Perspectives of Physical Layer Security (Physec) for the improvement of the subscriber privacy and communication confidentiality at the Air Interface

Results for WLANs, IoT and radiocells

François Delaveau, (Thales), Andreas Mueller (Bosch), Christiane Kameni Ngassa (Thales), René Guillaume (Bosch), Renaud Molière (Thales), Gerhard Wunder (Fraunhofer Heinrich Hertz Institut)

Abstract—Physical layer security (PHYSEC) is a promising new security approach in the context of the IoT and ubiquitously connected systems. PHYSEC exploits the intrinsic randomness of the radio channel between several nodes to establish cryptographic keys in a plug-and-play manner, to achieve information-theoretic security without complex ciphers, and to securely pair devices. Each of these opportunities has been successfully demonstrated by the German research project Prophylaxe for application to the Internet of Things (Wi-Fi and IEEE 802.15.4) and by the European project Phylaws for application to Wi-Fi and to Radio-cells (LTE).

Keywords—PHYSEC, SKG, Secrecy Coding, Tag Signals, Interrogation and Acknowledgement Sequences, Wi-Fi, LTE, IoT

I. INTRODUCTION

Recent news highlighting security failures of modern wireless communication systems [1-4] have recalled the limits of the cryptographic key distribution approach and the urge to improve security of the information exchanged over the air interface of wireless networks commonly used by citizens and industrials.

Many access technologies nowadays try to avoid the use of SIM cards. On the counterpart, existing security mechanisms for radio-cell communications, based on SIM cards, rely on pre-shared cryptographic keys to authenticate users and to encrypt exchanged data. However, recent news revealed that attackers can have access to these encryption keys by exploiting weakness of SS7 protocol and international roaming [2-3]. Furthermore, the recent hacking of SIM card manufacturers to get encryption keys [4] proves that the cryptographic key distribution approach can no longer be considered as completely secure for public networks.

To counter both passive eavesdropper and active radio hacking systems (such as advanced IMSI catchers for example [2]) that operate at the radio interface of wireless networks, physical layer security (Physic) has emerged as a promising approach, in complement of classical ciphering. Physic strengthens the security of wireless communications by catching and exploiting the intrinsic randomness of the radio propagation, which avoids the use of pre-shared keys and guarantees full secrecy independently of the adverse computing capabilities. Particularly,

- Secret Key Generation (SKG) from channel randomness has attracted an increasing interest from both academics and industrials researchers; it has now reached mature applications for SIM-less IoT and feasibility proof for WLAN and 4G wireless networks.
- In association with existing MIMO technologies such as Artificial Noise and Beam Forming (AN-BF), first Secrecy Coding (SC) schemes are developed, that provide highest grade secrecy over the radio interface, resilient from attacks with unlimited computational power.
- Secure Pairing (SP) mechanisms are studied in order to provide reliable and resilient association between legitimate radio devices by excluding any kind of non-authorized third party. Their purpose is to support enhanced authentication scheme and channel negotiation at the first stage of RAT access.

The figure below illustrated the studied configuration when legitimate nodes and terminals Alice (A) and Bob (B) may be intercepted or hacked by passive or active Eve (E).

Figure 1: Illustration of the studied configuration
The remainder of the paper is organized as follows. Section II describes step by step the Secret Key Generation scheme and provides some exemplary and promising experimental results. Section III deals with secrecy coding associated with Artificial Noise and Beam Forming and details simulation results. Section IV explains how secure pairing can be achieved using Tag Signals and dedicated Interrogation and Acknowledgement sequences and studies relevant applications. Section V concludes the paper.

II. SECRET KEY GENERATION FOR IoT AND MOBILE NETWORKS

SKG from channel randomness is a promising path in IoT-related scenarios, e.g. with massive connectivity or the tactile Internet [17], and was introduced in [18]. Here, Alice communicates with Bob (or several Bobs) representing resource-constrained devices. Moreover, if Alice represents a low-cost access point with “off-the-shelf” hardware, even Alice might be resource-constrained. Both Alice and Bob use lightweight symmetric ciphers, which require at least 128 bits entropy to be considered as secure against attacks by an eavesdropper Eve, notably assuming that Eve has no further side information. This entropy is extracted from the wireless channel using the general procedure illustrated in Figure 2.

