Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 21-29
https://doi.org/10.56471/slujst.v6i.301

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Hybridization of OFDM and Physical Layer Techniques for Information Security in Wireless System

Olawoyin, L.A[1], Abdul-Rahman Musrafah[2], Nasir Faruk[3], Oloyede A.A[4]. Adeniran T.C[5]. Imam-Fulani Y.O[6], Lasisi H.O[7], Ismaeel S.A[8] and Bashir Abdullahi Baba[9]

[1,2,4,5,6]Department of Telecommunication Science, University of Ilorin
[3]Department of Information Technology, Sule Lamido University, Kafin Hausa, Jigawa State
[7]Department of Electrical/Electronic Engineering, Osun State University, Osogbo
[8]Department of Information Technology, University of Ilorin
[9]Department of Cyber Security, Sule Lamido University, Kafin Hausa, Jigawa State
olawoyin.la@unilorin.edu.ng[1], faruk.n@slu.edu.ng[3] oloyede.aa@unilorin.edu.ng[4], adeniran.tc@unilorin.edu.ng[5], imam-fulani.yo@unilorin.edu.ng[6], hammed.lasisi@uniosun.edu.ng[7], ismaeel.as@unilorin.edu.ng[8], abashir.abdullahibaba@slu.edu.ng[9]

Abstract

Due to quest for high data rate, reliable and secure communication, this has motivated both wired and wireless network access service providers to deploy a next-generation network with ability to meet the required need. The use orthogonal frequency division multiplexing (OFDM) enables reliable transmission of various data traffic by optimizing subcarrier, power, and allocation of bits among different users. Traditionally, securing data in wireless system is always at the upper layer of open system interconnection (OSI) Model by using data encryption techniques. However, such techniques may not be acceptable for future decentralized networks due to their high complexity in implementation and computation. In this work, an OFDM IEEE 802.11a wireless system is used and physical layer encryption (PLE) schemes are implemented in securing the information transfer between two legitimate parties. In the simulation, the source data are encrypted by obfuscation with dummy data in between the encrypted data of which 52 subcarriers were considered of which 25 subcarriers are reserved for dummy data and 27 were for data. The simulation was conducted for four different modulation techniques i.e., BPSK, QPSK, 16 QAM, and 64 QAM. The result obtained shown that for all the modulation schemes, the key rate increases with an increase in the reserved subcarrier bits. Also, the security level increased when substantial percentages of the subcarriers are reserved for dummy data.

Keywords: *Cryptography, dummy data, optimization, physical layer encryption, Orthogonal frequency division multiplexing*

1. Introduction

Due to the benefits derived from wireless system in recent times, this has led to the deployment of wireless networks in offices, campuses, airports, and public areas. Due to the medium used for its transmission by wireless networks unlike wired networks, therefore the information sent is open to everybody, hence, security becomes an important feature in wireless networks, (Pamarthi and Narmadha 2022). The rapid growth in wireless networks over the last few years bear resemblance to the explosive growth of the internet within the last decade. Wireless communication will continue to enjoy exponential growth in the wireless internet, cellular telephony, and wireless home networking arenas. With the emergence of wireless local area network (WLAN) technology, computer networks could attain connectivity with a practical amount of bandwidth without being networked via a wall socket (Sharma, Bansal et al. 2013, Wang, He et al. 2017). In recent time, wireless networks have been found its applications in the home user markets, widely reported and easily exploited holes in the standard security system have stunted wireless deployment rate in enterprise environments. It became evident over time that some sort of security was needed to prevent outsiders from exploiting the connected resources Razaque et al., (2022). Physical Layer Security techniques exploit the dynamic characteristics of wireless communications, such as interference, channel randomness, and noise,

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

to prevent the eavesdropper from deciphering data while ensuring that the authorized user can decipher it successfully. In this literature, practical signal processing-based physical Layer Security techniques are proposed to secure communication between authorized parties. Many promising techniques have been proposed for OFDM which includes physical layer security (PLS) technique and secret key generation-based techniques which are aimed to extract random sequence from the wireless channel, (Haji M. Furqan 2018).

