Physical Layer Wireless Security Shaped with Noisy Symbol Keys

Vaishnavi.R
Department of Computer Science and Engineering
M.A.M College Of Engineering
Trichy. Tamilnadu.

Sri Santhoshini.E
Department of Computer Science and Engineering
M.A.M. College of Engineering Siruganur,
Siruganur, Trichy. Tamilnadu.

Abstract--**In the wireless networks, communication security is the major issue. So we are creating the artificial noise with the message during the communication. We use the multiple inter-symbol obfuscation (MIO) to utilize a set of artificial noisy symbols to obfuscate the original data symbols at the physical layer. In this paper we defend against the passive eavesdropping attack and fake packet injection attack in the wireless communication. A multiple inter-symbol obfuscation (MIO) scheme, which utilizes A set of artificial noisy symbols (symbols key) to obfuscate the original data symbols in the physical layer. MIO can effectively enhance the wireless communications security. An eavesdropper, without knowing the artificial noisy symbols, cannot correctly decrypt the obfuscated symbols from the eavesdropper packets. A legitimate receiver can easily check the integrity of the symbols key and then reject the fake packets from the received packets. The proposed secure technique is never breakup by the eavesdropper or any malicious hacker and there is no possibility** to **the fake packet injection attack and the passive eavesdropping attack on the original data packet during the communication in the wireless communication. By using this multiple inter symbol obfuscation technique we convert the unicast transmission into multicast transmission to transmit the data from single sender into multiple receivers. It is very useful in tv channels and fm stations for transmit the data to multiple receivers.**

Keywords-- Multiple inter symbol obfuscation, Physical layer, Cyclic redundancy check, Network security, Symbol key update.

I. INTRODUCTION

A network is a group of two or more computer systems linked together. The computer networks are mainly buildup with the combination of both hardware and software. The goal of network security is to provide security for the data transmission. Security is the process of providing some protection against any type of attacks during the transmission of data packets over the wireless communication between the legitimate sender and the legitimate receiver. Today's world there is nothing can doing without network. Because in recent few years information transmission and management process is highly developed. Some common attacks in wireless network are active attack, passive attack.

Active attack is easy to identify but passive attack is more dangerous than earlier. In network security cryptographic method widely used technique to data transfer process. Cryptographic includes encryption and decryption algorithms for security. Encryption means convert plain text to cipher text and decryption is its reverse process**.** Mostly in network security the encryption process will be done in the network layer during the transmission of data packets fro sender to receiver in the network so there is lot of possibilities for hijack the data packet over the network. For the reason to overcome this problem is to provide the security in the primary layer that is to done the encryption process in the physical layer by that way we can able to provide high level security to the data packets over the network during the data transmission. In this paper we will use the multiple inter symbol obfuscation technique to provide the security to data packets over the network.

The word obfuscation means confusion. In this paper we will make the confusion to eavesdropper by that way we can able to avoid the passive eavesdropper attack and the fake packet injection attack during the conversation. In this method we will add the extra additional noisy symbols in between the original message which is created by the sender but the location is send by the receiver in the previous acknowledgment. So there is no possibilities to send any type of key to the clarification purpose for the receiver because he will already knows the particular location where the noisy symbols are added by the sender in the original message. So there is no way to hijacking the data packets. And also the fake packet injection will be identified by the cyclic redundancy check process by that way we will provide the protection against the fake packet injection attack and passive eavesdropping attack. So we can assure that this technique is more powerful than the all other type of security mechanisms.

II.RELATED WORKS

There are several methodologies and techniques are used in the network for their security purpose. S.Gollakota proposed the new mechanism of ijam for the purpose of sending the data packets between the sender and receiver very fast. In this method to implement a new physical layer approach ijam to secret key generation that is both fast and independent of channel variations. This PHY technique that ensures that an eavesdropper cannot even demodulate a wireless signal not intended for it. The basic idea in the ijam is very simple that is the sender repeats its transmission. Then, the receiver can pick the correct samples from the signal and its repetition and rearrange them to get a clean signal, which it can decode using standard methods. The main merit of this method is eliminating the need for out-of-band channels and third party intervention. This Ijam method is fast and accurate and the major problem is the redundancy mechanism, the throughput is reduced and another one is it is also requires the signal synchronization between the sender and receiver.