First of all, suitable random and reciprocal channel parameters are estimated by both Alice and Bob. This raw information may then be \textit{pre-processed} in an appropriate way, for example by applying some filtering, followed by the \textit{quantization} stage, which derives an initial key on both sides based on the pre-processed channel estimates. Afterwards, potentially mismatching bits in the initial keys are corrected or discarded during the so-called \textit{information reconciliation} phase, which typically involves some (insecure) data exchange between both nodes. The results of this phase are in the ideal case aligned, i.e., identical bit strings on both sides. Next, it should be tested how “good” these bit strings are from a security point of view. This is done during the \textit{entropy estimation} phase. Here, statistical defects may be detected (e.g., due to insufficient randomness in the channel) and the information potentially revealed to an attacker during the information reconciliation phase may be quantified. This step is actually rather important and has been widely overlooked in literature so far, thus often leading to overestimates of the resulting key generation rates. Finally, the \textit{privacy amplification} phase produces the actual keys by extracting the entropy contained in the aligned bit strings and finally it is checked during the \textit{key verification} phase if both keys are indeed identical [19].

In the following subsections, some more details are given for selected aspects of the procedure shown in Figure 2.

A. Channel Estimation

Today, most available SKG schemes work based on Received Signal Strength Indicators (RSSIs), as this is typically the only type of channel information that is readily available with off-the-shelf hardware. However, an even better performance is expected with access to more fine-grained channel state information, such as estimates of the full channel impulse responses or phase information. In order to obtain suitable channel estimates, a fast exchange of pilot signals / packets between Alice and Bob is required in order to ensure channel reciprocity. In fact, typical indoor environments exhibit channel coherence times in the order to 50-100 ms, meaning that a round-trip measurement of the channel should be (much) faster than that in order to obtain good raw material of high reciprocity.

Some exemplary RSSI measurements are depicted in Figure 3 for the channels between Alice and Bob, Bob and Alice, as well as Bob and a passive Eavesdropper Eve.
There are several observations that can be made from Figure 3:

- The channels between Alice and Bob as well as Bob and Alice exhibit a high degree of reciprocity. There is still some approximately constant offset between both curves, which, however, is not really relevant for the subsequent processing.
- The channels between Bob and Eve and Bob and Alice are quite different, even though Eve is located relatively close to Alice. This is actually good from a security point of view.
- The channels exhibit some considerable randomness, which is good from a security point of view as well.

**B. Pre-Processing**

In order to improve the performance of the key generation process, instead of quantizing the channel profiles directly, they can be smoothened to enhance their reciprocity and, thus, reduce the probability of disagreement by low-complex methods including standards schemes such polynomial regression, spline interpolation [21] and possibly low-complex subspace variants of Kalman filtering [22]. A special case is Savitzky-Golay filtering, which smoothes the channel profiles without distorting the waveform’s shape and height. Like in the moving average process, a block of samples around a central point is averaged and the value at the central point smoothed. However, the averaging process is weighted by a polynomial least squares fit within the filter window. The polynomial order can be chosen so as to preserve higher order moments and reduce the bias introduced by the filter [21]. As Figure 4 shows, the correlation between the (pre-processed) channel estimates obtained by the two nodes can be greatly increased by reciprocity enhancing techniques. As can be noticed, reciprocity enhancement reduces the effect of normalized Doppler frequency and thus the sampling delay between the two nodes.

The enhanced sequence will be of increased temporal correlation. Hence, a mandatory subsequent step is to remove this redundancy by low-complex “de-correlation” methods. Here, the power spectrum distribution is condensed to downscaled components in the transformed dimension. By truncating higher-order components, the remaining samples hold a significant amount of the sequence’s power. Standard efficient methods are discrete cosine transform (DCT), Haar transform, Walsh-Hadamard transform. The well-known Karhunen-Loève transform depends on the given input data and requires a high-complex estimation of the correlation matrix though, and can serve only as a benchmark. In special cases, if, e.g., the access point can afford the complexity it can carry out the computation and reveal it publicly to Bob (and Eve then). Using standard statistical test suites (which are discussed in the next section), all mentioned de-correlation schemes show no significant difference and greatly increase the rate of passed tests and therefore the quality of the secret keys.

