Physical-Layer Security in LTE Cellular Links: Simulation Results and Standardization Perspectives

(Invited Paper)

Adrian Kotelba, Sandrine Boumard, and Jani Suomalainen
VTT Technical Research Centre of Finland, P.O. Box 1100, FI-90571 Oulu, Finland
E-mail: {adrian.kotelba, sandrine.boumard, jani.suomalainen}@vtt.fi

***Abstract*—In this paper, we discuss the applications of physical-layer security in LTE cellular networks. In particular, we consider three application areas of physical-layer security: authentication, key generation, and confidentiality. We present a few physical-layer security extensions targeting aforementioned application areas and demonstrate how they can be implemented in LTE systems. We also present their performance assessment in a simulated LTE cellular environment which was obtained with open-source LTE link-level simulators developed by Technical University of Vienna. Finally, we offer our view on standardization perspectives of the considered physical-layer security extensions.**

***Index Terms*—Long-term evolution, physical-layer security, secret-key generation, secrecy coding, tag signals.**

I. Introduction

Securing wireless networks is a challenging engineering task. Most of security methods currently in use rely on cryptographic techniques employed at the upper layers of wireless networks. For cryptographic solutions to work, users and network access points must first share a common secret, for example, a cryptographic key. In general, these secret keys could be pre-shared or they can be exchanged by key exchange protocols. Cryptographic solutions have, however, a number of disadvantages. First of all, shared secret keys are difficult to establish at the early stages of the radio access protocol. Furthermore, encryption and decryption processes introduce extra delays and require additional computing resources which reduce energy efficiency.

Physical-layer security (PHYSEC) solutions are not based on cryptographic algorithms or secret keys, though they may support such solutions. Physical-layer security techniques take advantage of the physical characteristics of radio transmitters and radio channels, for example, transmitter nonlinearities, channel dispersion, and channel fading. In physical-layer security solutions only the signals at the physical layer are processed and thus the security of wireless communication systems is enhanced in a simple and energy-efficient way.

In this paper we consider three possible applications of physical-layer security and discuss their implementation aspects in the LTE cellular systems. Namely, these applications areas are PHYSEC-based authentication, PHYSEC-based key generation, and PHYSEC-based confidentiality. The goal of this paper is to demonstrate the feasibility and usefulness of PHYSEC-based extensions by assessing their performance in a simulated LTE-based cellular environment.

This work was supported by the PHYLAWS project funded by the European Commission under Grant Agreement FP7-ICT-317562-PHYLAWS.

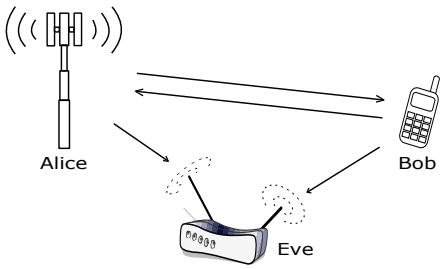

Fig. 1. A communication scenario with legitimate transmitter (Alice), intended receiver (Bob), and eavesdropper (Eve).

The remainder of the paper is organized as follows. First, in Section II we present the system model. We describe the selected physical-layer security extension that can be used in LTE cellular networks in Section III. The performance of the selected security extension is presented in Section IV. Finally, in Section V, the paper concludes with the discussion and summary of the main findings.

II. System model

We consider a communication scenario, shown schematically in Fig. 1, where Alice and Bob attempt to communicate securely in the presence of an eavesdropper Eve. We assume that Alice, Bob, and Eve can be equipped with many antennas.

The eavesdropper Eve is assumed to be passive, that is, Eve does not transmit any signals. Consequently, neither Alice nor Bob can be aware of Eve's presence which, in turn, implies that channel state information (CSI) of Alice-Eve and Bob-Eve channels is not available to Alice and, respectively, to Bob.

Since many physical-layer security techniques rely on the channel reciprocity property, the assumption which can be satisfied only in a time-division-duplex (TDD) mode, we exclusively focus on the TDD mode.

For performance assessment, we use MATLAB-based LTE link-level simulators [1] developed by Technical University of Vienna. The simulators implement standard-compliant LTE downlink and LTE uplink transceivers with their main features, i.e., basic channel models, modulation and coding,

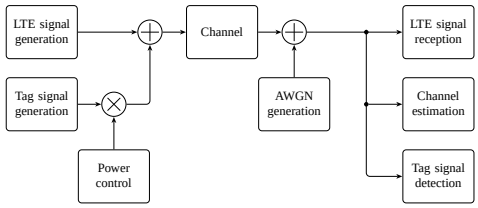

Fig. 2. Signal processing in a proposed LTE system with tag signals.

multiple-antenna transmission and reception, channel estimation, multiple-users scenarios, and scheduling.

