INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

IJARIIT

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 2)

Available online at: www.ijariit.com

Physical Layer Mechanism based Secure Key Exchange for 5G Networks

Bolla Sai Venu Kiran
saivenukiran_venkat@srmuniv.edu.in
SRM Institute of Science and Technology, Chennai, Tamil Nadu

T. Ramya
ramya.t@ktr.srmuniv.ac.in
SRM Institute of Science and Technology, Chennai, Tamil Nadu

ABSTRACT

5G wireless networks are evolving to meet the rapid increase in the demand of the users to get high-quality broadband services with high-speed data rate. This advance development came up with a lot of challenges such as coverage region, security, energy efficiency, spectrum utilization, cost, latency, and data rate. To ensure the security, there are many conventional key exchange algorithms that need complex infrastructure. In recent times, physical layer-based security has gained a lot of attention since it offers a simple and efficient way of key exchange by exploiting wireless channel characteristics. In this project, for secret key sharing between the two legitimate users through a correlated channel that is shared with eavesdropper, a pre-equalization transmit filter that inverts the main channel is employed. Further to decrease the probability of interception by eavesdropper while permitting successful decoding by the legitimate user. Low-Density Parity Check (LDPC) code is used to assure reliable communication. Modulation schemes such as basic QPSK and 64,128 and 256-QAM are used to achieve higher bit rates. To achieve high secrecy between the legitimate users zero forcing algorithm is used to invert the channel. Through simulations, the effect of channel correlation will be studied to analyze the low secret key mismatch between the Bob and Eve. Here Eve having high Bit Error Rate(BER) so that eve could not obtain the original bits. The simulation will be done using Matlab.

Keywords: *Physical Layer Security, 5G Security, Secure Communication, IoT, IoV, LDPC Codes, Eavesdropper.*

1. INTRODUCTION

As the 5G era is evolving, the volume of data traffic and variety of services will increase to unseen-before levels. IoT service is just one of the many. When it comes to 5G, it is not at all a simple thing about being a medium for communication. It can be seen as a catalyst for minimizing the boundary between the digital world scenario and physical world scenario.” 5G security design is an all-encompassing one that provides security protection for the everything-connected world. 5G needs an open platform to support a vast array of services from vertical industries, for instance, remote health care, Internet of Vehicle (IoV), and IoT. The platform can be further divided into units based on the functions. In this way, the service deployment can be more rapid and the operating cost can be reduced. In this security is one of the essential features.”

“To the next generation wireless network systems, such as 5G communications, the process of key management (key generation and secure key exchange) will become even more important as the number of nodes increases to a massive scale and nodes become more heterogeneous in their computational capabilities. Also, physical layer security offers a good solution for interoperability between different systems where pre-shared keys may not exist. We envision that physical layer security methods will be used as an additional layer of security to complement traditional cryptographic methods. Nowadays, physical layer security has gained a lot of attention since it offers enhanced wireless network security by exploiting wireless channel characteristics to generate a secret key between the communication nodes. Using training sequences (probing signals), both parties can measure the channel parameters such as the received signal strength indicator [1]- [4], the channel state information (CSI) [5]- [6] or the power spectral density [7] of the probing signals to agree on a secret key. However, the randomness that can be extracted from the channel through the signal processing techniques proposed in above references is limited by the randomness in the channel. For stationary or low-mobility users, the channel randomness is very low and the number of uncorrelated bits that can be generated from the channel is very few. Furthermore, the techniques proposed in above references are prone to manipulation. “

In this project, Rayleigh fading channel considers as a channel for communication and uniqueness of the main and eavesdropping channels shares secret keys over wireless medium. A pre-equalization transmit filter that inverts the main channel between legitimate users is employed to decrease the probability of interception at Eavesdropper while permitting successful decoding at Bob. To achieve a low error rate between Alice and Bob, LDPC channel coding is used. Once the secret key/message is established between Alice and Bob, the message/key is converted into 7-bit ASCII binary format at Alice before the LDPC encoding and basic QPSK modulation, while the inverse operations are carried out by Bob's receiver. Later the higher modulation scheme such as 128-QAM is comparatively used for very low latency communication between the legitimate users.

Below, the II Section gave by Existed System Model, III gives the Proposed Method and IV gives the Simulation results using MATLAB as follows respectively.