2. Related Works

Due to limited available bandwidth and power consumption, wireless devices need to be bandwidth constrained and should use little power. More so, some other challenges facing wireless networks are signal fading, data rate enhancements, mobility, high cost of deployment, Quality of Service (QoS), and user security. In order to curb some of the challenges facing wireless especially security issues, several researchers have proposed so many solutions such as noisy wiretap channels, Wireless padding (WiPad). Hamouid et al., (2020) investigated and examined the effect of security protocols on wireless network performance. The Wi-Fi Protected Access 2 – Pre-Shared Key (WPA2-PSK) was used as the security protocol in focus, while throughput was the network performance feature that was analyzed. Experiments were carried out which showed that throughput in a non-secured WLAN is a bit higher than throughput in a secured WLAN (Van Linh and Van Yem 2023). Their research contributes to the future development of WLAN protocols with low network resource consumption in other to contribute to improved network performance, Paramonov et al., (2017).

Qu, Z., Zhao, S., Xu, J., Lu, Z., & Liu, Y. (2021)., studied the security settings of WLAN, their vulnerability, and alternative solutions. The research work presented results from a comprehensive trace of wireless network security in a large wireless LAN. The author used CommView-for-Wi-Fi for packet capture on the network, and air-cracking for decrypting the encryption found in some Access Points (AP) within the network coverage range. This has been carried out using the campus-wide network of more than 100 access points (APs) spread over the buildings of the University. Potential problem(s) and appropriate solution(s) which is the use of WPA2 has also been discussed for the improvement of the wireless network in terms of security settings for effective and secure communication putting access control into cognizance. In 1975, Aaron (Wyner 1975) proposed a noisy wiretap channel model, the noisy wiretap channel is composed of one legitimate transmitter (Alice), one legitimate receiver (Bob), and one eavesdropper (Eve). For this model, Wyner formulated the condition for secure transmission, i.e., the transmission is information-theoretically secure if the decoding error probability at the legitimate receiver can be arbitrarily small while no source information can be obtained by the eavesdropper. The maximum rate under which the above condition can be met is termed as the secrecy capacity, which characterizes the performance limits for secure transmissions in noisy channels Banawan & Ulukus, (2020).

The authors Szczypiorski and Mazurczyk (2011) presented a new stenographic method called wireless padding (WiPad) which based their work on the insertion of hidden data into the padding of frames at the physical layer of wireless local area networks (WLANs). A performance analysis based on a Markov model, previously introduced and validated by the authors, is provided for the method in relation to the IEEE 802.11a/g standards. The result obtained proved that maximum steganography bandwidth for WiPad is as high as 1.1 Mbit/s for data frames and 0.44 Mbit/s for acknowledgment frames. The author showed that, to their knowledge, this is the most capacious of all the known stenographic network channels Tao et al., (2018). (Jameel, Haider et al. 2017) in their research efforts worked on the simultaneous wireless information and power transfer (SWIPT) in downlink multiuser orthogonal frequency-division multiple access (OFDMA) systems, where each user applies a power splitting scheme to coordinate the energy harvesting and secrecy information decoding processes. They proposed two suboptimal algorithms to solve the problem in the dual domain. The first one is an iterative algorithm that optimizes subcarrier allocation and power splitting in an alternating way while the second algorithm is based on a two-step approach that solves the subcarrier allocation and power splitting sequentially. The numerical results show that the proposed methods out-perform conventional methods. It was also shown that the iterative algorithm performs close to the upper bound and the step-wise algorithm provides good tradeoffs between performance and complexity.