The LTE link-level simulators include, among other basic channel models, WINNER II channel model. Unfortunately, WINNER II model is not suitable for our simulations. For some PHYSEC-based schemes, the channels seen by Bob and Eve need to show a distance-dependent correlation, which WINNER II model cannot model. For that reason, the QuaDRiGa channel model [2], which can produce correlation between Alice-Bob, Alice-Eve, and Bob-Eve channels, has been used. We mainly focus on indoor office (A1), urban micro-cell (B1), and rural macro-cell (C2) environments [3].

III. Proposed physical-layer security extensions

A. Authentication with tag signals

The main purpose of PHYSEC-based authentication is to recognize, already on the physical layer, the identities of the communication parties.

In LTE cellular networks, devices can authenticate each other by exchanging low-power signals, commonly referred to as tag signals [4]. Tag signals are transmitted at the same time, at the same frame/timeslot, and at the same carrier frequency as the user signal using uncoordinated spread-spectrum techniques to prevent jamming [5]. The full description of the tag-signal-supported authentication protocol can be found in [4]. A simplified block diagram of the LTE communication link which employs tag signals as means of early-stage authentication is shown in Fig. 2.

The dominant signal is generated by the standard-compliant transmitter model of the LTE link-level simulator. The low-power tag signal, on the other hand, is selected from the set of Kasami sequences. Since one subframe in LTE system consists of 30720 basic time units T_s, we select the set of Kasami sequences with length $N = 16384$ chips as the set of available tag signals. Thus, within one LTE subframe, or equivalently within $T_f = 1$ ms, Bob is guaranteed to receive a full copy of a sequence without a prior synchronization, cf. [5].

Kasami sequences have nearly optimal autocorrelation properties, which implies that the tag signal occupies the bandwidth comparable with the sampling frequency. Such wideband signals cannot normally be transmitted in LTE systems due to the strict requirements on the out-of-band RF emissions power levels. More precisely, the 3GPP technical specifications [6, Sec. 6.6.2] and [7, Sec. 6.6.2] define the maximum power levels of -30 dBc and -45 dBc for uplink and downlink transmissions, respectively. These out-of-band power levels are measured with respect to the carrier power level (dBc).

The out-of-band emissions are minimized by applying low-pass filtering. A standard root-raised-cosine filter with a roll-off factor $\alpha = 0.22$ is used. We assume that the transmission power level of tag signals is at most -10 dB with respect to the LTE signal power level. Consequently, the attenuation of low-pass filter in the stopband needs to be at least 35 dB. For example, we found that for transmission bandwidth $B = 20$ MHz, the sufficient length of the impulse response to meet the minimum attenuation level of 35 dB at frequencies $f > 11$ MHz is $M = 23$ taps.

For security purposes, the impulse response of the channel is estimated using tag signals rather than pilot signals, cf. [4]. In the receiver, we use compressive sensing method [8] to obtain channel estimates. The main reason to use compressive sensing method as an alternative to, for example, conventional least-squares channel estimation method, is taking advantage of channel sparsity. In other words, we do not estimate the channel over the full length of the cyclic prefix but estimate the $L = 20$ first strongest multipaths using compressive sensing method with extended orthogonal matching pursuit algorithm (OMP). See [8] for details of the channel estimation algorithm.

We define the estimation error of the channel impulse response as

$$\varepsilon = \sum\nolimits_{l=1}^{L} \left| \frac{h_l}{\|\boldsymbol{h}\|_2} - \frac{\hat{h}_l}{\|\hat{\boldsymbol{h}}\|_2} \right|^2 \tag{1}$$

where $\|\boldsymbol{x}\|_2$ is the 2-norm of the vector $\boldsymbol{x}$, the vector of channel estimates is denoted by $\hat{\boldsymbol{h}} = (\hat{h}_0, \hat{h}_1, \ldots, \hat{h}_{L-1})$, and the vector of true channel coefficients is $\boldsymbol{h} = (h_0, h_1, \ldots, h_{L-1})$.

The presence of tag signal is detected by a simple filter matched to the transmitted tag signal [4]. The output of the matched filter is sampled, normalized by the power of the interference signal and compared to the decision threshold. If the sample at the output of the matched filter exceeds the decision threshold, the tag signal is assumed to be present. The decision threshold is determined using cell-averaging constant-false-alarm-rate algorithm (CA-CFAR) [9, Sec. 7.2] with 64 guard samples, 20 training samples, and probability of false alarm set at 1 per cent.

B. Secret-key generation

The main purpose of PHYSEC-based secret-key generation is to use a small amount of secret information in key generation. In wireless systems, the secret information is typically extracted from the communication channel which acts as a shared source of randomness.

