Physical Layer Security in Wireless Communication: An Overview

Shrishti Gaur*, Neetu Sood

Dept. of Electronics and Communication, Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India

*Corresponding author

doi: https://doi.org/10.21467/proceedings.114.41

Abstract

In the past few decades wireless communication has been growing with leaps and bounds characterised by demand for safer, faster and enhanced communication systems. Exploiting the physical properties of communication through appropriate signalling and coding processes, the concept of Physical Layer Security (PLS) has intensified. Consequently, the pursuit for this fulfilment has led to surfacing of inevitable high data traffic and challenges with data security. For futuristic technologies like 5G and beyond, traditional technologies like Radio Frequency (RF) unaccompanied have proved to be rather inefficient and search for alternative and upgraded technologies like Visible Light Communication (VLC) has gained momentum. However, VLC technology is not sufficient in all terms and in combination with RF demonstrates superior capabilities. In this paper an attempt has been made to evaluate the importance of PLS systems and the depth and degree up to which engineers and researchers have been able to reach in attaining robustness and resilience in it as an integral aspect of RF and VLC systems.

Keywords: VLC, RF, Physical Layer Security.

1 Introduction

Over the last three decades, there has been tremendous progress in wireless communications ranging from the wireless telegraph to today's state-of-the-art technologies like smartphones, connected vehicles and the Internet of Things (IoT) [1]-[3]. All of these new technologies depend on wireless communications to keep pace with the common demand for high bandwidth and data rates. Due to this, a dramatic rise in data traffic can be observed. As a result, 5G networks [4] are urgently needed to provide transparent connectivity, robust security, ultra-low latency communications and high data rates. Therefore the already crowded conventional RF networks are not suitable to meet these high demands.

Consequently, engineers and researchers have got involved in a quest for technologies that not only help in overcoming the limitations and drawbacks of RF but also prove to be more efficient, secure and reliable. Parallely, VLC has emerged as a new technology, which makes use of a light source for both data transmission and illumination purposes simultaneously. VLC demonstrates supremacy by possessing unlicensed channels and exhibiting immunity against interference from electromagnetic sources. In addition, it also has low power consumption and has no health threats.

1.1 Significance of PLS

With the upsurge of wireless communications and the emergence of the Internet of Things (IoT), the security of wireless communications is gradually becoming significant. The physical layer improves the security performance of communication systems by using interference and random channels in order to reduce the information received and detecting it adequately by people who try to access it without permission. The groundwork for information theory was set by Shannon where he demonstrates that if there are equal amounts of messages, then the keys are of utmost necessity for complete secrecy [5]. Shannon's information theoretic secrecy analysis can be considered as the origin of PLS. In this analysis, it

Proceedings DOI: 10.21467/proceedings.114; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-947843-8-8

has been presented that the level of security is dependent upon the amount of information accessed by eavesdroppers. Achievement of complete robustness would comprise complete ignorance of transmitted information by the eavesdroppers, leaving them with the only option of guessing the information bit by bit. Wyner proposed a model, known as the wire tap channel [6], which without the need of a secret shared key, harnesses the channel's imperfections to safeguard transmission at the physical layer. Wiretap channel coding has been used to attain the maximum rate of transmission by confidential communication, defining rate as secrecy capacity. As illustrated in Figure 1, in Wyner's model, the transmitter attempts to convey a confidential message to an authorized receiver in the presence of an eavesdropper over a noisy link with no memory.