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 21-29
https://doi.org/10.56471/slujst.v6i.301
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Zhang et al. (2016) implemented a new encryption at the physical layer of wireless networks employing OFDM. The new scheme obfuscates the subcarriers by randomly reserving several subcarriers for dummy data and resequences the training symbol by a new secure sequence. Subcarrier obfuscation renders the OFDM transmission more secure and random, while training symbol resequencing protects the entire physical layer packet, but does not affect the normal functions of synchronization and channel estimation of legitimate users while preventing eavesdroppers from performing these functions (Junqing Zhang 2016). In 2017, Franičević, I. proposed an efficient security technique by i-scrambling OFDM constellation symbols to encrypt data transmission to resist malicious attacks. In order to improve the confidentiality and security of OFDM systems, a PLS enhancement scheme by using time-domain scrambling techniques is proposed. According to the scheme; samples in each OFDM symbol are scrambled in the time domain before transmission in order to eliminate the inherent signal statistics features. And the resultant signal at the receiver is de-scrambled for subsequent recovery, Hao Li (2013).

Der-chang et al., (2008), proposed a new technique based on the combination of an orthogonal frequency division multiplexing (OFDM) scheme and an appropriate QAM mapping method (64-QAM) to remove the residual intelligibility from the encrypted speech by permuting several frequency components since an FFT-based speech encryption system retains considerable residual information, such as talk spurts and the original intonation in the encrypted speech and makes it easy for eavesdroppers to deduce the information contents from the encrypted speech. The results show that the proposed scheme can greatly improve the level of security because the talk spurts and the original intonation have been removed from the encrypted speech. Khan et al., (2007) the issue of security was not considered in the Time-domain synchronous orthogonal frequency division multiplexing (TDS-OFDM) and this limits its application in commercial or military scenarios where secure communication is very important. Ruifeng et al. in their paper, propose an encryption scheme based on pseudo-random constellation rotation and weak artificial noise insertion, which jointly utilizes the pseudo-random key and the irreversible property of wireless channel to guarantee the physical layer security of TDS-OFDM system, Junejo et al., (2018).

In this work, an OFDM IEEE 802.11a wireless system is simulated and PLE schemes are implemented. The key rate for the PLE schemes were evaluated, the source data are encrypted by obfuscation with dummy data in between the encrypted data. 25 subcarriers are reserved for dummy data, while the remaining 27 available subcarriers for data. The simulation was conducted for four modulation techniques i.e., BPSK, QPSK, 16 QAM, and 64 QAM. The result obtained shown that for all the modulation schemes, the key rate increases with an increase in the reserved subcarrier bits, with slight differences amongst different modulation schemes. It was further revealed that the system will be more secured when substantial percentages of the subcarriers are reserved for dummy data.

3. System Design

Using different OFDM system for interleaving, coding and mapping a binary data, such as BPSK, QPSK, 16-QAM and 64-QAM in which this complex value is modulated by IFFT operation to different subcarriers to form an OFDM symbol. This system consists of a data symbol and the training symbol in which the data symbol transmits data and the training symbol is used for channel estimation and synchronization. The data part is randomized at the subcarrier level by reserving several subcarriers for dummy data transmissions and the training symbol is resequenced with a secure and random sequence. However, as information is sent between legitimate users, the recipient can decode the signal as usual but this becomes a rather difficult task for an eavesdropper as the training symbol is already resequenced and kept secret to the eavesdropper i.e., they cannot perform channel estimation and synchronization correctly. The received signal can be expressed as:

$$R(n) = X(n)H(n) + W(n) \quad (1)$$

Where $R(n)$ is the received signal, $X(n)$ is the complex data value in the subcarrier, $H(n)$ is the channel and $W(n)$ is the AGWN noise effect. The decoded signal can thus be presented as;