A general secret-key generation process consists of randomness extraction from the channel estimates followed by channel decorrelation, quantization, information reconciliation, and privacy amplification steps [10]. Since secret-key generation process does not require any significant changes in the LTE signal processing chain, we do not present a specific block diagram of the scheme.

In the random extraction sub-process, Alice and Bob estimate channel state, radio signal strength, or phase information.

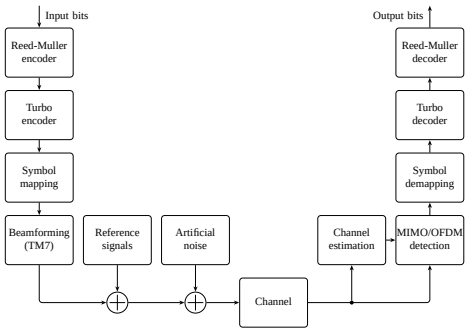

Fig. 3. Signal processing in a proposed LTE system with secrecy coding.

Since in the LTE systems, the estimates of the channel frequency response are readily available, we directly use them. In the downlink direction, Bob estimates the channel frequency response using downlink reference signal (DL-RS). In the uplink direction, on the other hand, Alice uses demodulation reference signal (DMRS) sent by Bob to estimate the channel. To ensure that the channel estimates obtained by Alice and by Bob are as similar as possible, the channel estimates are obtained at adjacent subframes, when transmission direction is switched from the uplink to downlink.

The main goal of the channel decorrelation step is to reduce the detrimental effect of possible correlation among estimates of channel coefficients by a careful selection of the estimates that will be later quantized, cf. [10].

The quantization of the channel coefficient estimates is performed based on the number of regions to be used and the empirical cumulative distribution function obtained from the real and imaginary parts of the channel coefficients. To improve the agreement between Bob and Alice, an alternating map is provided to Bob by Alice. The alternating map is obtained with the channel quantization alternating (CQA) algorithm [11].

Next, an information reconciliation step is performed to reduce a possible key mismatch between Alice and Bob. The information reconciliation step is based on secure sketches [12] with BCH error-correcting code, whose parameters depend on the SNR. However, some information about the key can be leaked to Eve through this step, hence a final step of privacy amplification is used to compensate for the information leaked to Eve about the secret key. This step uses two-universal family of hash functions [13].

Full details of the proposed secret-key generation algorithm can be found in [10].

C. Secrecy coding

The main purpose of PHYSEC-based secrecy coding is to maximize data transmission rate between Alice and Bob with a secrecy constraint on the information leakage towards eavesdropper Eve. The secrecy code must also provide a reliable link between Alice and Bob. In other words, the main task is to design secrecy-coding scheme that provides both reliability and secrecy without using secret keys [14].

Secrecy capacity, that is, the maximum transmission rate of secure communication between Alice and Bob, is a relative measure, involving the difference of data rates between Alice and Bob and Alice and Eve. It is thus intuitively understandable that to maximize secrecy capacity Alice needs to provide a radio advantage at Bob against Eve. Following the proposal in [14], Alice provides radio advantage by combination of beamforming and artificial noise generation. The radio advantage is the difference between the signal-to-interference-plus-noise (SINR) ratios at Bob and Eve:

$$\mathrm{SINR}_{\mathrm{Bob}} = \frac{\mathrm{E}[|\boldsymbol{H}_{\mathrm{Bob}}(k,n)\boldsymbol{w}(k,n)s(k,n)|^2]}{\mathrm{E}[|\boldsymbol{H}_{\mathrm{Bob}}(k,n)\boldsymbol{z}(k,n)|^2] + \sigma^2_{\mathrm{Bob}}} \quad (2)$$

$$\mathrm{SINR}_{\mathrm{Eve}} = \frac{\mathrm{E}[|\boldsymbol{H}_{\mathrm{Eve}}(k,n)\boldsymbol{w}(k,n)s(k,n)|^2]}{\mathrm{E}[|\boldsymbol{H}_{\mathrm{Eve}}(k,n)\boldsymbol{z}(k,n)|^2] + \sigma^2_{\mathrm{Eve}}} \quad (3)$$

where $\boldsymbol{H}_{\mathrm{Bob}}(k,n)$ is the channel frequency response at Bob, $\boldsymbol{H}_{\mathrm{Eve}}(k,n)$ is the channel frequency response at Eve, $\boldsymbol{w}(k,n)$ is the beamforming vector, $\boldsymbol{z}(k,n)$ is the artificial noise vector, and $s(k,n)$ is a sample of information-bearing signal at time k and subcarrier n. AWGN variances at Bob and Eve are denoted by σ^2_{Bob} and σ^2_{Eve}, respectively.