M. I. Husain proposed the technique physical layer security in wireless network through the constellation diversity. The main mechanism of this method is the constellation diversity to provide the security to the physical layer. At the physical layer, the source and the intended destination uses a custom constellation mapping which acts as a secret key to secure the communication from an eavesdropper. So, the eavesdropper will not even be able to decode the signal correctly without the knowledge of constellation mapping. The main advantage of this method is it will increases the bit error rate (BER) at the eavesdropper side by using different constellation maps in wireless transmissions, this constellation diversity mapping can hardly be detected by normal symbol detection attempts. But one major problem is occurred in the method is this scheme is more suitable for the complex modulation and the problem is the information-theoretic secrecy can be compromised under certain specific symbol detection attempts.

In the existing system they would provide the security during the transmission of packets between the sender and receiver by using number of antennas. They are adding the extra noise with the original data packet so that the hacker will be confused. The noisy data packet will make some obfuscation to the hacker that way we are provide the security to the data packet during transmission. MIMO method for multiplying the capacity of a radio link using multiple transmitter and receiver antennas to exploit multipath propagation. It is a practical technique for sending and receiving more than one data signal on the same radio channel at the same time via multipath propagation. In the existing system the original packet will be transmitted with more than one frequency or artificial noise to the receiver.

Compared with traditional asymmetric or symmetric cryptographic techniques which provide the computational secrecy? This method will achieve the information theoretic secrecy which makes the eavesdropper to hardly break the encryption even it has unlimited computing power. However the information theoretic secrecy requires a strict positive secrecy capacity that the sender and receiver have to be in a better quality channel than the attacker. The works have been shown by artificially interfering the transmitting signal the positive secrecy capacity requirement can be achieved.

The main demerits in the existing paper is we are using several antennas to create the noise. It is difficult to buy the number of antennas for the single transmission. It will decrease the performance of the system and it will also easy to guess the pattern of the noisy symbols. MIMO method needs to deploy trusted third Parties. It requires multiple antennas to generate the artificial noise. The positive secrecy capacity of these works may be compromised if the eavesdropper deploys at certain locations. So, wireless channels are susceptible to eavesdropping and malicious message injecting due to the openness and sharing of the wireless medium. And another important drawback is it is the unicast transmission process so the performance is low.

III. PROPOSED METHOD

In the proposed system we will provide the security by using the MIO method. It means the data from sender will be encrypting using MIO encryption we will add noise in between the message. The order of the noise injection is send by the receiver with the previous acknowledgement so the hacker will never identify the pattern. The time to live algorithm will be used to increase the performance of the network by discarding the time over data packet.

Adopt a multiple inter-symbol obfuscation (MIO) scheme to enhance wireless communications security at the physical layer. Multiple inter-symbol obfuscation (MIO) scheme, which utilizes a set of artificial noisy symbols (symbols key) to obfuscate the Original data symbols in the physical layer. Explore the feasibility of symbol obfuscation. Defend against the passive eavesdropping attack and fake packet injection attack during the wireless communications it improves the scalability and high security to wireless communication

This scheme is used to enhance wireless communications security at the physical layer. Multiple inter-symbol obfuscation (MIO) scheme, which utilizes A set of artificial noisy symbols (symbols key) to obfuscate the Original data symbols in the physical layer. Explore the feasibility of symbol obfuscation. Defend against the passive eavesdropping attack and fake packet injection attack during the wireless communications. This improves the scalability and high security to wireless communication.

The major advantage of this paper is this system will increase the performance of network by discarding the waste message in the network. We will provide the security to the message or data packet during transmission. Generate the eavesdropper, without knowing the artificial noisy symbols in the original data. Find & prevent the fake packet injection attack during the transmission in the wireless communication. Achieve information-theoretic secrecy against the passive eavesdropping attack and computational secrecy against the fake packet injection attack. And this paper supports the multicast transmission so the performance is very high.