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 21-29
https://doi.org/10.56471/slujst.v6i.301
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

$$X(n) = \frac{R(n)}{H(n)} \tag{2}$$

The data is encrypted and obfuscating by inserting dummy data in between the encrypted data. The location of the dummy data subcarrier changes for every data unit thus if dummy data insertion occurs before coding, this dummy data will be mixed with the data after coding and cannot be allocated to the specified subcarriers. Coding and interleaving are implemented before dummy data insertion so that inserted data cannot be in the same subcarrier with the data even if it is not encoded after it has been permutated by the interleaver. The data bits and dummy data bits are mapped to different subcarriers and the data subcarriers are obfuscated by dummy data subcarriers making the OFDM symbols random and making it difficult for the eavesdropper to sniff the data. The data part is encrypted, obfuscated, coded, interleaved, and then modulated using a mapping scheme. The modulated complex values are then passed to the IFFT module to form an OFDM symbol. The modulated data can be represented with

$$N_{OFDM} = \frac{I_d}{N_d R_b} \tag{3}$$

I_d is the length of the data, N_d is the number of data in the subcarrier, b is the number of bits per subcarrier and R is the coding rate.

This study is limited to physical-layer security for mobile users in future broadband wireless networks and the 802.11a Wireless LAN was used as the access network for the implementation of the project. The IEEE 802.11a/g OFDM signal contains 52 subcarriers symbols in which, 48 are data subcarriers and 4 are pilot subcarriers. However, the center, "DC" or "Null", zero subcarriers is not used in this implementation. All data subcarriers symbols use the same modulation format within a given burst. For experimentation, the modulation formats i.e., BPSK, QPSK, 16QAM, and 64QAM are varied. The total channel bandwidth is 20 MHz with an occupied bandwidth of 16.6 MHz In Fig 3.1, the signal generator flowchart is provided and Table 1 provides the simulation parameters used for the OFDM signal.

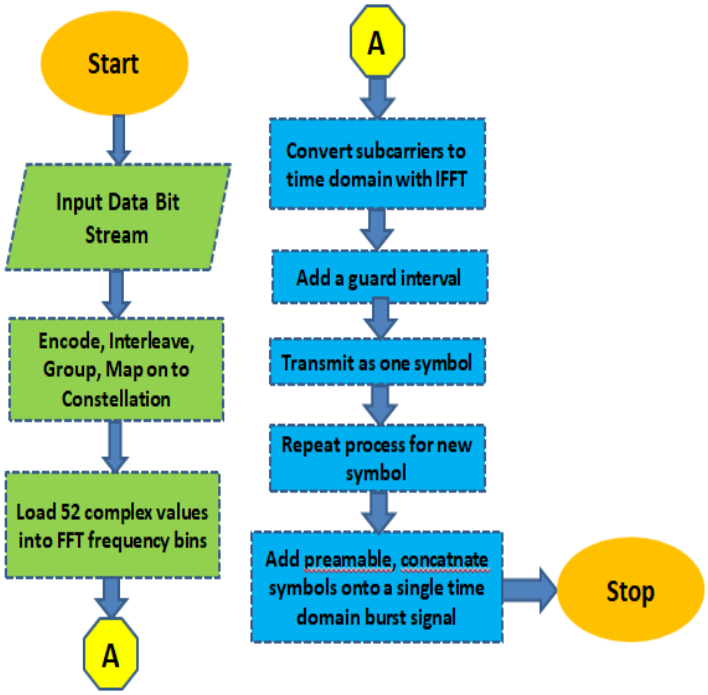

Figure 1: OFDM IEEE 802.11 signal generator flowchart.

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 21-29
https://doi.org/10.56471/slujst.v6i.301
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

4. Constellation Scrambling in the Frequency and Time Domain.

At the physical layer, the sender and the intended receiver use a custom constellation mapping which acts as a secret key to secure the communication from an eavesdropper and scramble the symbols in the frequency domain. In other words, a sequence of bits from the sender is converted into symbols on the constellation space using a mapping that is only known by the sender and the intended receiver. The intended recipient would be able to interpret the signal and recreate the original message using the correct mapping. However, the eavesdropper will not even be able to decode the signal correctly without the knowledge of constellation mapping, hence decoding the transmitted message will not be possible. In the time domain, the scrambling scheme rearranges the sample sequence in one symbol. Once scrambled in the time domain in a coded way, the transmitted signal will be greatly changed and varied on the frequency spectrum which no longer exhibits like an OFDM signal. The original data can only be obtained by the legitimate receiver who knows the time domain permutation order. Meanwhile, the illegitimate receiver who is ignorant of the permutation can merely convert the time-domain sequence of the intercepted signal into the frequency domain. Consequently, the data received and processed by the illegitimate receiver will not be the same as the original one. This approach requires matrix operations like division, multiplication, and determinant calculation all of which introduces additional computational complexity.