Designing secrecy codes for continuous channels is a challenging task. However, as discussed in [15], polar codes provide strong security for discrete channels. Thus, we propose to use a concatenated secrecy-coding scheme where the outer polar code is concatenated with the inner forward-error-correcting code, the scheme that is advocated in [14]. The inner code provides reliability and the outer code provides secrecy. The signal processing chain of the proposed secrecy-coding scheme is schematically shown in Fig. 3.

In LTE systems the beamforming is defined for downlink transmission direction as Transmission Mode 7 (TM7). For that reason, we consider only the secrecy coding in downlink direction. The optimal beamforming coefficients are determined from the channel coefficient estimates calculated by Alice from the uplink transmission of reference signals sent by Bob, assuming that TDD transmission mode is in use. We use a single beamforming coefficient per resource block.

The artificial noise implementation is based on the scheme presented in [16]. It uses the channel coefficients to extract an orthonormal basis of the channel vector space. The power allocated to the artificial noise is the same as the power allocated to the information-bearing signal, hence the signal power is halved compared to the case when no artificial noise is used. It should be noted that the artificial noise can be added to all symbols or only to the pilot symbols. The choice depends on the type of receiver Eve is able to implement. If Eve relies on the sole pilot tones, adding the noise to those is enough to degrade her performance and it is the most efficient choice as it does not degrade the performance at Bob by reducing only very little the power attributed to the signal.

In LTE systems, the channel coding is implemented with turbo codes. Consequently, the proposed secrecy-coding scheme is implemented by adding an outer polar code to the

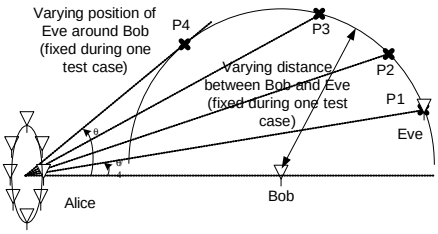

Fig. 4. Spatial location of Bob and Eve with respect to Alice.

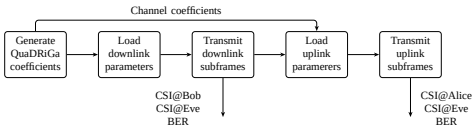

Fig. 5. Block diagram of the simulation process for the use of tag signals.

existing turbo code. The outer code could be one of the nested polar codes designed in [14].

IV. Simulation results

The main goal of simulations is to evaluate the performance of the proposed PHYSEC-based techniques in a realistic environments using QuaDRiGa channel models. The main focus is on indoor office (A1), urban micro-cell (B1), and rural macro-cell (C2) environments as defined in [3]. We study physical-key generation, secrecy coding with beamforming and artificial noise generation as well as tag-signal-based channel estimation, detection, and processing of tag signals.

The LTE carrier frequency is 2.6 GHz and the available channel bandwidth equals 10 MHz unless stated otherwise. The relative location of Alice, Bob, and Eve is shown in Fig. 4. All simulation runs include $1\,000$ subframes, i.e., 500 subframes in each transmission direction. In the downlink direction, Bob and Eve use least-squares method to estimate the respective Alice-Bob and Alice-Eve channels. Similarly, in the uplink direction, Alice and Eve use least-squares method to estimate, respectively, Bob-Alice and Bob-Eve channels. The average SNR are obtained by averaging corresponding instantaneous SNR values over the duration of the simulation. We assume that received signals are perfectly synchronized. The observed figures-of-merit include bit-error rate, block-error rate, throughput, channel estimation errors, signal-to-interference-plus-noise ratios, established radio advantage of Bob over Eve, and mismatch of secret-key bits.

A. Authentication with tag signals

The simulations process for testing the tag-signal processing algorithms is shown in Fig. 5. We assume that Eve knows neither the Kasami sequence used by Alice in downlink nor Kasami sequence used by Bob in uplink. She may try to guess it or she may use brute-force search method to find the right one. The channel bandwidth equals 20 MHz.

In Fig. 8 we plot the average bit-error rates obtained for a single-antenna system with 16-QAM modulation and 1/3 coding rate in an urban micro-cell scenario. The presence of tag signal impairs detection capabilities of LTE detector because the tag signal is seen as additional noise component. As expected, the larger the value of tag-to-signal ratio (TSR), the worse performance of LTE detector is. However, in some cases and scenarios, the turbo-decoder is able to compensate for the self-interference caused by an additional tag-signal.

We plot the mean value of the channel estimation error achieved by Bob and Eve in an urban micro-cell scenario in Fig. 9. It can be seen that Bob is able to accurately estimate the channel whereas Eve is not able to do that, mainly because she does not know the tag signal. As expected, the accuracy of the estimates improves with tag-to-signal ratio.

