International Journal of Research in Advent Technology (IJRAT) (E-ISSN: 2321-9637)
Special Issue
National Conference "CONVERGENCE 2016", 06th-07th April 2016

MIO: Security of Physical Layer in Wireless Communications Using Multiple Inter-Symbol Obfuscation

Ajit V. Gaikwad[1]
Computer Science & Engineering, *Sant Gadge Baba Amravati University*
Email: ajit.gaikwad007@gmail.com[1]

Abstract-The use of cryptographic techniques such as encryption and hashing largely increases the energy consumption of sensors, which aggravates the original critical energy constraint problem of wireless sensor networks (WSNs). To reduce the burden of sensors, compression can be utilized. Since the traditional chaos-based schemes are not directly applicable for WSNs, we present a hybrid security solution. The hybrid security consists of 8-bit integer chaotic block encryption and a chaos-based message authentication codes. It aims to promote the security and performance of data gathering. In this paper, a hybrid security and compressive sensing-based scheme for multimedia sensor data gathering is presented. It has light security mechanism and thus decreases the complexity and energy consumption of system. Performance analysis about security and compression is carried out. The results show that our scheme is more applicable for WSNs multimedia data gathering from security and compression efficiency

Index Terms- WSN1, Encryption2, Decryption3.

1. 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 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. In this paper, 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
- 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.

For the legitimate receiver, it can offset the obfuscation of the symbols key by employing the reversed symbols key to derive the intended data symbols from the legitimate transmitter. In addition, the legitimate receiver can discern the fake packets sent from the adversary as it will fail to pass the integrity check of the symbols key on the fake packets through symbol cross-correlation. Fig. 1 provides an overview about how MIO defends against both the passive eavesdropping attack and fake packet injection attack. Following figure shows the overview of Multiple Inter Symbol Obfuscation.

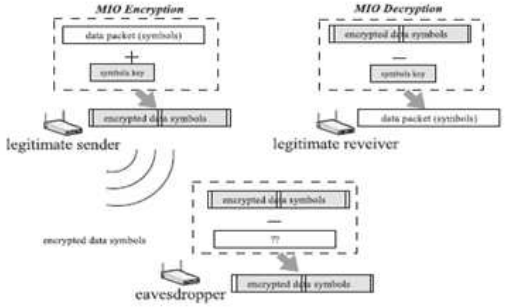

Fig. 1. MIO against Passive Eavesdropping Attack

2. APPROACHES TO THE PHYSICAL LAYER SECURITY

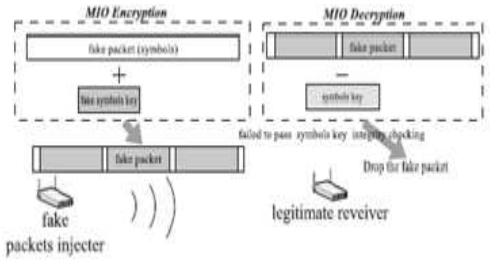

Fig. 2. MIO against fake packet injection attack

2.1. Channel Coding Approaches

Channel coding approaches can defeat packet interception and jamming problems. Code division multiple accesses (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.CDMA security based on the advanced encryption standard (AES) operation to solve the PN code size problem. It specifies 3 different AES-CDMA PN code sizes (128, 192, and 256 bits) to raise the security level against eavesdropping.

Unfortunately, like other channel coding approaches, this long size security code lags the wireless transmission rate, thus reduces the network good put. Moreover, CDMA is a spread spectrum multiple access technique in which the transmission data are combined via bitwise XOR with the PN code. Thus, CDMA is still a kind of bit-level symmetric cryptographic techniques which cannot provide the information-theoretic secrecy in the wireless communications. The low-density parity-check (LDPC) code can achieve the secrecy capacity of the wiretap channel, and proved this code can be used to provide perfectly secret communications at low data rates. However, it is under the assumptions that 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.

2.2. Signal Design Approaches

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. The symbols flipping method by rotating a preset 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. A constellation diversity mapping method to secure the wireless transmission. It increases the bit error rate (BER) at the eavesdropper side by using different constellation maps (e.g., change circular constellation to rectangular constellation) in wireless transmissions (under Gaussian noise), this constellation diversity mapping can hardly be detected by normal symbol detection attempts. However, this scheme is demonstrated to be more suitable for the complex modulation, like M-QAM Moreover, the information-theoretic secrecy can be compromised under certain specific symbol detection attempts.