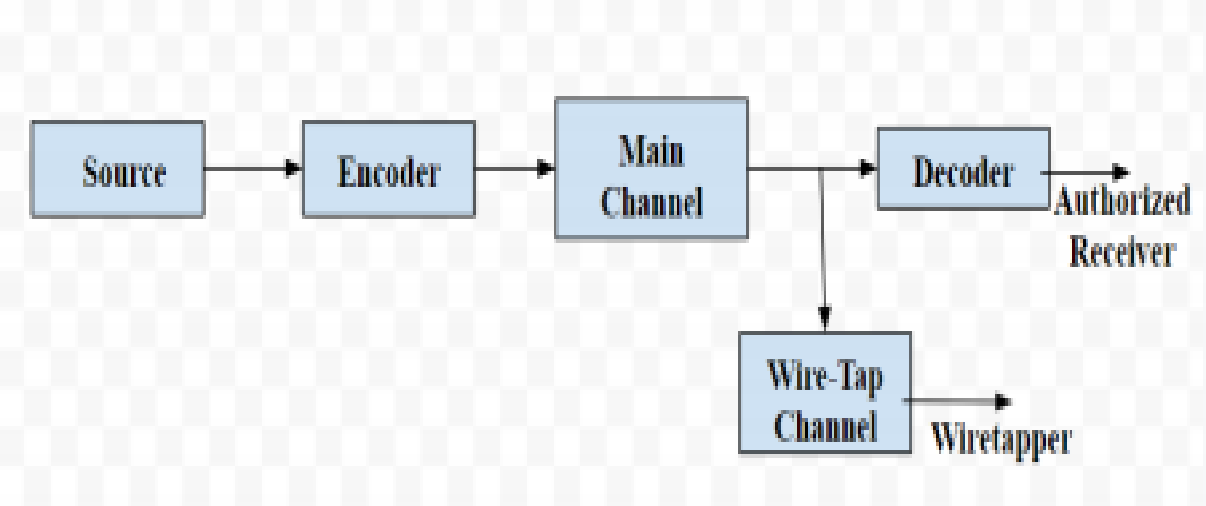

Fig 1: Wire-tap Channel

In [7]-[8], a comprehensive examination of the PLS in terms of the academic basis, realization, coding methods, challenges and contingencies are provided. For the security in wireless communications in the occupancy of whatsoever eavesdroppers, relay nodes [9] were utilized to exploit the properties of the physical layer so that assistance can be provided to ensure safe transmission between the source and destination. For massive MIMO (MaMIMO) [10] and Cognitive Radio (CR) Networks [11], security of the physical layer was taken into the account briefly.

In [15], a comprehensive outline was provided about the security of the physical layer with Channel State Information at the Transmitter (CSIT). Predominantly, in this paper, they had differentiated between the situations where the uncertainty was due to the CSIT estimation error which can be a feedback link of CSIT of limited capacity or due to an outdated CSI.

Comparing physical layer security with the rest of the cryptographic techniques which are implemented at higher levels, PLS accomplishes security at a significantly lower computational complexity by utilizing the fluctuations and randomness of the wireless channel. PLS utilizes fundamental and essential features of the wireless channels for instance, intervention, fading and

unwanted signals, in contrast to the approaches of the conventional cryptographic. These characteristics will facilitate and provide ease to elevate the reception of signal to the authorized and permitted user and at the same time to deteriorate the attributes and traits of the signal at the eavesdroppers end.

The advantages of PLS techniques over

cryptographic approaches are as follows:

- PLS helps to assist in conquering the management and allocation of the secret keys as it does not rely upon the functioning of encoding and decoding in comprehensive heterogeneous IOT systems.

- PLS profitably furnishes an adaptable and responsive structure of security, level and also provides assurance for Quality of Service (QoS). It does so by taking full use of wireless channel features to accomplish adaptive signal design and resource allocation.
- In comparison to the encryption method, PLS techniques consequently result in less overhead because it only needs to supplement the relatively simple signal processing algorithms.

2 Physical Layer Security in RF

Numerous studies have been done in PLS for RF systems till now, that can help to comprehend the basic principles, state of technology and future PLS trends [12]-[14].

An exhaustive study of the security aspects of LTE/LTE-A networks [16] was presented. For LTE WLAN heterogeneous network convergence introduced by 3GPP, hybrid cryptosystem and encryption techniques were suggested to enhance the protocols determined by the EAP-AKA. Safety designs from the perspective of signal optimization and processing were evaluated, and a summary of all PLS techniques related to the selection of antenna/selection of nodes, resource allocation, precoding/beam formation were presented.

