of public standards

Some annexes are given hereafter

- radio-environments
- complements on signal processing

Supported by PHYLAWS project FP7 ICT Id 317562