4.1 Modulation Symbols Rotation

When only the modulation type is the secret, the eavesdropper can identify the modulation type using machine learning-based techniques and decode the data using standard bit sequence to symbol mapping. However, if the sender and receiver add rotation to the modulation symbols and encrypts the training symbol to prevent the attacker from synchronizing and estimating the channel, the complexity of correct decoding becomes very high. The feasibility and performance too are low as denoted in equation (4)

$$\eta_{rot} = \frac{N_{bps}}{R_b} \tag{4}$$

where R_b is the bit rate, N_{bps} number of bits in seconds

The transmitted symbol is rotated at a fixed angle on a complex constellation plane in conventional constellation rotation. In order to weaken the eavesdropper data, a weak artificial noise is deliberately added to the rotated constellation symbols. In general, both constellation rotation and artificial noise insertion are used to enhance the security of the OFDM physical layer, which is important for consumer electronics as well as military usage where security has to be guaranteed. The modulation method forces noise into an eavesdropper's channel thereby making attacks on the cipher more difficult. However, the noise does not substantially affect legitimate users because there is a fore knowledge, (Ruifeng Ma 2010).

More so, in the OFDM techniques, subcarrier obfuscation increases the security and randomness of an OFDM transmission. Obfuscation is achieved by reserving several OFDM subcarriers to transmit dummy data to randomize the encrypted data streams, while training symbol re-sequencing protects the entire physical layer packet, it does not affect the legitimate user's normal functions of synchronization and channel estimation while preventing eavesdroppers from performing these functions. Thus, protection of the entire packet is achieved using equation (5) (Junqing Zhang 2016).

$$\eta_{sotsr} = \frac{K(\lfloor log_2(N_d s)\rfloor + b}{(N_d\ s - k)Rb} \tag{5}$$

where is the key rate for scrambling-based schemes, N_d is the number of data subcarriers, s is the data unit, k is used for reserve for dummy data, b is the number of bits per subcarrier.

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 21-29
https://doi.org/10.56471/slujst.v6i.301
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

These schemes have all taken measures to make the OFDM transmission more secure but they do have their limitations such as computational complexity, the key to data ratio greater than 1, eavesdroppers can easily decode messages, and so on. Due to the introduction of this proposed scheme, the computational overhead can be reduced, the key to data ratio can be made to be less than 1, and security of the entire physical layer can be achieved. By using different modulation schemes, the complex data value will be coded, interleaved and mapped by using several OFDM techniques such as BPSK, QPSK, 16-QAM, 64-QAM in which this complex value is modulated by IFFT operation to different subcarriers to form an OFDM symbol. This system consists of a data symbol and the training symbol in which the data symbol transmits data and the training symbol is used for channel estimation and synchronization.

Encrypting the initial data and obfuscating them is proposed, by inserting dummy data in between the encrypted data. The location of the dummy data subcarrier changes for every data unit thus if dummy data insertion occurs before coding, then the dummy data will be mixed with the data after coding and cannot be allocated to the specified subcarriers. Coding and interleaving are implemented before dummy data insertion to avoid the dummy data not being in the same subcarrier with the data even if it is not encoded after it has been permutated by the interleaver. In order to correct the transmission error, channel coding is used. The data and dummy bits are mapped to different subcarriers and the data subcarriers are obfuscated by dummy data subcarriers making the OFDM symbols random and difficult for the eavesdropper to sniff the data. The data part is encrypted, obfuscated, coded, interleaved, and then modulated using a mapping scheme. The modulated complex values are then passed to the IFFT module to form an OFDM symbol.