In this paper, conventional features of 5G IOT networks and their influence on its security were examined. After that, threats of physical layer were distinguished into various kinds, such as wiretapping, scrambling, and interference in 5G IOT networks. Also cutting-edge work on PLS techniques for mitigating physical layer threats in 5G IoT networks [28], involving NOMA, massive MIMO, full duplex radio, mmWave, VLC and UAV communications was studied

For the 5G IOT networks, this article examines physical layer authentication (PLA) systems [29] using machine learning technologies such as Kalman filtering prediction, AdaBoost classifier, reinforcement learning, autoregressive random process and kernel machine. These were used to upgrade performance of the characteristic features of multiple physical layers.

3 Physical Layer Security in VLC

Due to wireless broadcasting nature, the secure delivery of confidential signals through the available channel has become a pivotal matter in wireless communication. Hence, Visible light communication (VLC) is more worthy than radio frequency (RF) in terms of security due to its line of sight (LOS) propagation and the light waves do not penetrate through walls. IEEE 802.15.7 standard played a crucial role in the development of rolling out the VLC networks which were issued in 2011. However, VLC is also prone to eavesdropping by unauthorized users positioned in that lighted area due to unlicensed wireless channels. A number of physical layer safety schemes have been envisaged for VLC systems. In order to enhance the achievable rate of secrecy of visible light communication, two types of jamming schemes were established [17]-[18]. But since, the beam forming technique utilizes multiple antennas collaboration, the hardware design complexity of antennas got increased and also it may be the reason for non-uniform illumination. In contrast to this, a novel security scheme [19] was suggested to furnish high spectral efficiency and to conquer inter-symbol interference (ISI) for VLC links based on a method of key generation mechanism in VLC-OFDM systems. A revised edition of the Rivest-Shamir-Adleman (RSA) technique [20] was employed for coding of the data transmission in the media access control (MAC) layer to secure the MIMO-VLC system which depends upon the location of the user. Physical layer security approaches are categorized into two kinds: key based security approaches and keyless security approaches for enhancing the privacy of the VLC systems. Although these approaches increase the security of the VLC system with less complexity, still they would require pre shared keys and management of keys at the time of communication setup. As per Wyner's wiretap channel, cryptography is not required as they utilize the characteristics of the channel and execute the code

design to back up the licensed users in keyless security approaches. However, statistical and instant information on the status of the channel is required by licensed users. There are diverse fields of study in keyless security approaches that can be classified into: artificial-noise-assisted security, information-theoretic security, security focused beam forming techniques and huge Led Arrays Synthesis of Security-Oriented Pattern.

The key based security approach recruits communication channels so that it creates secret keys to cipher the information of the user prior to transmission. In [21], based on polar codes i.e. forward error correction (FEC), a keyless security approach was introduced which not only helped to attain accuracy in transmission but also physical layer security for binary discrete memory less channels (BDMCs) indoor VLC systems. In [22], the execution of the physical layer security was investigated in a three dimension multithreaded VLC network with the help of mathematical tools such as stochastic geometry. With this analytical expression were obtained for the ergodic secrecy rate, secrecy outage probability and also their lower and upper limits which were further confirmed with the help of Monte Carlo simulations. To strengthen the secrecy performance of the VLC system, optimizing theory may also be utilized by keeping in mind several restraints, for example, the peak power constraint to diminish eye damage [23], the optical power constraint of LED [25], and dimming control constraint and energy harvesting in light [24].

Lately, two new techniques of PLS based on VLC termed as superposition coding based NOMA and superposition coding based NOMA were envisaged in [26]. After considering a wide array of VLC systems including MISO, SISO, MIMO, VLC as well as hybrid RF/VLC systems an insight was made into the informational, theoretic and signal processing aspects of VLC systems [27]. Further in this, the influence of diverse features on VLC ranging from geometry and parameters of the network, secrecy fulfilment encompassing input signalling schemes, number of legitimate eavesdroppers and receivers, and the CSI accessibility at the transmitting nodes. PLS techniques have also been found useful in augmenting the secrecy and safety performance of VLC systems. On the whole it can hence be concluded that VLC systems are promising technology that is going to prove quite constructive in the advent of new generation wireless communication networks.

