Wireless channel-based ciphering key generation: effect of aging and treatment

Aqiel Almamori[1], Mohammed Adil Abbas[2]
[1]Electronics and Communication Department, Collage of Engineering, University of Baghdad, Baghdad, Iraq
[2]Continuing Education Center, University of Baghdad, Baghdad, Iraq

Article Info

Article history:

Received Jun 17, 2023
Revised Jul 8, 2023
Accepted Jul 17, 2023

Keywords:

Channel aging
Ciphering
Correlation
Encryption
Key generation
Spectral efficiency

ABSTRACT

Key generation for data cryptography is vital in wireless communications security. This key must be generated in a random way so that can not be regenerated by a third party other than the intended receiver. The random nature of the wireless channel is utilized to generate the encryption key. However, the randomness of wireless channels deteriorated over time due to channel aging which casing security threats, particularly for spatially correlated channels. In this paper, the effect of channel aging on the ciphering key generations is addressed. A proposed method to randomize the encryption key each coherence time is developed which decreases the correlation between keys generated at consecutive coherence times. When compared to the conventional method, the randomness improvement is significant at each time interval. The simulation results show that the proposed method improves the randomness of the encrypting keys.

Corresponding Author:

Mohammed Adil Abbas
Continuing Education Center, University of Baghdad
Baghdad, Iraq
Email: engimoh87@dcec.uobaghdad.edu.iq

1. INTRODUCTION

Wireless communication has become a mandatory portion of our everyday life. However, this portion requires gigantic efforts to have the wireless transmission secured. This issue has become significant after the ever-increasing amount of data transmitted, wirelessly [1]–[3]. Since electromagnetic waves can propagate anywhere, data transmission is fundamentally fraught with danger. The security and confidentiality of the transmitted information have therefore consumed a substantial amount of researchers' time and efforts. In order to ensure the confidentiality of transmissions, general transmission devices either use symmetric-key encryption or asymmetric-key encryption. However, neither of these methods is recommended due to the fact that asymmetric-key encryption necessitates a significant amount of complex processing power, and the second method necessitates a very secure link to transfer the unique encryption key, which is a crucial concern. Because sending sensitive information becomes impossible once the secret key is revealed [4], [5]. An alternative assumption is a keyless or physical layer security scheme was proposed. However, the keyless scheme limits the resources of wireless transmission. Furthermore, users of public networks face severe restrictions and costly additional expenses [6]–[10].

The concept of key generation was initially thought of and investigated theoretically in [11], [12]. Key generation is a crucial component of wireless transmission security. The process of generating a key entails the creation and distribution of an encryption code that can be used to secure the data at both ends of the transmission. Using a single code to encrypt the entire transmission is hazardous, however, because if the code is compromised, the entire transmission will be compromised [13], [14].

The improvement in the security of wireless networks is obtained by attaining information-theoretic secrecy, which provides network security with greater wireless adaptability. In contrast to conventional encryption key generation methods, a recent security technique exploits the randomness of the wireless channel. This method of key generation greatly complicates attempts to reveal the transmission by a third party (adversaries) other than the transmitter and receiver [15]–[17].

Hence, the randomness in wireless channels can be harvested to generate uncorrelated secret codes to guarantee transmission security [18]. This assumption does not always hold true. Specifically in a static environment, the wireless channel does not vary enough, resulting in a low level of introduced randomness in the following time interval. A practical example of this environment is the indoor internet of things (IoT). Correlated successive channels result in the generation of correlated secret codes which endanger transmission confidentiality. Due to the high correlation between encryption keys, compromising one key could be used to easily decrypt the next [18], [19].

Nevertheless, recent work on encryption key generation in the static environment has attracted considerable interest. The capacity of the encryption key was determined and addressed the parameters that affect the capacity [20]–[22]. However, efforts are directed toward reaping the advantages of randomness through the application of reconfigurable intelligent surfaces (RIS) [23]–[25]. The current efforts concentrate on reducing transmission losses and restricting the information leakage to the eavesdroppers in order to maximize link efficiency. So far as we can tell, though, there appears to be little effort to draw attention to the consequences of utilizing encryption keys correlated to the generated encryption keys at consecutive coherence times.

The contribution of this work addresses the impact of channel aging on the network security level to propose an alternative solution to overcome the issue of correlated successive encryption keys. This can be clearly seen in the low randomness environment or in other words, in the static environment when the user is sitting or moving lowly. Furthermore, the results of this paper show the impact of the proposed scheme and the speed of the moving user in enhancing network security. This study focuses on the design of a robust encryption key generation that avoids the correlation of consecutive encryption keys. The remainder of this paper is organized as follows, section 2 describes the system model of this study. The problem is brought up and formulated in section 3. The results are shown and discussed in section 4. Finally, section 5 concludes this study.

