URSI-B EMTS 2025, Bologna, 23–27 June

Performance Analysis of Physical Layer Security Secrecy Key Generation in Indoor Environment

Alessandro Santorsola[(1)(2)], Giovanni Magno[(1)], Vincenzo Petruzzelli[(1)], Sabino Roberto Caporusso[(2)], and Giovanna Calò[(1)]
(1) Department of Electrical and Information Engineering, Polytechnic University of Bari, Bari, Italy
(2) Cybersecurity Lab, BV TECH S.p.A., 20123 Milan, Italy

Abstract

The heterogeneous nature of the Sixth-Generation (6G) communication systems, jointly with the rapid expansion of sensitive applications, bring several challenges to systems security. The Secrecy Key Generation (SKG) is a Physical Layer Security (PLS) technique in which two legitimate nodes negotiate a session key, taking advantage of the physical layer phenomena as a source of entropy. In this contribution, we investigate the impact of Uniform Linear Array (ULA) dipole spacing on the SKG performance considering an indoor application environment. We considered two legitimate nodes, i.e., Alice and Bob, that adopt the SKG protocol to negotiate their session key. A malicious node, i.e., Eve, tries to eavesdrop on the communication to obtain the key by performing the *on-the-shoulder* attack. Results demonstrate that smaller dipole spacings, i.e., $d \leq 0.5\lambda$ result in lower channel and key correlations between Eve and the legitimate nodes, enhancing security. Larger spacings, however, create periodic zones of moderate correlation, potentially aiding Eve under certain angular positions.

Keywords— Secrecy Key Generation, Physical Layer Security, Antenna Array, Indoor Radio Propagation

1 Introduction

The rapid expansion of sensitive applications such as the Internet of Things (IoT), vehicle networks and emerging sixth generation (6G) technologies require efficient solutions that ensure secure data transmission [1]. In addition, the heterogeneous nature of the upcoming communication systems brings several challenges to communication security. In particular, the open nature of the wireless medium exposes such communications to several risks, e.g., communication eavesdropping, etc. [2]. Traditionally, cryptographic methods, such as symmetric and asymmetric encryption, have been widely adopted to address communication security [3]. However, these approaches are not immune to cyberattacks. In addition, the computational limitations, protocol weaknesses, and/or advanced attacks, such as those leveraging quantum computing, could lead to sensitive data leakage [4]. In recent years, the Physical Layer Security (PLS) paradigm has emerged as a novel and complementary solution to ensure communication security by leveraging the inherent channel characteristics [2, 4]. The PLS paradigm exploits the physical properties of the communication channel, such as channel fading, noise, multipath, etc., to enhance the communication security with respect to a malicious node, i.e., the attacker [5]. Therefore, the PLS paradigm is particularly useful in wireless communication environments [6]. A promising approach that can be used also in hybrid crypto-PLS systems is the PLS-based Secrecy Key Generation (SKG) [2, 7]. SKG takes advantages of the reciprocity and randomness of the wireless channel as a source of entropy to generate session keys between two trusted nodes, i.e., Alice and Bob [4]. This ensures that if an eavesdropper, i.e., Eve, is in proximity to one of the trusted node, it cannot reconstruct the same key due to the spatial decorrelation of the radio channel [2]. In the literature, different works analyzed specific parts of the SKG protocol, however there are only a few that analyzed the impact of the antenna characteristics [6, 7]. In this work, we extend the results presented in [7], where the impact of a Line-of-Sight (LoS) indoor radio environments on SKG Key Performance Indicators (KPIs) in a Wi-Fi application context has been analyzed. In particular, the authors analyzed the 3GPP 38.901 Indoor LoS indoor radio channel, in which two legitimate Wi-Fi nodes, i.e., Alice and Bob, adopt the SKG to negotiate a session key. Whereas, a passive eavesdropper, i.e., Eve, tries to guess the session key by performing the so-called *on-the-shoulder* attack, i.e., Eve is located very close to Bob [2]. The proposed layout considered Alice as a Wi-Fi Access Point (AP) equipped with a 5-dipole Uniform Linear Array (ULA). This paper aims at extending the analysis and at putting in evidence the effect of the antenna radiation pattern variation due the variation of the dipole spacing on the SKG KPIs considering an indoor application environment. The main contribution of this paper is twofold: *(a)* evaluation of the legitimate and eavesdropper channel correlations as a function of ULA dipole spacing, and *(b)* evaluation of the key correlation and key mismatch rate between a trusted node and a passive eavesdropper in connection with the variation of Alice ULA dipole spacing. The rest of the paper is organized as follows. Section 2 describes the SKG key concepts and the analysis methodology. Section 3 evaluates the results of the numerical analysis. Finally, Section 4 concludes the work and reports the main findings.

