JCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-4, Issue-11 E-ISSN: 2347-2693

# Study On Physical Layer Wireless Security Techniques

**Lemya S[1*], Meera V.M[2] and Thrupthi A[3]**

[1] Computer Science, APJ Abdul kalam Technological University, India
[2] Computer Science, Cusat University, India
[3] Computer Science, APJ Abdul Kalam Technological University, India

e-mail: lemya.sain@gmail.com, meeravm@royalcet.ac.in, thrupthymohan@gmail.com

**Available online at: www.ijcseonline.org**

Received: Oct/09/2016 Revised: Oct/21/2016 Accepted: Nov/20/2016 Published: Nov/30/2016

***Abstract*—**Communication security is an essential and progressively difficult issue in wireless networks. Physical-layer approach to secret key generation which is each quick and independent of channel variations is taken into account. This approach makes a receiver jam the signal during a manner that also permits it to decrypt the info, nevertheless prevents alternative nodes from cryptography. Another well-known approach for achieving information-theoretic secrecy depends on deploying artificial noises to blind the intruders' interception within the physical layer. A multiple inter-symbol obfuscation (MIO) theme is planned, that utilizes a collection of artificial vociferous symbols to alter the initial knowledge symbols within the physical layer. MIO will effectively enhance the wireless communications security.

***Keywords-*** *Wireless communications security, physical layer security, information-theoretic secrecy, artificial noise*

## I. INTRODUCTION

Wireless networks have become an imperative part of people's way of life. As a result, security is an important issue in wireless networks since the users may transmit their sensitive personal info (e.g., mastercard details)over the wireless networks. In wireless networks, physical (PHY) layer security permits nodes to communicate firmly while not victimization resource intensive coding mechanisms at the appliance layer. PHY layer security measures square measure resource friendly to their info suppositious construct supported good secrecy in distinction with the process hardness approaches [5]. Compared with the standard asymmetric/symmetric cryptologic techniques which offer the process secrecy, it's been established that, physical layer security techniques, like employing a correct channel cryptography, are able to do the information-theoretic secrecy that makes the snooper hardly break the coding even it's unlimited computing power. The guarantee of security provided by CD-PHY [3] is much stronger than just keeping the modulation type (BPSK, QPSK, and QAM 1 , for example) a secret between the sender and the receiver. However, the information- notional secrecy needs a strict positive secrecy capability that the legitimate transmitter and receiver need to be during a higher quality channel than the aggressor. In MIO, [2] upon sending every information packet, a random set of the corresponding information symbols are obfuscated with a group of artificial vociferous symbols, that is termed symbols key, so that (1) the snooper's channel quality is worse than the legitimate receiver's and (2) the eavesdropper cannot decipher the information symbols properly since it doesn't apprehend the symbols key, that is updated dynamically throughout the information packets' transmissions. Within the planned technique of ijam, the sender repeats its transmission. For every sample in these recurrent transmissions, the receiver arbitrarily jams either the sample within the original transmission, or the corresponding sample within the repetition. Since the snooper doesn't apprehend that signal sample is packed and that one is clean, it cannot properly rewrite the information. In distinction, the receiver is aware of that samples it packed. Thus, the receiver will decide the proper samples from the signal and its repetition and set up them to induce a clean signal, that it will rewrite victimization customary ways [1].

The following sections comprises of a brief decsription of the two methods. Followed by the detailed explanation of the comparison results between the ijam method and obfuscation technique. Finally the paper is concluded.

## II. MATERIAL AND METHOD

This survey focuses on the following two schemes:

The first paper deals with a replacement approach to physical layer security that is freelance of channel variations, and therefore works even when the channel is static. This strategy introduces iJam, a channel- freelance PHY technique that ensures that associate snooper cannot even extract a wireless signal not meant for it. And it additionally shows that iJam achieves orders of magnitude higher secrecy rates than existing schemes with no bit disagreement [1].

1. iJam : iJam is a PHY-layer technique that enables two wireless nodes to exchange an unencrypted secret key, in the presence of an eavesdropper without loss of generality .

iJam is a channel-independent PHY technique that ensures that an eavesdropper cannot even demodulate a wireless signal not intended for it .

The second paper describes about a method of multiple inter-symbol obfuscation (MIO) scheme to enhance wireless communications security at the physical layer. In MIO, upon sending each data packet, a random subset of the corresponding data symbols are obfuscated with a set of artificial noisy symbols, which is called symbols key. For the legitimate receiver, it can offset the obfuscation of the symbols key by employing the reversed symbols key to derive the intended data symbols from the legitimate transmitter.

2. MIO : MIO scheme, which utilizes a set of artificial noisy symbols (symbols key) to obfuscate the original data symbols in the physical layer .In addition, the legitimate receiver can discern the fake packets sent from the adversary as it will fail to pass the integrity check of the symbols key on the fake packets through symbol cross-correlation [2].