In Fig. 10 we plot the probabilities of successfully detecting the tag signals in an urban micro-cell scenario. It can be seen that Bob is able to detect the presence of the tag signals with high probability provided that both the signal-to-noise ratio and the tag-to-signal-ratio are sufficiently large. On the other hand, Eve is not able to detect reliably the presence of the tag signals. More precisely, Eve's probability of detection does not exceed 8 per cent regardless of the tag-to-signal ratio. The upper limit of 8 per cent comes from the fact that there are 127 Kasami sequences of length $N = 16384$ chips and Eve can guess the correct sequence with probability 1/127.

B. Secret-key generation

The simulations process for testing the secret-key generation algorithms is shown in Fig. 6. First, QuaDRiGa channel coefficients are created and stored in the file. The channel coefficients are first used in the downlink LTE simulator and then in the uplink LTE simulator. At the end of a single run, the secret keys generated at Alice, Bob, and Eve are compared.

We assume that Alice is a base station and thus her location is fixed. Bob and Eve, on the other hand, are mobile terminals and follow the same track at the same speed, which in our simulations is a straight line. Alice uses four antennas placed uniformly on a line and both Bob and Eve are equipped with two antennas. The minimum distance between Bob and Alice in indoor, micro-cell, and macro-cell scenarios has been set to 1, 10, and 50 m, respectively. Similarly, mobiles' speed has been set to 1 m/s, 2 m/s, and 14 m/s in indoor, micro-cell, and macro-cell environments, respectively. Eve can be placed at various distances from Bob. The radio propagation can either be line-of-sight (LOS) or non-line-of-sight (NLOS).

The secret-key generation algorithm produces 127-bit binary keys. In the decorrelation step, several decorrelation thresholds have been tested and the final choice was based on the trade-off between the number of keys and the extracted keys randomness. Namely, we found that fixing both timing and frequency decorrelation T_t and T_f to 0.5 offers the optimal trade-off. The results with and without spatial decorrelation are presented. When spatial decorrelation is used in a LOS environment, the LOS component is obviously removed by decorrelation step. In the quantization step, two regions are used for the quantization of the real and imaginary part of the

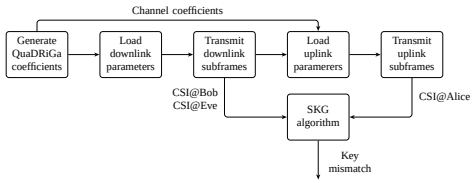

Fig. 6. Block diagram of the simulation process for the use of secret key generation.

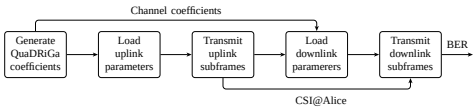

Fig. 7. Block diagram of the simulation process for the use of secrecy coding.

pre-processed channel coefficients. In information reconciliation step, the coding rate of the BCH code is selected such that Bob is able to correct the maximum number of errors at each simulation. Finally, the quality of keys is verified using the tests presented in [10].

The empirical cumulative distribution functions (cdf) of the bit-error-rate between the keys obtained by Bob and Eve are shown in Fig. 11. These results were obtained for an urban micro-cell radio propagation environment under assumption that Bob and Eve are moving on a straight line at 2 m/s. The first and the second rows show the results for the LOS scenario without spatial decorrelation step and with spatial decorrelation step, respectively. The third and fourth rows present the corresponding results for the NLOS scenario. The first column shows the results at Bob and the next columns at Eve for an increasing distance between Bob and Eve.

The results presented in Fig. 11 demonstrate that the mismatch between Bob's and Alice's keys reduces as the SNR increases. Furthermore, in a LOS micro-cell scenario, a minimum distance of one wavelength λ between Bob and Eve is needed to ensure that Eve cannot extract the correct key provided that spatial decorrelation pre-processing step is used. However, the drawback of spatial decorrelation is that the higher SNR is needed for Bob to estimate the right key. In terms of key quality, the randomness tests were passed for more than 99 per cent of the keys after amplification, with or without spatial decorrelation, and for both LOS and NLOS. The use of spatial decorrelation in LOS increased the number of keys extracted.

Similar results were obtained for the indoor radio propagation environment but are not presented due to space limitations. The situation in macro-cell environment is usually more challenging, the algorithm still does not protect well Alices and Bobs keys when Eve is at a distance 10 wavelengths from Bob in LOS even when using spatial decorrelation. In macro-cell environment spatial decorrelation protects Bob's and Alice's secrecy in both LOS and NLOS cases.

