2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) | 979-8-3503-5185-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/BLACKSEACOM61746.2024.10646260

A Novel Physical Layer Secret Key Generation Method for Wireless Sensor Networks

Mehmet Ali Aygül*†, Hakan Ali Çırpan*, Hüseyin Arslan‡
*Department of Electronics and Communications Engineering, Istanbul Technical University, Istanbul, 34467 Turkey
†Department of Research & Development, Vestel, Manisa, 45030 Turkey
‡Department of Electrical and Electronics Engineering, Istanbul Medipol University, Istanbul, 34810 Turkey

E-mails: {aygul21, cirpanh}@itu.edu.tr, huseyinarslan@medipol.edu.tr

***Abstract*—Wireless sensor networks are indispensable across various applications, from environmental surveillance to industrial automation, owing to their ability to collect and transmit data autonomously. However, due to the broadcast nature of wireless systems, these systems are vulnerable to eavesdropping attacks. Recently, channel-based secret key generation methods have been widely used in the literature. In these methods, Alice and Bob generate random signals and share these signals with each other. Then, using the secret key paired multiplication with the channel between them, a secret key is shared between legitimate users, while illegitimate nodes cannot access the key. However, these methods consider only two users. This paper proposes a novel method for multiple users. Extensive simulation proves the effectiveness of the proposed method. However, when the number of users increases, the performance of the proposed method decreases.**

***Index Terms*—Eavesdropping, physical layer security, secret key generation, TDD, wireless sensor networks.**

I. Introduction

Wireless sensor networks (WSNs) are known for their dynamic and decentralized nature, offering versatility across various applications [1]. However, ensuring robust security measures is paramount to safeguarding sensitive data and protecting against potential cyber threats to these networks. Symmetric key cryptography, which involves the use of a shared secret key to encrypt and decrypt messages exchanged between communicating users, emerges in securing these systems [2]. This approach ensures data confidentiality and integrity by scrambling information in such a way that only authorized recipients obtaining the secret key can decipher the encrypted data.

While cryptography-based solutions offer robust security measures, they often entail high computational overhead [3] and may not be suitable for resource-constrained WSN devices. Physical layer security-based methods present an alternative or complementary approach to providing security in wireless communication systems thanks to their lightweight implementation [4]. These methods leverage the inherent characteristics of wireless channels to establish secure communication channels. If the distance between the eavesdropper and any user in the network is more than a few centimetres, which is generally the case in wireless communication systems, their channels are assumed to be not correlated. In this case, wireless channel characteristics can be used as a common random resource for users to generate a secret key [5]. The wireless channel characteristics are especially used in time division duplex (TDD) systems where channel reciprocity is applicable [6].

Wireless channel characteristics-based secret key generation methods use three different approaches; when Alice and Bob use pilot signals [7]–[10], when Alice uses random signals while Bob uses pilot signals [11]–[14], and when Alice and Bob use random signals [15]–[19]. In [7]–[10], both Alice and Bob send public pilots and two-way channel estimations are required. In these methods, the secret key generation is limited by the randomness of the reciprocal channel [20]. In order to overcome these limitations, [11]–[14] introduce the randomness of a one-way transmitted signal and use the received signal as the common random source. For example, firstly, Bob sends a reverse public pilot to Alice, and then Alice transmits random signals, that can be locally generated by Alice, to Bob. Thus, Alice can estimate the reciprocal channel using the public pilots and compute the received signal at Bob using her own transmitted signal. Therefore, the received signal at Bob can be used as the common random source to generate secret keys, and vice versa. These secret key generation methods only require one-way channel estimation and the secret key generation rate (KGR) not only includes the randomness of the reciprocal channel but also includes the randomness of the one-way transmitted signal, so improving the secret KGR.

It is an intuitive idea to further promote the secret KGR by adding the randomness of two-way transmitted signals. Along with this line, [15]–[19] explore the secret key generation methods using two-way random signals, which can eliminate channel estimation and improve the secret KGR. However, these methods only consider two legitimate users (Alice and Bob). On the other hand, most of the WSNs consider more than two users in the network. In view of these discussions, this paper proposes a method for secret key generation in WSNs.

