International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.10, No.07, July 2021

# Symbol Obfuscation In Physical Layer For Achieving Security In Wireless Communications

**Venkatesh Thota**
**Asst. Professor**
**Department of CSE**
**Siddhartha Institute of Technology and Sciences**
**Narapally, Hyderabad, Telangana, India**

**Elukapalli Harish**
**Asst. Prof.**
**Department of CSE**
**Siddhartha Institute of Technology and Sciences**
**Narapally, Hyderabad, Telangana, India**

*Abstract*— **In wireless networks, secure communication is an important and challenging topic. Artificial noisy symbols are the most common method for achieving information theoretic secrecy. Multiple Inter-symbol Obfuscation (MIO) will be used in the physical layer to improve wireless communication security. MIO is a data transfer mechanism that ensures security in a wireless network. The MIO system will allow for broadcast data transfer while simultaneously preventing eavesdropper involvement and false packet injection. Using a set of symbol keys, the original data symbols are disguised. An eavesdropper will be unable to decrypt the original data symbols because information theoretic confidentiality will be achieved. During data transmission, the authentic receiver can readily validate the original data symbols and reject the bogus packet injection.**

***Keywords — Wireless communication security, Multiple Inter-symbol Obfuscation, Information theoretic secrecy, Physical layer.***

## I INTRODUCTION

Wireless communication encompasses a large chunk of the communication spectrum. It is the process of exchanging data between two or more systems. The use of public key and private key cryptography to secure privacy and authenticate wireless communication is the fundamental difficulty. Furthermore, due to malicious message injection and eavesdropping, wireless mediums are not secure. To protect against the interception of wireless communications, a redundancy system has been implemented. All signals must be delivered twice since additive noise could interfere with them randomly. The receiver can distinguish between the interfering and clean signals [3]. Low-Density Parity-Check (LDPC) Codes are used to achieve optimal communication. To

achieve wireless information-theoretic secrecy, four components were developed: common randomness vs. opportunistic transmission, message reconciliation, common key generation, and message protection with secret keys. A reconciliation technique based on multilayer coding and LDPC codes was also described as part of the key agreement protocol. The secret key agreement mechanism will be extended to allow for incomplete channel state information. When a valid user wants to transmit messages to other users, they will employ a wireless system configuration. Two criteria, average secrecy capacity and probability of secrecy capacity outage, would be used to assess the influence of fading on secure communication [10]. Specific distributed flow optimization algorithms serve as the foundation for the protocol, and a realistic distributed method is used to apply coding in real-world situations. End–to–End retransmission, End–to–End coding, Path coding, Link–by–Link retransmission, and Full coding are among the five processes available. The difficulty of establishing an efficient unicast connection can be solved using a distributed approach [8]. In a wireless network, network coding applications are employed to improve the bandwidth efficiency of reliable broadcast. Many retransmission broadcast schemes with and without network coding are presented. In a wireless network, network coding was used to exchange information. The XOR operation is used to exchange information between two wireless nodes. Various lost packets from different receivers are blended to recover lost data packets in a single transmission by numerous receivers [9].

## II RELATED WORK

A constellation diversity mapping method is the process of employing multiple constellation maps to secure wireless transmission and increase the bit error rate (BER) at the eavesdropper side. The three areas of physical layer security are channel coding approaches, signal design approaches, and artificial noise approaches [1]. The standard constellation shape is utilized to determine the modulation of received symbols, and the eavesdropper creates a scatter constellation map of the received symbols before recovering the robust constellation map using fuzzy c-means clustering. Maximum likelihood [7] is used to recreate a constellation map using predetermined digital modulation templates. The advanced encryption standard (AES) operation was employed to strengthen security in the Code division multiple access (CDMA) system, which utilized 128, 192, and 256 bits AES-CDMA PN code widths to increase security against eavesdropping [2]. In the field of wireless communications security, CDMA is a widely used channel coding technique. The legitimate user can only decrypt the encrypted transmission message using the bit-level pseudo noise code, and classical CDMA has a limited number of PN codes [12].

To protect against the interception of wireless communications, a redundancy system has been implemented. All signals must be delivered twice since additive noise could interfere with them randomly. The receiver can distinguish between the interfering and clean signals [3]. Adaptive power distribution based on channel realisation improves capacity insignificantly. The objective function will be used to optimise transmit power allocation between the artificial noise and the information signal by obtaining an analytical closed-form lower bound on secrecy capacity [4]. The average Secrecy Capacity (SC) has two methods: (i) without side information and (ii) with side information for active eavesdropping, which can be expressed as a one-shot two-player zero-sum game. Using game theoretic methods, they systematically assessed the effect of an active eavesdropper [5].

The ability of low-density parity-check (LDPC) code to accomplish the secrecy of the wiretap channel has been demonstrated, and it has been demonstrated that this code may be utilised to deliver totally secret communications at low data rates. The primary channel must be quieter than the eavesdropping channel, and the eavesdropping channel must be a general binary-input symmetric-output memory-less channel, which is unlikely to be the case in real-world wireless communications [6]. Computing the ideal secrecy capacity is the problem of the wire-tap channel to MIMO broadcast wire-tap channel. Perfect secrecy is attained when the suitable transmitter and receiver can communicate at positive rates. The multiple antenna wire-tap channel's secrecy capacity had been calculated. In order to ensure capacity computation, a proof technique for the converse has been provided [11].

## III SYSTEM DESIGN

The multiple inter-symbol obfuscation (MIO) design is described in this section, and it consists of two stages: MIO encryption (adding the noisy symbols key) and MIO decryption (offsetting the noisy symbols key). This system is built on MIO at the physical layer and requires an initial key to begin secure wireless communication.