C. Secrecy coding

The simulations process for testing the secrecy-coding scheme is shown in Fig. 7. We assume that Alice uses a circular antenna array with 4 antennas, Bob and Eve have one antenna each and use the same receiver algorithms. Furthermore, we assume that the distance between Alice and Bob is 15 m and the distance between Bob and Eve is 11.5 m, which corresponds to 100 wavelengths at carrier frequency 2.6 GHz. As shown in Fig. 4, Eve is located at position P1, P2, P3, or P4. We use (56,330,638) Reed-Muller code from [14] as secrecy code.

The cumulative distribution function (cdf) of Bob's SINR as well as the complementary cdf of Bob's radio advantage over Eve are shown in Fig. 12 under assumption of urban micro-cell radio environment with line-of-sight. We plot only two cases: beamforming without artificial noise and beamforming with artificial noise on all symbols. Application of artificial noise to the pilot tones only leads to slightly larger radio advantage results compared to the case when only beamforming is applied. For that reason, we do not plot separate results for the case where artificial noise is applied to pilot signals only.

The results in Fig. 12 suggest that combined beamforming and artificial noise provides a better radio advantage than beamforming alone. In the SNR range under study, beamforming is not so sensitive to channel estimation errors. On the contrary, artificial noise is rather sensitive to channel estimation errors because any error in channel estimation would cause a leakage of artificial noise into Alice-Bob channel. The channel estimation errors get smaller as SNR gets larger and the radio advantage improves with improvement in SNR.

The location of Eve with respect to Alice and Bob affects the radio advantage. For example, if Eve is closer to Alice than Bob, her signal is obviously stronger than Bob's signal and the radio advantage is reduced.

In Fig. 13 we plot Eve's bit-error rates as function of radio advantage in urban micro-cell scenario for QPSK modulated signal at SNR equal to 5 dB and artificial noise applied to all symbols. It can be seen that radio advantage of 5–6 dB is sufficient to preclude Eve from reliably decoding the transmitted signal.

V. Discussion and conclusions

We considered three possible applications of physical-layer security: authentication with tag signals, secret-key generation, and secrecy coding with combined beamforming/artificial noise generation. We presented how the aforementioned physical-layer security enhancements can be implemented in LTE cellular systems.

The main observation is that tag signals have to be specially designed to meet the out-of-band emission requirements of LTE systems. In practice it means that the direct-sequence spread-spectrum signal needs to be low-pass filtered to limit its bandwidth. It was also found that the presence of the tag signal impairs the proper detection of the LTE signal. The tag signal is seen as additional noise in the LTE receiver. However, in some scenarios, the turbo decoder is able to

compensate for the effect of the additional noise. The practical values of tag-to-signal-ratio should remain between -20 dBc and -10 dBc to achieve reasonable tradeoff between channel estimation performance, tag detection probability, and out-of-band transmission power levels.

LTE standardization of the proposed authentication scheme may require a lot of changes in LTE standards and thus a close cooperation between radio-access network and service and system aspects working groups is needed.

Secret-key generation algorithms implemented in the LTE simulator have proven to work well in most radio propagation environments. The minimum required distance between Bob and Eve to protect the keys extracted at Alice and Bob depends on the radio environments, whether LOS component is present or not, and whether spatial decorrelation is in use or not.

In indoor and micro-cell environments, the minimum distance between Bob and Eve that prevents Eve from deriving the correct key is typically comparable with the carrier wavelength in both LOS and NLOS environments. Moreover, spatial decorrelation needs to be used in LOS environments to prevent Eve from getting any keys correctly. However, using spatial decorrelation increases the SNR needed to get a match between Alice's and Bob's keys. In NLOS micro-cell environments, more keys can be produced within the same time interval and the use of spatial decorrelation is not required to generate good-quality keys.

In macro-cell environments, on the other hand, the keys are not protected if the distance between Bob and Eve is less than approximately 10 wavelengths in LOS. However, the separation distance of 10 wavelengths is sufficient in NLOS macro-cell environments. Furthermore, in macro-cell environments, spatial decorrelation helps protect Bob's and Alice's secrecy in both LOS and NLOS cases.

In all simulations, the quality of the key was quite high after privacy amplification, often leading to more than 99 per cent of the keys passing the randomness tests used.

LTE standardization of secret-key generations does not require any significant amendments to the current version of standards because the channel estimates are readily available in the physical layer. Depending on where the keys are needed, they may need to be made available to higher layers.

It is challenging to design a reliable secrecy coding scheme. The main difficulty comes from the fact that one needs to establish and precisely control the radio advantage, which is challenging because neither Alice nor Bob knows Eve's location or channel matrix when Eve is passive eavesdropper, the point-to-multipoint fading channel is constantly changing, and channel estimation errors cause leakage of artificial noise into Bob's channel. Thus, the combination of beamforming and artificial noise seems more appropriate for high SNR regimes where channel estimation errors are smaller. Furthermore, adaptive power allocation between artificial noise and information-bearing signal will also improve the radio advantage but would require higher output power to maintain the minimum required SINR for successful transmission. Finally, if some knowledge on the environment and possible locations of Eve can be obtained, chances of obtaining sufficient radio advantage are greatly improved. Further work is needed to either improve the artificial noise or apply a different transmit-precoding method.