**C. Channel Quantization & Information Reconciliation**

Channel quantization is a crucial step in the general procedure according to Figure 2, which maps the measured values (samples) into initial keys at both Alice and Bob. Information reconciliation is then a necessary step to reconcile the “raw” key material, i.e., to make sure that the initial keys become identical on both sides, which without any further ado is generally not the case due to different noise, interference and non-ideal channel reciprocity.

There are many proposals (see the overview in [29]) for channel quantization schemes. They can be classified into lossless and lossy ones. Lossless schemes process all the available information obtained from the samples. They are typically more robust to prediction attacks and sometimes do not even require communication to reconcile the key material. Lossy schemes though discard some of the measurements, e.g., by fixing some guard interval \([-q, q]\), \(q > 0\), such that samples which fall within this interval are dropped. At best, such material can be directly used as a shared symmetric key. On the other hand some additional overhead is typically required and the schemes are prone to attacks [29].

For assessing quantization schemes, typically the bit disagreement rate (BDR) is plotted over the correlation coefficient, as depicted in Figure 5, for example. The goal is clearly to achieve a low BDR when the correlation is high. A second criterion, which is often overlooked in the literature, is that BDR should quickly approach values close to 0.5 when correlation is weaker so as to make it difficult for an attacker to “guess” the quantized values from weakly correlated measurements. This requirement eliminates already some of the proposed schemes in the literature [29]. It is worth mentioning that such tradeoffs are not yet completely understood from a theoretical perspective.

A simple method is to quantize the measured input in a straightforward manner to a set of predefined values controlled by some threshold parameter \(\theta\), which can be adapted in the

![Figure 4: Effect of several smoothing techniques in Rayleigh distributed, temporally correlated fading channel with additive white Gaussian noise at each node and a sampling delay of half the sample period. Figure compares the resulting correlation coefficient normalized to sampling frequency for SNR = 20 dB](image-url)
process. Such method is often sufficient for resource-constrained IoT scenarios with [20].

This can be nicely combined with a simple information reconciliation procedure, where just the offsets between the true value and the quantized value are reported. Such offsets are presumably more or less independent of the actual value and no information is revealed to an attacker. More sophisticated methods to reconcile the measured values use the properties of codes such as parity-, syndrome-based or more generally secure sketches [9]. As part of IoT some of the more sophisticated methods must be carefully assessed regarding their require complexity and communication overhead.

D. Entropy Estimation, Privacy Amplification & Key Verification

With SKG, the wireless channel is considered as a random number generator (RNG), which is a critical component in every cryptographic system. In our case, the raw key material is derived from a complicated stochastic process, which not only depends on channel parameters (such as channel coherence time, channel delay spread, etc.), but also on the applied quantization scheme. Both factors typically lead to non-uniform first order distributions as well as dependencies in the bit strings. Therefore, in order to assess the actual key quality, the implementation of fast and low-complex “online” entropy estimation schemes and key material health test procedures is a mandatory design feature. Recent works [23] address the problem of these generally time consuming processes with rather high memory consumption, but focus rather on health tests than actual entropy calculation itself. In [19] and some follow-up work, low-complex entropy estimators based on the latest draft 800-90B of NIST [24] have been implemented, thereby avoiding floating-point units and by utilizing look-up tables to stay below required memory limitations. Notably, to avoid collecting useless noise entropy, the algorithms are applied after the information reconciliation procedure when both Alice and Bob have synchronized symmetric key material, which depends only on the reciprocal channel. Based on the estimated entropy, the synchronized key material can be evaluated and proper parameters of the information reconciliation scheme can be selected.