A. Basic terminologies:

1. Multiple inter symbol obfuscation

In this technique we will add the extra additional noisy symbols in between the original data packet which is created by the sender transfer to the receiver.

2. Physical layer

The physical layer is one of the osi layer mainly used to transfer the data packets from one user to another user. It is a basic layer and very closer to the sender.

3. Cyclic redundancy check

This method is one of the checking process used to identify the interruption in the original message which is transferred by the sender to receiver and this checking process done at the receiver side.

4. Network security

Now a days the network connection are very much essential to all the departments meanwhile the security is the major problem so we will go to improve the security.

5. Symbol key update

That means we will update the extra additional noisy symbols in between the original data packets to improve the security

.

B. Architecture:

The process of defining the sender will sends the data with the MIO encryption by adding the additional symbol keys to make obfuscation to the hacker the receiver will use the same MIO decryption method to decrypt the original message in the receiver side and finally use the CRC technique to verify the received message is correct or not. The sender will sends the data packet to the receiver in the way the data modulation is used to convert the data packets into binary format. Then the next stage is to update the keys into the original message which is created by the sender for receiver it is the encryption process then we will send the encrypted packet to the receiver, at the receiver side the update symbol keys will be removed then the original message in the binary format will be send the normal decoder will convert the binary type message into original message. The cyclic redundancy check will be used to check if any additional packet will added in the original packet. If yes means it will automatically drop the packet. If no means it transfer the data packet to the receiver.

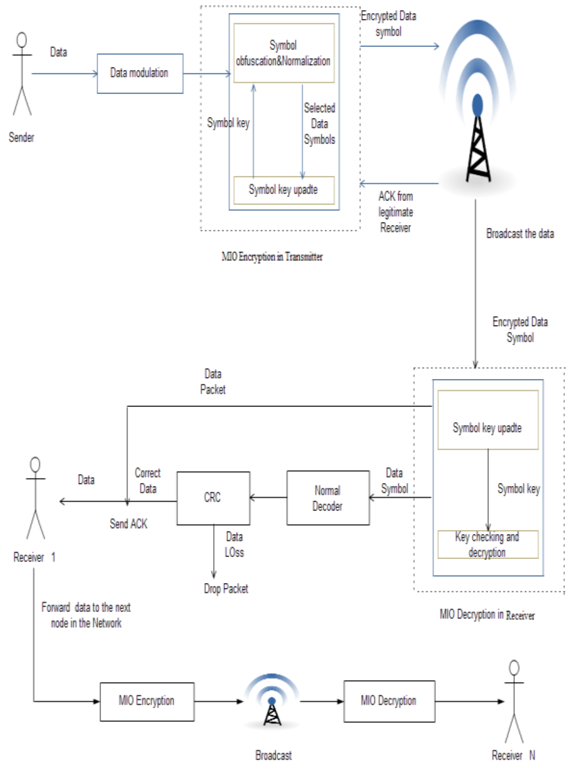

Figure 1.System architecture

Algorithm

1. Cyclic Redundancy Check (CRC).
2. Multiple Inter-symbol Obfuscation (MIO).
    a. Encryption Algorithm
    b. Decryption Algorithm

Send an empty packet to the receiver after packet delivery got an acknowledgement form the receiver and MIO decryption using that a acknowledgment to update the symbol key in the MIO encryption. The data from the transmitter converted into the data symbols then we added the update symbol key (noise key) to the converted data.

Example:

Symbol	Binary	Bit to Location add symbol key
**	00101010	1
#	00100100	2

Encrypted data=Data symbols + symbol keys The encrypted data symbol from the transmitter are decrypted by the MIO decryption block. In this block remove the added symbols key at MIO encryption block by using symbol key update Decryption=encrypted data symbols-symbol key. The CRC check the received data, check all the transmitted data received correctly or not. Finally the receiver got the transmitted data(Original data)

C. Modules decription:

1. Formation of Network Nodes

This figure shows the node registers the details such as Node IP address, port number, and distance. Nodes details are stored and maintained in sever database. After that Nodes enter the ip and port number to activate themselves in the network.

