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

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

Cong Ling

Imperial College London; London, United Kingdom; c.ling@imperial.ac.uk;

François Delaveau, Eric Garrido

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

Jean Claude Belfiore, Alain Sibille

Institut Mines Telecom Paris Tech; Paris, France; belfiore@enst.fr; alain.sibille@telecom-paristech.fr

Supported by PHYLAWS project FP7 ICT Id 317562

SUMMARY

Note : privacy weaknesses of wireless networks and counter measure principles were introduced in a previous paper

Supported by PHYLAWS project FP7 ICT Id 317562

About the Phylaws project
Context

- **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

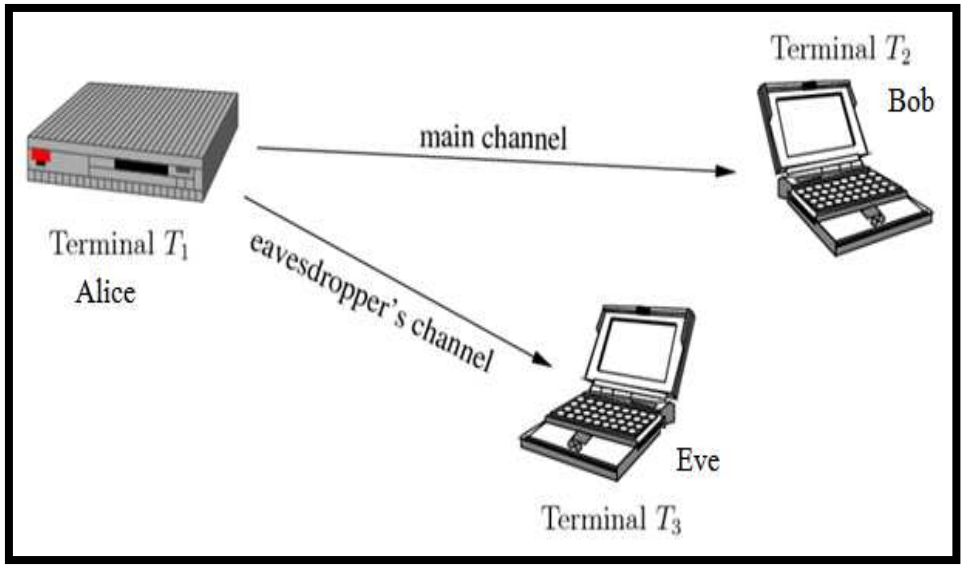
About protections of networks' radio interface

Basic definitions

LEGITIMATE link is Alice to Bob over the Main Channel

EAVESDROPPER link is Alice to Eve over the Eavesdropper Channel

Native study hypothesis is **complete information** of Eve about legitimate RAT



TRANSEC (Transmission Security) is the protection of the wave form of the legitimate link face to interception/direction finding of the transmitted radio signal, to jamming and intrusion attempts of the user receiver.

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 the user messages (voice, data). Most of solutions are based on ciphering + integrity control schemes

Supported by PHYLAWS project FP7 ICT Id 317562

Perspectives offered by physical layer security (PHYSEC)

General

PHYSEC (Physical Layer Security):

New concept for security of wireless networks

Exploits the properties of the local radio-environments, especially when dispersive and non-stationary

=> Will not replace existing solutions but may complement and simplify them

<u>Native physec is based on wiretap model + secrecy codes,</u>

Information-theoretic foundations

Avoids the use of ciphering keys, thus resilient to any attack

Information theoretic concepts and Wiretap model: see next pages

Secrecy codes are modified channel codes

- That approach Shannon capacity for legitimate link
- That mitigate information at “any” other location, under some hypotheses

⇒ **Today secrecy codes are known only for particular and un-realistic channels**

⇒ **Upper bound of performances of secrecy codes are known**

⇒ **Existing codes are known to tend toward capabilities of secrecy codes in more realistic channels (LDPC, polar, lattice), even imperfectly**

⇒ **Secrecy coding is still an active research domain**

Supported by PHYLAWS project FP7 ICT Id 317562

Perspectives offered by physical layer security (PHYSEC)

Practical

“Front end” solutions for upgrading privacy of wireless public networks

Operate mainly at the radio interface and demodulation/decoding stage
Software means only.
Low imbrication with upper layers and with network management

Mixing Physec solutions with more traditional security solutions

Compatibility with existing encryption solutions.
Compatibility with existing radio access technologies.
Negligible impact on spectrum efficiency.
Expected reduced impact on architectures of terminals and of networks.
Expected easy and low cost integration.

Address a wide class of wireless applications in the close future

Wireless radio-cells: GSM and UMTS evolutions, LTE and LTE–A.
Upgraded or new WLAN: WiFi, extension of 802.11a/b/g/n, 802.11i/w, 802.11ac, WiGi.
Broadband internet, machine to machine, internet of machines.
Cognitive networks: data base downloading, geo-referenced sensing and access.
Private transmission systems (PMR).
Short range rommunication devices: Bluetooth, Zigbee etc., even RFIDs

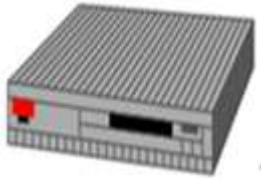
Supported by PHYLAWS project FP7 ICT Id 317562

About information theory
Simplified case of memoryless stationary discrete sources

S^K Memoryless Source Data
Blocks length K

Entropy:
(instantaneous)
$H_S = H(S^K)/K$

Transmitted Signal X^N
Blocks length N
Coding rate: K/N
Probability distribution P_X



ALICE

Propagation channel $P_{Y/X}$

Shannon capacity $C_{sh,AB}$

Corrupted Received Signal block Y^N
Probability distribution P_Y
Mutual information $I(X^N;Y^N)$

BOB

Decoded data $\hat{S}^K$

I/ Random signal X of discrete values $x_1 \ldots, x_M$

$\Rightarrow$ **probability distribution P_X ($P_X(X=x_m) \triangleq P_{Xm}$)**

=> Signal entropy (or P_X entropy): $H(X) \triangleq E_{PX}[-\log_2(P_{Xm,})] \triangleq -\sum_m P_{Xm}. \log_2(P_{Xm,})$

H(X) represents the degree of uncertainty of X.
$H(X) \leq \log_2(M)$ and H(X) is maximum when X is uniformly distributed.