4.2 Performance Metric

The performance of the proposed scheme is evaluated by using key rate and search space. Key rate is an essential factor considered in encryption. A higher key rate requires more computational complexity but an improved security system is achieved. In wireless communication, the system can adjust the coding rate and mapping scheme according to the channel's signal-to-noise ratio which helps reduce the bit error rate (BER) resulting in different data rates. The key rate is evaluated using equation (6):

$$D_R = 2D_{R\min}D_b \tag{6}$$

Where D_R is the data rate $D_{R\min}$ is the minimum data rate, R is the coding rate and b is the number of bits per subcarrier.

5. Simulation and Numerical Results

The figure 1 shows the OFDM signal for the IEEE 802.11a Wireless LAN, this signal is obtained by using BPSK modulation techniques with coding rate of ½. The signal contains 52 subcarriers symbols in which, 48 are data subcarriers and 4 are pilot subcarriers. The total channel bandwidth considered for simulation is 20 MHz with an occupied bandwidth of 16.6 MHz.
The simulation parameters used are presented below

Parameters	Value
FFT size. nFFT	64
Number of Used Subcarriers. nDSC	52
FFT Sampling Frequency (Bandwidth)	20MHz
Occupied Bandwidth	16.6 MHz
Information Rate	6/9; 12/18; 24/36; 48/54
Modulation	BPSK, QPSK, 16QAM, and 64QAM
Coding Rate	1/2, 2/3, 3/4
Subcarrier Spacing	312.5kHz
Used subcarrier index (Total Subcarrier)	52 {-26 to -1, +1 to +26}

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 21-29
https://doi.org/10.56471/slujst.v6i.301
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Data Subcarrier	48
Pilot Subcarrier	4
Cyclic Prefix Duration, TCP	0.8us
Data Symbol Duration, T_d	3.2us
Total Symbol Duration, T_S	4us
Null Subcarrier	0

In the simulation, the source data are encrypted by obfuscation with dummy data in between the encrypted data. For each group of s OFDM symbol as a data unit, k subcarriers are used for reserve for dummy data and the location of the dummy data change for every data unit. In this project, 25 subcarriers are reserved for dummy data. The simulation was conducted for the four modulation techniques i.e. BPSK, QPSK, 16 QAM, and 64 QAM. For all the modulation schemes, it was observed that the key rate increases with an increase in the reserved subcarrier bits which it translates to increase in secure level of the transmitted data. However, the increase in reserved subcarrier among different modulation is marginal as can be seen in the figure 2 below

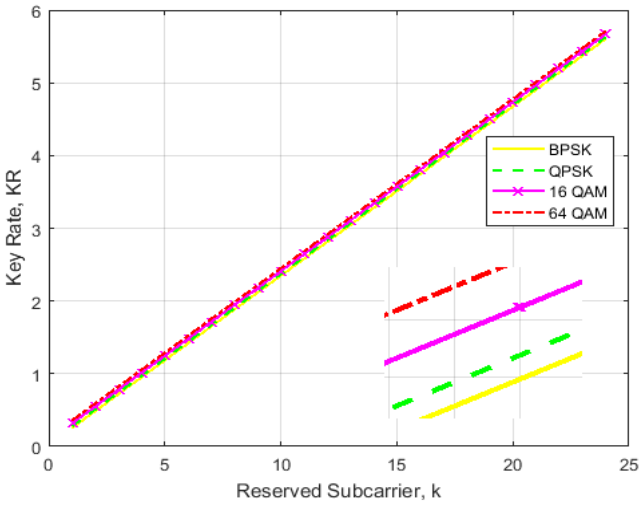

Figure 2. Key rate and Reserved Subcarrier for Different modulation schemes.