2. EXISTING SYSTEM MODEL

Considering two legitimate users Alice and Bob are present in a Rayleigh fading channel. A third-party user called eavesdropper is also sharing the same channel with legitimate users (Eve in future reference). To protect secret key/message from the Eve, Bob needs to find out the channel state information [3] with a pre-equalization filter. A pre-channel training sequence is transmitted to Alice, according to that the Alice sends the message/key to the Bob. At the same time, Eavesdropper will not able to obtain the channel information because uncorrelated with the legitimate users. Hence, there is high error probability occurs at the Eavesdropper. So, original key/message will not be available at any third-party users.

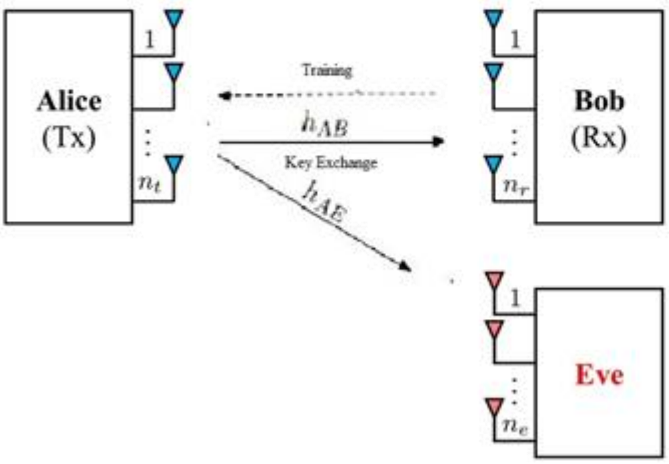

Fig. 1. System Model

The received key bits in the form of the equation at Bob and Eve can be respectively expressed as:

$$P_B \leq \frac{1}{kMN_b} \sum_{s_i^j \in \delta} \sum_{s_m^n \in \delta \neq s_i^j > e(s_i^j, s_m^n)} E_{H_b} P(s_i^j \mapsto s_m^n | H_b) \quad (1)$$

$$P_B \leq \frac{1}{kMN_b} \sum_{s_i^j \in \delta} \sum_{s_m^n \in \delta \neq s_i^j > e(s_i^j, s_m^n)} E_{H_b,H_e} P(s_i^j \mapsto s_m^n | H_b.H_e) \quad (2)$$

From the Fig. 1. system model, hAB, and hAE are channel impulse responses of legitimate users and Eavesdropper. Alice will send the encoded and modulated bits to Bob, at receiver obtained bits are demodulated and decoded by Bob. From the above equations (1) & (2) are known to the responses of bob and eavesdropper respectively [8]. The error probability is achieved between the legitimate and eavesdropper. So, secrecy is ensured with authenticate manner. Hence the existing system model is shown with the legitimate and eavesdropper blocks within the Rayleigh fading channel. Then the secured communication between users is obtained with pre-equalizing the channel by the Alice with the help of Bob’s signal training sequence.

3. PROPOSED METHOD

“The newly proposed physical layer mechanism based secure key exchange is explained as follows. As mentioned in the existing system model, the main objective is to securely share a private key between Alice and Bob. Before transmission, a secret key x with a length of N bits is processed by the transmitter (Alice) to ensure a low probability of interception at Eve. The step by step process of communication between the Alice & Bob with eavesdropper is as follows.”

- Input message consists of characters, numeric & symbols and it is converted into 7-bit ASCII format.
- Channel need to be estimated by Bob and send its training sequence to Alice to achieve high secrecy of transmission and reception.
- Alice will recognize that training sequence and performs inversion of the channel using transmit filter to secure communication in later aspects.
- The required secret key will be initiated from Alice with the transmit filter and encoded by LDPC at the rate r = ½.

- At the reception side, Bob will receive a pre-equalized signal that consists of a secret key. Then the obtained signal will undergo LDPC decoder to decode.
- Hence, the secret key is successfully transferred to Bob from Alice with error bits (due to Rayleigh fading channel) and it will iteratively process by LDPC Decoder.
- For faster communication possibly the QAM modulation is used with M=64,128 and 256 is used in this paper and compared basic QPSK simulation.