Here is a brief account of the contributions in this paper:

- A novel secret key-generation method is proposed for WSNs. In this method, several legitimate users can generate a secret key using channel information between them and random data sequences, while illegitimate users can not have access to the generated key.
- Extensive simulations prove the effectiveness of the proposed method in terms of key mismatch probability (KMP) and KGR.
- Although the proposed method works well, when the number of legitimate nodes increases, the KMP and KGR performances decrease.

Notation: Plain-faced letters demonstrate scalars and bold-faced letters demonstrate matrices.

II. System Model and Preliminaries

A. System Model

This paper considers a single-input single-output (SISO)-orthogonal frequency-division multiplexing (OFDM) system with a TDD configuration. Note that channel reciprocity is applicable in TDD systems due to the inherent symmetry between the uplink and downlink channels. In TDD, communication occurs over the same frequency band but in alternating time slots for transmission and reception. Because the physical environment between the transmitter and the receiver remains relatively constant over short time scales, the characteristics of the channel, such as path loss, fading, and multipath propagation, tend to be similar in both directions [21].

In this paper, single antenna transmitters, called Alice, Bob, Cindy, Dave, and Eve are used. We assume slow varying Rayleigh fading channel with L exponentially decaying taps between nodes. The rich multi-path environment ensures that Eve experiences an independent channel if it is half-wavelength apart from legitimate nodes. Eve's location and, consequently, its channel frequency response are unknown to Alice, Bob, Cindy, and Dave. The main goal of the proposed method is to provide secure communication between Alice, Bob, Cindy, and Dave, while eavesdroppers cannot listen to the communication between them. Figure 1 illustrates the system model that is considered in this paper. Here A, B, C, and D represent Alice, Bob, Cindy, and Dave, respectively.

B. Preliminaries

Used methods in the literature can be categorized into three categories, which are used to generate secret keys [20]. In the first category, both Alice and Bob use public pilots, and based on the channel information between Alice and Bob, the secret keys are generated. In the second category, Alice uses random signals, while Bob uses public pilots. Since the random signals that Alice uses create extra randomness in the system, the system is more secure. In the third method, both Alice and Bob use random pilots, which increases the security even more thanks to the original information (random signals) that are generated by both Alice and Bob. Along with this line, also this paper considers the third category. Note that, in this category, although the users generate their random sources (their signals), also the channel between them is used for common randomness between legitimate users.

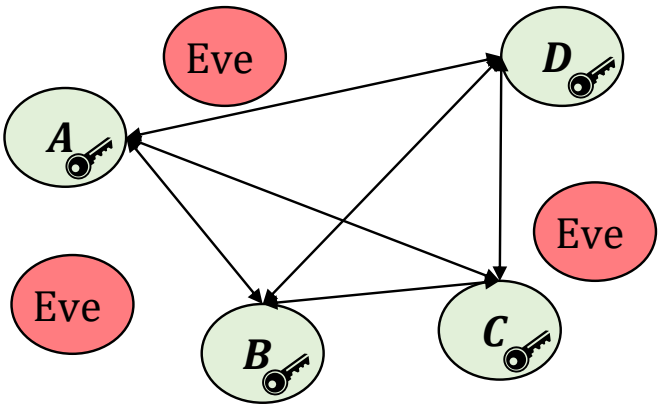

Fig. 1: System model: Alice, Bob, Cindy, and Dave want to communicate with each other, while eavesdroppers cannot listen to them.

The channel coherence interval is represented as

$$T_c = W_s T_s, \tag{1}$$

where T_s is the symbol duration time and W_s is the equivalent symbol number. We assume that channels stay unchanged during each T_c, and all the elements of the channel between the legitimate users are independent and identically distributed complex Gaussian random variables with zero mean, in different T_c. Additionally, the legitimate users work on the same carrier frequency in TDD mode. Thus, the legitimate channels satisfy reciprocity during a channel coherence interval.