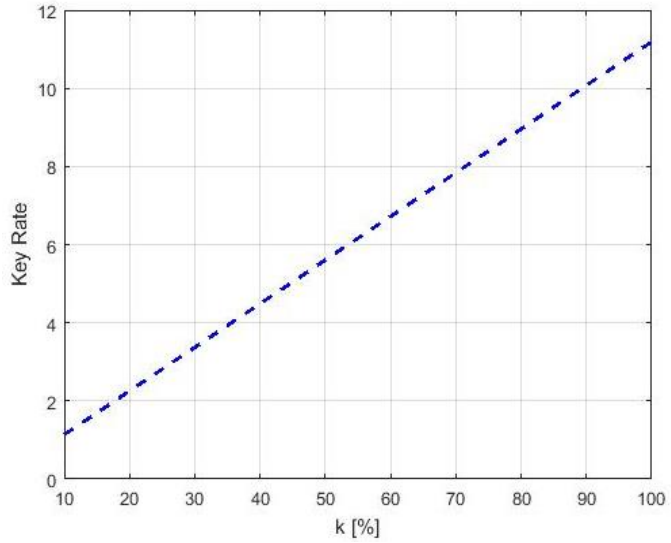

Figure 3. Key rate and Percentage of Reserved subcarrier

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 21-29
https://doi.org/10.56471/slujst.v6i.301
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

It can be seen from the figure 4, the security level increases when substantial percentages of the subcarriers are reserved for dummy data. However, the effects of increasing the percentage of the dummy data will reduce the overall amount of data to be sent on the data subcarrier. Also, the secrecy of the system can be enhance by increasing the search space but it is observed that at search space of 1 (s=1), the key rate is high which implies that the system is more secure. The scrambling scheme has a high key rate than the rotational scheme. However, the reserved subcarrier bit does not affect the key rate as constant key rates were observed regardless of the number of bits reserved for the dummy data. With the subcarrier obfuscation and training symbol resequencing, on the other hand, the key rate increases with the number of reserved bits.

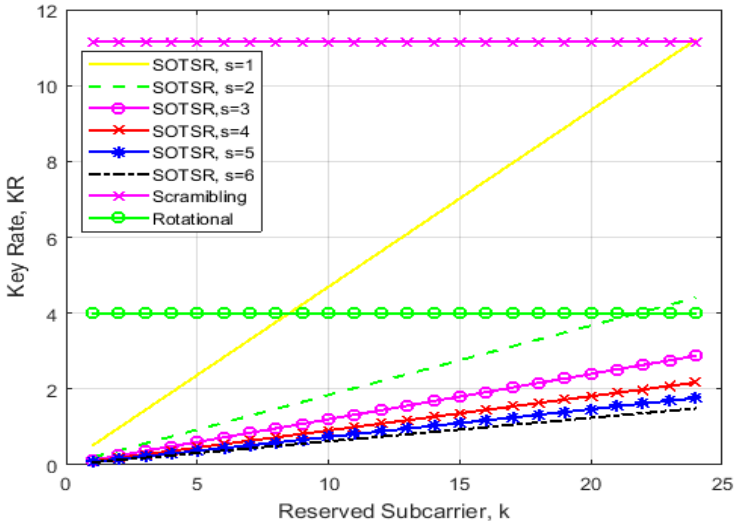

Figure 4. Result comparison of different schemes with SOTSR emerging as the best.

6. Conclusion

The key rate for the proposed method and other PLE schemes were simulated and evaluated. The simulation was conducted for the four modulation techniques i.e. At the end of the study, the following conclusions were obtained that for all the modulation schemes, the key rate increases with an increase in the reserved subcarrier bits. Slight differences were observed for the key rates amongst different modulation schemes. It was further revealed that the system will be more secured when substantial percentages of the subcarriers are reserved for dummy data. It was also observed that as the percentage of the dummy data will reduce the overall amount of data to be sent on the data subcarrier. Finaly, the scrambling scheme has a high key rate than the rotational scheme. However, the reserved subcarrier bit does not affect the key rate as constant key rates were observed regardless of the number of bits reserved for the dummy data.

References

Aniruddha Singh, A. V. P., Kumar Keserwani (2014). "Research Issues and Challenges of Wireless Networks." International Journal of Advanced Research in Computer Science and Software Engineering **Volume 4**(Issue 2): pp. 572-575.