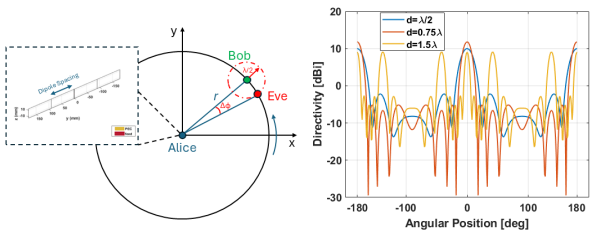
2 Background and Methodology

The SKG protocol typically consists of five stages [4]: *(i)* Authentication: Alice and Bob perform a series of operation to trust each other. *(ii)* Channel Probing: Alice and Bob

Parameters	Values	
	mean	standard deviation
Delay spread (DS)	-0.01 $\log_{10}(1+f_c)$ - 7.692	0.18
AOD spread (ASD)	1.60	1.18
AOA spread (ASA)	-0.19 $\log_{10}(1+f_c)$ + 1.781	$0.12\log_{10}(1+f_c)$ + 0.119
ZOA spread (ZSA)	$-0.26\log_{10}(1+f_c)$ + 1.444	$-0.06\log_{10}(1+f_c)$ + 0.264
Shadow fading (SF) [dB]	-	3
XPR [dB]	11	4
Number of clusters N	18	
Number of rays per cluster M	20	

Table 1. 3GPP 38.901 Indoor LoS channel model parameters [8]

exchange a pre-defined series of frames to probe the channel. *(iii)* Quantization: Alice and Bob generate a series of bits, i.e., a raw secrecy key, by quantizing the received signals at their side. *(iv)* Reconciliation: Alice and Bob correct mismatch errors that could occur during the data exchange. Finally, *(v)* Privacy Amplification: Alice and Bob apply a one-way cryptographic function to maximize the entropy. The SKG protocol relies on two fundamental hypotheses: *(a)* the propagation channel of the legitimate nodes is reciprocal. Thus, Alice and Bob experience the same radio channel, and *(b)* Eve cannot be superimposed. Therefore, Eve radio channel differs from the legitimate nodes channel [9]. We adopted the model presented in [6] and [7], where the radio channel model has been implemented with *QuaDRiGa*. *QuaDRiGa* is a well-known geometry-based stochastic model, taking into account all relevant propagation effects [10]. Fig. 1 (a) shows the selected simulation



(a) **(b)**

Figure 1. *(a)* Schematic of Alice, Bob and Eve positions. Bob and Eve move along a circle (i.e., black circle) of radius r centered at Alice position. Alice Uniform Linear Array (ULA) is also schematized in the inset. *(b)* Alice ULA directivity as a function of Bob angular positions for dipoles spacing d equal to $\lambda/2$, 0.75λ, and 1.5λ