## III. RESULT AND DISCUSSION

### I. iJam

iJam works by strategically jamming the transmission so as to prevent an eavesdropper from getting any information about the secret key, while allowing only the intended receiver to decode the key accurately (figure shown below).

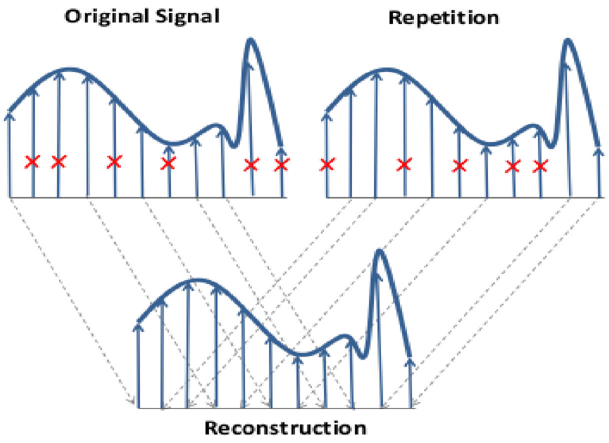

Fig 1: ijam at work

### A. *Stage 1 : Sequence generation- Salt*

The sender generates a random sequence of B bits, which we refer to as a salt. It delivers the salt to its PHY for transmission, along with the standard packet header. The PHY generates the OFDM signal corresponding to the packet. However, for each OFDM symbol corresponding to the salt, the PHY sends 2 copies of the symbol back-to-back. The PHY layer at the receiver starts by decoding the packet's header. If the header is marked to indicate an iJam packet and the MAC address matches the receiver's MAC address, the PHY waits until the end of the header, then starts jamming the transmission [1].

### B. *Stage 2: Signal jamming*

For each received signal sample from the salt, the PHY either jams the original sample or its repetition as shown in the above figure. Since an OFDM symbol and its repetition are back- to-back, the PHY knows how to match a sample and its repetition. To jam a sample, the PHY transmits a signal sample that is drawn randomly from a zero-mean Gaussian distribution whose variance is set to the variance of an OFDM signal with the same modulation [1].

### C. *Stage 3: Salt decoding*

To decode the salt, the PHY stitches the unjammed samples together to create a clean version of the OFDM signal corresponding to the salt. It then decodes this clean signal to obtain the bits in the salt. If the bits pass the checksum, the receiver sends an acknowledgment to the sender. If the sender does not receive an ack, it repeats the process with a different random salt. Once the sender and receiver have successfully exchanged a salt, they can use it to generate the secret key [1].

### 2. MIO: Multiple Inter-symbol Obfuscation

This paper describes about a scheme to secure the wireless transmissions between two legitimate entities. MIO does not need any trusted third party to interfere the packet interception by the eavesdropper or static channel condition to cancel artificial noises. Rather, it employs the data symbols from the previous data packets to generate the symbols key which obfuscates the current data packets.

MIO method includes two stages: MIO encryption and MIO decryption. MIO addresses two types of adversaries, passive eavesdropping attack and fake packet injection attack, during the wireless communication [2].

1) Passive Eavesdropping Attack: An adversary eavesdrops on the wireless medium and intercepts the wireless transmission between the legitimate transmitter and receiver. It can attempt to decode the signal from the intercepted signal with the presence of the MIO scheme. The MIO scheme will

provide the information-theoretic secrecy to enhance the wireless communications security.

2) Fake Packet Injection Attack: An adversary injects fake packets to the legitimate users, triggering the events to further disrupt the users's manner (e.g., mislead the users' operations). Unlike the passive eavesdropping attack, it can deploy the brute-force to test all possible symbols keys to inject a fake packet. The MIO scheme will enhance the computational secrecy to defend against this attack.

### *A. Stage 1: MIO Encryption*

In this first consider that legitimate transmitter A is about to send N data packets to legitimate receiver B. For each data packet, it goes through the MIO encryption process by two steps: (1) symbols obfuscation and normalization and (2) symbols key update at the transmitter. The average power of the encrypted symbols would not be the same as that of the original data symbols at the transmitter. This energy difference may let the eavesdropper distinguish the encrypted symbols from the non-encrypted ones according to the surge of the transmission power. To avoid this problem, the encrypted symbols should be normalized before they go to the digital to analog converter (DAC). After normalization, the energy of the encrypted symbols is almost the same as that of the data symbols. Consequently, the eavesdropper is hard to determine whether the received symbols are non-encrypted data symbols or encrypted symbols [2].

