Wireless Communication Security Through Symbol Obfuscation In Physical Layer

S. Niranjani and R. Nirmalan

1PG Scholar, Department of CSE, Sri Vidya College of Engineering and Technology, Virudhunagar, TN, India.
2Assistant professor, Department of CSE, Sri Vidya College of Engineering and Technology, Virudhunagar, TN, India.

Received February 2016; Accepted 18 April 2016; Available 25 April 2016

ABSTRACT

Wireless communication is an emerging trend in transfer of information. Secure communication is a main issue in wireless transformation. Artificial noisy symbol is a leading approach in achieving the information theoretic secrecy. Multiple Inter-symbol Obfuscation (MIO) method is deployed in the physical layer to enhance the security in wireless communication. In wireless data transmission MIO provides security for the information. MIO scheme supports both multicast and broadcast data transmission and also eliminate the fake packet injection and eavesdropper participation. By using set of artificial symbol keys the original data symbols are obfuscated. Because of these symbol key obfuscation an eavesdropper cannot able to get the original data symbols and an information theoretic secrecy will achieve. The legitimate receiver can able to reject the injected fake packet during the data transmission and achieve the original data symbols.

KEYWORDS: Wireless communication, Physical layer, Multiple Inter-symbol Obfuscation, Information theoretic secrecy, Multicast.

INTRODUCTION

Wireless communication is an broaden portion in communication method. It is a transferring information between two or more systems. The main challenge of wireless communication is the privacy protection and authentication by using public key and private key cryptography. Additionally, wireless mediums are not safe due to vicious message injecting and eavesdropping.

A redundancy mechanism have been adopted to defend against the wireless signals interception. All signals had been required to be sent twice that may be randomly interfered with additive noise. The receiver can identify the interfered signal and reconstruct the clean signal [3]. To achieve communication optimal Low-Density Parity-Check (LDPC) Codes are introduced. Secure communication protocols are developed to ensure wireless information-theoretic secrecy which used four parts: common randomness vs opportunistic transmission, message reconciliation, common key generation, message protection with secret keys. The key agreement protocol had been illustrated and also presented a reconciliation procedure based on multilevel coding and LDPC codes. For allowing imperfect channel state information the secret key agreement protocol will be extended. When a legitimate wants to send messages to other user wireless system setup will be used. The impact of fading on secure communication would be considered by two metrics such as average secrecy capacity and probability of outage of secrecy capacity[10].

A specific distributed flow optimization techniques form a basis of protocol and a practicable distributed method performs in practical situation to implement coding. That have five process like End-to-End retransmission, End-to-End coding, Path coding, Link-by-Link retransmission, and Full coding. And a distributed approach is to solve the problem of establishing efficient unicast connection[8].
Network coding applications is used to enhance the bandwidth efficiency of reliable broadcast in wireless network. Many retransmission broadcast scheme are described based on with and without network coding. Network coding had been employed to exchange the information in wireless network. For the information exchange between two wireless nodes XOR operation is used. Different lost packet from different receiver are merged to retrieve the lost data packets in one transmission by a multiple receiver[9].

Related Work:
A constellation diversity mapping method is to secure the wireless transmission and it increases the bit error rate (BER) at the eavesdropper side by use of different constellation maps. physical layer security had been the following three regions, channel coding approaches, signal design approaches, and artificial noise approaches [1]. The standard constellation shape is used for finding received symbol’s modulation and the eavesdropper constructs a scatter constellation map of the received symbols and used the fuzzy c-means clustering to recover the robust constellation map. The reconstruction of constellation map with predefined digital modulation templates is based on the maximum likelihood [7].

The Code division multiple access(CDMA) enhanced security based on the advanced encryption standard (AES) operation and it used 128, 192, and 256 bits AES-CDMA PN code sizes to raise the security level against eavesdropping [2]. CDMA is a popular channel coding scheme in the wireless communications security. The encrypted transmission message only be decrypted by the legitimate user by using the bit-level pseudo noise code and the traditional CDMA has limited PN codes[12].

A redundancy mechanism have been adopted to defend against the wireless signals interception. All signals had been required to be sent twice that may be randomly interfered with additive noise. The receiver can identify the interfered signal and reconstruct the clean signal [3]. Channel realization based adaptive power allocation provides insignificant capacity improvement. An analytical closed-form lower bound for secrecy capacity will be obtained and that will used the objective function to improve transmit power allocation between the artificial noise and the information signal [4].

