PHYSEC CONCEPTS FOR WIRELESS PUBLIC NETWORKS – INTRODUCTION, STATE OF THE ART AND PERSPECTIVES

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)

ABSTRACT

This paper aims at providing elements about advances in physical security (physec) and about relevant application perspectives in public wireless networks. After a short introduction of existing protection of communications signals, we will introduce several notions relevant to information theory and point out the main physec concepts. Then, we discuss their theoretic advantages and the current knowledge about secrecy codes. Finally, the paper will highlight practical implantation perspectives of physec in existing and future public radio-networks, as stand-alone added modules operating at the physical player, or as addedalgorithm combined with classical solutions in order to upgrade and/or to simplify existing security procedures. This work is supported by the PHYLAWS project (EU FP7-ICT 317562, www.phylaws-ict.org), starting Nov. 2012.

1. INTRODUCTION

Given the growing prevalence of wireless radio-communication technologies, security, privacy and reliability of the exchanged information becomes a major societal challenge for both personal and professional sphere. Moreover, the growing importance of sensing and cognitive procedures in future radio access technologies (white spectrum, cognitive networks) will occur numerous downloading and uploading procedures for geo-referenced sensing spectrum allocations, whose integrity and privacy are major industrial challenges for both operators and administrations. Secure air interface within wireless networks are thus crucial for various applications such as broadband internet, e-commerce, radio-terminal payments, bank services, machine to machine, health/hospital distant services. Most of citizens, professionals, stakeholders, services providers and economical actors are thus concerned by confidentiality lacks and by privacy improvements of the physical layer of wireless networks.

1.1. Existing protections within wireless networks

Several classical solutions already exist in order to protect privacy of radio transmissions.

. Wave forms can be designed in order to achieve Low Probability of Interception (LPI) and Low Probability of Detection (LPD), by using furtive frequency/time hopped or spread spectrum signals. LPD and LPI signal achieve transmission security (transec) at frame and at symbol level.

. At the signaling level, protocols can be designed in order to achieve low probability of decoding and low intrusion capabilities of the signaling messages by non-legitimate users, thanks to subscribers' and nodes' authentication procedures, thanks to advanced scrambling, interleaving, coding and ciphering techniques, etc. Such protections achieve network signaling security (netsec). They apply either at signal frame, at symbol level and at bit level. In addition, netsec may be re-enforced with early identification as Identification of Friend and Foe procedures.

. At the communication level, encryption algorithm and message integrity control schemes are used in order to avoid non legitimate interpretation and/or intrusion attempts of the users' messages. Such protections achieve communications security (comsec) by applying mainly at message/bit level.

1.2. Limits and drawbacks of existing protections

Nevertheless, all the classical protections above require a priori knowledge or exchanges of keys, thus improving the complexity of the network management and/or reducing the set of users of highest protected modes. In addition, these protections often require shared time references; thus induce added vulnerabilities or failure risks (ex: time reference is public itself - GPS for instance).

Moreover, all existing protections use added data, and thus decrease the spectrum efficiency, especially when facing short packet services. Finally, all their constraints trend to dramatically reduce the effective privacy of any wireless standards that targets a worldwide mass market.

1.3. New perspectives offered by physec.

Physical Layer Security (physec) is a radically novel concept that exploits the properties of the local radio-environments, especially when complex, dispersive and non-stationary.

. Since its introduction by Wyner [18], the fundamental model of wiretap channel (figure 1) has led to the definition of secrecy capacity for several propagation models (see [18-26] and to the design and/or to the re-use of advanced coding schemes in order to approach it (LDPC, lattice and polar, codes).

. A native and tremendous advantage of physec is the absence of keys: Security over radio-channel is achieved through channel coding in the same processing as signal transmission, thanks to "secrecy codes" that optimize information recovery by legitimate receiver and that mitigate information leakage about the legitimate link at any eavesdropper location. No external information is required nor exchanged.

. Because of its information-theoretic foundation, physec is intrinsically robust to any computer attack (unlimited computing power), even to quantum attack.

1.4. Practical expectations of physec for wireless networks

Physec appears as a potential "front end" solution for warranting privacy and security within wireless public networks. Physec mainly operates at the radio interface an uses software means only: Low imbrication should occur with upper layers of the transmission protocol and with network management.

Thus, many practical advantages may be expected from physec-native or physec-derivate security solutions:

- Reduced impact on terminal and on network architectures.
- Easy and low cost integration.
- Compatibility with existing encryption solutions.
- Compatibility with existing radio access technologies.
- Negligible impact on spectrum efficiency.

Therefore, physec solutions or security modules including physec concepts should address a wide class of wireless applications in the close future:

- Within wireless radio-cells: GSM and UMTS evolution, LTE and LTE–A.
- Within upgraded or new Local Loop standards: WiFi, extension of 802.11a/b/g/n, 802.11i/w, 802.11ac, WiGi.
- Within broadcast and point to point services supporting mobile broad band internet, machine to machine and internet of machines.
- Within cognitive networks: data base downloading, geo-referenced sensing and geo-referenced access procedures.
- Within private transmission systems (PMR).
- Within short range communications devices: Bluetooth Zigbee etc., even RFIDs

1.5. Structure of the paper

The following will first introduce several notions relevant to information theory and the main principle that are relevant to Physical Layer Security. Then, from a state of the current researches, we will highlight several security solutions that should take benefit of native physec concepts when facing passive eavesdroppers, such as adaptive modulation and coding schemes, cooperative jamming and space time diversity exploitation within MIMO RATs. We will then introduce physec perspectives to counter active threats such as radio-hacker intrusion attempts of signaling messages.

Possible drawbacks of physec will be discussed too, that may be relevant

- to secrecy codes determination,
- to implementation of coding and decoding schemes into standard wave forms, handsets and base stations,
- to embedded computing complexity (versus the expected performances of embedded computers),

The paper will conclude on practical implantation perspectives of physec in existing and future radio-networks, as stand-alone added modules operating at the physical player, or as added algorithm combined with classical solutions in order to upgrade and/or to simplify existing transec, netsec and comsec protections.