III. The Proposed Method

In the conventional method, where there are only Alice and Bob as legitimate users, Alice sends random signals ($\boldsymbol{X}_a$) to Bob and Bob sends random signals ($\boldsymbol{X}_b$) to Alice. Then, they obtain $\boldsymbol{Y}_a$ and $\boldsymbol{Y}_b$, respectively in frequency domain as follows.

$$\begin{aligned} \boldsymbol{Y}_a &= \boldsymbol{H}\boldsymbol{X}_b + \boldsymbol{N}_a, \\ \boldsymbol{Y}_b &= \boldsymbol{H}\boldsymbol{X}_a + \boldsymbol{N}_b, \end{aligned} \tag{2}$$

where $\boldsymbol{H}$ is the channel between Alice and Bob. Also, $\boldsymbol{N}_a$ and $\boldsymbol{N}_b$ represent zero-mean complex additive white Gaussian noise (AWGN) in the frequency domain. After that, they multiply the obtained signal by the signals they send. Then, they obtain the following signals:

$$\begin{aligned} \boldsymbol{X}_a\boldsymbol{Y}_a &= \boldsymbol{X}_a(\boldsymbol{H}\boldsymbol{X}_b + \boldsymbol{N}_a) = \boldsymbol{X}_a\boldsymbol{H}\boldsymbol{X}_b + \boldsymbol{X}_a\boldsymbol{N}_a, \\ \boldsymbol{X}_b\boldsymbol{Y}_b &= \boldsymbol{X}_b(\boldsymbol{H}\boldsymbol{X}_a + \boldsymbol{N}_b) = \boldsymbol{X}_b\boldsymbol{H}\boldsymbol{X}_a + \boldsymbol{X}_b\boldsymbol{N}_b. \end{aligned} \tag{3}$$

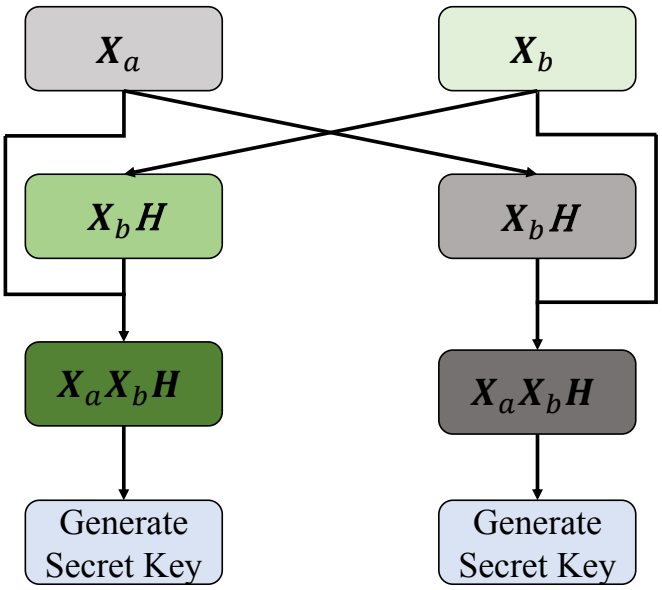

Fig. 2: The conventional method.

As seen from Eq. (3), when we ignore the noise, Alice and Bob obtain the same signals ($\boldsymbol{X}_a\boldsymbol{H}\boldsymbol{X}_b$). Finally, they generate secret keys from the obtained signals. To generate secret keys from the obtained signals, they may have a threshold and if the corresponding coefficient is below that threshold, the corresponding secret key coefficient can be 0, if it is higher, it can be 1. Many other methods in the literature such as [20], [22] can be used to generate secret keys from the obtained signal. The conventional method's steps are illustrated in Fig. 2. Despite the successes of this method in many applications, this method was not applied to multiple-user scenarios where multiple users want to share secret keys with each other as in most of the WSNs.