The active eavesdropping which can formulate as a one-shot two player zero-sum game and the average Secrecy Capacity(SC) had two method such as (i) with out side information and (ii) with side information. They systematically evaluated the effect of an active eavesdropper by applying game theoretic tools[5].

Low-density parity-check (LDPC) code can achieve the secrecy ability of the wiretap channel, and proved this code can be used to provide perfectly secret communications at low data rates. The main channel must be less noisy than the eavesdropping channel and the eavesdropping channel is a general binary-input symmetric-output memory less channel, which can hardly be true in the real wireless communications environment[6].

The problem of the wire-tap channel to MIMO broadcast wire-tap channel is computing the perfect secrecy capacity. When the appropriate transmitter and receiver can communicate at positive rates the perfect secrecy have been achieved. The secrecy capacity of the multiple antenna wire-tap channel had computed. A proof technique for the converse has provided in order to secrecy capacity computation[11].

System Design:
This section describes the multiple inter-symbol obfuscation (MIO) design which includes two stages: MIO encryption (adding the noisy symbols key), and MIO decryption (offsetting the noisy symbols key). This scheme is designed based on MIO at the physical layer and it needs an initial key to start the secure wireless communications.

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 a data is transmitted, transmitter will map data symbols using the set of symbol keys. These obfuscated data symbols are generated by the set of symbols. 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 distinguish the encrypted symbols from the non-encrypted ones according to the transmission power. Consequently, the eavesdropper had hard to determine whether the received symbols are non-encrypted data symbols or encrypted symbols.
2) Symbols Key Update at the Transmitter:
Following symbols encryption and normalization, the next data symbols are encrypted dynamically. The dynamic symbols key update mechanism requires all the symbols to be decrypted successfully for the upcoming data packet. At the legitimate receiver side to synchronize the noisy symbols key, consequently, the transmitter have been wait for the proper acknowledgment (ACK) from the receiver before it can process 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(blems) Decryption:
The received encrypted symbol $y_{k,i+j} = H \cdot E_{Key} \cdot j \cdot (mk,i+j) + wk,i+j$, where $H$ and $wk,i+j$ denote the wireless channel coefficient and Gaussian noise respectively. The appropriate receiver hard to locate those encrypted symbols blocks due to (1) the positions of those encrypted symbols cannot be carried in the last packet because the adjacent data packets sizes are independent from other and (2) the receiver cannot determine whether the received symbols are the packet’s data symbols at the physical layer.

(2) Symbols Key Update at the Transmitter:
When the data symbols are decrypted, the receiver maps the plain data symbols to digital bits in the normal decoder block so that the channel coefficient and the noise can be filtered out.
**Threat Model:**

The wireless security is to prevent communication from attackers in delivering contents to the legitimate recipients. In this paper, we address two types of adversaries such as passive eavesdropping attack and fake packet injection attack, during the wireless communications.

1) **Passive Eavesdropping Attack:**

An adversary eavesdropper can attempt to decode the signal with the presence of MIO from the intercepted signal. An adversary eavesdrops intercepts the wireless transmission among the legitimate transmitter and receiver.

2) **Fake Packet Injection Attack:**

An attacker injects fake packets to the valid users, triggering the events. Unlike the passive eavesdropping attack, it can deploy the brute-force to test all viable symbols keys to inject a fake packet.

The MIO scheme would enhance the computational secrecy to defend against this attack.

**Security Analysis:**

In this section, we describe the secrecy of the MIO in wireless communication. Then, we exhibit that, the MIO scheme could afford both information-theoretic secrecy to the passive eavesdropping attack in segment V-A and computational secrecy to the fake packet injection attack in phase V-B, respectively.

**A. Information-Theoretic Secrecy against the Passive Eavesdropping Attack:**

The secrecy capacity model is to prove the MIO method and that can achieve the information theoretic secrecy to the passive eavesdropping attack.

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

From the received encrypted symbols, the symbol key cannot be correctly derived then the attacker inject the fake packet by attempt the brute-force strategy to test all possible symbols keys.

**Conclusions:**

The noisy symbol have been employed in the original data symbol. For the symbol obfuscation the dynamic symbol key updating would be implemented to prevent information from passive eavesdropping and malicious message injection. The information theoretic secrecy would be achieved in both unicast and multicast scenario by implementing Inter-symbol obfuscation scheme in physical layer.

**REFERENCES**