2. EXISTING PROTECTIONS OF RADIO SIGNALS

2.1. Native causes of security lacks in public wireless

Intrinsic causes deteriorate privacy of the radio-interface of public networks that are roughly summarized hereafter:

- The worldwide mass market nature of modern digital standards induces a native weakness of the broadcast signaling channel and of the early steps of radio access (that should be understood everywhere by any terminal)
- Roaming and handoff procedures of mobile handsets cause regular signaling exchanges of subscriber and/or terminal IDs for updating their registration and location. The relevant protections are often not sufficient.
- Cipher procedures within digital standards often remain limited. In addition, they may suffer of unexpected publication ([16]). In practice, confidentiality of algorithm used for authentication, key computation, ciphering within public standards cannot be warranted over years.
- Multiple standard handset and ascending compatibility of radio communication protocols are others weaknesses. In many cases, active attacks re-enforced by selective jamming can force terminals to the use of the weakest RATs.
- Other weaknesses come from sub-optimal operators practices, from subscribers' misunderstood (bad parameterization of secret key, no regular change of passwords, etc.), from legal restrictions, etc.

In the following, Alice and Bod form legitimate transmitter and receiver link and Eve is the Eavesdropper or the Radio Hacking System (RHS). Several principles of passive and active attacks are described into [31] and into the associated references. Figure 1 briefly introduces the model of the threat and the main relevant information-theoretic notions developed § 3.

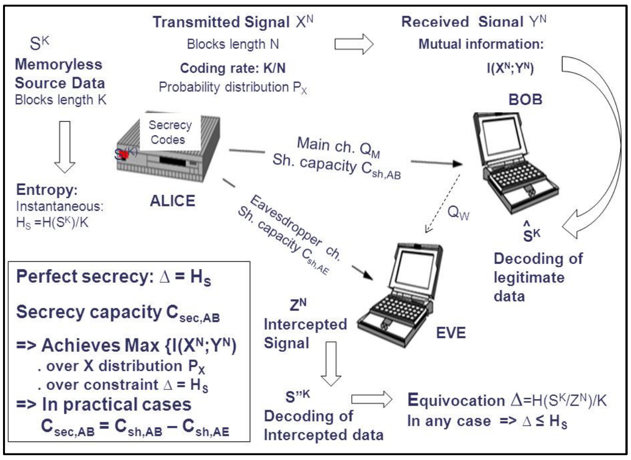

Figure 1: Model of wiretap channel - relevant information-theoretic notions (memoryless stationary source).

2.2 Transec with furtive LPI and LPD signals.

2.1.1 Principle of LPD LPI signals

"Interception" is the management (by Eve) of the concomitance of its own instantaneous carrier and bandwidth, with Alice's signal carrier and bandwidth.

. For fixed frequency signals, interception is achieved when Eve instantaneous bandwidth "meets" the signal carrier.

. For slotted signals and for hopped signals, interception is achieved when Eve's bandwidth "meets" at least one signal slot/burst during the acquisition duration.

«Detection» is a probabilistic estimation of the presence of an intercept signal, followed with a decision mechanism that maximizes the likelihood over two hypotheses H0: "signal non present" and H1: "signal present".

The main processing for detection use

- radiometer filters based on a signal power criteria, when no a priori information is available to signals
- Matched filter (inter-correlation processing) when a priori information is available to signals: this is usually the most efficient case when facing wireless standards (exceptions occur nevertheless for CDMA UL senses)

Basis of signal processing for spectrum monitoring on communication signals (including standards) can be found in [7-9]. Deeper considerations can be found in [10-11].

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

Frequency Hopped (FH) signal over wide frequency intervals and long periods are usual in military networks because they have good LPI characteristics - see fig 2. They are often merged with TDMA RATs (many VHF and UHF tactical radios) and with CDMA RATs (MIDS)

Signals used for opportunistic RATs within Cognitive radios (CR) or digital dividend of white space (DDWS) may have good LPI properties too thanks to their versatile spectrum access protocol (interaction with sensing capabilities and local spectrum usage) and their adaptive modulation.

Signals of Low Detection Probability (LPD) avoid most of classical detection mechanisms (such as radiometer and matched filter). DSSS signals [12] have good LPD properties when transmitted Spectrum Density Powers (SDP) remains low (thus countering radiometer), and when spreading and scrambling codes remain unknown (thus countering matched filters). Frequency hopped and Time hopped signal may have LPD properties when power remains weak (Short Range System, Ultra Wide Band RATs) and when carrier/slot allocation is random over wide periods. More generally, any highly non-stationary RAT (CR, DDWS) induce native LPD capabilities because it reduce integration duration, processing gain and association capabilities within adverse receivers.

2.2.2 Frequency Hopped (FH) signal in public wireless

GSM [3], Bluetooth and some other TDMA wireless use FH signals over a few carriers for their traffic channels. Similar procedures exist for Time Hopped Signals

The main motivation for FH in such networks is usually the use of frequency diversity (that averages effects of fading) and the flexibility of spectrum allocation within dense (urban) environments. Nevertheless, when taking place in high density network, when dealing with numerous carriers, when using unknown Frequency Hopped Sequences (FSH), TDMA/FH RATs may provide some LPI and LPD capabilities face to low bandwidth passive threats (fig 2).

Unfortunately, in many practical cases, cell frequency plans have a limited number of carriers and many of the FHS parameters remain stationary (even when ciphered - such as in GSM [3]).