2.3. Artificial Noise (AN) Approaches

Recent studies exploit the advantage of deploying artificial noise that can easily make the intruders' channel noisier than the legitimate users' channel to achieve the information theoretic secrecy. The obfuscation of the original signal by imposing the multiple orthogonal artificial noises through the multi-path transmissions. The receiver can retrieve the correct signal by having multiple orthogonal noises to offset each other while the eavesdropper is not able to retrieve the correct signal without correct location. However, their scheme is constrained to a static channel condition requirement for both the sender and receiver so that the receiver is able to receive the affected signals, together with that artificial orthogonal noise can offset each other through the multi-path effect. Such requirement on the static channel condition of sender and receiver might not be suitable for mobile networks.

Wire-connected third parties send the synchronized artificial noise when intended receiver receives the packet. It uses the secrecy capacity to prove that the AN approach can achieve the information theoretic secrecy. However, if the eavesdropper is closer to the transmitter, the secrecy capacity of the scheme can decrease to 0, in which the information-theoretic secrecy is weakened by the locations of eavesdroppers. The deploying a trusted third party to send anti-artificial noise during the wireless transmission, thus, the useful information is hard to be intercepted. However, their scheme requires an additional device and static channel condition for the legitimate sender, receiver and trusted third party so that the anti-artificial noise can be synchronously offset with the artificial noise to retrieve the transmitted signals.

The receiver can identify the interfered signal and reconstruct the clean signal. Given the redundancy mechanism, the throughput is reduced. It also requires the signal synchronization between the sender and receiver. They further improved their work by employing the full-duplex hardware to

impose the noise to the transmission between the implantable medical devices (IMDs) and the sink. As a result, the mission-critical commands to IMDs cannot be forged or overheard by the unauthorized third party.

The scheme requires an additional hardware to jam the channel. Moreover, an adversary is able to overhear the transmitted signal if it is sufficiently close to the legitimate transmitter or to inject the unauthorized commands to the legitimate receiver if it is close enough to the legitimate receiver. The MIO scheme is designed to leverage the advantages of both signal design and artificial noise approaches, and is adaptable to any wireless standard. Different from the prior work, by using the artificial noisy symbols obfuscation, it does not need any trusted third party, signal synchronization or static channel condition for the legitimate sender/receiver or adversary. Moreover, MIO can defend against the symbol detection attempts.

3. THREAD MODEL

The wireless communications security is to prevent attackers from intercepting the wireless communications, while still delivering contents to the intended recipients. There are two types of adversaries, passive eavesdropping attack and fake packet injection attack.

3.1. Passive Eavesdropping Attack

An adversary eavesdrops on the wireless medium and intercepts the wireless transmission between the legitimate transmitter and receiver. It can attempt to decode the signal from the intercepted signal with the presence of the MIO scheme. The MIO scheme will provide the information-theoretic secrecy to enhance the wireless communications security.

3.2. Fake Packet Injection Attack

An adversary injects fake packets to the legitimate users, triggering the events to further disrupt the user's manner (e.g., mislead the users' operations). Unlike the passive eavesdropping attack, it can deploy the brute-force to test all possible symbols keys to inject a fake packet. The MIO scheme will enhance the computational secrecy to defend against this attack. However, we do not consider the cases where the legitimate transmitter or receiver is physically compromised because the data confidentiality is no longer ensured no matter what security measure is adopted to secure the wireless communications between two hosts if any one of them is not secured. Additionally, we do not consider the jamming-based denial of service (DoS) attack in this paper, where the adversary simply jams the channel with extraordinary transmission power, since the legitimate sender and receiver fail to communicate with each other under this DoS attack.

4. 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)
- 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.