On account of the insufficiency and scarcity of spectrum, compel the engineers and researchers to discover new technologies so that it can support expanding demands and growth of mobile devices. But due to their own innate shortcomings existing in both RF and VLC, it has been able to deploy them successfully and calls for an improvement. To resolve the downsides of the RF and VLC systems, an amalgamation of these technologies was envisaged, termed as Hybrid RF/VLC technology. The authors in [30] clarified that using the beam forming strategy and power allocation schemes; it was possible to divert the signal away from the eavesdroppers successfully. In [31], in order to augment the performance of the network, the introduction of a joint relay-jammer selection algorithm has been proposed.

Furnished with amicable jamming capacity multiple decode-and-forward relaying nodes, the physical layer capacity of RF/VLC has been attempted to be thoroughly analysed. Since dissemination through RF/VLC is prone to eavesdroppers attack, it becomes imperative to safeguard an augment network securely. In [32], the authors have analysed the features of physical layer security of hybrid RF/VLC systems for authorized users in the occupancy of eavesdroppers situated in the same room. They have done this by splitting the expression of the problem in two stages. In the initial stage, the RF/VLC based BF vectors were acquired by utilizing the zero forcing (ZF) and beamforming (BF) schemes to optimize and upgrade the capacity of achievable secrecy. On the next stage, they manipulated the achieved vectors from the above results in order to resolve the problem of the power minimization to achieve the required secrecy goals.

4 Conclusion

With the drastic increase in data traffic and upcoming 5G networks, provision of superior and more capable transmission architectures and network techniques has surfaced as a new challenge. In order to cater this, RF has been indicated as inadequate but its assistance by VLC has however substantiated to be promising, owing to the complementing characteristics of RF and VLC in combination. This amalgamation itself is not immune to missing links and displays drawbacks such as adoption of continuous input signalling and secrecy performance of indoor VLC systems. Also, challenges like link blockage and device orientation which are innate problems associated with wireless communications, has called for demand of more realistic and non-uniform models. VLC as a newer technology has also presented itself with qualities like open and broadcasting nature and large unexploited spectrum. Nevertheless, this challenge is not limited only to difficulties related to higher data transmission rates but also to network safety and secrecy issues. Consequently, the concept of physical layer security has been witnessing rapid rise as an imperative segment of RF and VLC. Hence, on a concluding note, it may aptly be stated that post the investigation and redressal of shortcomings through well-defined PL techniques, VLC is a promising futuristic technology that holds capabilities in boosting the emergence and expansion of next generation wireless networks.

References

[1] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019.

[2] H. Tran-Dang, N. Krommenacker, P. Charpentier and D. Kim, "Toward the Internet of Things for Physical Internet: Perspectives and Challenges," in IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4711-4736, June 2020.

[3] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019.

[4] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 679-695, April 2018.

[5] C. E. Shannon, "Communication theory of secrecy systems," in The Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[6] A. D. Wyner, "The wire-tap channel," in The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[7] W. Trappe, "The challenges facing physical layer security," in IEEE Communications Magazine, vol. 53, no. 6, pp. 16-20, June 2015.

[8] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," in IEEE Communications Magazine, vol. 53, no. 4, pp. 20-27, April 2015.

[9] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," in IEEE Communications Magazine, vol. 53, no. 12, pp. 32-39, Dec. 2015.

[10] D. Kapetanovic, G. Zheng and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," in IEEE Communications Magazine, vol. 53, no. 6, pp. 21-27, June 2015.

[11] Y. Zou, J. Zhu, L. Yang, Y. Liang and Y. Yao, "Securing physical-layer communications for cognitive radio networks," in IEEE Communications Magazine, vol. 53, no. 9, pp. 48-54, September 2015.

[12] P. Ramabadran et al., "A Novel Physical Layer Encryption Scheme to Counter Eavesdroppers in Wireless Communications," 2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Bordeaux, France, 2018, pp. 69-72.

[13] Á. Vázquez-Castro and M. Hayashi, "Physical Layer Security for RF Satellite Channels in the Finite-Length Regime," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 981-993, April 2019.

