ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 4, April 2018

Enhancing Performance of MIO Security in Wireless Communications through Shannon-Kotel' nikov Mapping

Jeena Jacob[1], Mercy George[2], Elda Bose[3]

Assistant Professor, Dept. of ECE, MBITS Engineering Collage, Nellimattom, Kerala, India [1 2]

PG Student [ACIS], Dept. of ECE, MBITS Engineering College, Nellimattom, Kerala, India[3]

ABSTRACT: Secure communication is a critical and 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. 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. 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 increased performance to the existing system can be achieved by Shannon's –kotel'nikov mapping. The scheme is based on the geometrical interpretation of communication by Kotel'nikov and Shannon where amplitude continuous, time-discrete source samples are mapped directly onto the channel using curves or planes. The source and channel spaces can have different dimensions and thereby achieving either compression or error control, depending on whether the source bandwidth is smaller or larger than the channel bandwidth

KEYWORDS: Symbol key, Symbol obfuscation, Eavesdropper, Fake packet injection, Shannon-Kotel'nikov mapping.

I. INTRODUCTION

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 traditional symmetric or asymmetric 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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 4, April 2018

II. RELATED WORK

Although the communications security has been a popular research topic in the research community of wireless networks, the development of wireless communications security, particularly in the physical layer, remains at its early stage. Prior physical layer security research mainly falls in the following three areas, channel coding approaches, signal design approaches, and artificial noise approaches.

Channel coding approaches can defeat packet interception and jamming problems. Code division multiple access (CDMA) is a well-known channel coding scheme in the wireless communications security area. By using the bit-level pseudo noise code (PN code), the encrypted transmission message can only be decrypted by the legitimate user. However, traditional CDMA has limited PN codes, and users have to share those PN codes. To solve this PN code size problem, Li et al enhanced the CDMA security based on the advanced encryption standard (AES) operation. It specifies 3 different AES-CDMA PN code sizes (128, 192, and 256 bits) to raise the security level against eavesdropping.

The advantage of the signal design approaches is that, by designing a different signal constellation mapping method, the eavesdropper cannot correctly map the received digital symbols into bits, which leads to the incorrect decoding of the packets. Popper et al. proposed the symbols flipping method by rotating a pre-set angle for the baseband data symbol vectors before transmissions. The legitimate receiver can retrieve the data symbol vectors by reversing the angle rotation. However, the rotating angle in their scheme is fixed and the eavesdropper can brute-force the rotating angle after intercepting sufficient data packets for demodulation

Recent studies exploit the advantage of deploying artificial noise that can easily make the intruders' channel become noisier than the legitimate users' channel to achieve the information-theoretic secrecy. Sperandio and Flikkema proposed to obfuscate the original signal by imposing the multiple orthogonal artificial noise through the multi-path transmissions. The receiver can retrieve the correct signal by having multiple orthogonal noise to offset each other while the eavesdropper is not able to retrieve the correct signal without correct location.

III. SYSTEM DESIGN

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

To initiate the first symbols key in a non-secure wireless channel, we first take the conventional key agreement protocols, e.g., or augmented key to achieve a bit-level authenticated key. Then, the bit-level authenticated key can be used to generate parameters by a one-way harsh function. After that, the parameters, which include the size of the symbols key γ, the angle between the key symbol and the Real-axis Vk, j and the magnitude ratio of the key symbol and unit-power symbol α, are used to generate the first symbols key without any trusted third party.

We 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)

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 4, April 2018

symbols key update at the transmitter.