layout. Bob and Eve move around a circular track of a radius r equal to 10 m, i.e., the black circle. Their trajectory is centered at Alice position. Alice, Bob and Eve height is fixed at 1.5 m. Bob and Eve are both equipped with a half-wavelength dipole antenna. The chosen Wi-Fi standard is the 802.11ax [11] at a carrier frequency f_c of 5 GHz, and the transmitted power is set to be equal to 20 dBm both in uplink and downlink. As described in [7], the selected propagation scenario is the 3GPP 38.901 Indoor LoS [8], in which Alice represents a Wi-Fi Access Point (AP), whereas Bob and Eve are two Wi-Fi Stations (STAs). Table 1 reports some of the overall 3GPP 38.901 Indoor LoS channel model parameters, including the mean and the standard deviation of the Angle-of-Departure (AOD), the Angle-of-Arrival (AOA), the Zenith-of-Angle-of-Arrival (ZOA), and the Cross Polarization Ratio (XPR). Detailed description of the selected scenario can be found in the reference documentation [12]. To perform the *on-the-shoulder* attack, Bob and Eve Euclidean distance is set to be equal to $\lambda/2$, i.e., radius of the red circle in Fig. 1 (a). In fact, the eavesdropper channel decorrelates at a distance of half wavelength [13]. To perform the proposed analysis, we set Alice ULA to a 5-dipoles array. Each element of the ULA consists of a half-wavelength dipole. Finally, each dipole is optimized for operation near to their first resonance according to the selected operating frequency, i.e., 5 GHz. To observe the effect of the dipole spacing, we varied the Alice ULA element spacing in the range of $[\lambda/2, 2\lambda]$. Fig. 1 (b) shows the Alice ULA directivity as a function of Bob angular positions reported for three dipoles spacing values, i.e., d, equal to $\lambda/2$, 0.75λ, and 1.5λ. The Alice ULA radiation pattern is computed by adopting the array factor theory. Hence, the mutual coupling between dipoles is left out of this contribution, and its effect on KPI will be analyzed in future work. The Chanel Impulse Response (CIR) can be modelled as follows:

$$h(t,\tau) = \sum_{i}^{N_p} a_i(t) e^{-j\theta_i(t)} \delta(t-\tau_i(t)) \qquad (1)$$

where N_p represents the number of multipath components, $\delta(t)$ is the Dirac Impulse function, and a, τ, and θ are the complex signal amplitude, the propagation delay, and the phase, respectively. Finally, t is the time. Hence, the received signal at each endpoint is evaluated as:

$$y_{i,j}(t) = x_i(t) * h_{i,j}(t,\tau) + n_j(t) \qquad (2)$$

where $i \neq j$ and $i, j \in \{Alice, Bob, Eve\}$. The transmitted signal is represented by $x_i(t)$, while the channel between the i-th and the j-th users is given by the impulse response $h_{i,j}(t,\tau)$. The $*$ denotes the convolution operator. The SKG-based keys are extracted from the baseband received signal spectrum by applying a single threshold filtering process [6, 7, 4]. In such a method, a main threshold is evaluated as the average value of the received signal

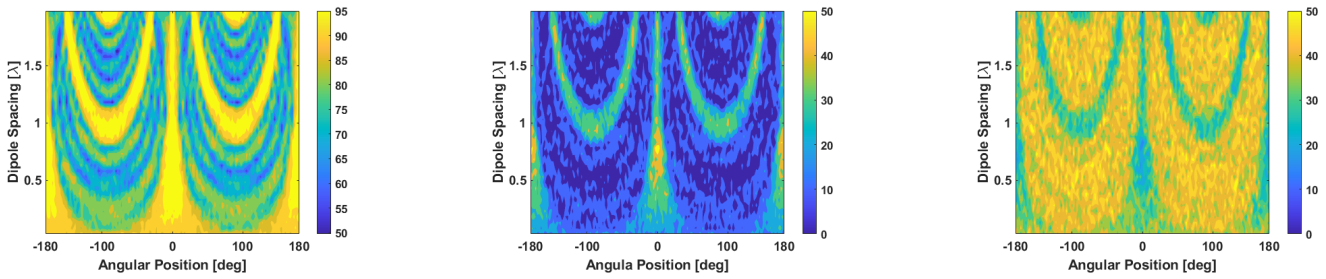


Figure 2. *(a)* Alice/Bob and Eve Channel Impulse Response (CIR) Correlation in percentage as a function of Bob/Eve angular position and Alice Uniform Linear Array (ULA) dipole spacing, *(b)* Alice/Bob and Eve Raw Key Correlation in percentage as a function of Bob/Eve angular position and Alice ULA dipole spacing, and *(c)* Alice/Bob and Eve Raw Key Mismatch Rate in percentage as a function of Bob/Eve angular position and Alice ULA dipole spacing.