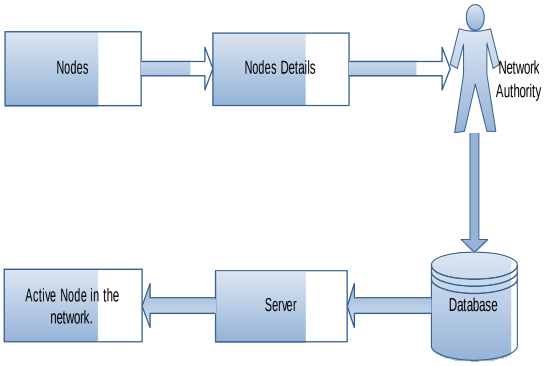

Figure 2. Formation of network nodes

2. Data Conversion on Sender

This figure shows generally in network before transmission the data's are converted into the data packets, only these data packets are transmitted on the network. In this module the transmitted data packets are converted to data symbols by using the coding and modulation technique.

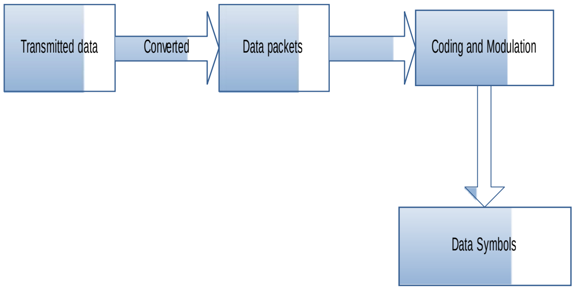

Figure 3. Data conversion on sender

3. Receiver updating the symbol key by Acknowledgement

This figure shows transmitting the original data, we send an proper packet (Empty packet) to the receiver. This packet transmitted via MIO encryption and decryption .after successfully receive the data at the receiver side ,the receiver send an acknowledgement to the transmitter via MIO decryption .the MIO decryption update the simple key then send an updated keys with acknowledgement. MIO encryption also updates the symbol key by using the acknowledgement from the MIO decryption.

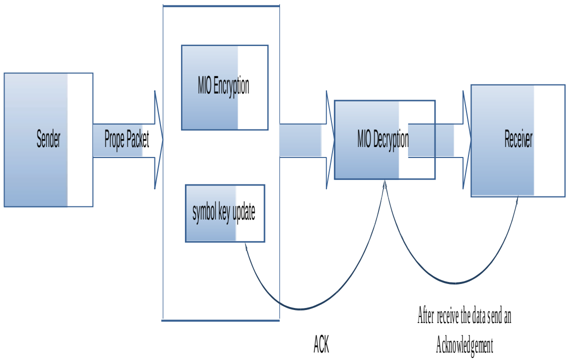

Figure 4.Receiver updating the symbol key by acknowledgment

4. MIO Encryption &Decryption

This figure shows the MIO encryption get an data symbols, add an updated noise symbol key's to the data symbol .then the updated data symbol transmitted to the MIO decryption. In MIO decryption they check the key and decrypt the data symbol with using the symbols key update.

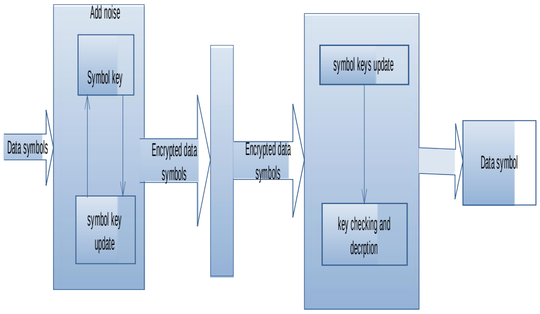

Figure 5. MIO Encryption & Decryption

5. Drop the corrupted Packet using CRC technique

This figure shows the module we drop the corrupted packet by using the Cyclic Redundancy Check (CRC). Once the data symbols are decrypted, the receiver maps all these plain data symbols to digital bits in the normal decoder block .so that the channel noise can be filtered out. After decoding the digital bits, receiver will check if the packet is correct through cyclic redundancy check (CRC).

