Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

MIO: Enhancing Wireless Communications Security through Physical Layer Multiple Inter-Symbol Obfuscation

S.Sridhar, M.Tech (Ph.D)
Assistant Professor,
Department of CSE
Miracle Educational Society Group of Institutions.

Govardini Vempada
M.Tech Student,
Department of CSE
Miracle Educational Society Group of Institutions.

Abstract:

Communications security is a critical and increasingly challenging issue in wireless networks. A well-known approach for achieving information-theoretic secrecy relies on deploying artificial noises to blind the intruders' interception in the physical layer. However, this approach requires a static channel condition for the transmitter and receiver to generate and offset the controllable artificial noise, which can hardly be implemented in real wireless environments. In this paper, we explore the feasibility of symbol obfuscation to defend against the passive eavesdropping attack and fake packet injection attack during the wireless communications. We propose 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. On the one hand, an eavesdropper, without knowing the artificial noisy symbols, cannot correctly decrypt the obfuscated symbols from the eavesdropped packets. On the other hand, a legitimate receiver can easily check the integrity of the symbols key and then reject the fake packets from the received packets. The security analysis reveals that, without considering the initial key, the MIO scheme can achieve information-theoretic secrecy against the passive eavesdropping attack and computational secrecy against the fake packet injection attack. Moreover, we have implemented our approach in a USRP2 tested and conducted simulations with Simulink tools to validate the effectiveness of MIO in enhancing wireless communications security.

INTRODUCTION

About the project:

WIRELESS networks are becoming an indispensable part of people's daily life. As a result, security is an imperative issue in wireless networks since the users might transmit their sensitive personal information (e.g., credit card details) over the wireless networks. In addition, wireless channels are susceptible to eavesdropping and malicious message injecting due to the openness and sharing of the wireless medium.

Recent research has shown that physical layer security techniques become a more essential part in the wireless communications. Compared with the traditional asymmetric/symmetric cryptographic techniques which provide the computational secrecy, it has been proved that, physical layer security techniques, such as using a proper channel coding, can achieve the information-theoretic secrecy which makes the eavesdropper hardly break the encryption even it has unlimited computing power. However, the information theoretic secrecy requires a strict positive secrecy capacity that the legitimate transmitter and receiver have to be in a better quality channel than the attacker. Later works have shown that by artificially interfering the transmitting signal, the positive secrecy capacity requirement can be achieved in practical wireless communications. But, most of these techniques need to deploy trusted third parties or multiple antennas (MIMO) to generate the artificial noise. Moreover, the positive secrecy capacity of these works may be compromised if the eavesdropper deploys at certain locations.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In this project, we adopt a 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, so that the eavesdropper's channel quality is worse than the legitimate receiver's and the eavesdropper cannot decrypt the data symbols correctly since it does not know the symbols key, which is updated dynamically during the data packets' transmissions.

Problem Speciation:

MIO means multiple inter-symbol obfuscation through wireless communication main difference is in MIMO method for multiplying the capacity of a radio link using multiple transmit and receive antennas instead of this MIO method is used Explore the feasibility of symbol obfuscation and also defend against the passive eavesdropping attack and fake packet injection attack.

Existing systems:

Multiple-Input and Multiple-Output(MIMO):

- MIMO method for multiplying the capacity of a radio link using multiple transmit and receive 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.

Disadvantages:

- MIMO method Need 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.
- Wireless channels are susceptible to eavesdropping and malicious message injecting due to the openness and sharing of the wireless medium.

Proposed system:

- 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.
- This improves the scalability and high security to wireless communication.

Advantages:

- Generate the eavesdropper, without knowing the artificial noisy symbols.
- Find& prevent the fake packet injection attack during the wireless communications.
- Achieve information-theoretic secrecy against the passive eavesdropping attack and computational secrecy against the fake packet injection attack.
- Less complex compare to the existing system.

System Architecture:

In general, architecture is a set of rules that defines a unified and coherent structure consisting of constituent parts and connections that establish how those parts fit and work together. Architecture may be conceptualized from a specific perspective focusing on an ascent or view of its subject. These architectural perspectives themselves can become components in a higher-level architecture serving to integrate and unify them in to a higher-level structure.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The architecture must defines the rules, guidelines, or constrains for creating conformant implementations of the system. While this architecture does not specify the details on any implementation, it does establish guidelines that must be observe by making implementation choices. These conditions are particularly important for component architectures that embody extensibility features to allow additional capabilities to be added to previously specified parts.

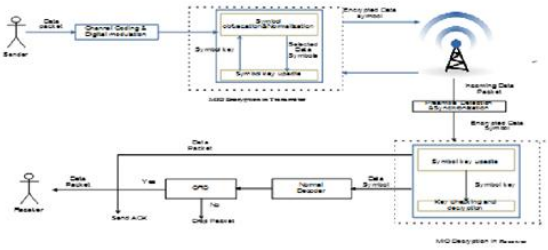

Fig 1System architecture

Modules of the proposed system:

In my project we have the mainly four modules they are:

- Sender
- Network
- Attacker
- Receiver

Sender:

This is the first module in which sender wants to send a theoretical file through wireless so sender is send a file with the help of MIO concept. While he transmitting the file the sender will split the files in to packets and assigning a data symbols to each packet. So that any attacker unable to decrypt the data and unable in inject fake packets. After splitting the sender will send a packet.