2. SYSTEM MODEL

In this paper, the transmitter base station (BS) or access point (AP)) is equipped with M transmit antennas and serves multiple users (total number of users is K) each user is equipped with a single antenna, as shown in Figure 1. Symmetric key encryption is considered that is used to encrypt the data transmission between the transmitter and each individual user, u_k.

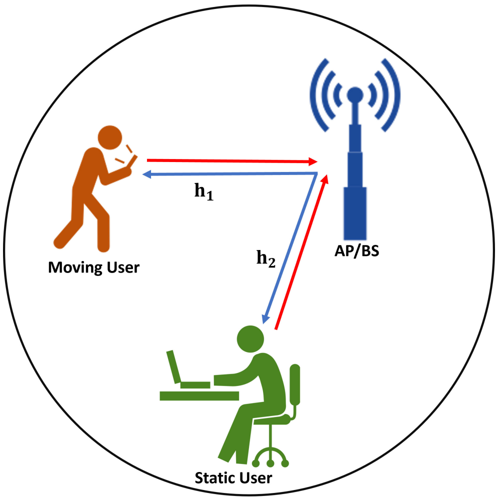

Figure 1. System model

The link between each single user and the transmitter is secured with a unique secret code. The encryption key for each link is derived from the randomness of its acquired channel state information (CSI). The CSI of all users is gathered by the transmitter. For each coherent time of transmission, the transmitter creates a new encryption key for each user and conveys it via a confidential channel to all of the active users. However, when u_k is in a static or slowly moving environment, the channel aging of u_k may be low, and the subsequent coherent time may be correlated. In this way, the transmission would operate with correlated secret codes, and the disclosure of a single transmission's encryption key would have adverse consequences [26]. Thus, breaking a single transmission's encryption key would be used by adversaries employing brute-force attacks to break the next hop's secret code since they are highly correlated, breaking a single hop's secret code is a weakness that could cause a threat. As well, spatially correlated adversaries will have time to brute force attack.

3. PROBLEM FORMULATION

This paper focuses on capturing the impact of the user in the slow-moving or static environment at the generated encryption key from the randomness of the wireless channel. The process of encryption key generation involves three main steps: probing, quantization, information reconciliation, and privacy amplification. The channel is measured in the first step and converted into binary in the second. The error correction and secrecy evaluation are done in the last two steps. The comprehensive explanation of each of these stages is detailed in [15]. However, the channel between the transmitter and u_k is given in (1) according to the assumptions in [17].

$$\mathbf{h}[n] = \alpha\mathbf{h}[n-1] + \mathbf{e}[n] \tag{1}$$

where $\mathbf{h}[n-1]$ represents the channel vector for the prior time slots while the effect of channel aging is represented by the error vector $\mathbf{e}[n]$. The temporal correlation parameter is given by $\alpha = J_0(2\pi f_D T_s)$. Where $J_0()$ is the zeroth-order Bessel function of the first kind. T_s, and f_D are the channel sampling duration and the maximum Doppler shift, respectively. The value of the Doppler shift is given by (2):

$$f_D = \frac{v f_c}{c} \tag{2}$$

where v is the moving velocity of the user u_k, c is the speed of light, and f_c refers to the carrier frequency. [17].

For the successive time slots, the successive channel is correlated which leads to generating a correlated encryption key. The key to mitigating and improving the quality of encryption keys is to introduce artificial randomness. The introduced randomness is added to the acquired channel during the process of generation of the encryption key. For simplicity, the permutations for the required channel vector can be used to generate uncorrelated successive encryption keys. After permutating the channel vector a decimal-to-binary conversion has to be done.

$$h_{01} = dec2bin(h) \tag{3}$$

where the vector h_{01} is binary vector of the length n bit. For a given vector h_{01} of length n it is simply to generate a matrix with the dimensions $P = n! \times n$, every single row in matrix P has the same length as v but with different permutations. The transmitter and receiver are able to use any permutated row vector according to a pre-decided algorithm.

4. RESULTS AND DISCUSSION

This section shows the simulation results that shows our proposal. The simulations of results were performed using MATLAB software. All generated simulations were made by averaging out 1,000 trails.