4.1. Initialization

To initiate the first symbols key in a non-secure wireless channel, we first take the conventional key agreement protocols, e.g., EKE or augmented EKE 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. Obviously, the legitimate transmitter and receiver have to exchange some redundant packets and deploy the same set of hash functions to generate these parameters. As the bit-level key agreement schemes can only provide computational secrecy but not information-theoretic secrecy, the key can be compromised if the eavesdropper has enough computational power. Moreover, the initial key still requires the legitimate transmitter and receiver to exchange redundant packets to generate different keys for different data packets, which introduces a high overhead. During the later data packet transmissions, the legitimate parties would employ the MIO scheme to generate the subsequent dynamic noisy symbols keys and deploy the multiple inter-symbol obfuscation schemes to interfere the eavesdropping channel, which can provide information theoretic secrecy to wireless communications.

4.2. MIO Encryption

Consider that legitimate transmitter A is about to send N data packets to legitimate receiver B. As shown in Fig. 2, for each data packet, it goes through the MIO encryption process by two steps:

- Symbols obfuscation and normalization
- Symbols key update at the transmitter.

4.2.1. Symbols Obfuscation and Normalization

When a data packet Pk ($1 \le k \le N$) 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 ($0 \le l \le L-1$) is represented as

Notation	Description
γ	The size of symbol key
keyk	The symbol key superimpose for k^th data packets
Keyk,j	The j^th key symbol for keyk to be encrypted with data symbol
Ekeyk,j (S)	Encrypted data symbol using key symbol keyk,j using data symbol S.
Vk, j	Angle between key symbol and real axis
α	Magnitude of ratio of key symbol and unit power symbol alpha
$\hat{O}$	Expect normalization factor for encrypted symbol
βc	Cross correlation that the encrypted symbol can be deleted
βSNR	SNR threshold that the receive packet correctly decoded
Rre	Maximum transmission time for each packet

Table 1. Notations

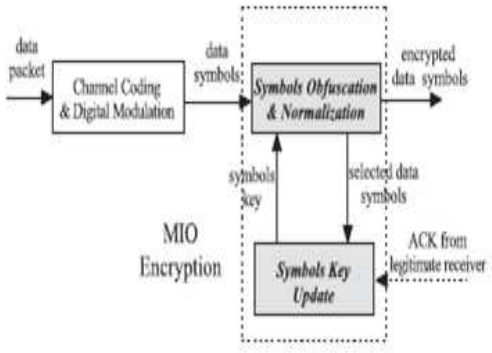

Fig. 3. MIO encryption process for legitimate transmitter

Mkl = | mkl e^jǾkl Eq. (1)

Where mkl , jǾkl are the magnitude and angle of the l^th symbol vector, respectively. These data symbols are generated by the channel coding & digital modulation block in Fig. 2. After mapping, the transmitter randomly picks up ξ blocks of data symbols, where

$\xi = \left\lfloor \frac{L}{\gamma} \right\rfloor$, For each chosen data symbols block that begins with the i th data symbol, the corresponding (i + j)th data symbol vector mk,i+j is added with the j th key symbol vector Key k, j to generate an encrypted data symbol EKeyk, j(mk,i+j)= Keyk, j + mk,i+j , which is illustrated in Fig.3. The obfuscation of a baseband data symbol mk,i+j with a key symbol Keyk, j on the constellation diagram

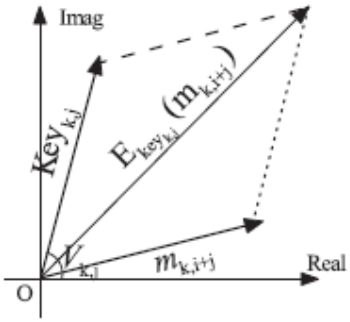

Fig. 4. The obfuscation of a baseband data symbol mk,i+j with a key symbol Keyk, j on the constellation diagram

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 normalization, the energy of the encrypted symbols (dot-dash-line curve) is almost the same as that of the data symbols. Consequently, the eavesdropper is hard to determine whether the received symbols are non-encrypted data symbols or encrypted symbols. The normalized factor θ can be calculated as

$$\theta = \frac{\frac{1}{\gamma\xi}\sum_{j=0}^{\gamma\xi-1}\left|m_{k,i+j}\right|}{\frac{1}{\gamma\xi}\sum_{j=0}^{\gamma\xi-1}\left|E_{Key_{k,j}}(m_{k,i+j})\right|}.$$

Eq. (2)

Eq. (2) implies that the calculation of θ relies on the information of all original and encrypted data symbols, which is hard for the receiver to obtain before the MIO decryption. Fortunately, as the data symbols and key symbols are generally uniformly distributed, when γ is large enough, MIO can use the expected normalized factor ˆ θ to replace θ.The calculation of θˆ considers all combination possibilities of data symbols and key symbols.

