5. Conclusions and Proposals for Standardization

5.1. Conclusions

Tag Signals

The simulator for testing transmission, reception, and processing of tag signals in LTE has been implemented and extensive simulations have been performed. The transmission, interception, and processing of tag signals was simulated in pre-selected QuaDRiGa scenarios. Namely, we studied indoor office scenario, urban micro-cell scenario, and urban macro-cell scenario. We considered both single- and multiple-antenna scenarios. We have also studied the impact of self-interference caused by tag signals on the detection and decoding of LTE signals with different modulation and coding schemes. Finally, we separately considered downlink and uplink directions.

Based on the results presented in the previous deliverable, that is, Deliverable 6.2, and the current deliverable the following conclusions can be drawn regarding the use of tag signals for physical-layer-based authentication.

The main observation is that tag signals have to be specially designed to meet the out-of-band emission requirements of LTE systems. More precisely, the 3GPP technical specifications [3GPP 36.101, Section 6.6.2] and [3GPP 36.104, Section 6.6.2] define the maximum power levels for uplink and downlink transmissions, respectively. The maximum power level for out-of-band transmissions is -30 dB for the user equipment (UE) and -45 dB for the base station (BS). These out-of-band power levels are measured with respect to the carrier power level. Consequently, to meet those requirements, the highest allowable value of tag-to-signal ratio is -45 dB in downlink direction and -30 dB in the uplink direction. However, as the tag detection probability results suggest such low-power tag signals cannot be reliably detected by matched filter detectors and will generally result in poor channel estimation accuracy. For those reasons, the tag signals need to be transmitted at higher power levels and undergo low-pass filtering to limit their bandwidth. A number of low-pass filters have been tested in [PHYLAWS_D6.2], including truncated ideal low-pass filters, filter designs based on prolate spheroidal wave functions, and conventional root-raised-cosine filters. It was found that root-raised-cosine filters offer reasonable trade-off between performance and complexity.

In addition, it was found that least-squares method of estimating the channel works reasonably well when tag signals are not low-pass filtered. On the contrary, when tag signals are low-pass filtered, the least-squares method performs quite bad. The main reason for bad performance is the noise amplification during estimation process. For that reason, another method of estimating the channel was proposed and tested. Namely, instead of least-squares method, we have used a channel estimation method based on compressive sensing with extended Orthogonal Match Pursuit algorithm proposed in [Sahoo2015]. With compressive sensing method, one estimates the multipath components in iterative way. In other words, there is no need to invert the signal matrix.

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. Low-order modulation, such as QPSK, is virtually not affected by the presence of additional tag signals. On the contrary, high-order modulations such as 16-QAM and 64-QAM are affected by the presence of additional source of interference. In practice, for 64-QAM modulation, the power of the tag signal needs to be limited to more than 10 dB below dominant LTE signal to facilitate reliable decoding of LTE signal. This observation suggest that the power level of tag signal should be adaptively controlled depending on the modulation format. However, advanced and sophisticated decoders are able to cope with additional self-interference caused by tag signals. This fact is reflected in our simulation results where base station decoder performs better than the user equipment decoder.

In all simulation cases which we studied, the tag signal power level of –30 dB with respect to the LTE signal was too small to guarantee reliable tag detection. Much better results were obtained for tag signals at power levels of –20 dB and –10 dB with respect to LTE signal. No significant difference in tag signal detection probabilities were observed in different radio scenarios, antenna configurations, and modulation formats. One challenge in the design of tag signals is related to the relatively small number of available Kasami sequences of length 16 384 chips. Namely, there are only 127 of unique sequences which makes the task of checking all possible sequences relatively easy for Eve, especially in single-antenna channels. In multi-antenna channels, where each transmit antenna can send unique Kasami sequence, the task of the eavesdropper is somewhat more difficult because it needs to identify a tuple of Kasami sequences. More precisely, if Alice uses two transmit antennas, Eve needs to check each of 127*126/2 = 8 001 possible pairs of Kasami sequences rather than only 127 Kasami sequences. With just 4 transmit antennas, the number of 4-tuples to be checked by Eve exceeds 10 million.