=> Source entropy H_S is taken as the normalized entropy of a signal block S^K (length K): $H_S=H(S^K)/K$

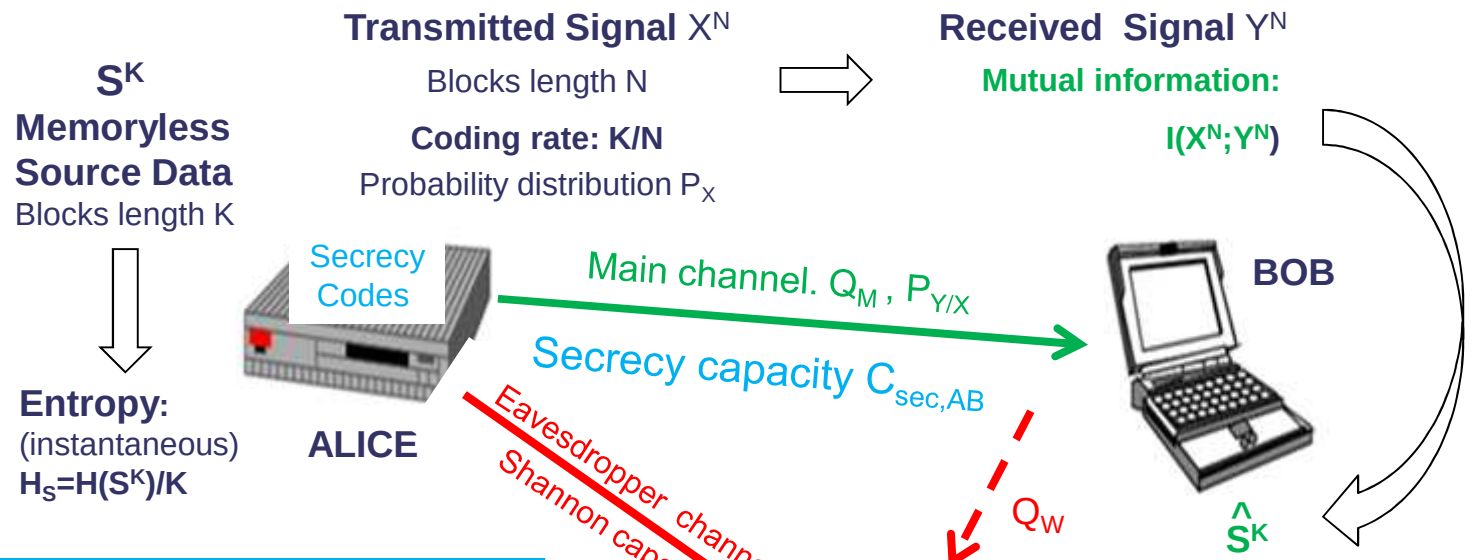
II/ Propagation channel from Alice (X discrete values $x_1 \ldots, x_M$) to Bob (Y signal values $y_1 \ldots, y_{M'}$)
=> defined by the conditional probability $P_{Y/X}$, (perfect ch. is $p_{Y/X} \equiv 1$; full noisy ch. is $p_{Y/X} \equiv p_y$)
=> conditional Shannon entropy: $H(X/Y)$ $(= E_{PX,Y}[-\log_2(P_{Xm/Ym'})] \triangleq -\sum_m P_{Xm,Ym'}.\log_2(P_{Xm/Ym'})$

III/ Information: $I(X ; Y) = H(X) - H(X/Y)$ Amount of knowledge about X after observing Y
Shannon capacity $C_{sh,AB} \triangleq \text{Sup}\{I(X ; Y) ; P_X\}$. Maximun value of information over channel

Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity

Simplified case of memoryless stationary discrete sources



Perfect secrecy: $\Delta=H_S$, $I(S^K;Z^N)\equiv 0$

Secrecy capacity $C_{sec,AB}$

=> Achieves Max $\{I(X^N;Y^N)$
. over X distribution P_X
. over constraint $\Delta = H_S$

=> (Non constructive) existence of secrecy codes is proven.

=> In practice: $C_{sec,AB}=C_{sh,AB} - C_{sh,AE}$

Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity

Existing results

Perfect secrecy condition (Shannon): $H(S^K|Z^N) = H(S^K)$ or $I(S^K;Z^N) = 0$

⇒ the Eve signal Z does not contain any information about the source data S.

⇒ impractical to achieve perfect secrecy, since it essentially requires one-time pad.

Weak secrecy coding: $\lim I(S^K;Z^N)/K = 0$ as $K \rightarrow \infty$.

⇒ the average information leakage per symbol tends to zero.

⇒ Not enough: the absolute information leakage $I(S^K;Z^N)$ can still tend to infinity, for example, on the order of $K^{1/2}$.

Strong secrecy coding: $\lim I(S^K;Z^N) = 0$ as $K \rightarrow \infty$.

⇒ means that the information leakage may be arbitrairy small as $K \rightarrow \infty$.