Assume that the symbol set used for mapping data on the constellation diagram is {Su} and the probability that Su is chosen is au; the set of key symbols is {Keyv } and the probability that Keyv is used for encrypting data symbol is bv . Then, the encrypted symbol EKeyv (Su)= Su + Keyv and the probability that EKeyv (Su) is generated is au · bv. Theϑ can be computed as:

$$\hat{\theta} = \frac{\sum_{u} a_u \, |S_u|}{\sum_{v,u} a_u \cdot b_v \cdot \left| E_{Key_v}(S_u) \right|},$$

Eq. (3)

Where |Su|,| EKeyv (Su)| are the magnitudes of Su and EKeyv(Su) on the constellation diagram. Obviously, both the legitimate transmitter and receiver can calculate the value of θˆ without knowing information of original and encrypted data symbols in advance. In Fig. 4, the QPSK modulation is used for data mapping. Both data symbol and key symbol are unit-power vectors.

The angles of the data symbols are {π/4, 3π/ 4, 5π/ 4, 7π/ 4} and the probability of each data symbol is ¼. For the key symbols, the angles are set {π2, −π2} and the probability of each key symbol is ½. As the figure shows, with γ = 60, the energy of the two normalized encrypted data symbols (dot-dash-line curve and dash-line curve) are almost the same. Please note that this normalization may decrease the transmission power of the data symbols and we detail this power loss, called as dB loss.

4.2.2. Symbols Key Update At The Transmitter

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 γ ξ 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 γ ξ data symbols without knowing the noisy symbols key Keyk.

Thus, the γ ξ data symbols are completely confidential to the adversary. After the MIO encryption, as the selected γ ξ data symbols are stored in array t, this array is completely confidential to the adversary. By using the array t as input to the privacy amplification with one-way hash function, the distilled symbols key Keyk+1 is also confidential to the adversary. Here, the one-way hash function can guarantee that the symbols keys are not correlated even if the data symbols in consecutive packets are correlated.

A problem with this key update scheme is that, the first noisy symbols key is not protected by the noise symbols, just like other physical layer security schemes. Fortunately, under certain situations, even if the first symbols key is cracked, it cannot help the adversary decrypting other encrypted data packets from the first symbols key because the succulent noisy symbols keys are dynamically updated. However, this dynamic symbols key update mechanism requires all the symbols to be decrypted successfully for the next data packet at the legitimate receiver side to synchronize the noisy symbols key, consequently, the transmitter has to wait for the correct acknowledgment (ACK) from the receiver before it can process the next packet. In a hostile scenario, an adversary might inject forged ACKs to disrupt the symbols key update process between the legitimate transmitter and receiver. The MIO encryption process algorithm is shown in 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;
4: Store all *γ ξ* selected data symbols in the array *t*;
5: **for** each selected data symbols block begins with the *i th* data symbol **do**
6: **for** *j* = 0 to *γ* − 1 **do**
7: *EKeyk, j (mk,i+j) = Keyk, j + mk,i+j* ;
8: *mk,i+j* ← ˆ *θ · EKeyk, j (mk,i+j)*;
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 ∧ *ck* ≤ *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

4.3. MIO Decryption

When those encrypted symbols arrive at the legitimate receiver through the wireless channel, the receiver would conduct the MIO decryption process in two steps:

- Key checking and symbols decryption and
- Symbols key update at the receiver.

4.3.1. Key Checking & Symbols 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. In MIO, for any given transmitted encrypted symbol (EKeyk,j, (mk,i+j)).