In general, the LTE simulation results are similar to WiFi simulation results presented in Deliverable 2.4 and Deliverable 4.1 with respect to the probability of reliable detection of tag signals and tag-signal-based channel estimation. The performance of channel estimation in LTE environment is slightly worse than in the WiFi environment

due to longer cyclic prefix and consequently the need to estimate the channel over longer period. Furthermore, in LTE systems, the tag signal needs to be low-pass filtered to meet the strict out-of-band transmission levels. This, in turn, constraints the tuning range of the tag-to-signal-ratio and the relevant design of the lengths and sets of tag signal according to the studies of WP4 task T4.1. More specifically, the practical values of tag-to-signal-ration should be in the range between -20 dB and –10 dB in order to achieve reasonable channel estimation performance and still meet the out-of-band transmission constraints.

In our simulations we have assumed baseline implementation of tag signal processing where tag signal decoder and LTE signal do not exchange any information. We speculate that significant performance improvement, especially in channel estimation and bit error rate performance, is possible when both decoders use self-interference cancellation blocks. More specifically, LTE signal receiver could try to subtract a local replica of the tag signal from the received signal before further processing. Similarly, the tag detection and channel estimation blocks could create a replica of a dominant LTE signal which is later subtracted from the received signal. This should improve the bit error rates of communicating parties and reduce the channel estimation error.

SKG

The SKG algorithm has been implemented in the LTE simulator and has proven to work well in most radio propagation environments. We shall note that compared to the results shown in WP5 our system is perfectly calibrated, hence the reciprocity is easy to assume and maintain. The mobility does not seem to impact the key establishment. Indeed, the channel estimates are extracted at adjacent subframes in the downlink and uplink hence the delay between channel estimates is 1 ms and the speeds considered in each propagation scenarios vary between 1 to 14 m/s. Time and frequency decorrelation need to be used to get good keys and reduce Eve's capability to extract keys. The minimum distance between Bob and Eve in order to protect the keys extracted at Alice and Bob depends on the radio environments (A1, B1, C2), whether there is LOS or NLOS, the use of spatial decorrelation, and the SNR.

In A1 and B1, the keys can be protected from Eve at a distance of λ in both LOS and NLOS. Spatial decorrelation needs to be used for LOS in A1 to prevent Eve from getting any keys correctly at a distance λ. The use of spatial decorrelation impacts the needed working SNR, as spatial decorrelation needs a higher SNR to lead to the same match between Alice and Bob compared to the situation when it is not used. Indeed, the LOS component is removed in the spatial decorrelation process. NLOS environments lead to more keys and does not require the use of spatial decorrelation.

The situation in C2 is more challenging, the minimum distance between Bob and Eve need to be larger than 10λ in LOS. In NLOS the situation is better as the algorithm already works already at a distance of 10λ. Spatial decorrelation protects Bob's and Alice's secrecy in both LOS and NLOS cases. The curved movement seems to be more challenging in LOS for which even spatial decorrelation does not prevent Eve from getting some keys right even at a distance of 100λ from Bob.

In all simulations, the quality of the key was quite high after amplification, leading often to all the keys satisfying the NIST frequency mono bit test randomness test. The MATLAB runstest were somehow less successful but still very high. These results are obtained using time and frequency decorrelation that greatly improves the keys' quality. Without time and frequency decorrelation some trials led to no key passing the test.

Secrecy coding

The main objective of the work has been in studying the radio advantage by combining beamforming and AN. We assumed that Alice had 4 or 8 antennas and Bob and Eve both used 1 antenna. Artificial noise applied to all subcarriers has proven to be the best choice to create radio advantage, at a cost of a higher transmission power for the same receiver SINR level at Bob.

The main observation from the simulations is that the secrecy coding scheme works provided that radio advantage is large enough. However, the required radio advantage level cannot be reliably created in most of the simulated test cases. This is a direct consequence of several causes. First of all, Eve is passive and thus Alice and Bob lack the knowledge of Eve's channel. Other plausible causes include the variations in the communication channel, the channel model itself, and inaccuracies in channel estimation which affect the calculation of the AN. It is also to be noted that the LTE transmission mode 7, which allows the use of beamforming, requires the beam vector to be constant over a whole resource block, which further decreases the effectiveness of beamforming and AN.