### *B. Stage 2: MIO Decryption*

When those encrypted symbols arrive at the legitimate receiver through the wireless channel, the receiver would conduct the MIO decryption process in two steps: (1) key checking and symbols decryption and (2) symbols key update at the receiver. Encryption and decryption process is shown in the figure below:

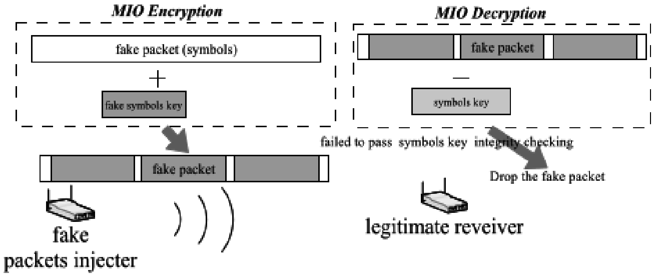

Fig 2: Overview of MIO scheme

The encrypted symbols blocks are randomly selected when a new packet (data symbols) goes to the symbols obfuscation & normalization block at the legitimate transmitter. This randomly pick-up mechanism can enhance the security level. However, at the receiver side, it would make the legitimate receiver hard to locate those encrypted symbols blocks due to: (1) the positions of those encrypted symbols blocks cannot be carried in the last packet because the sizes of adjacent data packets are independent from one other and (2) the receiver cannot precisely determine whether the received symbols are the packet's data symbols at the physical layer during the wireless communications.

To precisely discern those encrypted symbols blocks, the legitimate receiver adopts a cross- correlation operation with the assistance of the symbols key, called key checking. It is clear that by using this cross-correlation operation, the legitimate receiver can eliminate the channel noise influence to locate the correct position for each encrypted symbols block without any packet information (e.g., the first symbol of the packet and the relative positions of the encrypted symbols blocks in the packet). This makes MIO more practical during wireless communications [2].

### C. Stage 3: Computational Secrecy of the Initial Key

The MIO scheme has to use the conventional key agreement protocols to start the secure wireless communications. As the MIO scheme does not deploy any trusted third party to issue a certificate authority to the legitimate pairs, it would inevitably make the secrecy of the first symbols key, which is generated by the password-authenticated key agreement scheme, computationally bounded. Thus, the adversary with enough computational power can crack the first symbols key if the same symbols key has been used over a long time. Furthermore, if the eavesdropper can correctly receive all the subsequent encrypted data packets, it can determine all the symbols keys and crack the encrypted data packets. In this situation, the MIO's secrecy is bounded by the first key agreement scheme. Moreover, to avoid the long-term use of the pairwise authenticated password, the password also has to be updated when each communication session is completed. Please note that the MIO scheme is not restricted to the key agreement protocol described in the paper. It can apply to any bit-level key agreement schemes as the symbols key's parameters and the first symbols key can be generated from any bit-level keys by using the one-way hash function [2].

## IV. **CONCLUSIONS**

The first section of the survey relies on an easy mechanism that introduces iJam, a unique PHY technique that allows two wireless devices to communicate secret bits, within the presence of a snooper, and without cryptography. This technique however solely focuses on securing the information once being received by the intended receiver in an exceedingly communication system. This report enlightens the strategy of securing wireless communication through obfuscating the eavesdroppers by utilizing a collection of artificial noisy symbols. MIO doesn't want any trustworthy third party to interfere the packet interception by the snooper.By dynamically changing the symbols key as the packets are disseminated, it's difficult for somebody to brute-force the symbols key by intercepting variety of encrypted symbols and analyzing them offline.

## REFERENCES

[1] S. Gollakota and D. Katabi, “Physical layer wireless security made fast and channel independent,” in Proc. IEEE INFOCOM, Apr. **2011**, pp. **1125–1133**.

[2] Tao Xiong, Wei Lou, Jin Zhang, Hailun Tan, MIO: Enhancing Wireless Communications Security Through Physical Layer Multiple Inter-Symbol Obfuscation, *IEEE*, VOL. **10**,NO. **8**, pp.**1678-1691**, **2015**.

[3] M. I. Husain, S. Mahant, and R. Sridhar, “CD-PHY: Physical layer security in wireless networks through constellation diversity,” in Proc. IEEE MILCOM, Oct./Nov. **2012,** pp. **1–9**.

[4] Block Cipher Encryption Process, www.nist.gov/bcencrypt, Mar 12, **2015**.

[5] Charalampos N. Pitas, Christos E. Tsirakis, “Emerging communication technologies and security challenges in a smart grid wireless ecosystem”, Int. Journal of Wireless and Mobile Computing,Vol. **7**, No.**3** pp. **231 – 245**, **2014**.

## Authors Profile

*Mrs. Lemya S* pursued Bachelor of Technology in Information Technology from University of Calicut, India in 2014 and is currently pursuing Master of Technology from Kerala Technological University. She has published few papers in important conferences. Her main research work focuses on Physical layer security techniques.

*Ms Meera V.M* pursued Bachelor of Science and Master of Science from Cusat University. She is currently working as Assistant Professor in Department of Computer Science, Royal College Of Engineering and Technology since 3 years. She has published many papers and has attended conferences including IEEE and it’s also available online. Her main research work focuses on data security and networking.

*Mrs. Thrupthi A* pursued Bachelor of Technology in Computer Science from University of Calicut, India in 2012 and is currently pursuing Master of Technology from Kerala Technological University. She has published few papers in important conferences. Her main research work focuses on network security.