Privacy amplification is an important step to remove inter-dependencies in the final key material using randomness extractors. For example, as its randomness extractor, 6doku adopts CBC-MAC, as suggested in [9]. CBC-MAC can be efficiently implemented on 6LoWPAN [30] nodes since virtually any IEEE 802.15.4 transceiver has a hardware-accelerated AES block cipher implementation. Key verification can be simply done by encrypting an empty message and authenticated acknowledgements [20].

E. Experimental results for TDD RATs - Wifi and LTE

Given that the propagation channel is reciprocal and inherently random, it may be considered as a shared pool of random secure key bits, between a pair of legitimate nodes and terminals [7]. Furthermore, measuring the radio channel at signaling and access channels is a common process within mobiles handsets BS and AP for equalization purposes. Thus, SKG could be applied from equalization outputs for establishing SIM-less pre-shared keys before the classical subscriber’s authentication and computation of cipher keys. From recent experiments [12], it appears that (slow) mobile environment induce significant CIR diversity and entropy at keys. On the counter part, the time stationarity is reduced in mobile scenarios and real time constraints for establishing keys are thus more severe.

The Figure 6 below issued from [12] show real field SKG results performed with a 6 Rx SIMO receiver facing LTE BS in outdoor urban zones by processing the 1.4 MHz beacon signaling (PPS signal) and facing Wifi AP in indoor office by processing the synchronization probes (STF and LTF). Several hundred Keys of 128 bits with good random quality (verified with NIST criterias) are generated in each case in a few second signal time.

Finally, all the previous results show that, as for IoT, SKG well applies to mobiles networks and could be a crucial help to privacy of negotiation stage in 2/3/4/5 G RAT, before establishment of traditional authentication and cryptography techniques.

III. SECRECY CODING (SC) HELPPED BY ARTIFICIAL NOISE (AN) AND BEAM FORMING (BF)

A. Artificial Noise and Beam-Forming

1) Artificial Noise (AN) and Beam Forming (BF) for achieving radio advantage (RA) or User Data (UD)

Artificial Noise (AN) schemes apply both to MISO and MIMO RATs. They combine Beam Forming (BF) of User Data (UD) stream towards the legitimate receiver and emission of Noisy Signals (NS) elsewhere, such as illustrated in Figure 7. The powers $NS_{Alice}$ and $UD_{Alice}$ of the noisy and user data
signals are controlled and steered to limit the link budget of eavesdroppers while optimizing the transmission scheme for the legitimate link.

3) A.N. and B.F. for initiating Secrecy Coding schemes

Secrecy Codes conceal the information sent by Alice in the difference of channel capacity between Bob and Eve (difference of SINR in simplest cases such as AWGN channel) leading to a secrecy capacity (SC) most often equal to the difference of the Shannon capacity at Bob and Eve. Therefore a Radio Advantage (RA) is needed for achieving a Shannon capacity better at Bob than at Eve. As seen above, AN and BF can ensure such a controlled RA.

Then Secrecy codes ensure reliable communication at the legitimate link and avoid any information leakage elsewhere up to a value as close as possible of the SC. Moreover, RA being controlled: a minimum rate of secret bit is ensured and Alice and Bob can select and transmit them as follows.

2) Generation and processing of Artificial Noise

Most promising AN schemes in the literature proceed as follows [6]:

- Estimation of the legitimate Channel Frequency Response (CFR) or Channel Impulse Response (CIR), from Alice to Bob, and extraction of orthogonal directions of the legitimate CFR or CIR.
- Transmission of NS on orthogonal directions. As Eve cannot estimate the legitimate channel matrix, she is forced into low Signal to Interference Noise Ratio (SINR\text{Eve} ≤ UD_{Alice}-NS_{Alice}) unable to decode.
- BF of the UD stream then optimizes legitimate link for Bob. In ideal cases, the interferences at Bob’s side completely vanish and the SINR at Bob’s side is equal to the Signal to Noise Ratio (SINR_{Bob}=SNR_{Bob}).