LTE standardization of the proposed secrecy-coding scheme requires the provision that base station is allowed to add artificial noise to the transmitted signal. This provision is not defined in the standards. Given the current trend in wireless communication of intensification of usage of resources, e.g. through spatial multiplexing, with an increase of the level of interference, this could be a challenge. However, artificial noise could still be allowed in specific scenarios such as Internet of Things or machine-to-machine communications, where chances of interfering with other cells or users are minimal.

REFERENCES

[1] C. Mehlfuehrer, J. C. Ikuno, M. Simko, S, Schwarz, M. Wrulich, and M. Rupp, "The Vienna LTE simulators – Enabling reproducibility in wireless communications research," *EURASIP Journal on Advances in Signal Processing*, vol. 21, 2011.

[2] S. Jaeckel, L. Raschkowski, K. Brner and L. Thiele, "QuaDRiGa: A 3-D multicell channel model with time evolution for enabling virtual field trials," *IEEE Trans. Antennas Propag.*, vol. 62, pp. 3242–3256, June 2014.

[3] P. Kyösti *et al.* (2007). *WINNER II Channel Models*, [Online] Available: https://www.ist-winner.org/WINNER2-Deliverables/D1.1.2v1.1.pdf.

[4] R. Molière, F. Delaveau, T. Mazloum, and A. Sibille, "Tag signals for early authentication and secret key generation in wireless public networks," in *Proc. EuCNC*, 2015.

[5] C. Pöpper, M. Strasser, and S. Capkun, "Anti-jamming broadcast commmunication using uncoordinated spread spectrum techniques," *IEEE J. Sel. Areas Commun.*, vol. 28, pp. 703–715, Jun. 1998.

[6] 3GPP TS 36.101, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception," v12.6.0 (2015-04).

[7] 3GPP TS 36.104, "Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception," v12.5.0 (2015-01).

[8] S. K. Sahoo and A. Makur, "Signal recovery from random measurements via extended Orthogonal Matching Pursuit," *IEEE Trans. Signal Process.*, vol. 63, pp. 2572–2581, May 2015.

[9] M. A. Richards, *Fundamentals of Radar Signal Processing*. McGraw Hill, 2005.

[10] C. Kameni Ngassa, R. Molière, F. Delaveau, T. Malzoum, and A. Sibille, "Secret key generation from WiFi and LTE reference signals" in *Proc. SDR-WinnComm*, 2016.

[11] J. Wallace and R. Sharma, "Automatic secret keys form reciprocal MIMO wireless channels: Measurements and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, pp. 381–392, Sep. 2010.

[12] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 28, pp. 97–139, Jan. 2008.

[13] C. Bennet, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, pp. 1915–1923, June 1995.

[14] C. Kameni Ngassa, J.-C. Belfiore, R. Molière, F. Delaveau, and N. Shapira, "Combining artificial noise, beamforming, and concatenated coding schemes to effectively secure wireless communications" in *Proc. SDR-WinnComm*, 2016.

[15] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, pp. 6428–6443, Oct. 2011.

[16] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO-OFDM systems by beamforming and artificial noise generation," *PHYCOM: Physical Communication*, vol. 4, pp. 313–321, Apr. 2011.

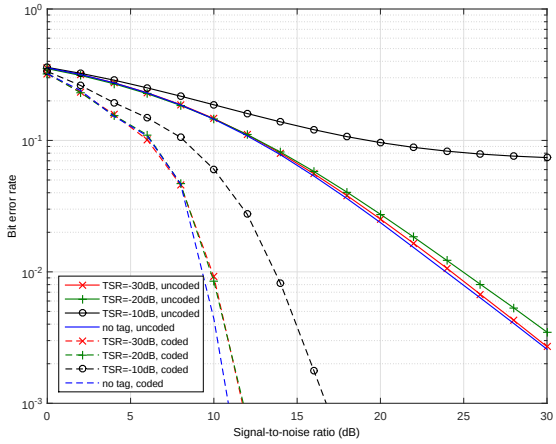

Fig. 8. Bit error rate performance in an urban micro-cell scenario with 16-QAM modulation and 1/3 coding rate.