⇒ closely related to the standard notion of semantic security

⇒ Well accepted in the security community

Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity

Existing results

Secrecy capacity $C_{sec,AB}$ is the maximum rate of the legitimated link Alice-Bob **under the constraint that secrecy is achieved with respect to Eve.**

$C_{sec,AB}$ is defined under the condition $C_{sh,AE} \leq C_{sh,AB}$ and verifies:

$$C_{sh,AB} - C_{sh,AE} \leq C_{sec,AB} \leq C_{sh,AB}$$

Condition $C_{sh,AE} \leq C_{sh,AB}$ can be assumed with intentional jamming:
Example is artificial noise send by Bob in conjunction of MISO or MIMO RATs

$C_{sec,AB}$ is equal for weak or strong secrecy

$C_{sec,AB}$ is an achieved maximum, thus secrecy codes exist
even if they are complex
even if they are unknown in most of realistic cases

In most of practical cases (i.e. where the channel satisfies certain symmetry) :

$$C_{sec,AB} = C_{sh,AB} - C_{sh,AE}$$

Practical challenges of today:

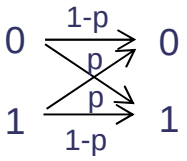
- find channel codes that approach $C_{sec,AB}$ with reasonable complexity
- Mixt secrecy codes with existing security solutions of wireless networks

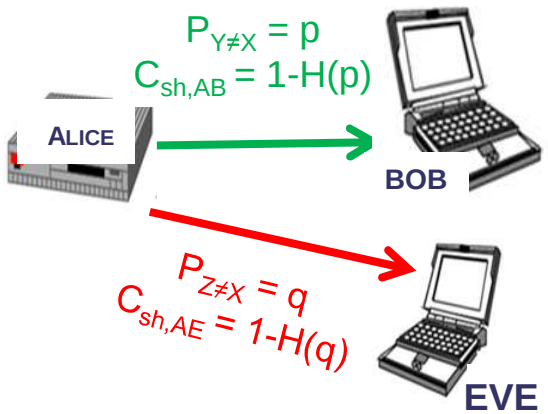
Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity
Existing results

Secrecy capacity $C_{sec,AB}$ for binary symmetric channels (b.s.c)

$P(Y \neq X)=p$ and $P(Y=X)=1-p$.
$P(Z \neq X)=q$ and $P(Z=X)=1-q$.
$H(p)= - p.\log_2 p - (1-p).\log_2(1-p)$
Shannon capacities: $C_{Sh,AB} = 1-H(p)$
: $C_{Sh,AE} = 1-H(q)$

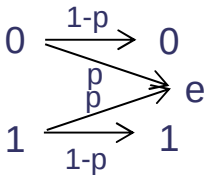


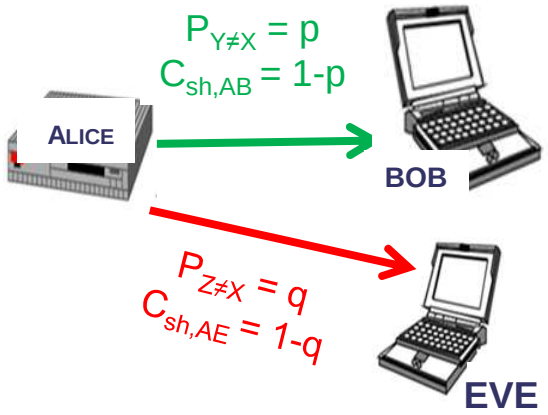


=> When $p < q \leq 1/2$
$C_{sec,AB} = H(q) - H(p)$

Secrecy capacity $C_{sec,AB}$ for binary erasure channels (b.e.r)

$P(Y=X)=1-p$ and $P(X \text{ is erased})=p$.
$P(Z=X)=1-q$ and $P(X \text{ is erased})=q$.
Shannon capacities: $C_{Sh,AB} = 1- p$
: $C_{Sh,AE} = 1-q$





=> When $p < q$
$C_{sec,AB} = q - p$

Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity
Existing results

Secrecy capacity $C_{sec,AB}$ for gaussian SISO channels

$Y(k) = \alpha.X(k)+n(k)$, $E[X(k)]=0=E[Y(k)]$

α : One tap propagation attenuation (constant)

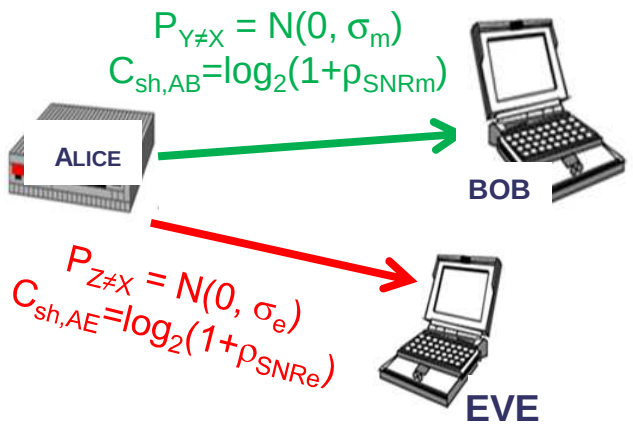
$\pi_x = E[|x(k)|^2]$: X power

$P(Y=y/X=x)=P(n=y-x)=\exp[-(y-x)^2/2/\sigma_m^2]$

Signal to noise ratio: $\rho_{SNRm,e} = |\alpha_{m,e}|^2.\pi_x/\sigma_{m,e}^2$

Per Hz Shannon cap.: $C_{sh,AB} = \log_2(1+ \rho_{SNRm})$

$C_{sh,AE} = \log_2(1+ \rho_{SNRe})$



=> When $\sigma_m < \sigma_e$

$C_{sec,AB} = \log_2(1+ \rho_{SNRm}) - \log_2(1+ \rho_{SNRe})$

=> Intentional Alice jamming helps to achieve secrecy (SISO+, MISO, MIMO)

decrease SNR at Eve's part (nemes "cooperative jamming" in many publications).