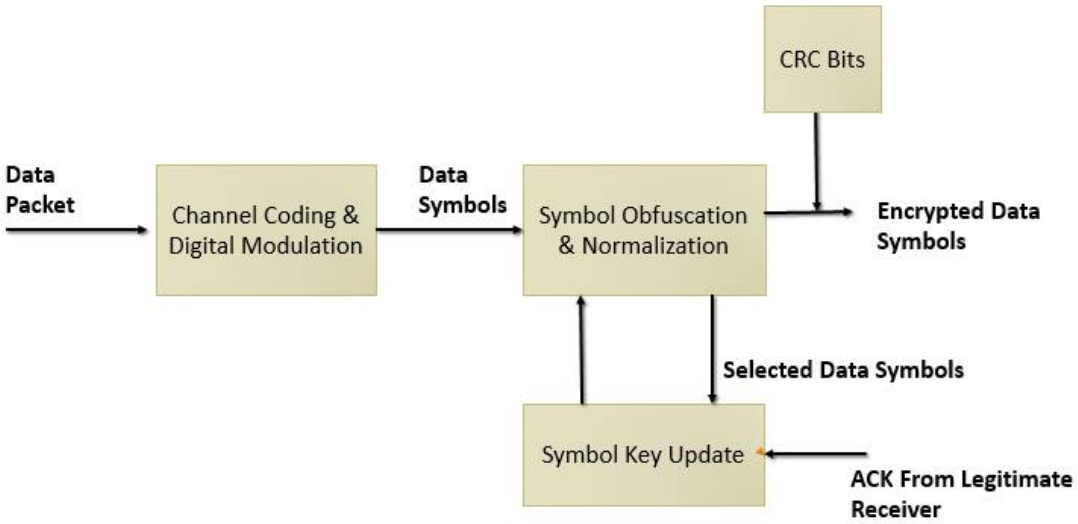

Fig 1: MIO Encryption

When a data packet Pk ($1 \leq k \leq N$) is transmitted, transmitter A will map Pk to a series of L baseband data symbols Mk = _mk,0. . .mk, l. . . mk, L−1 using the modulation constellation diagram. Each |data symbol mk, l($0 \leq l \leq L-1$) is represented as $mk,l=|mk,l|e\ j\phi k,l$, where |mk,l|, $\phi k,l$ are the magnitude and angle of the lth symbol vector, respectively. These data symbols are generated by the channel coding & digital modulation block

After mapping, the transmitter randomly picks up ξ blocks of data symbols, where $\xi = L/\gamma$, from Mk for encryption. For each chosen data symbols block that begins with the ithdata symbol, the corresponding (i+ j)thdata symbol vector mk,i+j is added with the j thkey symbol vector Keyk, j to generate an encrypted data symbol E Keyk, j (mk,i+j) = Keyk, j + mk,i+j , After symbols encryption and normalization, the symbols key to encrypt next data symbols is dynamically updated by using the privacy amplification with one-way hash function. The symbols key Keyk+1 for the next data packet is generated from the data symbols which are encrypted in the current data packet. Because $\gamma\ \xi$ data symbols are randomly and independently selected, and encrypted with the noisy symbols key Keyk, when they are transmitted, the noise symbols interfere the eavesdropping channel, which makes the eavesdropping channel's quality much worse than the legitimate channel, so the adversary has a small chance to decrypt the $\gamma\ \xi$ data symbols without knowing the noisy symbols key Keyk. Thus, the $\gamma\ \xi$ data symbols are completely confidential to the adversary. The average power of the encrypted symbols (dot-line curve) would not be the same as that of the original data symbols (solid-line curve) 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 the MIO encryption we have the MIO decryption, upon receiving signals by the legitimate receiver (or adversary), the RF down converter samples the incoming signal, and observes a stream of discrete complex baseband symbol vectors. 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. 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 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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 4, April 2018