In Figure 2, the correlation of the successive coherent encryption keys for the two schemes was analyzed and compared. For the conventional scheme, highly correlated encryption keys result from the correlation between successive time slots. The correlation between the encryption keys decreases as a result of the effects of aging, However, the correlation between the first six encryption keys is considerably high. In contrast to the conventional approach, the proposed approach has shown considerable improvements. Hence, comparing the first and second-time slots generated keys, the correlation drops from 6.3799 in the conventional scheme to 0.0013 in the proposed scheme. The results reveal that the generated keys are uncorrelated with the encryption keys that come from the second time slot. Hence, the impact of the permutation of the received channel vector can be clearly captured. Figure 3, demonstrates the influence of user speed on the correlation between two successive encryption keys that come from successive time slots. It can be clearly seen that for the slow-moving user or the static user, the channel is highly correlated due to the low-level impact of channel aging. Hence, the generated encryption keys from the highly correlated channel vectors are correlated accordingly. Contrarily, the correlation level drops for the fast-moving user. Accordingly, the key will be more vulnerable due to this correlation and a third party can get an advantage.

Eventually, the eavesdropper has to find the permutation index which changes in coordination between transmitter and receiver before breaking the encryption which requires a huge computation power and time. The permutation index sharing between transmitter and receiver gives the key high randomness in which high computational power is needed to find it by the eavesdropper.

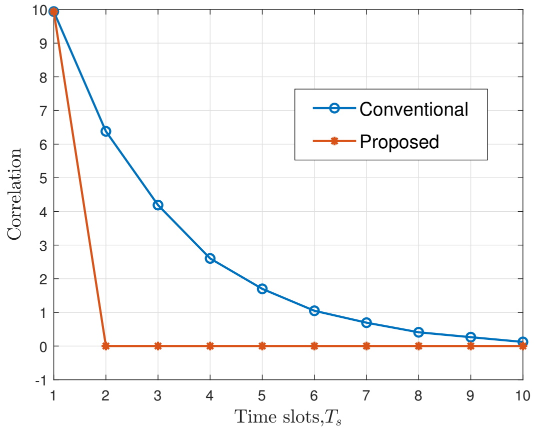

Figure 2. A comparison of the correlation between the successive time slots

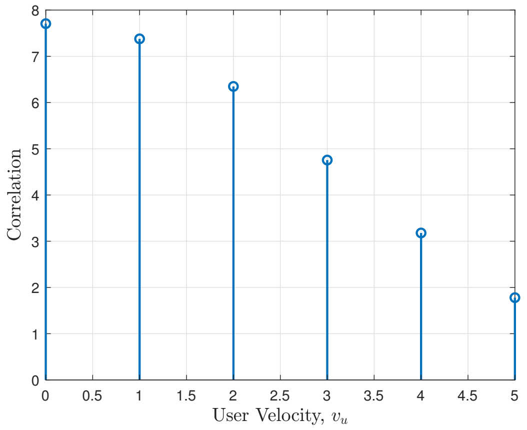

Figure 3. The correlation between the successive time slot versus the speed of the user

5. CONCLUSION

Security of transmitted data is important in wireless communications. Consequently, data encryption with the proper key is necessary. The encryption key has to be random and challenging to revoke its regenerate by a third party. The randomness of the wireless channel has been utilized to generate the encryption key. The correlation between the generated keys at consecutive intervals of coherence times is high, particularly in slow-moving mobile phones. This correlation is a weakness in network security and causes a threat. A proposed key generation method to overcome this threat is adding new randomization of binary key bits based on the bits permutations. This method highly improves the randomness and makes key regeneration by eavesdropper harder. The proposed method has improved the performance of the key.

REFERENCES

[1] N. M. Mukhammadovich and A. Rakhmatillo Djuraevich, “Working with cryptographic key information,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 1, pp. 911–919, Feb. 2023, doi: 10.11591/ijece.v13i1.pp911-919.

[2] N. Ibraheem and M. Hasan, “Combining several substitution cipher algorithms using circular queue data structure,” *Baghdad Science Journal*, vol. 17, no. 4, Dec. 2020, doi: 10.21123/bsj.2020.17.4.1320.

[3] A. N. Mazher and J. Waleed, “Retina based glowworm swarm optimization for random cryptographic key generation,” *Baghdad Science Journal*, vol. 19, no. 1, Feb. 2022, doi: 10.21123/bsj.2022.19.1.0179.

[4] R. Yudistira, “AES (advanced encryption standard) and RSA (Rivest–Shamir–Adleman) encryption on digital signature document: a literature review,” *International Journal of Information Technology and Business*, vol. 2, no. 1, pp. 1–3, 2020.

[5] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Yudistira Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[6] M. A. Abbas, H. Song, and J. P. Hong, “Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel with potential eavesdroppers,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 969–980, 2019, doi: 10.1109/TIFS.2018.2868494.

[7] S. A. Mohammed, “Securing physical layer for FHSS communication system using code andphase hopping techniques in CDMA, system design and implementation,” *Journal of Engineering*, vol. 26, no. 7, pp. 190–205, Jul. 2020, doi: 10.31026/j.eng.2020.07.13.