power. Then, the nominal bandwidth of the received signal is subdivided into a fixed number of sub-bands, i.e., equal to the number of filters. The average received power in the sub-bands is compared with the main threshold to get the bit, i.e., 0 or 1. The main threshold $\bar{\gamma}_{i,j}$ can be evaluated as $\bar{\gamma}_{i,j} = \mathbb{E}\left[|Y_{i,j}(f)|^2\right]$, where $Y_{i,j}(f)$ represents the received signal at the j-th STA in the frequency domain, and $\mathbb{E}$ denotes the expectation operator. The k-th filter output could be represented as $C(k) = \int_{(k-1)t}^{kt} y_{i,j}(t) * F_k(t)dt$ [4], where $F_k(t)$ represents the k-th filter impulse response. Finally, the key $K_{i,j}$ is obtained as follows:

$$K_{i,j}(k) = \begin{cases} 0 & \mathbb{E}\left[|C(k)|^2\right] < \bar{\gamma}_{i,j} \\ 1 & otherwise \end{cases} \quad (3)$$

Given the statistical nature of the radio propagation processes, a Monte Carlo simulation has been adopted. The well-known Monte Carlo methods rely on repeated random sampling to obtain results from numerical simulations. In particular, the Monte Carlo methods are particularly useful in case of phenomena characterized by significant uncertainty [14]. In the proposed work, the following operations have been performed for each iteration of the Monte Carlo: *(a)* generating the CIR modeled with the QuaDrIGa framework according to the selected Alice ULA dipole spacing d, *(b)* evaluating the convolution between the transmitted Wi-Fi signal with the QuaDrIGa CIR, *(c)* adding White Gaussian Noise on the baseband received frame samples by considering a reference temperature of 290 K and 5 dB of Noise Figure, *(d)* applying the SKG protocol on the received frames to generate keys, and *(e)* evaluating the Alice/Bob and Eve channels correlation, key correlation, and key mismatch. The optimal number of trials of the Monte Carlo method was determined by a convergence analysis by compromising the computational resources and statistical significance. The following simulation results refer to 100 Monte Carlo realizations. For the sake of brevity, the convergence analysis is not reported in this work. Three KPIs have been chosen: *(a)* the channels correlation, *(b)* the key correlation, and *(c)* key mismatch rate as a function of Bob/Eve angular positions and Alice ULA dipoles spacing. To evaluate channels and keys correlation, we considered the Pearson Correlation Coefficient [15] evaluated on the CIR. The key mismatch rate δ is evaluated on the raw keys, i.e., the key obtained after the quantization phase, as the Hamming Distance in percentage over the key size (i.e., 128 bit) as $\delta_{AB|E} = \frac{HD(K_{AB},K_E)}{|K|}$. As a final remark, all the following results represent the average value of the selected KPIs evaluated over the Monte Carlo trials.

3 Results Discussion

Fig. 2 (a) represents the Alice/Bob and Eve channels correlation in percentage as a function of Bob/Eve angular position and Alice ULA dipoles spacing. As depicted in the figure, the channels correlation varies from a minimum value of 50 % up to 95 %. SKG relies on the channel diversity to generate session keys. Therefore, a higher correlation between Alice/Bob and Eve channels is not desirable, because it would lead to a higher attack success rate. Periodic patterns are observed as a function of the angular position, linked to the symmetrical behavior of the Alice ULA radiation pattern over the azimuth angle, i.e., ϕ. The correlation shows more complex models and multiple lobes in corrispondence of the ULA grating lobes for distance larger than λ. On the other hand, the correlation is relatively uniform, suggesting a lower sensitivity to angular variation for smaller ULA dipoles distances, i.e., 0.5λ. The regions of higher correlation, i.e., yellow zones, are mainly located in the angular positions in which main radiation lobes are located (Fig. 1 (b)). Finally, blue and green regions indicate a lower correlation located within the angular position in which the Alice ULA radiation pattern exhibits minima of radiation. Fig. 2 (b) represents the Alice/Bob and Eve raw key correlation in percentage as a function of Bob/Eve angular position and Alice ULA dipoles spacing. The figure highlights a periodic behavior as a function of the angular position, with areas of higher correlation, i.e., yellow-green zones, alternating with areas of lower correlation, i.e., blue zones. For small distances, i.e., $d \leq 0.5\lambda$, the correlation