Banawan, K., & Ulukus, S. (2020). Private information retrieval through wiretap channel II: Privacy meets security. IEEE Transactions on Information Theory, 66(7), 4129-4149.

Franičević, I. (2017). *Simulacija LTE mreže na području Borongaja* (Doctoral dissertation, University of Zagreb. Faculty of Transport and Traffic Sciences. Division of Transport. Department of Information and Communications Traffic).

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Haji M. Furqan, J. M. H., Huseyin Arslan (2018). "Adaptive OFDM-IM for Enhancing Physical Layer Security and Spectral Efficiency of Future Wireless Networks." Research Article **2018**: pp 1-16.

Hamouid, K., & Adi, K. (2020). Privacy-aware authentication scheme for electric vehicle in-motion wireless charging. In 2020 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6).

Irving, P. A. O. a. P. (2016). "Performance Analysis of Wireless Network Throughput and Security Protocol Integration." International Journal of Future Generation Communication and Networking **Vol. 9**(No. 1): pp. 71-78.

Jameel, Furqan, Haider, M Asif Ali Butt, and Amir Aziz (2017). A technical review of simultaneous wireless information and power transfer (SWIPT). 2017 International Symposium on Recent Advances in Electrical Engineering (RAEE),

Junqing Zhang, A. M., Roger Woods and Trung Q. Duong. (2016). "Design of an OFDM Physical Layer Encryption Scheme." IEEE Transactions on Vehicular Technology: pp 1-14.

Khan, M. A., Asim, M., Jeoti, V., and Manzoor, R. S. (2007). On secure OFDM system: Chaos based constellation scrambling. 2007 International Conference on Intelligent and Advanced Systems.

Mazurczyk, K. S. a. W. (2011). "Steganography in IEEE 802.11 OFDM symbols." Research Article **9**(2): pp 118–129.

Pamarthi, S. and R. Narmadha (2022). "Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: Network attacks and detection mechanisms." International Journal of Intelligent Unmanned Systems **10**(4): 482-506.

Razaque, A., Jararweh, Y., Alotaibi, B., Alotaibi, M., & Almiani, M. (2022). Hybrid energy-efficient algorithm for efficient internet of things deployment. *Sustainable Computing: Informatics and Systems*, *35*, 100715.

Qu, Z., Zhao, S., Xu, J., Lu, Z., & Liu, Y. (2021). How to Test the Randomness From the Wireless Channel for Security?. *IEEE Transactions on Information Forensics and Security*, *16*, 3753-3766.

Ruifeng Ma, L. D., Zhaocheng Wang and Jun Wang (2010). "Secure Communication in TDS-OFDM System Using Constellation Rotation and Noise Insertion." IEEE Transactions on Consumer Electronics **Vol. 56**(No. 3): pp1328-1332.

Sharma, Sukhwinder, Bansal, Rakesh Kumar and Bansal, Savina (2013). Issues and challenges in wireless sensor networks. 2013 International Conference on Machine Intelligence and Research Advancement, IEEE.

Singh, A., et al. (2014). "Research issues and challenges of wireless networks." International Journal of Advanced Research in Computer Science and Software Engineering **4**(2): 572-575.

Tao, J., Li, S., Zhang, X., & Wang, Z. (2018). Towards robust image steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, *29*(2), 594-600.

Van Linh, D. and V. Van Yem (2023). "Key Generation Technique Based on Channel Characteristics for MIMO-OFDM Wireless Communication Systems.

Liu, Jiangchuan, Wang, Feng, Ma, Xiaoqiang and Yang, Zhe (2017) . "Integration of networking, caching, and computing in wireless systems: A survey, some research issues, and challenges." IEEE Communications Surveys & Tutorials **20**(1): 7-38.

Wyner, A. D. (1975). "Wire-tap channel." The Bell System Technical Journal **54**(8): PP 1355–1387.

Zhang, J., et al. (2016). "Design of an OFDM physical layer encryption scheme." *IEEE Transactions on Vehicular Technology* **66**(3): 2114-2127.