Alice's Transmitted signal is $X'(k)=X(k)+X_n(k)$

Bob's Received signal is $Y'(k)=\alpha_m.(X(k)+X_n(k))+n(k)$, X_n been mitigated

=> SNR_m is kept: $\rho_{SNRm} = |\alpha_m|^2.\pi_x/\sigma_m^2$

Eve's Received signal is $Z'(k)=\alpha.(X(k)+X_n(k))+n(k)$,

=> SNR_e is decreased : $\rho_{SNRe} = |\alpha_e|^2.\pi_x/(\sigma_e^2+|\alpha_e|^2\pi_{xn})$

Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity
Existing results

Secrecy capacity $C_{sec,AB}$ for Fading SISO channels

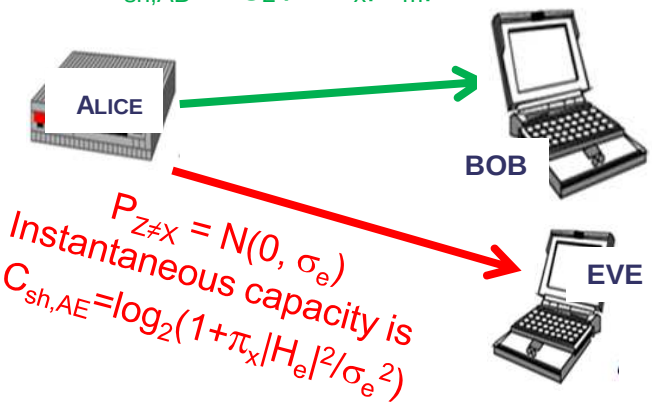
$Y(k) = H(k).X(k)+n(k)$, $E[X(k)]=0=E[Y(k)]$
H(k): Propagation attenuation (ex: Rayleigh law)
$\pi_x = E[|X(k)|^2]$: X power
$P(Y=y/X=x)=P(n=y-x)=\exp[-(y-x)^2/2/\sigma^2]$

Instantaneous Signal to noise ratio :

$$\rho_{SNRm,e} = |H_{m,e}(k)|^2.\pi_x/\sigma_{m,e}^2$$

Per Hz instant. capacity $C_{sh,\,m,e} = \log_2(1+\rho_{SNRm,e})$

$P_{Y\neq X} = N(0, \sigma_m)$
Instantaneous capacity is
$C_{sh,AB}=\log_2(1+\pi_x|H_m|^2/\sigma_m^2)$



$P_{Z\neq X} = N(0, \sigma_e)$
Instantaneous capacity is
$C_{sh,AE}=\log_2(1+\pi_x|H_e|^2/\sigma_e^2)$

=> Alice strategy is supposed
- **to know** $H_m(k)$, σ_m and $H_e(k)$, σ_e
- **to adapt its Tx power** $\pi_x(H_m,H_e)$ over power constraint $\pi_x(H_m,H_e) \leq \Pi$

=> Leads to secrecy capacity :

$$C_{\text{sec},AB} = \max_{\pi_x(H_m,H_e)\leq\Pi} \left\{ \log_2\left(1+\frac{\pi_x(H_m,H_e)|H_m|^2}{\sigma_m^2}\right) - \log_2\left(1+\frac{\pi_x(H_m,H_e)|H_e|^2}{\sigma_e^2}\right) \right\}$$

Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity
Existing results

Secrecy capacity $C_{sec,AB}$ for MIMO channels

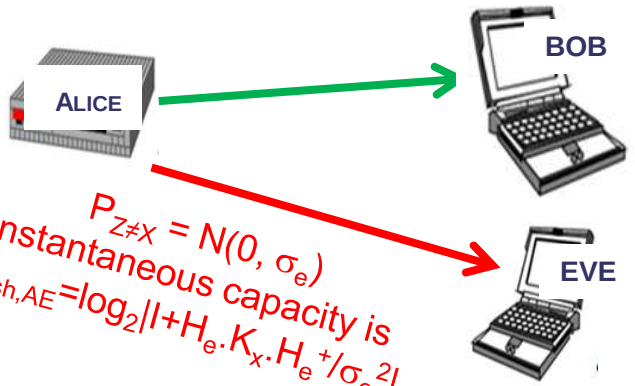
$Y(k) = H(k).X(k)+N(k)$, $E[X(k)]=0=E[Y(k)]$
H(k): MIMO Propagation matrix
X(k) covariance is $K_x = E[X(k).X(k)^+]$
N(k) covariance is $R_N = E[N(k).N(k)^+] = \sigma^2.\mathbf{I}$

Instantaneous covariance matrix ratio:

$$P_{SNRm,e} = H_{m,e}(k).K_x.H_{m,e}(k)^+/\sigma_{m,e}^2$$

Per Hz Instant. capacity: $C_{sh,m,e} = \log_2 |\mathbf{I} + P_{SNRm,e}|$

$P_{Y\neq X} = N(0, \sigma_m)$
Instantaneous capacity is
$C_{sh,AB}=\log_2|I+H_m.K_x.H_m^+/\sigma_m^2|$



=> Alice strategy is supposed
- **to know** $H_m(k)$, σ_m and $H_e(k)$, σ_e
- **to adapt its power and coding strategy $\mathbf{K_x}$** over power constraint $tr(K_x) \leq \Pi$

=> Leads to secrecy capacity :

$$C_{\text{sec},AB} = \max_{tr(K_x)\leq\Pi} \left\{ \log_2 \left| \mathbf{I} + \frac{1}{\sigma_m^2} \mathbf{H}_m \mathbf{K}_X \mathbf{H}_m^+ \right| - \log_2 \left| \mathbf{I} + \frac{1}{\sigma_e^2} \mathbf{H}_e \mathbf{K}_X \mathbf{H}_e^+ \right| \right\}$$

Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity

Existing results

About existing channels codes that could be candidate for achieving Secrecy

Low Density Parity-Check Codes (LDPC):

- well known and good for main channel capacity (close to theory)
- long periods restrict the potential use for TDMA RATs or short messages
- used to build secrecy codes with limited success
- were proven to achieve secrecy capacity for noisyless main channel and for Binary Erasure Eve Channel

Polar Codes (PC)

- offer a powerful approach to design wiretap codes
- can achieve strong secrecy when facing discrete noisyless channel (with minor modifications of the original design)
- however, bad suited to continuous noisy main channels: poor reliability of the legitimate link in this case.