When AN-BF is active from Alice to Bob, a better SINR is provided to Bob than to Eve in any case and the SINR\text{Eve} at Eve’s side is controlled by Alice. Thus, a guaranteed Radio Advantage RA=SNR_{Bob}-SNR_{Eve} can be controlled by Alice and further exploited to compute secrecy codes from Alice to Bob. Same considerations apply when AN-BF is applied from Bob to Alice.

B. Secrecy Coding Scheme

Even if the design of optimal secrecy codes for continuous channels is challenging [4], Polar Codes (PC) and Reed Muller Codes (RMC) have provided strong security for discrete channels [7]. Thus, a first idea is to concatenate them to a capacity approaching code (LDPC, turbo, other) such as illustrated in Figure 8. In this way, the continuous channel processed by the inner code is viewed as a discrete Binary Symmetric Channel by the outer encoder and decoder, what is a suitable condition for exploiting PC and RMC.

The inner code is chosen among classical FEC codes of wireless communications (LDPC, Turbo codes, etc.) that follow the requirements defined in standards.
For the outer code, we use two nested PCs or RMCs of length $N = 2^k$. The first code is a sub code of the second one. The rate $R_B$ of the first code is the target rate for Eve and the rate $R_{th}$ of the second code is the target rate for Bob. As the legitimate users have a controlled RA advantage over Eve, $R_B < R_{th}$. Therefore, Eve can correctly decode $N.R_{B}$ bits and Bob $N.R_{th}$ bits. In order to perfectly confuse Eve, we want to ensure an error probability of 0.5 on information bits at her side. So, we send random bits over Eve’s perfect bit-channels, and information bits over Bob’s remaining perfect bit-channels. For small and moderate code lengths, RMCs provide interesting alternatives to PC [8]. Indeed, RMC usually have larger minimum hamming distances and better reliability performances than PCs.

Applied to nested PCs, the design strategy of the polar-based outer codes is the following.

- Battacharyya parameters (BP) are computed for Bob target’s error probability at the output of the inner decoder
- Bit-channels are sorted in ascending order of their BP.
- Random bits $R$bits are sent at the first $N.R$ bit-channels. 
- User Data bits $UD$bits are sent at the $N.(RB-RE)$ following bit-channels.
- Predefined bits $P$bits are sent at the remaining bit-channels.
- Applied to nested RMCs, the design strategy of the outer code is slightly modified as follows.
- Hamming Weights (HW) of generator matrix’s rows are computed
- Bit-channels are sorted in ascending order of their HW
- Then same procedure than for PC is applied.

**C. Practical design - Simulation – Performance analysis**

To illustrate our secrecy coding scheme, we use the LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard as the inner code. The outer code is either a polar code of length $2^{10} = 1024$ or a Reed-Muller code of the same length designed with different rates. The parameters of these five secrecy codes (SC1 to SC 5) are given in the table below.

<table>
<thead>
<tr>
<th>Inner code</th>
<th>SC 1</th>
<th>SC 2</th>
<th>SC 3</th>
<th>SC 4</th>
<th>SC 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outer code</td>
<td>LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eves’s target rate</td>
<td>PC</td>
<td>PC</td>
<td>PC</td>
<td>RMC</td>
<td>RMC</td>
</tr>
<tr>
<td>Bob’s target rate</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.05</td>
<td>0.05</td>
</tr>
<tr>
<td>$R$ bits, UD bits, P bits</td>
<td>102, 512</td>
<td>102, 490</td>
<td>102, 307</td>
<td>56, 430</td>
<td>56, 330</td>
</tr>
<tr>
<td>Theoretical SC</td>
<td>0.5</td>
<td>0.4</td>
<td>0.3</td>
<td>0.45</td>
<td>0.35</td>
</tr>
<tr>
<td>Achieved Rate for Secret Bits</td>
<td>0.4</td>
<td>0.33</td>
<td>0.24</td>
<td>0.33</td>
<td>0.25</td>
</tr>
</tbody>
</table>

Simulations were carried out using MATLAB and messages were sent over an AWGN channel using a QPSK modulation.

1) Performance analysis

The Figure 10 below shows simulated performances of the designed secrecy codes.