However, if some knowledge of the environment and possible position of Eve can be obtained, this can greatly improve the reliability of obtaining adequate radio advantage. We speculate that a realistic channel will provide more diversity and hence a more reliable RA level. Nevertheless, AN seems more appropriate for higher order modulation

and coding schemes for which the SNR at which they are applied is higher. Increasing the ratio of AN at the detriment of the data signal improves the RA but requires higher output power to maintain the required SINR for successful transmission. More work is needed to either improve the AN created or apply a different technique to increase the reliability. This is very challenging and a current research topic in academia with no solutions so far.

5.2. Proposals for standardization

Standards are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed or performed. Standards typically define protocols, procedures, and the minimum acceptable performance of a product or service. The actual selection of algorithms and their implementation such that the minimum acceptable performance is reached, is a task of product vendors or service providers.

For all the techniques studied herein, the standard-compliant model of an LTE system has been used with the least possible changes. In other words, we have focused on studying methods that require evolutional changes to the existing standards rather than revolution changes. The rationale for that approach is the fact that standards are difficult to change or alter once commercial services based on those standards are in use. Focusing on evolutional changes also allows a quicker acceptance and deployment of the techniques devised. However, some changes may still be needed and are listed in the following paragraphs.

Tag Signals

The authentication protocol that employs tag signals at physical layer is described in details in [PHYLAWS_D4.1, Section 4.1.2]. The protocol is based on exchange of messages between base station and user equipment. The protocol is potential subject of standardization because it describes how the tag-signal based authentication should be performed. We propose that the tag-signal based authentication procedure be optional. Since we have proposed physical-layer based authentication protocols, the proposition for altering the current standard should be addressed to Radio Layer 1 Working Group (RAN WG1) of 3GPP Radio Access Network Technical Specifications Group (TSG RAN) and Security Working Group (SA WG3) of 3GPP Service and Systems Aspects Technical Specifications Group (TSG SA).

In addition to that, the generation of tag signals should be subject to standardization. Kasami sequences, which were used in this study for simplicity, are not good candidates because their design is deterministic and the set of possible Kasami sequences is relatively small. Thus, for actual standardization, alternative methods of generating tag signals, which were described in [PHYLAWS_D4.2, Chapter 3], should be considered. The actual transmission power levels of tag signals should also be standardized. As our simulation results suggest, different power levels should be selected for difference modulation and coding formats. In other words, the values of tag-to-signal ratios for each modulation and coding scheme should be subject to standardization.

The combined signal, that is, a sum of dominant LTE signal and low-power tag signal, should satisfy the limits for out-of-band transmission. The maximum power levels of spurious emissions and corresponding spectra masks are already defined in the LTE standards. In this work, we have tested low-pass filtering as possible method to limit the out-of-band signal power levels. However, the selection and implementation of the method to limit the out-of-band transmission power levels should be left to the vendor.

In general, minimum acceptable performance levels for tag signal detection and relative channel estimation error given by (3.4) should be defined in the standards. A reasonable choice for tag signal detection probability is 99 per cent with 1 per cent false alarm probability. The relative channel estimation error, on the other hand, should remain below 0.2 to facilitate reliable and accurate channel estimation, see [PHYLAWS_D4.1, Section 4.4.3]. In this work, we have tested matched-filter detection, least-squares estimation, and compressive sensing estimation. However, the selection and implementation of the tag detection and channel estimation methods should be left to the vendor.

SKG

The needed inputs for the SKG algorithm, namely the channel estimates, are readily available in the physical layer, so there is no need for any changes in the standard regarding acquisition of channel state information. The simulations have shown the channel estimates obtained from available reference signals can be used successfully. Depending on which application uses the SKG algorithm, the estimates may need to be made available to higher layers.