The proposed method considers sharing secret keys between multiple legitimate users called Alice, Bob, Cindy, and Dave. Here note that the number of users can increase without changing the logic of the proposed method. In the proposed method, first, Alice sends random signals ($\boldsymbol{X}_a$) to Bob over $\boldsymbol{H}_1$ while Dave sends random signals ($\boldsymbol{X}_d$) to Cindy over $\boldsymbol{H}_3$

$$\begin{aligned}\boldsymbol{Y}_b &= \boldsymbol{H}_1\boldsymbol{X}_a + \boldsymbol{N}_b,\\ \boldsymbol{Y}_c &= \boldsymbol{H}_3\boldsymbol{X}_d + \boldsymbol{N}_c.\end{aligned} \tag{4}$$

Then, Bob and Cindy add their signal $\boldsymbol{X}_b$ and $\boldsymbol{X}_c$ to their received signals

$$\begin{aligned}\boldsymbol{X}_b\boldsymbol{Y}_b &= \boldsymbol{X}_b(\boldsymbol{H}_1\boldsymbol{X}_a + \boldsymbol{N}_b),\\ \boldsymbol{X}_c\boldsymbol{Y}_c &= \boldsymbol{X}_c(\boldsymbol{H}_3\boldsymbol{X}_d + \boldsymbol{N}_c),\end{aligned} \tag{5}$$

Afterward, Bob and Cindy send their obtained signals to each other again, and they obtain

$$\begin{aligned}\boldsymbol{Y}_b^{'} &= \boldsymbol{H}_2(\boldsymbol{X}_c\boldsymbol{Y}_c) + \boldsymbol{N}_b^{'} = \boldsymbol{H}_2\Big(\boldsymbol{X}_c(\boldsymbol{H}_3\boldsymbol{X}_d + \boldsymbol{N}_c)\Big) + \boldsymbol{N}_b^{'},\\ \boldsymbol{Y}_c^{'} &= \boldsymbol{H}_2(\boldsymbol{X}_b\boldsymbol{Y}_b) + \boldsymbol{N}_c^{'} = \boldsymbol{H}_2\Big(\boldsymbol{X}_b(\boldsymbol{H}_1\boldsymbol{X}_a + \boldsymbol{N}_b)\Big) + \boldsymbol{N}_c^{'}.\end{aligned} \tag{6}$$

Then, again Bob and Cindy add their signal $\boldsymbol{X}_b$ and $\boldsymbol{X}_c$ to the received signals

$$\begin{aligned}\boldsymbol{X}_b\boldsymbol{Y}_b^{'} &= \boldsymbol{X}_b\Big(\boldsymbol{H}_2(\boldsymbol{X}_c\boldsymbol{Y}_c) + \boldsymbol{N}_b^{'}\Big),\\ \boldsymbol{X}_c\boldsymbol{Y}_c^{'} &= \boldsymbol{X}_c\Big(\boldsymbol{H}_2(\boldsymbol{X}_b\boldsymbol{Y}_b) + \boldsymbol{N}_c^{'}\Big).\end{aligned} \tag{7}$$

Afterward, Cindy sends her obtained signal to Dave, while Bob sends his obtained signal to Alice and Alice and Dave obtain

$$\begin{aligned}\boldsymbol{Y}_a &= \boldsymbol{H}_1\boldsymbol{X}_b\Big(\boldsymbol{H}_2(\boldsymbol{X}_c\boldsymbol{Y}_c) + \boldsymbol{N}_b^{'}\Big) + \boldsymbol{N}_a,\\ \boldsymbol{Y}_d &= \boldsymbol{H}_3\boldsymbol{X}_c\Big(\boldsymbol{H}_2(\boldsymbol{X}_b\boldsymbol{Y}_b) + \boldsymbol{N}_c^{'}\Big) + \boldsymbol{N}_d.\end{aligned} \tag{8}$$

Then, Alice and Dave add their signal $\boldsymbol{X}_a$ and $\boldsymbol{X}_d$ to their received signals

$$\begin{aligned}\boldsymbol{X}_a\boldsymbol{Y}_a &= \boldsymbol{X}_a\Big(\boldsymbol{H}_1\boldsymbol{X}_b\Big(\boldsymbol{H}_2(\boldsymbol{X}_c\boldsymbol{Y}_c) + \boldsymbol{N}_b^{'}\Big) + \boldsymbol{N}_a\Big),\\ \boldsymbol{X}_d\boldsymbol{Y}_d &= \boldsymbol{X}_d\Big(\boldsymbol{H}_3\boldsymbol{X}_c\Big(\boldsymbol{H}_2(\boldsymbol{X}_b\boldsymbol{Y}_b) + \boldsymbol{N}_c^{'}\Big) + \boldsymbol{N}_d\Big).\end{aligned} \tag{9}$$