- The black curve represents the Bit Error Rate (BER) at the output of the LDPC decoder
- Red curves represent the BER at the output of secrecy polar decoders
- Blue curves represent the BER at the output of secrecy Reed-Muller decoder.
- These simulations show the following trends:
  - When $\text{SINR} \leq 2 \text{ dB}$, the BER at the output of the SC1 to SC5 is equal to 0.5, meaning that every secrecy codes guarantees no information leakage if Eve’s $\text{SINR}$ is less than 2 dB. Only the polar based secrecy code with rate 0.4 (Secrecy code 1) guarantees no information leakage until 3 dB.
  - All Reed-Muller based secrecy code have better reliability performance than polar based secrecy codes.
  - For a target error probability of 5.10-5 for Bob, the required radio advantage is between 3 dB and 4 dB.

Finally, these results show
- that Eve cannot retrieve any transmitted information as soon as a slight radio advantage (< 4 dB) is provided to legitimate users
- that secrecy is achieved through a slight increase of software cost with a limited rise in coding and decoding complexity.
2) **Performance illustration**

To illustrate the performance of SC5, we simulate in the figure below the transition of MATLAB cameraman image over an AWGN channel, for different values of the SINR.

![Image of SC5 (QPSK, AWGN) with four parts showing received images for different SINRs](image)

Part a of the previous figure shows the received image when the targeted SINR for Eve is lower than 2 dB. The BER at the output of the secrecy code is equal to 0.5. No clue on the transmitted image can be deduced from the received image.

Part b represents the received image when the SINR is increased to 3 dB, leading to a BER=0.3. In this case, even for such a high value of BER, Eve can still successfully decode some information. Consequently, Eve’s BER shall be as close as possible of 0.5 and SINR\(_{Eve}\) shall be lower than 2 dB to guarantee no information leakage.

Part c shows the received image for higher SINR value, 1.5 dB less than the targeted value for Bob. The BER at the output of SC5 is 4.10^{-2}. Some decoding errors remain even if the overall image is note fully proper but it is very intelligible.

Part d shows the received image for the SINR value of 4.7 dB targeted for Bob leading to a BER=5.10^{-5} meaning that Bob correctly receives the transmitted information.

3) **Tuning of the radio advantage**

From the previous results, only a few dB of radio advantage (typically 3 dB to 4 dB) is required to provide reliability and secrecy to legitimate users. These reasonable values ensure the compatibility of SC schemes with exiting AN-BF schemes.

Our simulation results show, as expected, that the BER at the output of the polar or Reed Muller decoder is 0.5 up to a given “attacker threshold” of the Signal to Interference + Noise Ratio (SINR\(_{Eve}\)), depending on the modulation and of concatenated coding scheme, that ensures no information leakage. As expected, when the SINR\(_{Bob}\) grows at Bob’s side, the BER at the output of the polar decoder falls. When SINR\(_{Bob}\) is high enough (meaning more than a “user threshold” SINR\(_{user}\)) the BER at the output of the polar decoder tends to zero. Finally, UD and NS shall be tuned in order to achieve SINR\(_{Eve}\) ≤ 2 dB and suitable SINR\(_{Bob}\) for Bob side thanks to the BF capabilities. BF being operant, these two basic radio parameters drive both the link budget (and thus the reliability of the transmission scheme) and the radio advantage (and thus the efficiency of the secrecy scheme).

IV. **SECURE PAIRING (SP)**

A. “6doku” Protocol

Before the actual processing of the key material in channel-based SKG, Alice and Bob “pair” and exchange Ping-Pongs to collect the channel “samples”, i.e. Bob answers with a Pong immediately after receiving a Ping from Alice and so on. The “pairing and sampling” is vulnerable to various attacks (evil twin, stepmother, Man in the Middle - MitM) and must be suitably secured. In a recent paper various pairing methods are discussed including “6doku” “button-based” pairing [20]. Moreover, “6doku” secures the sampling phase with JaneDoS, a new entity recognition protocol which introduces several hash chains for the Pings, the Pongs, as well as for the message authentication codes (MACs) and acknowledgements (ACKs), whereby the roots of the hash chains are exchanged in the pairing phase. If the root is actually trusted, subsequent messages can be secured generation and management of hash trees using one-way functions, such as Davies-Meyer [20]. This makes the sampling phase quite robust to interception, spoofing, replay attacks etc.