The newly proposed transmitter and receiver are shown in fig. 2. The role of each block is explained below.

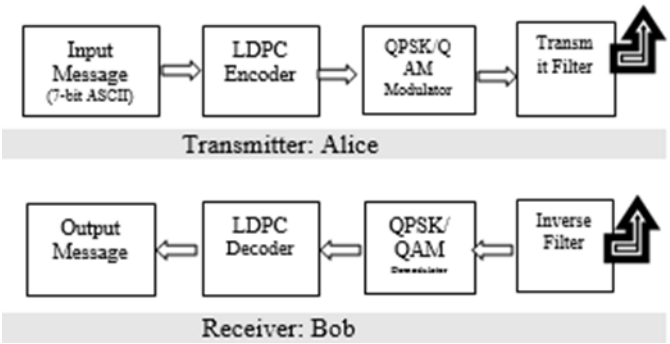

Fig. 2. Proposed Method Block Diagram

A. LDPC Coding

The Low-Density Parity Check code (LDPC code) is a kind of the linear error correcting code. Basically, it is a block code with a low-density parity check matrix H. The low density here means that there are only a few ones in the matrix H, and the other elements of H are all zeros. The LDPC code has the following advantages. First, it can achieve performance close to the Shannon limit provided that the codeword length is long [9]. Second, it has a lower decoding complexity than that of the Turbo code. The commonly used decoding algorithm for LDPC is belief propagation, which is parallelizable and can be accomplished at significantly greater speeds than the decoding of Turbo codes. Third, the decoding algorithm is verifiable in the sense that decoding to a correct codeword is a detectable event [10].

B. Quadrature Amplitude Modulation

• A modulation technique that employs both Phase Modulation (PM) and Amplitude Modulation (AM). Widely used to transmit digital signals such as digital cable TV and cable Internet service, QAM is also used as the modulation technique in orthogonal frequency division multiplexing (OFDM). The “quadrature” comes from the phase modulation states are 90 degrees apart from each other.

• Using 128-QAM, it will take 7 bits per symbol then the rate of the symbol is 1/7. It provides more bandwidth than QPSK. It is higher order modulation with greater flexibility in modulation and demodulation.

C. Channel Inversion Method

• Zero Forcing Equalizer: It refers to a form of linear equalization algorithm used communication systems which apply the inverse of the frequency response of the channel. So it means, zero forcing algorithm is used to inverse the frequency response of the channel.

• “The Zero-Forcing Equalizer applies the inverse of the channel frequency response to the received signal, to restore the signal after the channel.[1] It has many useful applications. For example, it is studied heavily for IEEE 802.11n (MIMO) where knowing the channel allows recovery of the two or more streams which will be received on top of each other on each antenna. The name Zero Forcing corresponds to bringing down the inter symbol interference (ISI) to zero in a noise-free case. This will be useful when ISI is significant compared to noise.”

• “For a channel with frequency response F(f), the zero forcing equalizer C(f) is constructed by C(f)=1/F(f). Thus, the combination of channel and equalizer gives a flat frequency response and linear phase F(f)*C(f)=1.”

4. SIMULATION RESULTS

In this, simulation results of the proposed method of secure communication between the Bob and Alice with the third party unauthorize user called eavesdropper. The graphs between legitimate and Eve is shown in the Rayleigh fading channel. We have simulated the proposed method using MATLAB simulation results, through Bit Error Probability (BER) of both the Bob and Eve with the channel mismatch.

Fig. 3. Will represents the secured communication of the message bits by both the users in Rayleigh Fading Channel with the QPSK as modulation Scheme. Using QPSK only 2-bits/symbol is transmitted across the channel but bit error rate is small as compared to higher order modulation schemes.