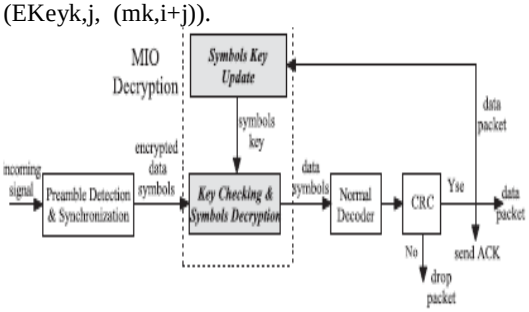

Fig. 5. MIO decryption process at legitimate receiver

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. However, at the receiver side, it would make the legitimate receiver hard to locate those encrypted symbols blocks due to

- 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
- 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. The cross correlation value at position i with γ symbols key for kth encrypted packet, C (i, γ, k), can be computed as:

$$C(i,\gamma,k) = \left| \sum_{j=0}^{\gamma-1} \overline{Key}_{k,j} \cdot y_{k,i+j} \right| \quad \text{Eq. (4)}$$

Where Keyk, j is the complex conjugate of Keyk, j. Assume mk,i is the first encrypted data symbol of one selected encrypted symbols blocks at transmitter A, by replacing yk,i+j in Eq. (6) with Eq. (4), the correlation value can be calculated.Since Keyk, j is independent of either the data symbol mk,i+j or the noise symbol wk,i+j , $|O(i,\gamma, k)| \approx 0$ .In MIO, when the correlation value C(i, γ, k) is larger than a threshold value βc, the corresponding symbols are identified as the encrypted symbols, which is shown in Fig. 6. Normally, the threshold βc can be defined as $\beta c = \psi \cdot \gamma \cdot$ RSSI signal. Where ψ is a constant (e.g., ψ = 0.9) and RSSI signal is the received signal strength indicator. Thus, the encrypted symbols' localization is conducted by checking if the in equation holds:

$$\frac{C(i,\gamma,k)}{\gamma \cdot \hat{\theta} \cdot RSSI_{signal}} \geq \psi. \quad \text{Eq. (5)}$$

It is clearly that by using this cross-correlation operation, the legitimate receiver can eliminate the channel noise influence to locate the correct position i for each encrypted symbols block without any packet information (e.g., the first symbol of the packet and the relative positions of the encrypted symbols blocks in the packet). This makes MIO more practical during wireless communications. After identifying the position of an encrypted symbols block, the legitimate receiver can offset the symbols key by using Eq. (5) to **calculate the clean data symbols** in each block. We call this symbols decryption. To demodulate the clean data symbols same as the non-encrypted data symbols in the normal decoder (Fig. 5), the receiver has to increase the power of the clean data symbols by the factor 1/θ̂ Thus, we can have

Note that the MIO requires frequent cross-correlation operations in the key checking and symbols decryption block to identify the encrypted symbols blocks, which introduces extra time and computation overhead on correlation calculations. However, the complexity of the key checking and symbols decryption block is at the same order as that of the preamble detection and synchronization block, because the preamble detection and synchronization block also deploys the cross-correlation to detect and synchronize the preamble.

4.3.2. Symbols Key Update at the Receiver

Once the data symbols are decrypted, the receiver maps all these plain data symbols to digital bits in the normal decoder block (Fig. 5) so that the channel coefficient and the noise (i.e., H and wk,i+j /θ̂ in Eq. (9)) 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 acknowledgment will trigger A to update the symbols key for the next packet (Fig. 2). 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. It is noted that in the MIO decryption process, after filtering noises and channel coefficient the digital bits which are mapped into the data symbols for the key updating are exactly the same as those for the transmitter. Associating the selected data symbols with their position information in the array r, the receiver can store the corresponding selected data symbols in the array t. Thus, it would guarantee that the array t at the receiver for the key updating is the same as the array at the transmitter. The MIO decryption process algorithm is shown in Algorithm 2

Algorithm 2 MIO Decryption Process
Input: *Key*1 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 $y_{k,i}$ is identified through the cross-correlation with symbols key *Keyk* (Eqs. (6) to (8)) **then**
3: **for** $j = 0$ to $\gamma - 1$ **do**
4: Calculate clean decrypted data symbol $\hat{}y_{k,i+j}$ by Eqs. (5) and (9);
5: $y_{k,i+j} \leftarrow \hat{}y_{k,i+j}$;
6: Append the position information $i + j$ of $\hat{}y_{k,i+j}$ 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 (m_k,0,. ,m_k,i ,m_k,$L-1$);
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

5. CONCLUSION

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 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. 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.
[5] 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.
[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[7] 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.
[8] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1125–1133.