### *A. MIO Encryption*

MIO encryption method have two steps:
(1) symbols obfuscation and normalization.
(2) symbols key update at the transmitter.

#### *1) Symbols(emblems) Obfuscation and Normalization:*

When data is transferred, the transmitter uses the set of symbol keys to map data symbols. The collection of symbols generates these obfuscated data symbols. The average power of the encrypted symbols at the transmitter would not be the same as the original data symbols. According to the transmission power, this energy difference may be used to identify encrypted symbols from non-encrypted symbols. As a result, determining whether the received symbols are non-encrypted data symbols or encrypted symbols was difficult for the eavesdropper.

2) *Symbols Key Update at the Transmitter:*

The next data symbols are dynamically encrypted after the symbols have been encrypted and normalised. For the next data packet, the dynamic symbols key update method requires that all symbols be correctly decrypted. To synchronise the noisy symbols key on the legal receiver side, the transmitter has been waiting for the right acknowledgment (ACK) from the receiver before processing the next packet.

### *B. MIO Decryption*

MIO decryption process is in two steps:

(1) key checking & symbols decryption.
(2) symbols key update at the transmitter.

(1) *Key Checking* & *Symbol(emblems) Decryption:*

The received encrypted symbol yk,i+j is equal to H EKeyk, j (mk,i+j) + wk,i+j, where H and wk,i+j are the wireless channel coefficient and Gaussian noise, respectively. Because (1) the positions of those encrypted symbols cannot be carried in the last packet because the adjacent data packets sizes are independent of one another, and (2) the receiver cannot determine whether the received symbols are the packet's data symbols at the physical layer, the appropriate receiver has a difficult time locating those encrypted symbol blocks.

*Symbols Key Update at the Transmitter:*

The receiver transfers the plain data symbols to digital bits in the standard decoder block when the data symbols are encrypted, allowing the channel coefficient and noise to be filtered out.

## IV THREAT MODEL

The purpose of wireless security is to prevent attackers from communicating with legitimate recipients and sending stuff to them. During wireless communications, we handle two types of adversaries in this paper: passive eavesdropping and fake packet injection attacks.

1) *Passive Eavesdropping Attack:* An adversarial eavesdropper could try to decipher the intercepted signal with the presence of MIO. The wireless signal between the lawful transmitter and receiver is intercepted by an enemy.

2) *Fake Packet Injection Attack:* An attacker sends bogus packets to legitimate users, causing events to occur. It can use brute-force to try all feasible symbols keys to inject a bogus packet, unlike passive eavesdropping.

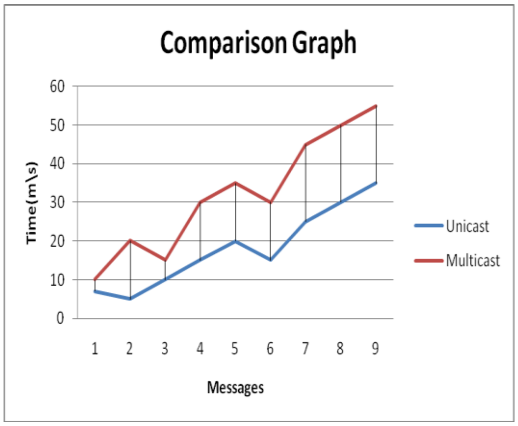
To fight against this attacks, the MIO technique will improve computational secrecy.

## V. SECURITY ANALYSIS

The secrecy of the MIO in wireless communication is discussed in this section. The MIO system then shows that it can provide both information-theoretic and computational secrecy to the passive eavesdropping attack in segment V-A and the false packet injection assault in phase V-B, respectively.

### ***Information-Theoretic Secrecy against the Passive Eavesdropping Attack***

The purpose of the secrecy capacity model is to demonstrate that the MIO approach may achieve information theoretic secrecy against passive eavesdropping attacks.



### *B. Computational Secrecy against the Fake Packet Injection Attack*

If the symbol key cannot be accurately deduced from the received encrypted symbols, the attacker will insert the bogus packet using a brute-force approach to test all possible symbol keys.

## VI. CONCLUSIONS

In the original data symbol, the noisy symbol was used. To avoid information from passive eavesdropping and malicious message injection, dynamic symbol key updating would be developed for symbol obfuscation. By adopting an inter-symbol obfuscation strategy on the physical layer, information theoretic secrecy can be accomplished in both unicast and multicast scenarios.

## VII. REFERENCE

[1] 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.

[2] 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.

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

[4] Xiangyun Zhou, Matthew R. McKay, “Physical Layer Security with Artificial Noise Secrecy Capacity and Optimal Power Allocation”, in proc. *IEEE ICSPCS*, Sep.2009, pp. 1 – 5

[5] Arsenia Chorti, Samir M. Perlaza, Zhu Han, H. Vincent Poor, “Physical Layer Security in Wireless Networks with Passive and Active Eavesdroppers”, in *proc. IEEE GLOCOM,* Dec. *2012,* pp. 4868 – 4873

[6] 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.

[7] B. G. Mobasseri, “Digital modulation classification using constellation shape”, *Signal Process.*, vol. 80, no. 2, pp. 251–277, Feb. 2000.

[8] Desmond S. Lun , Muriel M´edard & Ralf Koetter, “Network Coding for Efficient Wireless Unicast”, in *proc.* Feb 2006, pp. 74-77.

[9] Dong Nguyen, Thinh Nguyen, Bella Bose, “Wireless Broadcasting Using Network Coding”, in proc. IEEE TVT, June 2008, pp. 914 – 925.

[10] Matthieu Bloch, João Barros, Miguel R. D. Rodrigues, Steven W. McLaughlin, “Wireless Information-Theoretic Security”, in proc. IEEE TIT, June 2008,pp. 2515 – 2534

[11] 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.

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