is generally lower than 10 % for most of the angular range, with few areas of higher correlation, i.e., 35-50 %, around the 0° and $\pm 180^\circ$ angular positions. For dipole spacing equals to or larger than λ, 2 (b) highlights periodic zones of moderate correlation, i.e., $30-35$ %. The comparison of Figs. 2 (a) and 2 (b) suggests that the variation of Alice ULA dipole spacing reduces Eve ability to obtain useful information, especially in certain regions of space. Finally, Fig. 2 (c) represents the Alice/Bob and Eve key mismatch rate in percentage as a function of Bob/Eve angular position and Alice ULA dipoles spacing. Lower key mismatch regions, i.e., green zones light blue zones, are mainly concentrated around specific angles, i.e., 0°, $\pm 180^\circ$, and $\pm 90^\circ$ for dipole spacing within the range of $[0.5\lambda, \lambda]$. In particular, the key mismatch is generally high, i.e., 50 % for dipole spacing lower then λ, suggesting that Eve cannot eavesdrop keys similar to those of Alice and Bob. For larger dipole spacing, i.e., $d \geq \lambda$ there are additional zones with a lower mismatch, i.e., 30 %.

4 Conclusions

This study investigated the impact of dipole spacing in a Uniform Linear Array (ULA) on the performance of Secrecy Key Generation (SKG) in indoor environments. The analysis demonstrated that smaller dipole spacings, i.e., $d \leq 0.5\lambda$ yield higher security levels by reducing the channel and key correlations between the legitimate nodes, i.e., Alice and Bob, and an eavesdropper, i.e., Eve. This ensures a higher key mismatch rate, making it difficult for Eve to reconstruct the session key. Conversely, increasing the dipole spacing to values, i.e., $d \geq \lambda$, introduced periodic regions of moderate correlation, potentially creating vulnerabilities in certain angular positions relative to Alice ULA. The findings suggest that optimizing ULA configurations, particularly dipole spacing, is critical to enhancing the robustness of SKG protocols against eavesdropping attacks. The results emphasize the importance of integrating antenna design with PLS techniques to improve the resilience of next-generation communication systems. Future research will analyze the impact of mutual coupling between antenna elements and other propagation scenarios to provide a comprehensive understanding of SKG performance.

References

[1] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6g internet of things: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 359–383, 2021.

[2] A. Mayya, M. Mitev, A. Chorti, and G. Fettweis, "A skg security challenge: Indoor skg under an on-the-shoulder eavesdropping attack," *arXiv preprint arXiv:2305.09251*, 2023.

[3] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, "Advanced encryption standard (aes), federal inf. process. stds.(nist fips), national institute of standards and technology, gaithersburg, md," 2001.

[4] M. Zoli, A. N. Barreto, S. Köpsell, P. Sen, and G. Fettweis, "Physical-layer-security box: a concept for time-frequency channel-reciprocity key generation," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, pp. 1–24, 2020.

[5] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[6] A. Santorsola, M. Zoli, A. N. Barreto, V. Petruzzelli, and G. Calò, "Effect of radio channel and antennas on physical-layer-security key exchange," *IEEE Access*, vol. 9, pp. 162 175–162 189, 2021.

[7] A. Santorsola, G. Magno, V. Petruzzelli, S. R. Caporusso, and G. Caló, "Effect of indoor radio propagation on physical layer security secrecy key generation," in *2024 IEEE INC-USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*. IEEE, 2024, pp. 180–181.

[8] Q. Zhu, C.-X. Wang, B. Hua, K. Mao, S. Jiang, and M. Yao, "3gpp tr 38.901 channel model," in *the wiley 5G Ref: the essential 5G reference online*. Wiley Press, 2021, pp. 1–35.

[9] M. Zoli, M. Mitev, A. N. Barreto, and G. Fettweis, "Estimation of the secret key rate in wideband wireless physical-layer-security," in *2021 17th International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, 2021, pp. 1–6.

[10] S. Jaeckel, L. Raschkowski, K. Boerner, L. Thiele, F. Burkhardt, and E. Eberlein, "Quadriga-quasi deterministic radio channel generator," *User Manual and Documentation*, p. 260, 2019.

[11] IEEE, "Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. amendment 1: Enhancements for high efficiency wlan." *IEEE Standard for Information Technology*, 2021.

[12] G. T. 38.901, "Study on channel model for frequencies from 0.5 to 100 ghz," 2017.

[13] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*, 2011, pp. 211–224.

[14] N. Metropolis and S. Ulam, "The monte carlo method," *Journal of the American statistical association*, vol. 44, no. 247, pp. 335–341, 1949.

[15] M. G. Kendall, "The advanced theory of statistics." 1943.