B. **Tag Signals (TS) and dedicated Interrogation and Acknowledgement Sequences (IASS)**

A Tag Signal (TS) is a self-interfered Direct Spread Spectrum (DSS) signal or a Multiple Carrier-Direct Spread Spectrum (MC-DSS) signal that is emitted at low power under dominant beacon signal, as indicated in Figure 12 - left part.
TSs are designed to allow Matched Filtering (MF) and accurate estimations of the Channel Impulse Response (CIR) as indicated in Figure 12 - right part.

Interrogation and Acknowledgement Sequences (IAS) involve successive exchanges of forward (“ping”) and return “pong”) TSs. These TSs are specifically re-designed at each new exchange from CIR measurements (Figure 13).

- the “full arbitrary” design of DSSS codes studied in [12] avoids deterministic pseudo random algorithm in order to prevent recovery techniques of PN sequences [25] and it applies suitable orthogonally and selection tests [26] for keeping good synchronization and CIR estimation capabilities,
- the choice of each new forward and return TS is made dependent on the on-going CIR estimation at Alice’s and Bob’s side.

IASs thus combine techniques of Identification Friend or Foe (IFF) with CIR estimations and channel dependent interrogation and acknowledgment in the same procedure.

By the previous procedure, the first IAS remains resilient to MitM attacks or (protocol aware) Intelligent Jamming (IJ) attacks of the first IAS by active Eve. Same considerations apply for the following IASs.

C. TS and IAS for initiating and enhancing AN schemes

As seen above, combination of AN and BF provides a RA for Bob, which is fully controlled by Alice. Nevertheless, the critical step of this basic scheme is the first shared determination of the CIR used for computing the BF scheme. This step is the current flaw [28] of Channel State Information (CSI) in many MIMO systems using explicit feedback sounding [6]. This feedback exposes to Eve the private knowledge of Alice-Bob CIR and must absolutely be protected. Moreover, active Eve can often anticipate the CIR estimation procedure and prevent it by intelligent jamming (IJ) [28]. With the same kind of techniques, MitM Eve can decoy it, and passive Eve can even intercept and decode CIR messages before the establishment of AN, what facilitates the rejection process. Finally, AN is efficient once set up, but its establishment protocol in the RATs of nowadays is weak. For these reasons, we propose to use TS and IASs schemes to protect CIR negotiation in MIMO RATs before enabling AN-BF. Then, AN-BF being securely established for data signals, SC, SKG and other physic protections can take benefit of it.

D. TS and IAS for initiating SKG schemes in TDD RATs

SKG schemes require the authentication of the legitimate channel supporting CIR estimation. Otherwise, active Eve (I of MitM) can anticipate, replay, decode the CIR negotiation, and passive Eve can get information. TSs and IASs are typically designed to provide a secure pairing from the very first stage of the radio access protocol, allow authenticated CIR measurements; in addition they provide discrimination capabilities of any active attack.

Moreover, the specific design of TS makes their CIR estimation more accurate and more resilient to harsh propagation conditions, self-interferences and to multiple paths, what finally provides added entropy and degrees of freedom in the SKG computations.

E. TS and IAS for supporting SC schemes

The Radio Advantage (RA) required for secret coding can directly be achieved with the use of TSs and IASs. From the second IAS, Eve can no more follow the design of the forward and return TSs. Thus Eve cannot apply Matched Filtering (MF) contrary to Bob and Alice. Moreover, the self-interfered nature of TS enhances this advantage. Finally, the RA on TS is directly given by the processing gain of the MF and secrecy coding could thus be applied to TS for transmitting low data rate information at the beginning of the access protocol in a protected manner instead of in clear text and then to support privacy and integrity control of data messages. Such information may be at first authentication vectors, subscriber identities, authentication and cipher acknowledgements, then header for integrity control and for cipher schemes.
F. TSs and IASs for supporting ‘6doku’ Protocol

As above, the Radio Advantage achieved with the use of TSs and IASs, and the USS and TJ procedures could be used for coding pings and pongs in pairing and sampling protocol such as described in part A. By providing trusted links and roots of the hash chains without any prior clear text exchange, this would enhance their global resilience to various attacks (interception, spoofing, replay, MitM…).