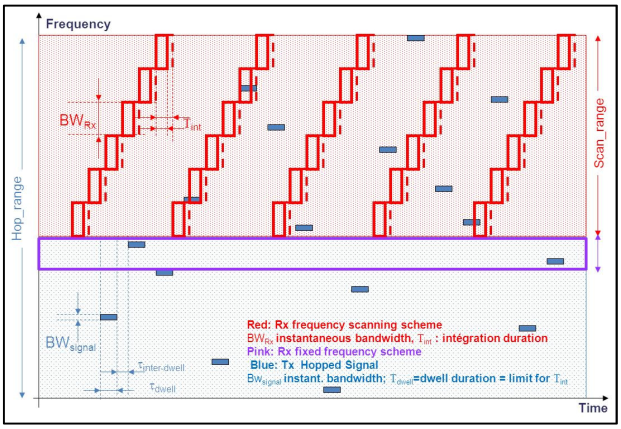
Frequency
Hop_range
Scan_range
BW_{Rx}
T_{int}
BW_{signal}
$\tau_{inter\text{-}dwell}$
τ_{dwell}
Red: Rx frequency scanning scheme
BW_{Rx} instantaneous bandwidth, T_{int} : intégration duration
Pink: Rx fixed frequency scheme
Blue: Tx Hopped Signal
Bw_{signal} instant. bandwidth; T_{dwell}=dwell duration = limit for T_{int}
Time

Figure 2: Low bandwidth receiver: fixed frequency or frequency scanning facing LPI frequency hopped signals

2.2.3. DSSS signals in public wireless

3GPP/UMTS, 3GPP2/CDMA2000 and several other systems such as GPS and Globalstar satellite constellations use DSSS signals (fig 3) and CDMA codes for achieving the best use of time and space diversity (Rake processing, Soft handoff) and the best flexibility of random radio access (numerous codes with flexible spreading factors).

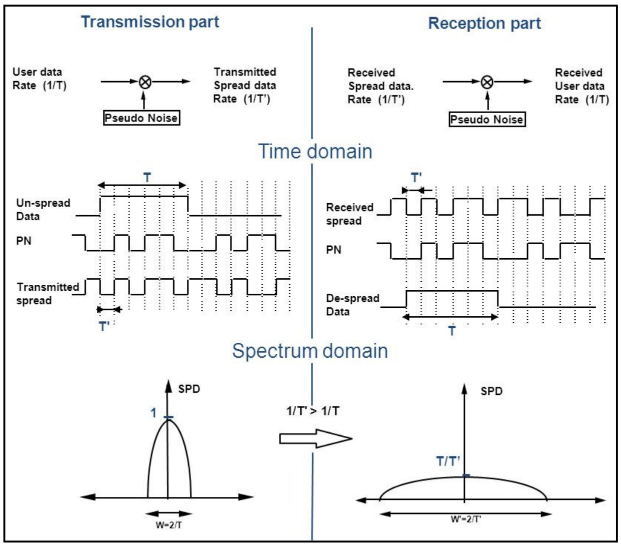

Figure 3: Principle of DSSS signals

Thanks to the fast control power, to the high combinatory of long scrambling codes, to accurate time resolution DSSS/CDMA could provide high LPI and LPD capabilities especially for uplink (weaker SPD), when facing passive and active threats. Unfortunately, in many practical cases, additional determinism is introduced into the wave form in order to facilitate the synchronization and the quality control of legitimate link, which largely deteriorates the transec:

3GPP/UMTS examples [1]: low combinatory synchronization codes (P/S-SCH) are included in the DL Frames. The combinatory of Pilot codes is then largely reduced (from 8192 to 8 hypothesis), which allows an easy and accurate recovering of Frame synchronization and DL codes (common control, paging and of traffic channels) over large distances ([27]),

Pilots symbols are included in UL traffic control channel. Their low combinatory allows an efficient external recovery of the UL slot and frame synchronization and then of the UL scrambling code for further dispreading ([28]).

3GPP2/CDMA2000 examples [2]: such networks are clocked by GPS system time, that facilitate frame cock recovery at first, and then long range detection and de-spreading of DL signaling paging and traffic channels. Then for public services, symbol scrambling and punctuation of power control bits are achieved with a sequence that is very similar to the UL spreading sequence (depending on a Long code Mask (LCM) linked to the Electronic Serial Number of the terminal). In the UL sense, the same LCM manages the long spreading code and the 64-Hadamard modulation scheme induces significant redundancy over time that facilitates the recovery of the LCM. Finally combining both DL UL analyses may provide all spreading and scrambling parameters to Eve [2][28][29].

2.3 Netsec aspects : signaling and access negotiation protocol, authentication and identification

2.3.1 Current netsec within public wireless

First of all, broadcast signaling and early access signals are usually transmitted with significant power and without transec because no power control is active at the early steps of the Radio access protocol and no transec secret could been exchanged. This facilitates long range detection and decoding of both signaling and access messages.

Moreover existing netsec protections of current wireless public network are usually very poor, providing thus much information about network engineering to any man in the middle (mitm) attacker or to external watchers of the network:

- Nowadays, no real protection of broadcast signaling applies in wireless public network neither to on-going access attempts. Thus, after decoding, their content is intelligible
- Subscriber initial registration often requires the complete IDs of terminals and/or subscribers.
- Authentication during access attempts is usually based on random parameter exchanges and on secret algorithms that are shared by terminals and by network nodes, but the integrity control of the relevant messages is often poor or inexistent.
- On-going identification and roaming procedure are usually managed with Temporary IDs (TMSI). In several standards, Ids are transmitted in clear text. Even when cipher mechanism is activated prior to TMSI reallocation (such as in GSM [3]), old TMSI are transmitted in clear text. Finally TMSI reallocation procedures in general induce a severe privacy weakness.

The examples above are detailed in [31]. They show the necessity for strong netsec upgrades of wireless public networks (especially crucial for CR). Several ways for this are introduced in the following.