Lattice Codes (PC)

- prominent approach to implement information-theoretic security when facing Gaussian continuous channels, first for weak secrecy, then for strong secrecy
- relevant notion of secrecy gain
- still complex nowadays for practical implantations
- extension to realistic channel are in progress (SISO with fading, MIMO), even if explicit design is still lacking

Supported by PHYLAWS project FP7 ICT Id 317562

General overview of wiretap model and of secrecy capacity
General perspectives

Theoretic advantages of secrecy coding

- secrecy coding simultaneously provides capacity and security without computational hardness assumptions (which are often unproven in practice)
- Secrecy comes from the Shannon capacity difference of the channels => resilient to quantum computation attacks

Current limitations

- still a long way to go in the direction of Secrecy Capavity.
- The state of the art suffers a number of significant shortcomings:
  - LDPC and polar codes are limited to some special channel models,
  - explicit design of wiretap lattice codes is missing

Expectations

- Short term: improve existing wireless security with SC–derived concepts
- Mid/long term: offer Secrecy Codes for real radio environments with suitable implantation compromises.

Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections
Perspectives for Transec upgrades

Conventional transec solutions: LPI signals

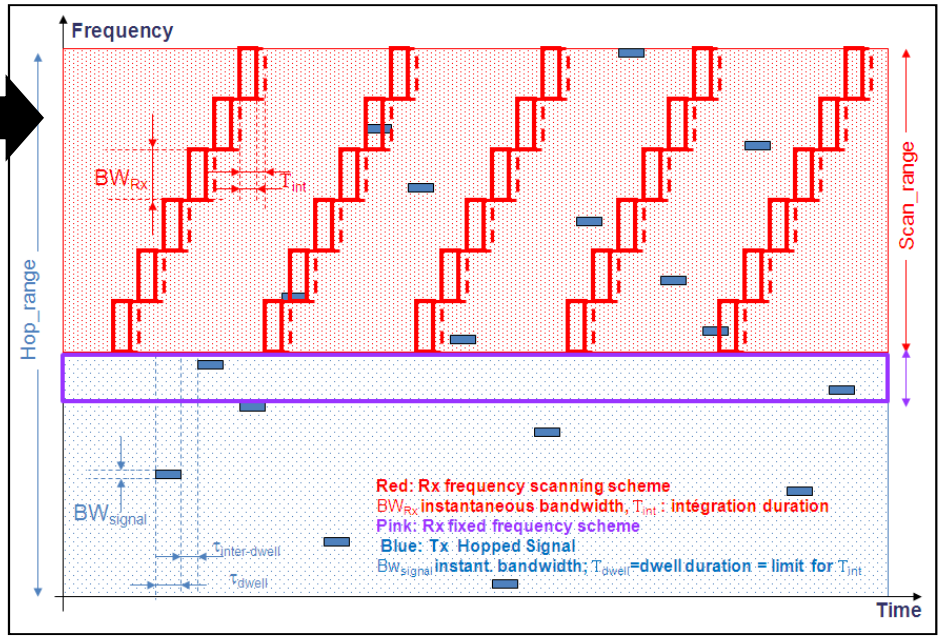
Signals of Low Interception Probability (LPI) avoid most of classical interception mechanisms (such as frequency scanning of low bandwidth interceptors)

Usual solutions are frequency hopping over wide frequency range, and time Hopping that is good too for LPI

- when low duty cycle signal

and/or

- when dense environment



Current drawbacks in public wireless

- Limited number of carriers for cell frequency planning
- A priori knowledge or clear text broadcast of cell frequency List
- Many of the FHS parameters remain stationary in practice
- TDMA middamble (of public wireless standards) have low combinatory and no time jitter => easy to recognize and synchronize

Supported by PHYLAWS project FP7 ICT Id 317562

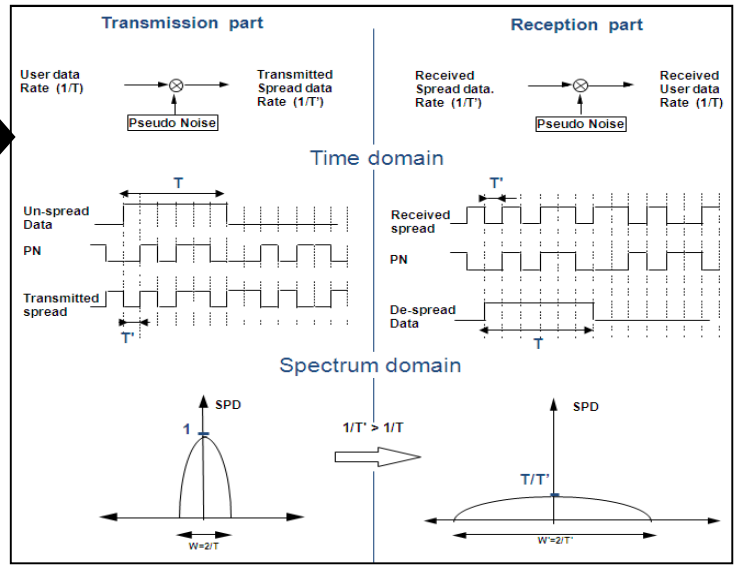
Merging secrecy concepts and existing protections
Perspectives for Transec upgrades