V. BEYOND CHANNEL-BASED SKG

An interesting extension to SKG is detection of so-called “hidden wormhole” attacks (similar to MitM). In such an attack malicious nodes set up out-of-band links that relay traffic between non-neighboring nodes verbatim. Obviously, wireless multi-hop networks of IoT devices (such 6LoWPAN networks [30]), are vulnerable to so-called hidden wormholes, as shown in Figure 14 since the network’s routing protocols will actually start using such “shortcuts” which enables an attacker to carry out traffic analysis, drop certain messages while letting others through and so on. Moreover, an attacker can switch wormholes on and off so as to force a network to constantly reorganize the routing topology which expends valuable battery power of the IoT devices.

![Diagram of wormholes](image)

Figure 14 Hidden wormholes relay traffic between non-neighboring nodes in a network

There are many wormhole detection schemes described in the literature (for details see [31]). Interestingly, Jain et al. proposed a channel reciprocity-based wormhole detection scheme, which is advanced in [32]. In general, such schemes have as well a sampling and a judgment phase. The sampling phase is used to collect samples using Ping-Pongs like in PHY key agreement. During the judgment phase, one party sends its collected samples to the other party, which calculates a so-called reciprocity metric. Depending on whether this metric is below or above a predefined threshold, a wormhole is suspected or not. The key is that channel reciprocity breaks if and only if the Ping-Pongs were relayed by a wormhole.

This scheme has been recently generalized in [31] revealing the flaw that in the original scheme, when using just received signal strength, channel reciprocity can be faked by dynamically adapting transmission powers. Moreover, the scheme introduces power control scheme to impede such attacks. While this attack merely requires a transceiver that supports a wide range of transmission powers, it is conjectured that using additional (reciprocal) phase information complicates such attacks.

VI. CONCLUSION

This paper has first recalled the basic schemes and principle of Secret Key Generation, and its efficient application cases to SIMless IoT scenarios, to Wifi and to LTEs radio cells. Results performed in various radio-environments and scenarios show that significant number of keys of good length and randomness quality can be extracted, which robustness is enhanced by pre/post processing, reducing mismatch risks in key agreement between legitimates while efficiently mitigating information leakage towards any third parts in stationary environment. To the best of our knowledge, this is the first work on a full SKG applied to real IoT devices and real field WiFi and TDD-LTE signals. Our promising results prove that SKG is now a mature technology ready for standardization.

Then, we have described, implanted and simulated a secrecy coding scheme. Even suboptimal, it significantly approaches the theoretical secrecy capacity driven by the Radio Advantage provided in Artificial Noise and Beam-Forming schemes of MISO/MIMO nodes and terminals. The excellent performances shown by our simulations raise great hopes for practical implantations in both TDD and FDD RATs in the future, and a technological readiness for standardization proposal in the next year.

Finally, we introduced a new approach for securely pair electronic devices, supporting establishment of SKG and SC, enhancing privacy, authentication and integrity control from the first negotiation steps in 2/3/4/5G RATs. The promising results of our current studies raise great hopes for a technological readiness into IoT WLAN in the close future, and for proposals to standardization in the next two years.

ACKNOWLEDGMENT

This research was conducted within the scope of the Phylaws project which is funded by The European Community EC-FP7-ICT-2011-8 under the grant number 317562 (http://www.phylaws-ict.org) and the PROPHYLAXE project, which is funded by the Federal Ministry of Education and Research (BMBF) under grant number 16KIS0005K (http://www.ict-prophylaxe.de).
REFERENCES