2.3.2 Use of low power tag signals

Electronic marker of radio-electric source can be achieved by using DSSS weak SPD heterogeneous signals [30]. These tag signals are transmitted at the same time, at the same frame/slots and at same carrier than the user signal. Power, interference level and spreading factor of the tag signal are adjusted such a s in figure 4 in order to achieve

- Transec protection of the tag signal at first, thanks to the native interference (face to non-authorized receiver that do not know the tag spreading code),
- Easy detection and recognition of the tag signal by a suitable matched filter in any authorized receiver (thanks to the spreading factor exceeding the interference ratio).

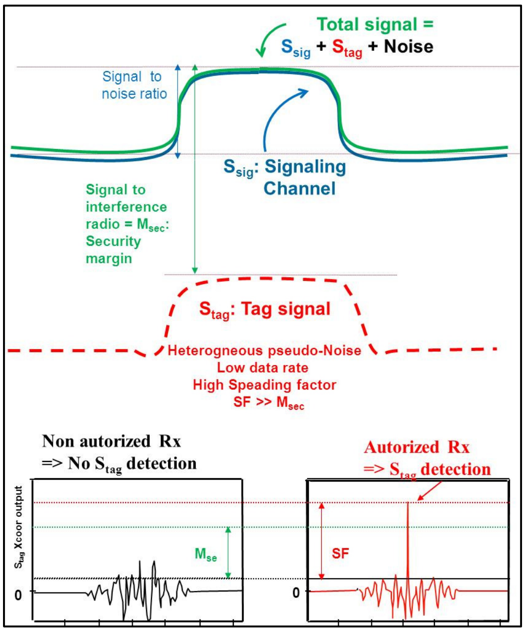

Figure 4: Principle of radio-electric tag signals

2.3.3 *IFF-derived techniques*

Netsec may be re-enforced with early identification such as Identification of Friend and Foe procedures. Most common Identification Friend and Foe (IFF) are fixed frequency interrogation (1 030 MHz) and response (1 090 MHz) protocols that use low duty-cycle signals for many applications such as airborne Traffic Control (both civilian – modes A C S - and military – modes 1 to 5-), battlefield surveillance, fratricide avoidance, etc. Various secure mechanisms (including time hopping, cryptography, DSSS) are developed in these systems. One challenge is to define similar procedures for public wireless.

From the current knowledge of IFF standards, several extensions could be imagined into wireless public frequency plans and into standard RATs in order to re-enforce security of access attempts:

. Electronic tag of networks nodes (§ 2.3.2) would achieve a preliminary recognition of networks by terminals and contribute thus to avoid most of active threats.

. Electronic tag of terminals would achieve a preliminary recognition of terminals before network download.

. Dedicated “early identification channels” would achieve preliminary interrogation and response before tuning into intelligible signaling paging and access messages.

2.4 Comsec aspects : ciphering of user’s data

2.4.1 Providing comsec with classical cryptography

In the context of comsec and netsec protection of radio-communication with classical cryptography, the transmitter (Alice) and the receiver (Bob) share a common symmetric key that is used in authentication, integrity and confidentiality symmetric mechanisms.

Confidentiality is performed in such a way that it avoids demodulation/decoding error propagation after decipherment. The solution is based on a synchronized encryption mechanism, using

- a block cipher in counter mode
- or a Key Stream Generator that produces an pseudo random sequence to be xored to the plaintext.

When both confidentiality and integrity/authentication are required, an Authenticated Encryption (AE) scheme such as Galois Counter Mode (GCM) [14] is used to encrypt the plaintext and to compute an additional Message Authentication Code (MAC).

All these mechanisms use an Initial vector (IV). This IV may be random or a determinist nonce built with an ad-hoc frame counter and/or time reference, signalization information, addresses, physical information, etc. that are shared by Alice and Bob.

In traditional cryptography, the IV and MAC data are managed separately. Two main features must be outlined.

a) Additional bandwidth is required for security

Especially when security is applied on short durations (the frames of the radio link), the part of the bandwidth purely dedicated to security management (to transport MAC and IV materials) is often significant with respect to the part dedicated to the data itself. As examples

- The size of MAC is at least n = 64 bits for a standard security level and must be 128 bits for a upper security level. Each frame must include a MAC for integrity control.
- The length of a random IV is typically more than 48 bits to insure that the probability of IV collisions is small. When the IV is a determinist nonce based on an ad-hoc frame counter or a time reference, it should not be transmitted in each frame (depends on Alice and Bob synchronization), anyway, a synchronization pattern must be regularly transmitted to maintain the correct synchronization between Alice and Bob crypto.

b) The resilience in case of IV misuse (ex: IV repeated)

When using an Authenticated Encryption (AE) scheme like GCM mode, the security is dramatically lowered when the same IV value is used with the same key. A major point for security is therefore the real robustness of IV generation process (possibly based on the time reference, on some frame counter, or on a random generator) to guarantee the uniqueness of the IV for each frame.

2.4.2. New cryptography concepts

In the future, some new enhanced cryptographic mechanisms may be adopted in order to provide an enhanced security at frame level (especially regarding the added data consumption and IV misuse), by managing both encryption and integrity control into a unique processing.

Good candidates may be taken from Determinist Authenticated Encryption Scheme such as the Synthetic Initial Vector mode (SIV) (see [13] and [15]).

In this kind of solution, a MAC=SIV is first computed on a message that includes the useful frame content and that can include an added context header, whose content is built for example with shared and non-transmitted signaling data. The computation itself uses a deterministic mechanism.

In a second step, the resulting MAC=SIV is also used as the IV for the encryption of the plaintext.

In this setting, the traditional couple of security data (IV, MAC) to be included in each frame is reduced to the single SIV pattern that plays both IV and MAC roles.

In [15], the specific good resilience feature of the Deterministic Authentication Encryption (DAE) scheme is outlined as following:

a) It is an IV-based AE scheme that is secure when its IV is an arbitrary nonce, not just when it is a random value.
b) In case of IV misuse (if the IV does get repeated) then
   - authenticity remains;
   - privacy is compromised only to the extent that some minimal amount of information is revealed: the almost information that may be revealed is the fact that the plaintext of a frame is equal to the plaintext of a prior frame. In addition, it is revealed only when the plaintext and the header content are equal over two frames.