Let us remove the noise interfered signal, and then Alice and Dave obtain

$$\begin{aligned}\boldsymbol{Y}_a &= \boldsymbol{X}_a\boldsymbol{X}_b\boldsymbol{X}_c\boldsymbol{X}_d\boldsymbol{H}_1\boldsymbol{H}_2\boldsymbol{H}_3,\\ \boldsymbol{Y}_d &= \boldsymbol{X}_a\boldsymbol{X}_b\boldsymbol{X}_c\boldsymbol{X}_d\boldsymbol{H}_1\boldsymbol{H}_2\boldsymbol{H}_3.\end{aligned} \tag{10}$$

Besides Alice and Dave, Bob and Cindy can obtain the same signals using received signals in Eqs. (4) and (6) and their own signals, $\boldsymbol{Y}_b\boldsymbol{Y}_b^{'}\boldsymbol{X}_b$ and $\boldsymbol{Y}_c\boldsymbol{Y}_c^{'}\boldsymbol{X}_c$, respectively. Therefore, Alice, Bob, Cindy, and Dave can have the same keys. These steps are also represented in Fig. 3. Here note that for the sake of simplicity and to explain the method more clearly noise effects are not represented in this figure. Lastly, based on the obtained signal, the secret keys are generated. If the real terms of the obtained signal coefficients are close to 0, they are rounded to 0, or if they are close to 1, they are rounded to 1. Finally, the obtained bit sequence is assumed to be the secret key between the users. Note that this rounding operation can be used for binary phase-shift keying (BPSK). On the other hand, there are many other methods in the literature such as [20], [22], which can be used to generate secret keys from the obtained signal as in the conventional methods and they can be applicable to other modulation types.

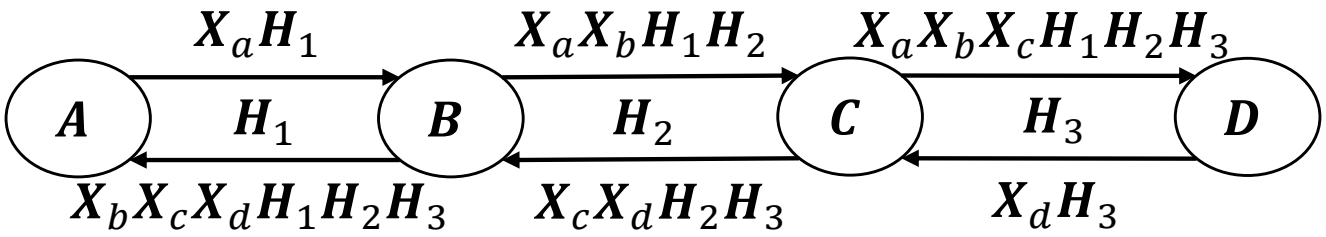

Fig. 3: The proposed method: Alice sends known signals to Bob. Bob multiplies with his own signal and sends it to Cindy, Cindy obtains the signal, adds her signal and sends it to Dave and Dave multiplies the received signal with his own signal. Meanwhile, Dave sends known signals to Cindy. Cindy multiplies with her own signal and sends it to Bob, Bob obtains the signal, adds his signal and sends it to Alice and Alice multiplies the received signal with his own signal.

IV. Simulation Results and Discussions

Illustrative simulations are conducted to show the performance of the proposed method in various signal-to-noise ratio (SNR) values (0 to 30 with a step size of 5) and the number of channel taps (4, 7, and 10). A practical SISO-OFDM system is considered with a fast Fourier transform size of 64, a number of data subcarriers size of 52, a number of bits per OFDM symbol size of 52, and 10000 number of symbols. BPSK is used as a modulation technique. As a channel model, Rayleigh is used. The noises are modeled by $\mathcal{CN}(0, \sigma_N^2)$, i.e., zero-mean complex Gaussian samples with variance σ_N^2. The performance of secret key generation methods can be assessed regarding the KMP and KGR. Note that a KMP is widely used in physical layer security, which is the ratio of the number of different bits of Bob and Alice keys to the total number of bits and a KGR is the rate at which two entities can securely create a common secret key during communication.