[8] M. A. Abbas, H. Song, and J.-P. Hong, “Secure wireless communications in broadcast channels with confidential messages,” *IEEE Access*, vol. 7, pp. 170525–170533, 2019, doi: 10.1109/ACCESS.2019.2955603.

[9] W. Trappe, “The challenges facing physical layer security,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, Jun. 2015, doi: 10.1109/MCOM.2015.7120011.

[10] 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, Apr. 2018, doi: 10.1109/JSAC.2018.2825560.

[11] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography. I. Secret sharing,” *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993, doi: 10.1109/18.243431.

[12] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993, doi: 10.1109/18.256484.

[13] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “A survey of key management schemes in wireless sensor networks,” *Computer Communications*, vol. 30, no. 11–12, pp. 2314–2341, Sep. 2007, doi: 10.1016/j.comcom.2007.04.009.

[14] M. Masdari, S. Ahmadzadeh, and M. Bidaki, “Key management in wireless body area network: challenges and issues,” *Journal of Network and Computer Applications*, vol. 91, pp. 36–51, Aug. 2017, doi: 10.1016/j.jnca.2017.04.008.

[15] K. Ren, H. Su, and Q. Wang, “Secret key generation exploiting channel characteristics in wireless communications,” *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, Aug. 2011, doi: 10.1109/MWC.2011.5999759.

[16] S. Ribouh, K. Phan, A. V. Malawade, Y. Elhillali, A. Rivenq, and M. A. Al Faruque, “Channel state information-based cryptographic key generation for intelligent transportation systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 12, pp. 7496–7507, Dec. 2021, doi: 10.1109/TITS.2020.3003577.

[17] K. T. Truong and R. W. Heath, “Effects of channel aging in massive MIMO systems,” *Journal of Communications and Networks*, vol. 15, no. 4, pp. 338–351, Aug. 2013, doi: 10.1109/JCN.2013.000065.

[18] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: a review,” *IEEE Access*, vol. 4, pp. 614–626, 2016, doi: 10.1109/ACCESS.2016.2521718.

[19] N. Aldaghri and H. Mahdavifar, “Physical layer secret key generation in static environments,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020, doi: 10.1109/TIFS.2020.2974621.

[20] J. Zhang, B. He, T. Q. Duong, and R. Woods, “On the key generation from correlated wireless channels,” *IEEE Communications Letters*, vol. 21, no. 4, pp. 961–964, Apr. 2017, doi: 10.1109/LCOMM.2017.2649496.

[21] J. Li, P. Wang, L. Jiao, Z. Yan, K. Zeng, and Y. Yang, “Security analysis of triangle channel-based physical layer key generation in wireless backscatter communications,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 948–964, 2023, doi: 10.1109/TIFS.2022.3224852.

[22] A. Almamori and M. A. Abbas, “Channel state information estimation for reconfigurable intelligent surfaces based on received signal analysis,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2,

pp. 1599–1605, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1599-1605.

[23] V. Shahiri, H. Behroozi, and A. Kuhestani, "Intelligent reflecting surface assisted secret key generation under spatially correlated channels in quasi-static environments," Dec. 2022, *arXiv:2212.01563*.

[24] Z. Wei and W. Guo, "Random matrix based physical layer secret key generation in static channels," Oct. 2021, *arXiv:2110.12785*.

[25] Z. Wei, B. Li, and W. Guo, "Adversarial reconfigurable intelligent surface against physical layer key generation," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2368–2381, 2023, doi: 10.1109/TIFS.2023.3266705.

[26] A. Almamori and S. Mohan, "Estimation of channel state information for massive MIMO based on received data using Kalman filter," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2018, pp. 665–669, doi: 10.1109/CCWC.2018.8301698.

BIOGRAPHIES OF AUTHORS

Aqiel Almamori received the B.Sc. degree in electronics and communications engineering and the M.Sc. degree in communications engineering from Nahrain University in Baghdad, Iraq in 1999, 2002, respectively. He received a Ph.D. in telecommunications and networking from the University of Arkansas at Little Rock, USA, in 2018. In 2005–2013, he joined Motorola Solutions as a radio frequency engineer. He has been working as a lecturer in the Electronics and Communication Department, College of Engineering, University of Baghdad. He can be contacted at email: a.eced@coeng.uobaghdad.edu.iq.

Mohammed Adil Abbas received the B.Sc. degree from the Department of Electronics and Communications, University of Baghdad, Baghdad, Iraq, in 2009, and the M.S. degree from the Department of Information and Communications, Pukyong National University, Busan, South Korea, in 2017. He is currently a lecturer with the Development and Continuing Education Center, University of Baghdad. He can be contacted at email: engimoh87@dcec.uobaghdad.edu.iq.