3. OVERVIEW OF PHYSEC CONCEPTS

3.1. Notation and statement of the problem.

3.1.1. Entropy, Information and secrecy.

Figure 1 introduced briefly the kind of threat to be countered and the main relevant theoretic notions. Alice wants to send her data to Bob through the main channel, while Eve is an eavesdropper who overhears the signal. To maintain data confidentiality, Alice uses a secrecy code of rate K/N, namely, the input data block S^K is of length K, and the codeword length is N. Alice sends the codeword X^N. Bob and Eve receive corrupted versions of the codeword Y^N and Z^N due to channel noise or fading.

The Shannon entropy of a random signal X (of discrete values $x_1 \ldots, x_M$) is $H(X) = E_{PX}[-\log_2(Px_m)]$, where P_X ($P_X(X=x_m) \triangleq P_{Xm}$) is its probability distribution. H represents the degree of uncertainty of X. Its maximum $\log_2(M)$) occurs when X is uniformly distributed.

When considering a discrete stationary source S, and K outputs $S_1,\ldots S_K$ of S, the source entropy is then $H_S \triangleq \lim_{K\to\infty}[H(S_1,\ldots, S_K)/K]$. For more general cases, see [32].

When two random discrete signals are considered, such as X transmitted by Alice and Y received by Bob, the conditional Shannon entropy is $H(X/Y) = E_{PX,Y}[-\log_2(P_{Xm/Ym'})]$, that involves the conditional probability distribution $P_{X/Y}(X=x_m/Y=y_{m'})=P_{X,Y}(X=x_m,Y=y_{m'})/P_Y(Y=y_{m'})\triangleq P_{Xm/Ym'}$.

The mutual information is defined by $I(X;Y)=H(X)-H(X/Y)$. The "propagation" channel being defined by the probability $P_{Y/X}$, $I(X;Y)$ represents the amount of information about X that could be inferred after observing Y. "Perfect" channel $p_{Y/X}\equiv 1$ implies $H(X,Y)=H(X)$, $H(X/Y)=0$ and $I(X;Y)=H(X)$, while "full noisy" channel $p_{Y/X}\equiv p_Y$ implies $H(X,Y)=H(X)+H(Y)$, $H(X/Y)=H(X)$, $I(X;Y)=0$).

All these concepts lead to the definition of instantaneous (or stationary) Shannon capacity of channel $P_{Y/X}$, that is the superior bound of the mutual information $I(X;Y)$ over any distribution P_X of the transmitted signal X:

$$C_{sh,AB} \triangleq \mathrm{Sup}\{I(X;Y)\ ;\ P_X\}.$$

For more general cases see [32].

To measure the secrecy against Eve, the equivocation is defined as the conditional Shannon entropy $H(S^K|Z^N)$, which is the remaining uncertainly of Eve about the source block after receiving Z^N. Initially, Shannon defined perfect secrecy as [17]:

$$H(S^K|Z^N) = H(S^K)$$

Which means that the signal Eve receives does not contain any information about the source data. Alternatively, perfect secrecy can be measured by information leakage, i.e., the mutual information is zero: $I(S^K;Z^N) = 0$. However, it is impractical to achieve perfect secrecy, since it essentially requires one-time pad.

3.1.2 Weak secrecy

To make secrecy coding practical, one may consider the limit of the ratio [20]:

$$\lim I(S^K;Z^N)/K = 0 \text{ as } K \to \infty.$$

It means that the average information leakage per symbol tends to zero. However, a major weakness of this notion is that the absolute information leakage $I(S^K;Z^N)$ can still tend to infinity, for example, on the order of the square root of K. This is not considered secure enough. For this reason, it is usually referred to as weak secrecy.

3.1.3 Strong secrecy

Strong secrecy overcomes this weakness by considering the un-normalized limit:

$$\lim I(S^K;Z^N) = 0 \text{ as } K \to \infty.$$

This notion of secrecy is now widely accepted in the community, and is regarded as secure enough. It can be shown that it is closely related to the standard notion of semantic security widely used in the crypto community. It is important to note that although the information leakage is not absolutely zero, it can be made arbitrarily small by increasing the block length K. As long as the information leakage vanishes fast (for example, exponentially), the system with sufficiently large K is secure in practice.

3.1.4 Secrecy Capacity

The Secrecy capacity $C_{sec,AB}$ is defined as the maximum transmission rate of the legitimated link Alice-Bob under the constraint that secrecy is achieved with respect to Eve. It is known [18-20]:

. that the secrecy capacity is defined under the condition $C_{sh,AE} \leq C_{sh,AB}$ and verifies: $C_{sh,AB} - C_{sh,AE} \leq C_{sec,AB} \leq C_{sh,AB}$

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

. that in most practical cases where the channel satisfies certain symmetry, the following equality holds:

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

3.1.5 Intentional cooperative jamming

Another important direction to providing physical-layer security is the use of jamming/artificial noise. The limitation of the basic wiretap channel is that a positive secrecy capacity can be achieved only if the legitimate receiver has a better channel than the eavesdropper (see above). However, this assumption is not always true. When the receiver's channel is worse than the eavesdropper's channel, a promising technique is the use of interference or artificial noise to confuse the eavesdropper. In this scenario the transmitter has a helping interferer, which has a more detrimental effect on the eavesdropper than on the legitimate receiver [20]. Therefore, the secrecy capacity can be positive under the help of the relay.

3.1.6 Secret key generation

If Alice and Bob insist on using conventional crypto, they can use the noisy channel to generate a secret key. From a practical perspective, the design of such a scheme might be less challenging than the construction of secrecy codes. This is because the wiretap code needs to simultaneously guarantee reliability and security, while secret key generation from noisy channels makes it possible to handle them separately. It is still possible to ensure information-theoretic security if the key is used as a one-time pad. Of course, this requires the rate of the key is quite high.