However, the secret key generation procedure [PHYLAWS_D4.3, Chapter 4] consisting of pre-processing of channel estimates, quantization of channel estimation, information reconciliation step, and privacy amplification should be subject of standardization.

Secrecy coding

The radio advantage inducing technique is the key to the application of secrecy coding. In this study, the artificial noise and secrecy encoder are the only features that have been added to the standard LTE.

Artificial noise can only be applied when the interference it creates does not impair other transmissions. Given the current trend in wireless communication of intensification of the usage of resources, for example through spatial multiplexing, with an increase of the level of interference, this could be a challenge. However, AN could still be allowed on specific scenarios in which there is no chance to interfere with other cells or users.

Secrecy encoding schemes [PHYLAWS_D4.3, Chapter 5] should also be subject of standardization. Otherwise, interoperation of hardware from different vendors cannot be guaranteed.

The implementation of secrecy decoder is vendor specific. However, the minimum acceptable performance measured as achievable bit error rate for a given signal-to-noise-plus-interference ratio should be defined in the standard, e.g., for example, the minimum acceptable BER should be 10^{-5} at SINR = 5 dB for QPSK modulated signals, cf. Figure 38 of [PHYLAWS_D4.3].

6. References

[3GPP36.101] 3GPP TS 36.101, “Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception,” v12.6.0 (2015-04).

[3GPP36.104] 3GPP TS 36.104, “Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception,” v12.5.0 (2015-01).

[3GPP36.201] 3GPP TS 36.201, “Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description,” v12.0.0 (2014-09).

[3GPP36.211] 3GPP TS 36.211, “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation,” v12.5.0 (2015-01).

[3GPP36.212] 3GPP TS 36.212, “Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding,” v12.3.0 (2015-01).

[3GPP36.213] 3GPP TS 36.213, “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures,” v12.4.0 (2015-01).

[Berger2010] C. R. Berger, Z. Wang, J. Huang, and S. Zhou, "Application of compressive sensing to sparse channel estimation ", *IEEE Communications Magazine*, vol. 48, pp. 164-74, November 2010.

[BlochBarros2011] Physical-Layer Security, Cambridge University Press, 2011.

[Cepheli2013] Cepheli O. and G. Kurt, "Efficient PRY Layer Security in MIMO-OFDM: Spatiotemporal Selective Artificial Noise", 2013 IEEE 14th Inter. Symp. On WoWMoM, 6 p., June 2013.

[Holma2012] H. Holma and A. Toskala, LTE-Advanced – 3GPP Solution for IMT-Advanced, John Wiley & Sons Ltd, UK, 2012.

[Kyösti2007] IST-WINNER D1.1.2 P. Kyösti, et al., "WINNER II Channel Models", ver 1.1, Sept. 2007. Available: https://www.ist-winner.org/WINNER2-Deliverables/D1.1.2v1.1.pdf.

[Jaeckel2014] S. Jaeckel, L. Raschkowski, K. Börner and L. Thiele, "QuaDRiGa: A 3-D Multicell Channel Model with Time Evolution for Enabling Virtual Field Trials", *IEEE Transactions on Antennas Propagation*, vol. 62, pp. 3242-3256, June 2014.

[Landolsi1999] M. A. Landolsi and W. E. Stark, "DS-CDMA chip waveform design for minimal interference under bandwidth, phase, and envelope constraints", *IEEE Transactions on Communications*, vol. 47, pp. 1737-1746, November 1999.

[QuaDRiGa] http://www.hhi.fraunhofer.de/quadriga.

[Richards2005] M. A. Richards, *Fundamentals of Radar Signal Processing*, McGraw Hill, 2005.

[Sahoo2015] S.K. Sahoo and A. Makur, "Signal recovery from random measurements via extended Orthogonal Matching Pursuit ", *IEEE Transactions on Signal Processing*, vol. 63, pp. 2572-2581, May 2015.

[Walter2005] G. Walter and T. Soleski, "A new friendly method of computing prolate spheroidal wave functions and wavelets", *Applied and Computational Harmonic Analysis*, vol. 19, pp. 432-443, November 2005.