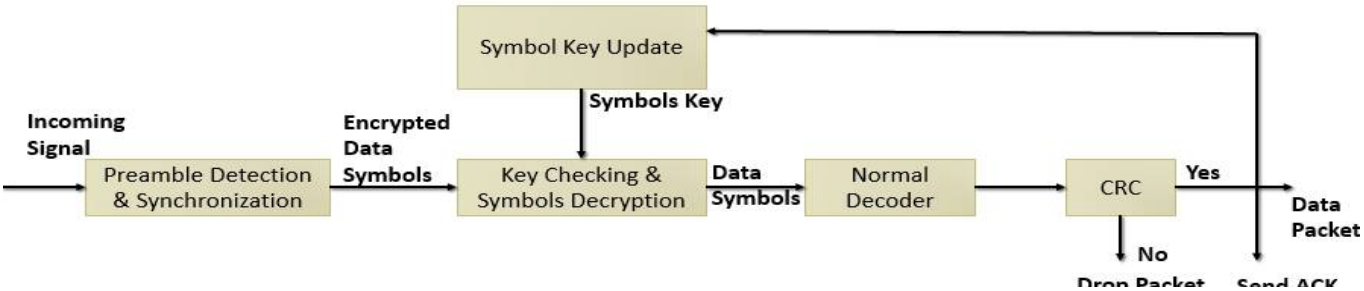

Fig 2: MIO Decryption

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 coefficient and the noise can be filtered out. After decoding the digital bits, receiver B will check if the packet Pk is correct through cyclic redundancy check (CRC) (With some small probability, it may contain undetected errors even if the packet passes the CRC checking**.**

If the received data packet is correct, the packet acknowledgment will be sent back to transmitter A and this acknowledgment4 will trigger A to update the symbols key for the next packet. Synchronously, the symbols key for the next packet at receiver B will be updated exactly the same as at the transmitter side .Otherwise, the receiver drops the corrupted data packet and waits for the packet retransmission.

IV. SIMULATION AND RESULT

The performance graph of the MIO system, i.e., the BER graph of MIO system is plotted. By applying Shannon Kotel's mapping better performance of MIO can be obtained.