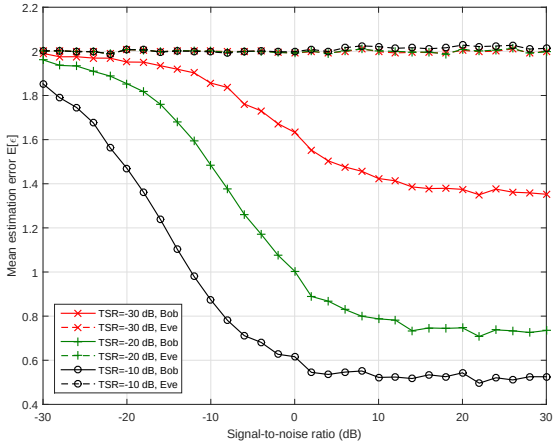

Fig. 9. Mean estimation error $E[\varepsilon]$ in an urban micro-cell scenario.

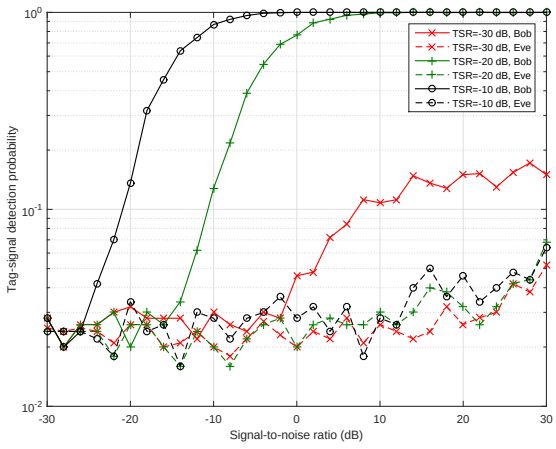

Fig. 10. Tag signal detection probability in an urban micro-cell scenario.

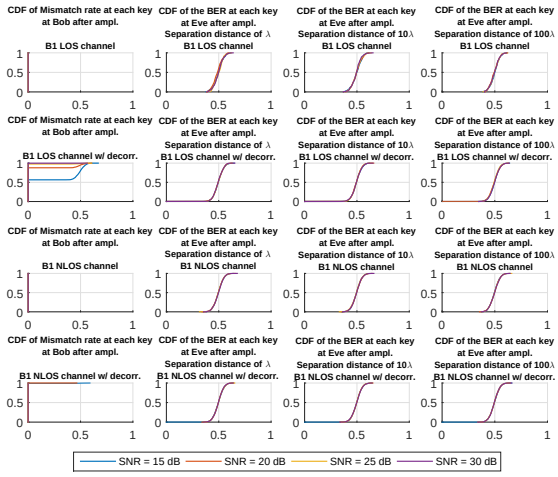

Fig. 11. Cdf of the BER between the keys (over all channel realizations) after privacy amplification at Alice and those at Eve versus the separation distance between Bob and Eve and for various SNR values, for the SKG-B1 straight movement cases, with LOS or NLOS and with or without spatial decorrelation.

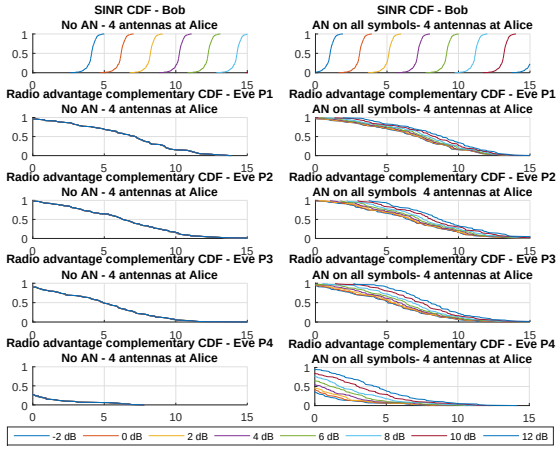

Fig. 12. Radio advantage in an urban micro-cell scenario.

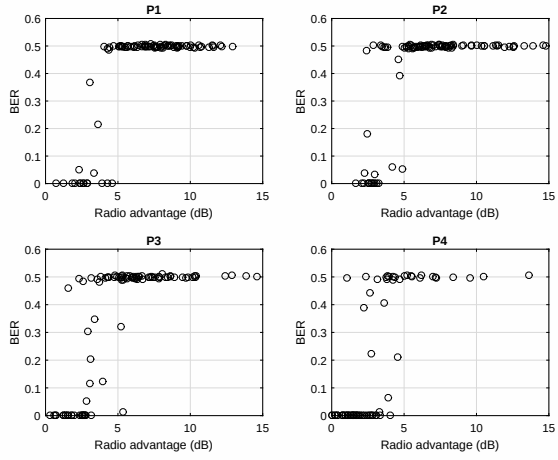

Fig. 13. Eavesdropper's BER after secrecy decoding as function of radio advantage in an urban micro-cell scenario.