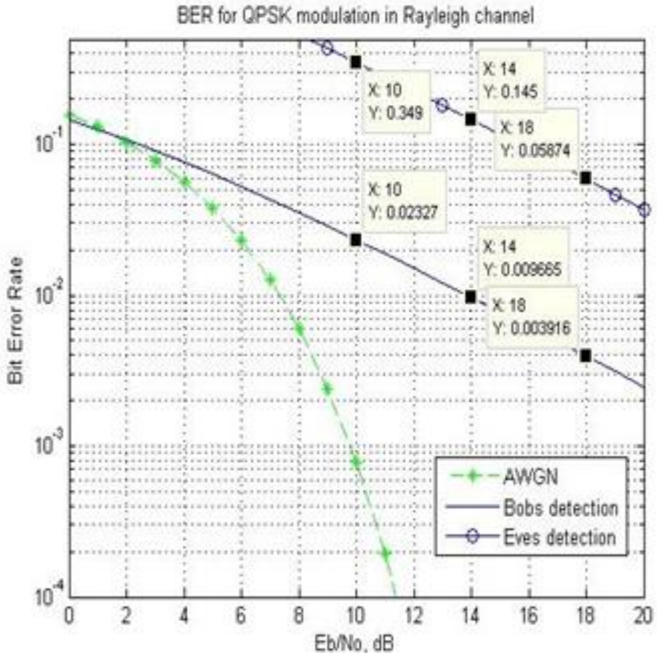

Fig.3. Bob's BER results and Eves BER results using QPSK

At SNR = 10dB both Bobs and Eves detection of the signal is un correlated. Hence, secure communication is obtained. By checking different SNR values of the simulated plot with the reference of AWGN channel is shown. Here, Table 1 shows the BER simulations of the legitimate and eavesdropper channel using QPSK modulation scheme.

Table: 1 BER simulations using QPSK modulation

SNR in dB	Bobs detection	Eves detection
10	0.023	0.349
14	0.009	0.145
18	0.003	0.058

Fig. 4. Will represents the secured communication of the message bits from the transmitter to receiver in Rayleigh Fading Channel. Here, we used a 128-QAM modulation scheme to achieve higher bit rate and low latency communication. Using 128-QAM there is 7-bits per symbol is transmitted across the channel. Hence the bit rate of the 128-QAM is given by 1/7. Table:2 will give the SNR vs BER values of both bob and eves detection using 128-QAM with different SNR values.

Table: 2 BER simulations using 128-QAM

SNR in dB	Bobs detection	Eves detection
9	0.091	0.261
12	0.058	0.248
15	0.034	0.240

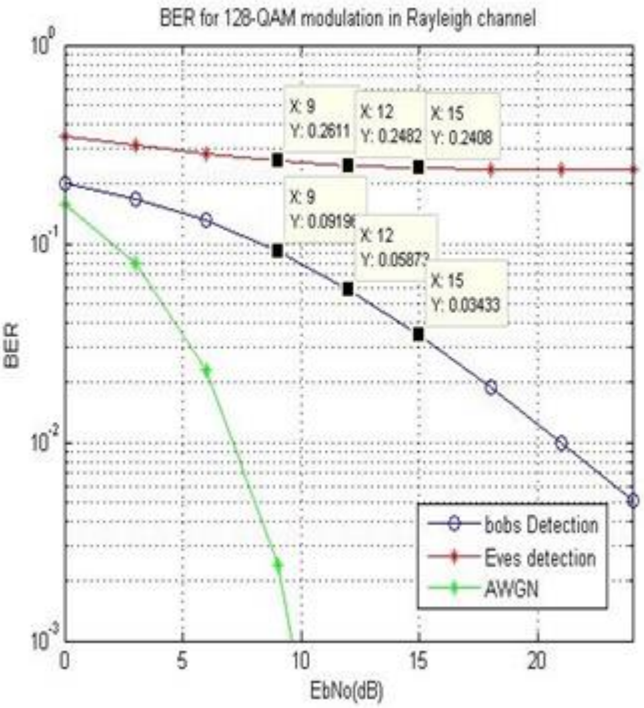

Fig. 4. Bob's BER results with Eves results to give low probability mismatch between them using 128-QAM

The comparison of both QPSK and QAM modulation with M=64,128 and 256 types is given below with the eavesdropper BER values are shown in Fig.5.

From this analyzing simulation results, a key mismatch between the Bob and Eve is perfectly shown with different SNR values in Rayleigh fading channel. As per considering of ASCII conversion, zero padding is required to achieve more secrecy and accurate processing of the bits. When we use ASCII conversion to convert plain text to bits, there is no need of Random Number Generator (RNG). In case of Unique Code Generation RNG may be suitable. In this paper clearly mentioned that a set of plain text (combination of characters, symbols and numbers) are used to transmit a signal. The communication wireless channel is Rayleigh fading and considering it is the noisiest channel among all different channels.