3.2. Secrecy capacity for ideal channels.

3.2.1 Binary symmetric SISO channel

Binary symmetric channel (bsc) is defined for a binary source X=S (="0" or "1", with probability p_{x0} and $1-p_{x0}$), and crossover probabilities when X is transmitted:

. for the legitimate $P(Y\neq X)=p$ and $P(Y=X)=1-p$.

. for the eavesdropper $P(Z\neq X)=q$ and $P(Z=X)=1-q$.

When $p < q \leq 1/2$, the relevant Bernoulli law entropies verify $H(p)<H(q)$ and the secrecy capacity of the bsc wiretap channel is:

$$C_{sec,AB} = C_{sh,AB} - C_{sh,AE} = [1-H(p)]-[1-H(q)] = H(q)-H(p)$$

3.2.2 Gaussian SISO Channel

The Gaussian channel is defined by $Y(k) = \alpha.X(k)+n(k)$,

. x being a memoryless stationary signal of power $\pi_x=E_{PX}[X(k).X^*(k)]$, submitted to propagation attenuation α

. n being a X-independent centered Gaussian noise of variance σ^2, thus $P(Y=y/X=x)=P(n=y-x)=\exp[-(y-x)^2/2/\sigma^2]$.

. The signal-to-noise ratio (SNR) is $\rho_{SNR} = |\alpha|^2.\pi_x/\sigma^2$

Considering now the main channel defined by α_m and $\sigma_m{}^2$, the eavesdropper channel defined by α_e, and $\sigma_e{}^2$, the secrecy capacity of the Gaussian wiretap channel is given by:

$$\begin{aligned} C_{sec,AB} &= C_{sh,AB} - C_{sh,AE} \\ &= \log_2(1+ \rho_{SNRm}) - \log_2(1+ \rho_{SNRe}) \end{aligned}$$

Where $\rho_{SNR,AB}$ and $\rho_{SNR,AB}$ ($\rho_{SNRm} > \rho_{SNRe}$) are the SNRs of the main and eavesdropping channel, respectively.

3.2.3 Secrecy capacity of Rayleigh Channels

The Rayleigh channel is defined by $y(k) = H(k).x(k) + n(k)$, H being a fading coefficient following Gaussian centered law (attenuation $|H|^2$ follows an exponential probability distribution over $[0 +\infty[$). In the following, secrecy capacity is defined for a power strategy of Alice who is supposed to perfectly know the fading coefficients H_m and H_e and the noise variance $\sigma_m{}^2$ and $\sigma_e{}^2$ of the main and eavesdropping channels, respectively (full channel state information). Alice adapts its transmitted power $\pi_x(H_m,H_e)$ over the max power constraint Π, to the instantaneous signal to noise ratios at Bob's and Eve's part $\pi_x(H_m,H_e)|H_m|^2/\sigma_m{}^2$ and $\pi_x(H_m,H_e)|H_e|^2/\sigma_e{}^2$, respectively. The relevant secrecy capacity is thus given by:

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

3.2.4 Secrecy capacity for realistic SISO and SIMO Channel

In realistic cases, it is essential to investigate the degree of security generated from the channel, which strongly depends on the nature of the multi-link channel between Alice, Bob and Eve. Several strategies can be developed in order to maximize the security, e.g. by exploiting as much as possible the degrees of freedom of the channel and thus avoiding as much as possible channel knowledge leakage to Eve. All dimensions providing at least partially uncorrelated channel gains can be used, in the frequency (for wide band), time (for time variant) and spatial (for multi-antenna) domains.

3.2.5 Extension of secrecy capacity to MIMO Channels

The MIMO channel is defined by $Y(k) = \mathbf{H}(k).X(k) + N(k)$, X being a vector signal over an transmitter antenna (size $N_{Tx}.1$), Y being a vector signal over a receiver antenna (size

$N_{Rx}.1$), N being a noise vector (size $N_{Rx}.1$) of covariance matrix $\sigma^2.I_{NRx}$ (size $N_{Rx}.N_{Rx}$), **H** being a propagation matrix (size $N_{Rx}.N_{Tx}$).

Let $\mathbf{H}_m$ and $\mathbf{H}_e$ denote the channel matrices of the main and eavesdropping channel, respectively. The secrecy capacity of the Gaussian MIMO wiretap channel is

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

Where the maximization is carried over all positive semi-definite matrices $\mathbf{K}_X$ such that the power $\mathrm{tr}(\mathbf{K}_X) \leq \Pi$ is satisfied.

3.3. Coding schemes that approach secrecy capacity.

The vast majority of work on physec is based on non-constructive random-coding arguments to establish the theoretic results. Such results demonstrate the existence of codes that achieve the secrecy capacity, but are of little practical usefulness. In recent years, significant progress has been made on the construction of practical codes for physec, to a more or less extent. The design methodology can be traced back to Wyner's work on coset coding [18].

3.3.1 Low Density Parity-Check Codes (LDPC)

LDPC codes have been used to build wiretap codes, with limited success. When the main channel is noiseless and the wiretap channel is the binary erasure channel (BEC), LDPC codes for the BEC, was presented in [21,22] and proved to achieve secrecy capacity.

3.3.2 Polar Codes (PC)

In the meantime, polar coding seems to offer a more powerful approach to design wiretap codes. In [23], it was shown that, with a minor modification of the original design, polar codes achieve strong secrecy (and also semantic security). However, they could not guarantee reliability of the main channel when it is noisy.

3.3.3 Lattice Codes (LC)

The aforementioned designs based on LDPC and polar codes only tackled discrete channels, yet the physical channels are continuous. For Gaussian wiretap channels, lattice coding is emerging as a prominent approach to implement information-theoretic security. In [24], the weak-secrecy rate for lattice coding over Gaussian wiretap channel was derived. The notion of secrecy gain was introduced in [25], which has great practical significance as a criterion to design wiretap lattice codes. It has also extended to fading channels later. In a more recent paper [26], semantically secure lattice codes were proposed.