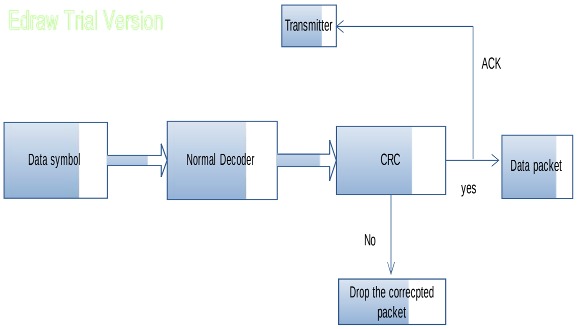

Figure 6. Data corrupted packet using CRC technique

IV. CONCLUSION

In this paper, we propose a multiple inter-symbol obfuscation (MIO) scheme to secure the wireless transmission between two legitimate entities. In this work we have propose a multiple inter-symbol obfuscation (MIO) 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. By dynamically updating the symbols key as the packets are disseminated, it is hard for an adversary to brute-force the symbols key by intercepting a number of encrypted symbols and analyzing them off-line. We establish the mathematical model for MIO, and prove that MIO can provide both the information-theoretic secrecy and computational secrecy without considering the initial key.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. *J.*, vol. 54, no. 8,pp. 1355–1387, Oct. 1975.

[2] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," in Proc. ESORICS, Sep. 2011, pp. 40–59

[3] D. León, S. Balkir, M. Hoffman, and L. C. Pérez, "Fully programmable, scalable chaos-based PN sequence generation [CDMA]," Electron. Lett., vol. 36, no. 16, pp. 1371–1372, Aug. 2000

[4] D. R. Stinson, "Universal hashing and authentication codes," Designs, Codes, Cryptogr., vol. 4, no. 3, pp. 369–380, Oct. 1994.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[6] G. Van Assche, Quantum Cryptography and Secret-Key Distillation. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[7] GNU GPL. (2015). *GNU* Radio—The Free and Open Source Software Radio Project.

[8] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[9] J. Thomson et al., "An integrated 802.11a baseband and MAC processor," in IEEE Int. Solid-State Circuits Conf., Dig. Tech. Papers, Feb. 2002, pp. 126–127.

[10] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[11] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[12] 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.

[13] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019,Sep. 2008.

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

[15] 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.

[16] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[17] I. Csiszár and J. Körner, "Broadcast channels with confidential messages,"IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[18] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[19] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[20] Ettus Research. (2015). Universal Software Radio Peripheral.

[21] D. León, S. Balkir, M. Hoffman, and L. C. Pérez, "Fully programmable, scalable chaos-based PN sequence generation [CDMA]," Electron. Lett., vol. 36, no. 16, pp. 1371–1372, Aug. 2000.

[22] T. Li, J. Ren, Q. Ling, and A. Jain, "Physical layer built-in security analysis and enhancement of CDMA systems," in Proc. IEEE MILCOM, Oct. 2005, pp. 956–962.

[23] C.-C. Chen, K. Yao, K. Umeno, and E. Biglieri, "Design of spread spectrum sequences using chaotic dynamical systems and ergodic theory," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol. 48, no. 9, pp. 1110–1114, Sep. 2001.

[24] S. Bhashyam and B. Aazhang, "Multiuser channel estimation and tracking for long-code CDMA systems," IEEE Trans. Commun., vol. 50, no. 7, pp. 1081–1090, Jul. 2002.

[25] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevi´c, "Secure nested codes for type II wiretap channels," in Proc. IEEE Inf. Theory Workshop, Sep. 2007, pp. 337–342.