5. CONCLUSION

In this paper, we proposed the simulation results for secured message transformation across the channel with eavesdropper.

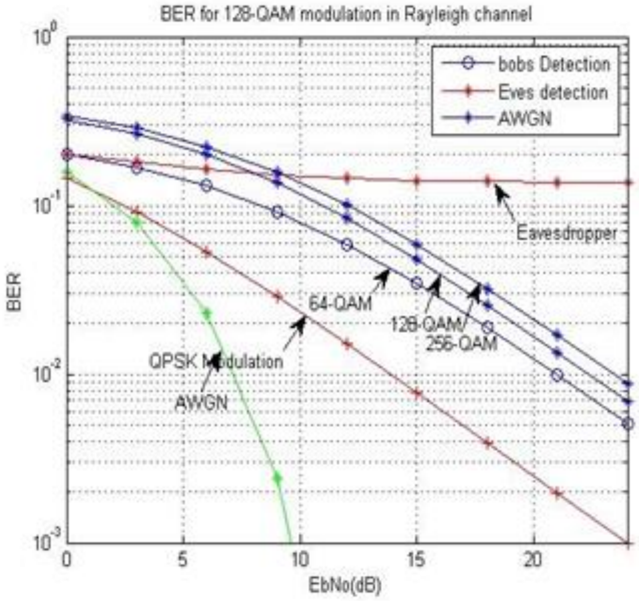

Fig. 5: Comparison of both QPSK and QAM modulated Alice & Bob with Eve simulation results

The uniqueness of legitimate users and eavesdropper are exploited to achieve more secrecy between them and to prove low secret key mismatch occurrence at different SNR values. When usage of 128-QAM gives a low BER is obtained but signal gets transmitted very accurately. Flexible and secured coding mechanism called LDPC is used in this proposed method. This simulation results will give the secured way of communication when legitimate and eavesdropper are almost correlated with each other. Future research ways of this project are to achieve low latency with secured communication.

6. ACKNOWLEDGEMENT

In this paper, all simulations and theory based on the understanding of reference papers attached here. The above statements made herein are responsibility of the authors.

7. REFERENCES

[1] S. Mathur, W. Trappe, N. Mandayam, and C. Ye, "Radio- telepathy: extracting a secret key from an unauthenticated wireless channel," Proceedings of the 14th IEEE, pp. 128– 139, 2008.
[2] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-Theoretically secret key generation for fading wireless channels," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 240–254, 2010.
[3] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," Proceedings – IEEE INFOCOM, 2010.
[4] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 1779–1790, 2013.
[5] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," IEEE Transactions on Information Forensics and Security, vol. 7, no. 5, pp. 1484–1497, 2012.
[6] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," Proceedings - IEEE INFOCOM, pp. 3048– 3056, 2013.
[7] Y. Qiao, K. Srinivasan, and A. Arora, "Shape matters, not the size: A new approach to extract secrets from channel," 1st ACM MobiCom Workshop on Hot Topics in Wireless, HotWireless 2014, pp. 37–41, 2014.
[8] C. Y. Wu, P. C. Lan, P. C. Yeh, C. H. Lee, and C. M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 1687–1700, 2013.
[9] G. Strang, Introduction to linear algebra. Wellesly, MA: Wellesley-Cambridge Press, 2003.
[10] H. Taha and E. Alsusa, "Physical layer secret key exchange using phase randomization in MIMO-OFDM," in Proc. IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA,December 2015, pp. 1–6
[11] Mansoor Shafi, Andreas F. Molisch, Peter J Smith, "5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment and Practice," IEEE journals on Selected Areas in Commun., Vol. PP, no. 99, April 2017.
[12] IMT Vision, "Framework and overall objectives of the future development of IMT for 2020 and beyond," Recommendation ITU-R, M.2083, September 2015.
[13]Huawei Whitepaper, "New Air Interface and radio Access Virtualization", April 2015.
[14] G.Durisi T. Koch, "Towards Massive, ultra-reliable, and low-latency wireless: The art of sending short packets," Proc.IEEE, vol.104, no. 9, pp.1711-1726, Sep.2016.