Figures 4 and 5 demonstrate the performance of the proposed method for illegitimate and legitimate users in terms of KMP and KGR, respectively. Note that, KMP and KGR results are given by comparing to secret keys of two legitimate users in the network, but results are the same when other legitimate users are compared. In Figs. 4 and 5, the length of the multipath channel between any communicating node pair is equal to $L = 4$ for Figs. (a), $L = 7$ for Figs. (b), and $L = 10$ for Figs. (c), where an exponentially decaying power delay profile is considered. In the case of sensor networks, when two users (Alice and Bob), three users (Alice, Bob, and Cindy), and four users (Alice, Bob, Cindy, and Dave), are in the system are simulated. Simulation results show that the illegitimate user cannot learn the secret key which is generated by legitimate users as can be understood from high KMP and low KGR results. On the other hand, legitimate users are able to obtain the same secret key. However, the performance of the KMP increases while the KGR decreases when the number of users in the network increases, which means decreased performance when the number of users increases. All these inferences are consistently true for all SNR values and the number of channel taps.

V. Conclusions

This paper proposed a novel method for secret key generation in wireless sensor networks. In the proposed method, each user generated random sequences and shared this signal in sequence to obtain the same signals, which were then used to obtain the secret keys between them. The proposed method allowed legitimate users to generate a secret key while illegitimate users could not learn it. However, the performance of the proposed method was decreased, when the number of users in the network was increased. Extensive simulations validated these in various SNR and channel tap values in terms of KMP and KGR. In future work, noise effects on the proposed method will be investigated.

Acknowledgement

This work was supported in part by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under Grant No. 119E433. Also, this work was supported in part by Vestel Elektronik Sanayi ve Ticaret A.Ş.

References

[1] L. M. Borges, et al., "Survey on the characterization and classification of wireless sensor network applications," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 4, pp. 1860–1890, 2014.

[2] Z. Rezki et al., "Secret key agreement: Fundamental limits and practical challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 72–79, 2017.

[3] A. Mukherjee et al., "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[4] H. Luo, N. Garg, and T. Ratnarajah, "A channel frequency response-based secret key generation scheme in in-band full-duplex MIMO-OFDM systems," *IEEE J. Sel. Areas Commun.*, 2023.

[5] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, 2011.

[6] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2018.

[7] J. Zhang, et al., "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[8] ——, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[9] Y. Peng, et al., "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, 2017.

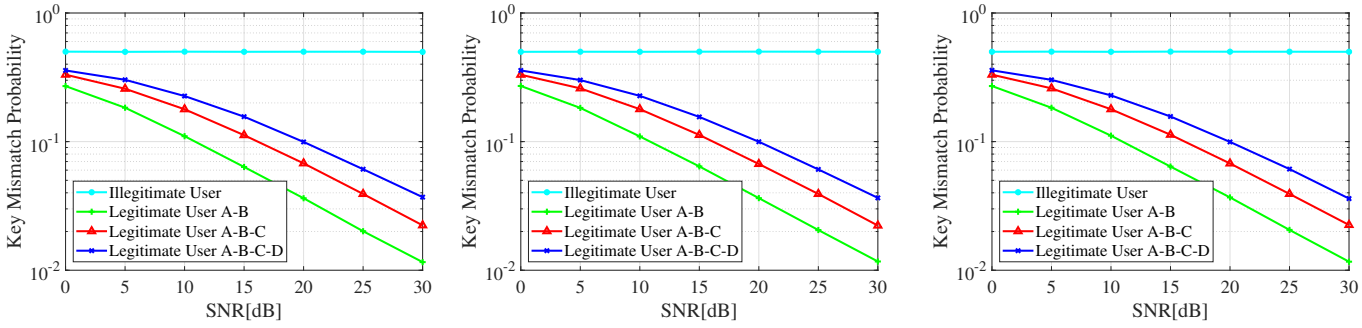

Fig. 4: KMP results when the number of taps is (a) 4, (b) 7, and (c) 10.