Conventional transec solutions: LPD signals

Signals of Low Detection Probability (LPD) avoid most of classical detection mechanisms (such as radiometer and matched filter)

Usual solutions are Direct Spread Spectrum over wide band carriers range, and management of low DSPs

- Generally poor efficiency for BS->MS link
- Can be efficient in UL sense (power control, codes combinatory)



Current drawbacks in public wireless

- Limited carrier bandwidth => reduced spreading factors
- Limited number of codes at early stage of the radio access protocol
- "Clear text" transmission of scrambling/spreading codes at early access stages
- Low combinatory pilot symbols inside channels for control of QoS

=> help Eve to recover DSS codes

Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections
Perspectives for Transec upgrades

Physec oriented solutions for improving transec

- **Make resource allocation and modulation coding schema more adaptive to radio propagation:**

  - TDMA: regular re-allocation of Frequency/Time hopping parameters based on Channel State Inform. (measured at signaling and access channel and/or coupled with handoff procedures)

  - CDMA: regular re-allocation of spreading codes depending on CSI measurements performed at previous allocated codes
    Coupling with power control and Rake processing
    Coupling with soft handoff procedures

  - OFDM: regular re-allocation of modulation/coding/multiplexing scheme depending on CSI measurements
    Easy with MFN planning => seems OK
    Case of SFN planning => require specific studies

Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections
Perspectives for Transec upgrades

Physec oriented solutions for improving transec (follow-on)

- **Combine artificial jamming and signaling**

  - Use tag signal of low DSP under signaling channel
    => see next pages.

- **Exploit signal mixtures within dedicated RATs**

  - Extend MISO and MIMO RATs to advanced transec
  - Exploit Full Duplex RATs (cf. FP7/ICT project Duplo in progress)

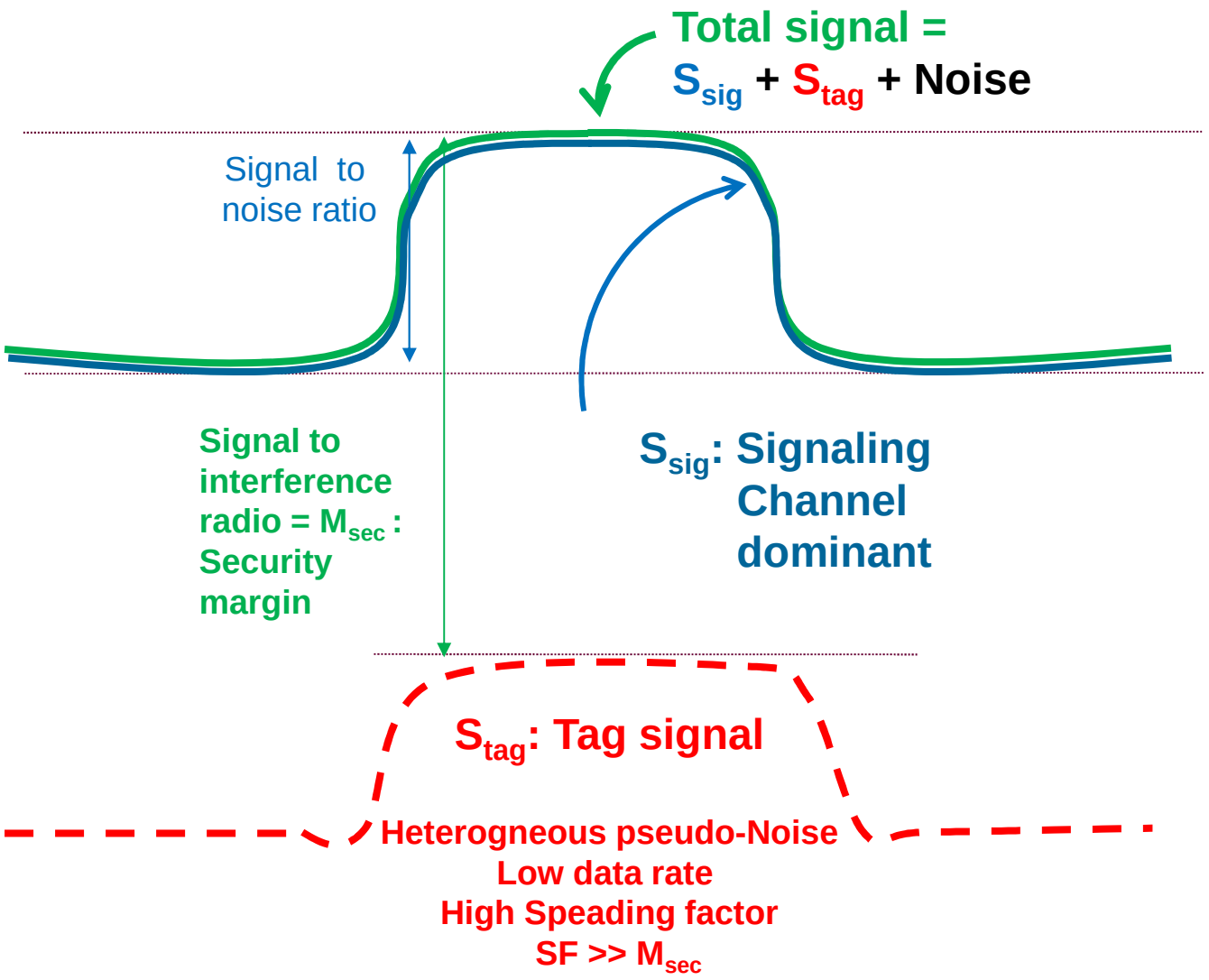
- **Exploit sensing procedures/outputs for a better transec of SDR and C.R.**