[14] W. Wang, Z. Sun, S. Piao, B. Zhu and K. Ren, "Wireless Physical-Layer Identification: Modeling and Validation," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2091-2106, Sept. 2016.

[15] A. Hyadi, Z. Rezki and M. Alouini, "An Overview of Physical Layer Security in Wireless Communication Systems With CSIT Uncertainty," in IEEE Access, vol. 4, pp. 6121-6132, 2016.

[16] J. Cao, M. Ma, H. Li, Y. Zhang and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 283-302, First Quarter 2014.

[17] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," 2014 IEEE Globecom Workshops (GC Wkshps), Austin, TX, USA, 2014, pp. 524-529.

[18] H. Zaid, Z. Rezki, A. Chaaban and M. S. Alouini, "Improved achievable secrecy rate of visible light communication with cooperative jamming," 2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Orlando, FL, USA, 2015, pp. 1165-1169.

[19] Y. M. Al-Moliki, M. T. Alresheedi and Y. Al-Harthi, "Robust Key Generation From Optical OFDM Signal in Indoor VLC Networks," in IEEE Photonics Technology Letters, vol. 28, no. 22, pp. 2629-2632, 15 Nov.15, 2016.

[20] F. I. K. Mousa, N. Al Maadeed, K. Busawon, A. Bouridane and R. Binns, "Secure MIMO Visible Light Communication System Based on User's Location and Encryption," in Journal of Lightwave Technology, vol. 35, no. 24, pp. 5324-5334, 15 Dec.15, 2017.

[21] Z. Che et al., "A Physical-Layer Secure Coding Scheme for Indoor Visible Light Communication Based on Polar Codes," in IEEE Photonics Journal, vol. 10, no. 5, pp. 1- 13, Oct. 2018.

[22] L. Yin and H. Haas, "Physical-Layer Security in Multiuser Visible Light Communication Networks," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 1, pp. 162-174, Jan. 2018.

[23] A. Mostafa and L. Lampe, "Physical-Layer Security for MISO Visible Light Communication Channels," in IEEE Journal on Selected Areas in Communications, vol. 33, no. 9, pp. 1806-1818, Sept. 2015.

[24] X. Liu, Y. Wang, F. Zhou, S. Ma, R. Q. Hu and D. W. K. Ng, "Beamforming Design for Secure MISO Visible Light Communication Networks With SLIPT," in IEEE Transactions on Communications, vol. 68, no. 12, pp. 7795-7809, Dec. 2020.

[25] S. Cho, G. Chen and J. P. Coon, "Physical Layer Security in Multiuser VLC Systems with a Randomly Located Eavesdropper," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6.

[26] A. Yesilkaya et al., "Physical-Layer Security in Visible Light Communications," 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 2020, pp. 1-5.

[27] A. Arfaoui et al., "Physical Layer Security for Visible Light Communication Systems: A Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1887-1908, thirdquarter 2020.

[28] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8169-8181, Oct. 2019.

[29] J. -R. Jiang, "Short Survey on Physical Layer Authentication by Machine-Learning for 5G-based Internet of Things," 2020 3rd IEEE International Conference on Knowledge Innovation and Invention (ICKII), Kaohsiung, Taiwan, 2020, pp. 41-44.

[30] M. F. Marzban, M. Kashef, M. Abdallah and M. Khairy, "Beamforming and power allocation for physical-layer security in hybrid RF/VLC wireless networks," 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, 2017, pp. 258-263.

[31] J. Al-Khori, G. Nauryzbayev, M. M. Abdallah and M. Hamdi, "Joint Beamforming Design and Power Minimization for Friendly Jamming Relaying Hybrid RF/VLC Systems," in IEEE Photonics Journal, vol. 11, no. 2, pp. 1-18, April 2019.

[32] J. Al-khori, G. Nauryzbayev, M. Abdallah and M. Hamdi, "Physical Layer Security for Hybrid RF/VLC DF Relaying Systems," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 2018, pp. 1-6