4. THEORETIC ADVANTAGES AND PRATICAL EXPECTATIONS OF INFORMATION THEORIC SECURITY CONCEPTS

4.1. Theoretic advantages of secrecy coding

Unlike conventional cryptography, secrecy coding simultaneously provides capacity and security without resorting to computational hardness assumptions (which are often unproven in practice). Even if the eavesdropper has unlimited computation power, it is impossible to break the code, because physec comes from the Shannon capacity difference of the channels. Therefore, physec is resilient to the would-be forthcoming quantum computation attacks.

4.2. Determination of secrecy codes, even sub-optimal, that approach secrecy for real field radio-environments

However, there is still a long way to go in the direction of physec. The state of the art suffers a number of significant shortcomings. In particular, LDPC and polar codes are limited to some special channel models, while explicit design of wiretap lattice codes is still lacking.

4.3. Complexity and embedding constraints

In principle, the complexity of secrecy coding is the same as that of conventional channel coding. Thus, it may be seamlessly integrated into an existing communication system. However, the state of the art does not offer such a code for real radio environments yet. In addition, when code lengths are great, practical applications are reduced for burst signals or for short messages services.

4.4. Practical perspectives of physec: towards a merging of secrecy codes with existing protections.

Further, physec can be complementary to existing transec netsec and comsec protocols. At the very least, it offers another layer of protection to vulnerable wireless communications. Therefore, there is a strong potential that physec can be merged with existing protections.

There are many open problems in this direction. In addition to the design of explicit wiretap codes, the issue of attacks warrants more attention. So far, only passive eavesdropping is assumed in most of the literature, and often, an implicit hypothesis is done that legitimate links is established, and channel propagation measured for applying secrecy codes. Finally, it seems that the threat of active attacks has not been considered carefully neither the early steps of radio access protocols.

4.5 Secrecy Coding for fading channels

A layered broadcast approach may be used when the channel is varying. The basic idea is to employ multi-layered coding to encode information into a number of layers and use stochastic encoding for each layer in order to keep the corresponding information secret from an eavesdropper. The advantage of this approach is that the transmitter does not need to know the channel states to the legitimate receiver and the eavesdropper, but can still securely transmit certain layers of information to the legitimate receiver. The layers that can be securely transmitted are determined by the channel states to the legitimate receiver and the eavesdropper. So, in practice, the data that have to be transmitted are ranked in such a way that the bits which have to be the most secure will be encoded in the layers corresponding to the most critical channel (finest granularity), and so on. This approach guarantees the best security for data as a function of Eve's instantaneous Signal-to-Noise Ratio.

5. PERSPECTIVES OF PHYSEC INSIDE WIRELESS NETWORKS

Many radio measurements that are needed in nodes and terminals for achieving communications: equalization of SISO SIMO MIMO RATs, RAKE processing of CDMA RATs, control of Quality of Service (QoS), sensing procedures and adaptive modulation/coding schemes of cognitive radios, etc. The relevant information may provide added protections based on the relevant physical randomness during access phases and during established calls. We list below some perspectives for privacy upgrades.

5.1. Re-enforce transec with adaptive resource allocation

Existing transec protections, such as selection of FHS inside TDMA RATs and selection of scrambling/spreading codes inside CDMA RATs (§ 2.2) should be highly improved by adding physical randomness into the resource allocation of legitimate links. Adaptive resource allocation for establishing radio-links usually induce high disturbance at the eavesdropper part, especially in dense networks. Therefore, combining signal mixtures (full duplex RATs, MISO, MIMO, artificial jamming) and physical-dependent allocation process should be an efficient alternative: the resource allocation would thus depend on both propagation channel and interference level at Alice and Bob parts. Moreover, sensing outputs of cognitive and opportunistic radios would induce more versatility.

5.2. Upgrade netsec with "tag channels"

Privacy of early negotiation protocols should be highly improved by taking advantage of existing (high power) signaling channels that are broadcasted by network nodes, with added heterogeneous tag signals sharing the same carrier and slots. The existing broadcast channels, being initially protected by dedicated codes or encryption schemes (thus not intelligible), would play the role of cooperative jammers. DL and UL tag signals of DSSS type, of low data rate, of low SPD and of high spreading factor would be transmitted "under" the broadcast channels by following the principles of §2.2.2 and § 2.2.3. These tag signals would support early radio exchanges such as the following:

- Terminal's and node's preliminary identification based on the spreading codes and on low data rate spread messages
- Channel measurements based on the spreading codes (such as in rake receiver techniques)
- Computation of secrecy codes at terminal and node part (supported by channel measurements)
- Exchange of acknowledgement messages.

Then after successful acknowledgement,

- Broadcast signaling would commutate into intelligible text
- Radio access would continue such as specified in the standard by adding "tag channels" under each "main channel". Tag channels would apply computed secrecy codes that would be adapted to radio environment during the process; even normal channels could apply secrecy codes.

Moreover, information could be shared among main rate channel and (low rate) tag channels. Finally

- each of the main channel would plays the role of a cooperative jammer for the associated tag channel,
- the integrity control of each of the main channels would be achieved thanks to its associated tag signal,
- the most private data (that remain low rate), such as subscribers IDs, encryption characteristics for future traffic messages etc., would be transmitted by the (more protected) tag channels.

The whole procedure should highly disturb:

- Any passive eavesdropper thanks to the native jamming of tag channel and to thank the added secrecy coding,
- Any active eavesdropper because of the heterogeneous nature of tag signals and because of native advantages of DSSS signals (spreading factor and time resolution). Note that even if the computed secrecy codes remains suboptimal for capacity of the legitimate link, this has no great importance for the tag channels that remain low data rate.