  - recurrent re-allocation of spectrum resources and modification of modulation/coding schemes
  - make re-allocation dependent of sensing at current carriers + other carriers

Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections

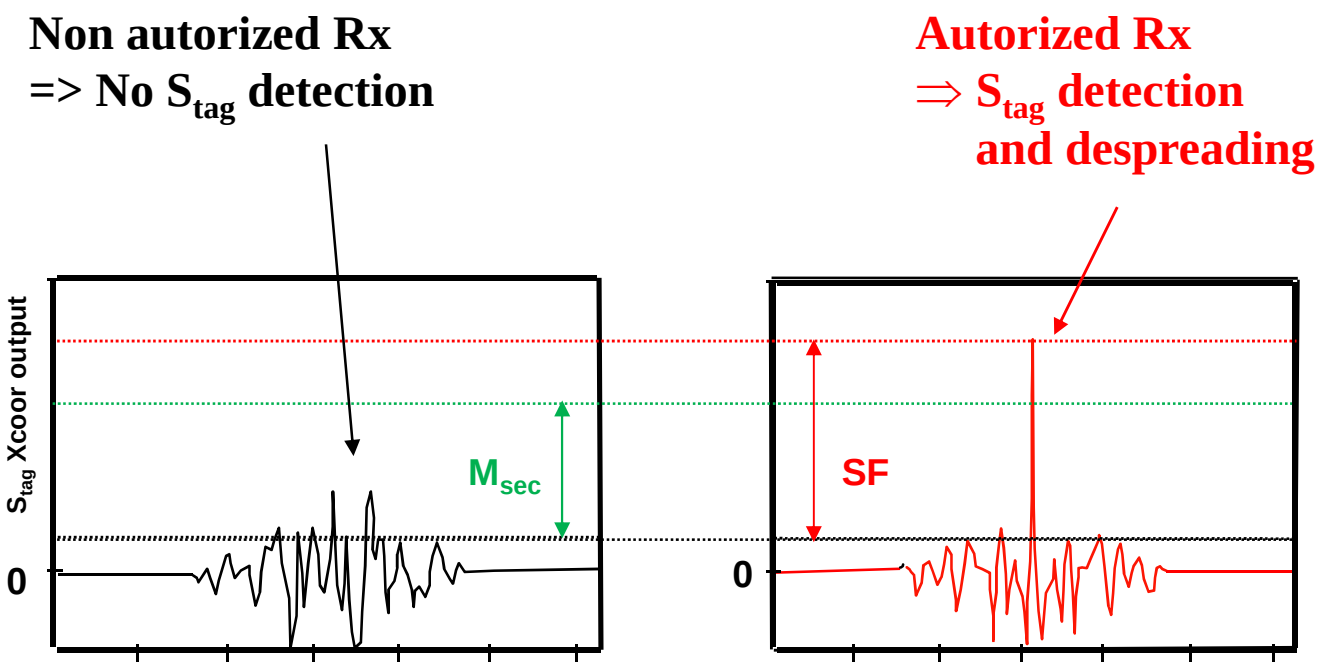
Simplified illustration of tag signals



Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections

Simplified illustration of tag signals



Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections
Perspectives for Netsec upgrades

Conventional netsec solutions:

=> Initial access being usually the security-weakest phases of RAT

LPI, LPD and Ciphering of signaling, access and paging channels

. Basis of military communications

Current drawbacks for public wireless

. Need a previous shared secret (Keys)

. Need a common system time (usually secret)

=> Not really achievable for world-wide mass market standards

IFF systems (Identification Friend and Foe)

. Civilian and military standards

Current drawbacks for public wireless

. Dedicated frequency plans: usual is 1030 MHz (interrogation) 1090 MHz (response)

. Low duty cycle signals (=> latencies within dense networks / numerous subscribers)

Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections
Perspectives for Netsec upgrades

Physec oriented solutions for improving netsec

=> More secrete early Tx/Rx procedures using tag signals

Preliminary identification modes based on dual sense tag signals

The idea is close to intentional cooperative jamming of tag signals
Same carrier than (strong) signaling signals for DL and UL tag signals (TDD)
DSS low data rate, low DSP (SF is designed to overhead the native C/I)

Introduce secrecy codes within tag signals

"Noisy" signaling channels play the role of cooperative intentional jammer
Channel State Information is based on DSS codes of tag signals and Rake Rx

Commute then signaling, downloading and uploading into "intelligible mode"

Non-random broadcast is achieved only after preliminary Identification
Simplified cipher procedure or use of secrecy code is another opportunity.

Transmit most sensitive data through protected tag messages (Low rate**)**

Subscriber IDs, random parameters for Key computations, etc.
Assignment of radio resource for further channels

Continue association of main + tag signals up to resource allocation for traffic and complete protection establishment (Secrecy codes and Cipher at Traffic)

Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections

Perspectives - Comsec upgrades

Conventional comsec solution:

(Alice) and the receiver (Bob) share a common symmetric key, and use it in symmetric mechanisms for authentication, integrity and ciphering

Authenticated Encryption schemes such as Galois Counter Mode are usual:

to encrypt the plaintext

to compute an additional Message Authentication Code (MAC).

Xoring plaintext with pseudo random cryptographic sequence is ideal for resistance to error on the line as it is the case with counter mode.

But need a refreshed unique IV (or nonce) per protected frame.

IV are random or based on frames counter, or system time, signaling information, addresses, *physical information sh*ared by Alice an Bob.