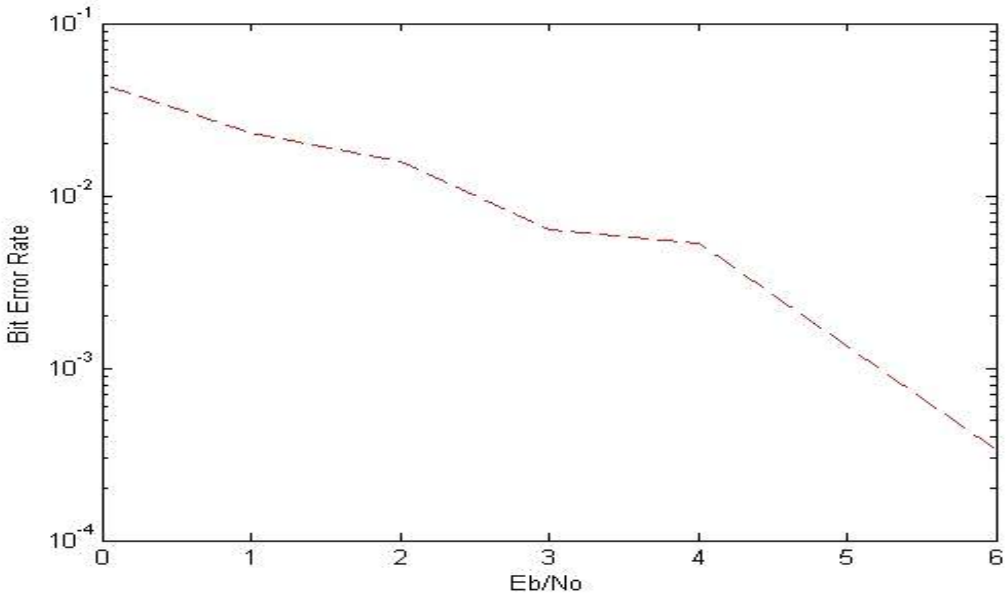

Fig 3:BER graph of MIO system

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 4, April 2018

V. MODIFICATION TO MIO SYSTEM

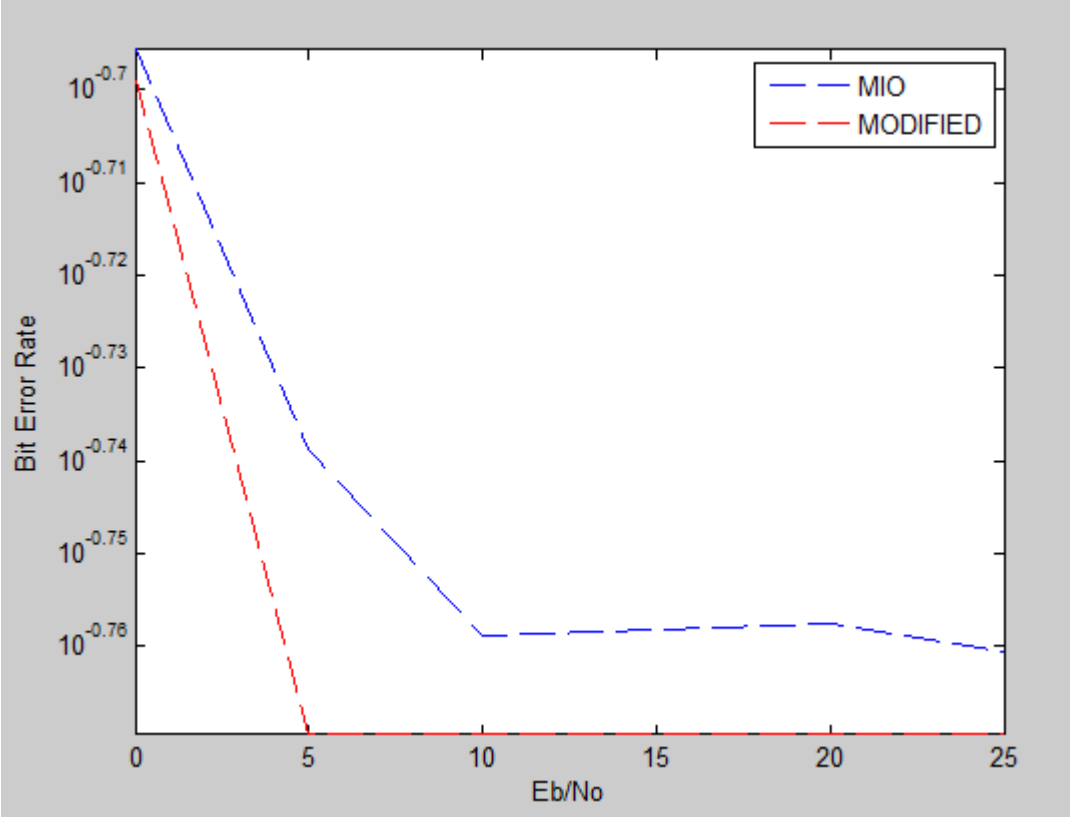

Fig 4: BER graph of modified MIO system

The performance of MIO system can be further improved by Shannon's nikov kotel's mapping. When transmitting analog source signals like images and sound over waveform channels, the most common approach is to use separate source and channel coders. Separation of source and channel was proven to be optimal by Shannon. However, the price to pay to achieve near-optimality involve very high encoding/decoding complexity, significant delays, specific design fordesired rate/distortion and threshold effect, lack of robustness to small changes in parameters. So in practice, digital systems based on joint source-channel coding (general transformation) may have performance advantages when complexity is constrained. Shannon-Kotel'nikov mapping is a kind of non-linear transformation which can provide both bandwidth reduction and bandwidth expansion. As opposed to quantizing the source and thereby creating a discrete set of representation points which are then mapped onto the channel, the Shannon-Kotel'nikov mappings perform either a projection of the source onto a lower dimensional subset (lossy compression), or map the source into a higher dimensional space (error control).

VI. CONCLUSION

In this paper, 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

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 4, April 2018

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 analysing 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.

Also, we have presented the concept of dimension changing Shannon-Kotel'nikov mappings, proposed independently by Kotel'nikov and Shannon, for reliable and efficient communication of discrete-time analog sources over AWGN channels which provide better performance to the existing MIO system.

REFERENCES

[1] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, andS. V. Krishnamurthy, "On the effectiveness of secret key extraction 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, "Theycan 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. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigationof signal and message manipulations on the wireless channel," in Proc. ESORICS, Sep. 2011, pp. 40–59.
[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEETrans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008
[6] 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.
[7] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in Proc. IEEE INFOCOM, Apr. 2011, pp. 1125–1133.
[8] 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.
[9] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages, IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.
[11] 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.