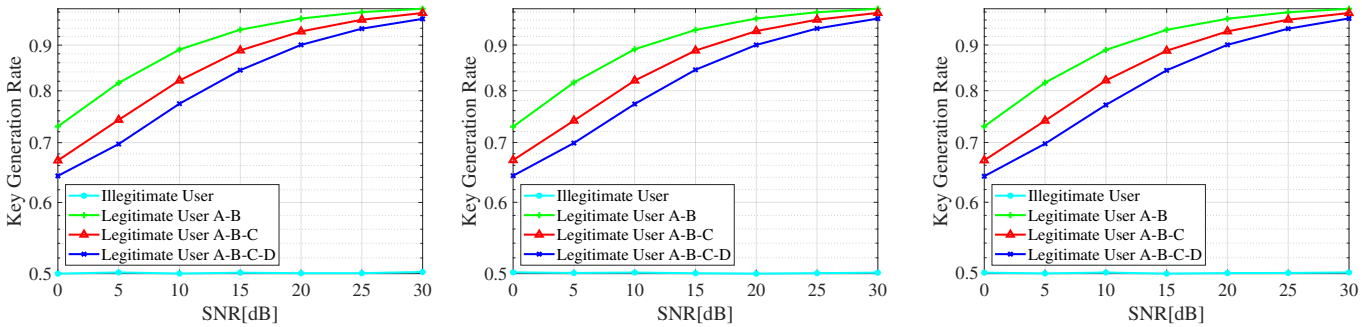

Fig. 5: KGR results when the number of taps is (a) 4, (b) 7, and (c) 10.

[10] K. Moara-Nkwe, et al., "A novel physical layer secure key generation and refreshment scheme for wireless sensor networks," *IEEE Access*, vol. 6, pp. 11 374–11 387, 2018.

[11] F. Renna, M. R. Bloch, and N. Laurenti, "Semi-blind key-agreement over MIMO fading channels," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 620–627, 2012.

[12] H. Taha and E. Alsusa, "Secret key exchange using private random precoding in MIMO FDD and TDD systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4823–4833, 2016.

[13] G. Li, et al., "Security analysis of a novel artificial randomness approach for fast key generation," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2017, pp. 1–6.

[14] Y. Lou, et al., "Secret key generation scheme based on mimo received signal spaces," *Scientia Sinica Informationis*, vol. 47, no. 3, pp. 362–373, 2017.

[15] S. Sharifian, F. Lin, and R. Safavi-Naini, "Secret key agreement using a virtual wiretap channel," in *Proc. IEEE Conf. Computer Commun. (INFOCOM)*. IEEE, 2017, pp. 1–9.

[16] A. Khisti, "Secret-key agreement over non-coherent block-fading channels with public discussion," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7164–7178, 2016.

[17] G. Wunder, R. Fritschek, and K. Reaz, "RECiP: Wireless channel reciprocity restoration method for varying transmission power," in *Proc. IEEE 27th Annual Int. Symp. Personal, Indoor, Mobile Radio Commun. (PIMRC)*. IEEE, 2016, pp. 1–5.

[18] S. Zhang, et al., "Secret key generation based on two-way randomness for TDD-SISO system," *China Commun.*, vol. 15, no. 7, pp. 202–216, 2018.

[19] ——, "High-rate secret key generation method using two-way random signal," in *Proc. IEEE Int. Conf. Cyber-Enabled Distributed Comput. Knowledge Discovery (CyberC)*, 2018, pp. 32–324.

[20] L. Jin, et al., "Secret key generation with cross multiplication of two-way random signals," *IEEE Access*, vol. 7, pp. 113 065–113 080, 2019.

[21] H. Xu, et al., "An empirical study on channel reciprocity in TDD and FDD systems," *IEEE Open J. Veh. Technol.*, 2023.

[22] H. Liu, et al., "Fast and practical secret key extraction by exploiting channel response," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, 2013, pp. 3048–3056.