Supported by PHYLAWS project FP7 ICT Id 317562

Merging secrecy concepts and existing protections

Perspectives - Comsec upgrades

Possible enhancement :

Main purposes are

- to limit the bandwidth dedicated to security (transmission of (IV, MAC))

Typical length for MAC is 64 to 128 bits and 32 to 128 bits for IV, not negligible for short frame

- to limit the impact of an IV misuse on security.

In case the same IV is used, security is dramatically damaged with counter mode.

Means are:

- The message content itself can be an input to build the IV

- MAC = IV = Synthetic IV

- Replace the couple (MAC, IV) by a unique Synthetic Initial Vector (SIV)

- Compute SIV = MAC by using both message content + shared context.

As frame of radio communication are short, no real problem with latency (when computing the SIV with the plaintext itself)

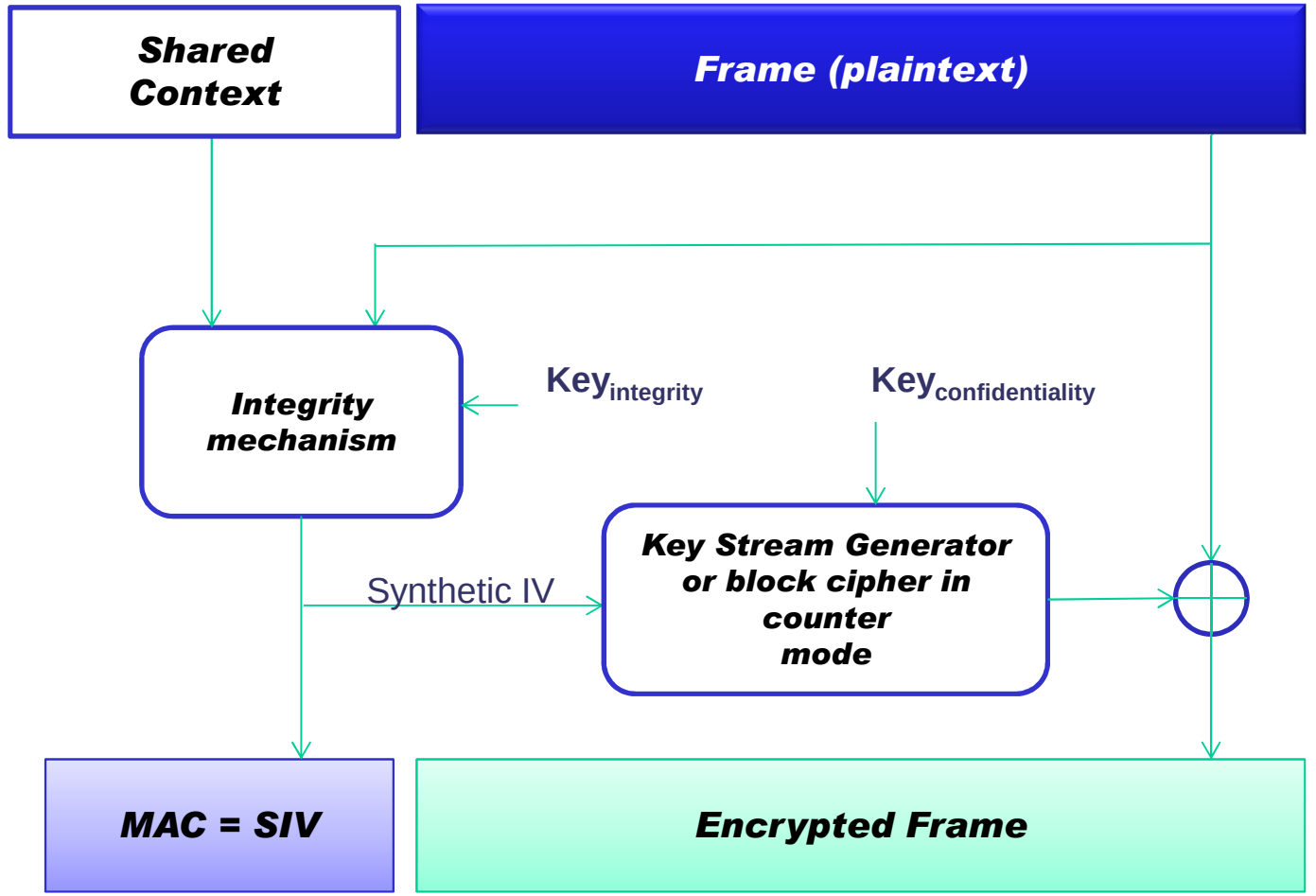
Resilience has been proven much better (see standard mode SIV).

Merging secrecy concepts and existing protections

dedicated SIV mode to provide confidentiality and integrity

Here physical information of legitimate should be taken into account in order to build the shared context of each frame:

Sensing outputs,
Channel State Information
Equalizer taps
Rake fingers,
QoS measurement
Secrecy codes
…



Supported by PHYLAWS project FP7 ICT Id 317562

Conclusion

Physec offer practical perspectives for improving wireless security

- ***Associating SC and (intentional) jamming and or intentional signal mixtures provide significant perspectives for transec,***
- ***Specially interesting are dedicated MIMO and Full Duplex RATs.***
- ***Significant improving of transec seems achievable with "physical random" adaptive resource allocation of Cognitive radios, the "physical random" being got from sensing outputs.***
- ***Significant improving of transec seems achievable with low DSP tag signals under main signals.***
- ***Improving of netsec of signaling and early negotiation messages seems achievable by associating of SC and dual sense tag signal under signaling channel***
  - Early identification before making signaling intelligible
  - Re-enforced authentication
  - Better integrity control of signaling paging access and negotiation messages
- ***Enhanced comsec schemes using shared context should involve added radio dependent random sources and sec. codes***

Supported by PHYLAWS project FP7 ICT Id 317562