5.3. Merge physec and advanced comsec schemes

Within established traffic messages, combining SIV computation of advanced AE (see§ 2.4.2) and propagation-dependent random issued from receiver processing (equalization, rake etc.) appear as a promising way. In such a privacy improvement, outputs from receiver processing and from radio measurements (QoS estimates etc.) would be taken into account in order to build part of the context header of each frame.

6. CONCLUSION

In this paper, we introduced several concepts based on physical layer properties that may compensate security lacks occurring in civilian wireless networks when facing passive eavesdropper and active radio hacker systems.

By focusing on practical perspectives of secrecy codes in realistic radio-environments, we pointed out that the best perspectives for significant privacy upgrades for wireless networks rely in merging of traditional techniques, of cooperative jamming and of advanced channel codes (involving secrecy coding concepts) in order to build:

- Protected signaling channels
- Confidential negotiation schemes in the early stages of the radio access protocol
- Enhanced ciphering schemes that involve added propagation dependent random sources.

By this, it should be possible to hardly penalize any basic eavesdropper and radio-hacking systems that more or less re-use existing radio-components and protocol stacks.

Moreover, we conjecture that even facing advanced threats, the protection principles above should be efficient, relevant to privacy aspects, when they exploit radio-environment advantages that can be catch and/or generated locally by legitimate base stations, communication nodes and terminals for their proper communication services. The core idea is to convert in secrecy benefits

- radio-interferences and strong signals (such as signaling channels) that are present in the radio spectrum.
- information got by sensing, by equalization processing and by QoS management at each termination point of the radio link,

Based on this information, the final achievement is to embed adaptive modulation and coding schemes:

- that approach mean channel capacity in realistic radio-environment
- that maximize confusion at any threat location,
- that keep implantation complexity compatible with the performances of the future embedded computers.

We are confident that current national and European research programs will discover and proof feasibility of such adaptive modulation and coding schemes thus preparing standardization and industrial development of trustworthy and full-secure public RATs.

7. REFERENCES

[1] www.3GPP.org

[2] www.3GPP2.org

[3] Lagrange (X.), Godlewski (P.) and Tabbane (S.). Réseaux GSM. 5e édition, Éditions Hermès (2000).

[4] Bluetooth Vulnerability Assessment Tech. Publication ITSPSR-17A, Communications Security Establishment Canada, 06/2008.

[5] http://fr.wikipedia.org/wiki/Identification_friend_or_foe

[6] ITU-R SM 1600 « Technical identification of digital signals »

[7] QoSMOS project "Radio Context Acquisition algorithms » Deliverable D3.3. FP7-ICT-2009-4/248454

[8] F. Delaveau, D. Depierre, F. Sirven «Oriented processing of Communication signals for Sensing and Disseminated Spectrum Monitoring», SDR Winncomm Forum 2011 Brussels.

[9] F. Delaveau Y Livran "Radiosurveillance du spectre - TE 6890 Rôles et tendances, TE 6891 Interception Réception et Détection, TE 6893 Analyse et identification des transmissions» in Techniques de l'Ingénieur. 2012.

[10] J.G. Proakis, M. Salehi Prentice Hall Int. Ed2 2001., "Communication System Enginnering".

[11] H.L. Van Trees, "Detection, estimation and modulation Theory". Ed. J. Wiley (1968).

[12] Pickholtz (R.L.) and al. – Theory of Spread Spectrum Comm - A Tutorial. IEEE Trans. Com., vol. com 30-5,1982.

[13] D. Harkins "Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)", 2008.

[14] McGrew, D. and J. Viega, "The Galois/Counter Mode of Operation (GCM)".

[15] Rogaway, P. and T. Shrimpton, "Deterministic Authenticated Encryption, A Provable-Security Treatment of the Key-Wrap Problem", Advances in Cryptology -- EUROCRYPT '06 St. Petersburg, Russia, 2006.

[16] B. Shneier "Applied Cryptography, Protocols, Algorithms, and Source Code in C". Wiley.

[17] C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28,pp. 656–715, 1948.

[18] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1367, October 1975.

[19] U. Maurer, S. Wolf, « Information-theory Key afgreement From Weak to Stong secrecy for Free. EUROCRYPT 2000, International Conference on the *Theory* and Application of Crypto. Techniques

[20] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.

[21] A. Thangaraj, S.Dihidar, A.R.Calderbank, S.W.McLaughlin, and J.Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inform. Theory,* vol. 53, no. 8, pp. 2933-2945, 08/2007.

[22] A. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S.W.McLaughlin, "Strong secrecy for erasure wiretap channels," *Proc. IEEE Inf. Theory Workshop*, Dublin, Ireland, September 2010.

[23] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," IEEE Trans. Inform. Theory, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[24] L.-C. Choo, C. Ling, and K.-K. Wong, "Achievable rates for lattice coding over the Gaussian wiretap channel," in *ICC 2011 Physical Layer Security Workshop*, 2011.

[25] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," Mar. 2011.

[26] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," 2012.

[27] « Procédé d'optimisation de la planification dans un système de communications de type CDMA » Patent Thales FR 04.01475

[28] « Procédé ''protocole orienté'' de traitement des signaux stationnaires, partiellement stationnaires, ou cyclo-stationnaires, patent Thales FR 10.05017, PCT/EP2011/073420 WO2012.084956

[29] R. Gautier, G. Burel, J. Letessier and O. Berder « Blind estimation of Scrambler offset using encoder redundancy », in IEEE 2002

[30] « Procédé de taggage radio-électrique des signaux de brouilleurs et d'autres émetteurs» Patent Thales FR 12.03071

[31] F. Delaveau, A. Evestti ; A. Kotelba; R. Savola, N. Shapira; "active and passive eavesdropper threats within public and private civilian networks-existing and potential future countermeasures – an overview". Winncomm2013, Munich

[32] T.M Cover, J.A Thomas « Elements of Information Theory», Wiley 1991