Network:

This is the second module after sending the data it will come in to the network. In network we are having three networks in each network we are using some nodes these nodes act as a transformation media. So the data is going to transfer from that nodes.So what we are proving here is if there is no attacker the data is atomically transferred to sender .If we found any attacker is attacking through the symbols we will provide a data efficiency with the help of MIO concept to my project even though the attacker is present it should be transmitted normally to sender. Even though Collisions also occurred in the network nodes but due to the data efficiency as we are providing data is transmitted normally.

Attacker:

This is the third module while sending the data through the network the attacker is going the attack the data and want to change the hack the information. Here the attacker wants to inject a fake packets in to the network same as the packets what the sender is send. But the fake packets can't inject in to the data what is user is sending because here we are proving data efficiency with the help of MIO concept so that the data is send to the sender even though the attack is happened.

Receiver:

This is the last module of my project after sender the data through the network the receiver is going to receive the data here the data will come in the form of packets the receiver is going to decrypt the data symbols to the packets which we are assigned after the decryption the user will get the information which is send by the sender. The information which is came from the sender can be able to know to the receiver only any hacker can't know the information.

Algorithm:

Algorithm 1 MIO Encryption Process

Input: *Key*1 is generated at initialization stage. *N* data packets are to be transmitted.

Output: Encrypted symbols of *Pk* .

1: **for** $k = 1$ to N **do**

2: Map the *kth* packet *Pk* to *L* data symbols $mk,0, ...mk,i , ...mk,L-1$;

3: Randomly select ξ blocks of data symbols out of *L* data symbols;

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

4: Store all $\gamma \xi$ selected data symbols in the array t;
/*for next symbols key generation*/
5: **for** each selected data symbols block begins with the i *th* data symbol **do**
6: **for** $j = 0$ to $\gamma - 1$ **do**
7: $EKeyk, j\ (mk,i+j\ ) = Keyk, j + mk,i+j$;
8: $mk,i+j \leftarrow \hat{}\ \theta \cdot EKeyk, j\ (mk,i+j\ )$; /*encrypted symbol normalization*/
9: **end for**
10: **end for**
11: Set retransmission counter $ck = 0$;
12: Send the encrypted data symbols Mk to the receiver;
13: **while** receive no ACK packet $Packk$ from the receiver before timeout $\wedge ck \leq Rre$ **do**
14: Retransmit Mk to the receiver;
15: ck ++;
16: **end while**
17: Generate $Keyk+1$ for $Pk+1$ by using the array t as input
to the privacy amplification with one-way hash function;
18: **end for**

Algorithm 2 MIO Decryption Process

Input: $Key1$ generated at the initialization stage; encrypted
data symbols of the kth packet Pk .
Output: the kth packet Pk .
1: **while** receiving encrypted data packet Pk **do**
2: **if** the first encrypted data symbol yk,i is identified through the cross-correlation with symbols key $Keyk$(Eqs. (6) ∼(8)) **then**
3: **for** $j = 0$ to $\gamma - 1$ **do**
4: Calculate clean decrypted data symbol $\hat{}yk,i+j$ by Eqs. (5) and (9);
5: $yk,i+j \leftarrow \hat{}yk,i+j$;
6: Append the position information $i + j$ of $\hat{}yk,i+j$ in the array r ;
7: **end for**
8: **end if**
9: Map the received decrypted data symbols yk to digital bits;
10: **end while**
11: **if** Pk passes the CRC check **then**
12: Send $PACKk$ to the transmitter;
13: Map Pk to L data symbols $mk,0, \ldots, mk,i, \ldots, mk,L-1$;
14: Find the selected data symbols according to the position information in the array r , and store the data symbols into the corresponding positions in the array t;
15: Generate $Keyk+1$ for $Pk+1$ by using the array t as input to the privacy amplification with one-way hash function;
16: **else**
17: Discard Pk and wait for retransmission;
18: **end if**

Conclusion

In this project, we 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. Additionally, the experimental results reveal that without knowing the symbols key, the BER in the MIO scheme can effectively ruin the packet reception at the eavesdropper side, and the key checking process would defend against the packet injection attack in wireless networks.

References:

1. S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, “On the effectiveness of secret key extraction

Volume No:2, Issue No:5 (October-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

from wireless signal strength in real environments," in Proc. 15th Annu. Int. Conf. ACM MobiCom, Sep. 2009, pp. 321–332.

2. S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in Proc. ACM SIGCOMM, Aug. 2011, pp. 2–13.

3. Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE Wireless Commun., vol. 18, no. 2, pp. 66–74, Apr. 2011.

4. C. Sperandio and P. G. Flikkema, "Wireless physical-layer security via transmit precoding over dispersive channels: Optimum linear eavesdropping," in Proc. IEEE MILCOM, Oct. 2002, pp. 1113–1117.

5. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

6. With the RTS/CTS, the unicast transmission is implemented with the RTS-CTS-DATA-ACK model. XIONG et al.: ENHANCING WIRELESS COMMUNICATIONS SECURITY THROUGH PHYSICAL LAYER MIO 1691