International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 7
July 2017

Academic Science

Performance Evaluation of Dynamic MIO Scheme Using LFSR Protocol and ER Approach

Amina A K
Department of Electronics & Communication Engineering
Mar Baselios College of Engineering & Technology
Kerala, India

Teena Rajan
Department of Electronics & Communication Engineering
Mar Baselios College of Engineering & Technology
Kerala, India

***Abstract*- Over the past decades, the way to obtain information and communication with others has fundamentally changed with the development of wireless technology. In existing method, to achieve the information theoretic secrecy, the leading approach relies on deploying artificial noises. Multiple Inter-symbol Obfuscation (MIO), being a method for data transfer, it provides security in wireless network. The possibility of symbol obfuscation is to eliminate the eavesdropper participation and the fake packet injection. The original data symbols are obfuscated by using set of symbol keys. In existing method, there is disadvantage of low security level and high complexity. These problems can be overcome by using adaptive LFSR protocol based key generation unit. LFSR protocol when compared to existing method gives high security and low complexity. Performance of the proposed algorithm is evaluated using an efficient detector, named energy ratio detector (ERD), by exploring the asymmetry of received signal power levels at the transmitter and the legitimate receiver if pilot spoofing attack is present.**

Keywords— Physical layer security, energy ratio detector, Wireless communications security, encryption, decryption, information-theoretic secrecy, LFSR, MIO.

I INTRODUCTION

Wireless communication is a biggest contribution of technology. The transmission of information in wireless communication occurs without wires, cables or any other forms of electrical conductors. Instead of wires, this mode of communication uses free space. Wireless communication is quite swift with better outputs. Data can be exchanged in less time. . The prevention of unauthorized access or damage to computers using wireless networks can be termed as wireless security.

Protecting transmissions from being eavesdropped is an important research topic in modern wireless communications. Conventionally, encryption methods have been used to achieve such protection by implementing secrecy keys in the transmissions. With the advances of computational capability of digital devices, however, the encryption methods face more and more challenges in secrecy key design and management. In recent years, the physical layer security (also known as information theoretical security) has drawn much attention, which studies the security problems from the information theoretic perspective. Different from passive eavesdropping, another security threat is active attack, including, e.g., identity-based attack (spoofing attack). The original idea of the spoofing attack is that the adversary pretends to be the legitimate transmitter and sends the fake information to the receiver.

Multiple inter-symbol obfuscation (MIO) schemes is adopted 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.

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 7
July 2017

Academic Science

II MULTIPLE INTER-SYMBOL OBFUSCATION

MIO scheme combines the data symbols encrypting and channel interfering at one step.

- In MIO, the symbols key not only encrypts the baseband data symbols but also interferes these symbols, which guarantee that the secrecy capacity of the wireless communication would always stay positive regardless of the location of the eavesdropper. Thus, the information-theoretic secrecy can be achieved.
- A dynamic key extraction mechanism changes the artificial noisy symbols key to defend against the eavesdroppers from retrieving the correct information of symbols key in MIO. In this mechanism, as the legitimate transmitter can randomly encrypt the data symbols without notifying the legitimate receiver, the receiver has to employ the key checking process to locate the symbols key's position and the corresponding dynamic encrypted symbols.
- MIO can defend against the symbol detection attempts as well as the acknowledgement-based key disruption attack. Thus, MIO can greatly enhance the wireless communications security.

A. Initialization

To initiate the first symbols key in a non-secure steps: (1) symbols obfuscation and normalization and (2) symbols key update at the transmitter.

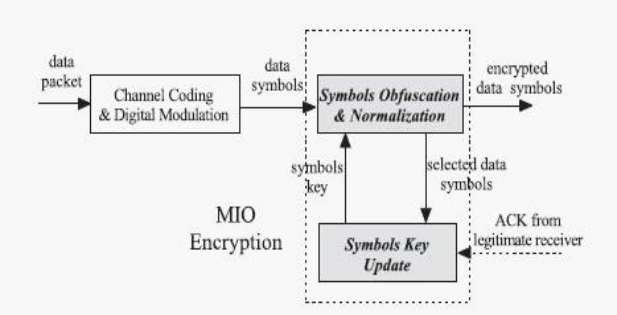

Fig 1. MIO Encryption process at legitimate transmitter

1) Symbols Obfuscation and Normalization: When a data packet P_k ($1 \le k \le N$) is transmitted, transmitter A will map P_k to a series of L baseband data symbols $M_k = (m_{k,0}, \ldots, m_{k,l}, \ldots, m_{k,L-1})$ using the modulation constellation diagram. Each data symbol $m_{k,l}$ ($0 \le l \le L$ −1) is represented as:

$m_{k,l}=|m_{k,l}|\, e^{\varphi}$,

vector, respectively.

After mapping, the transmitter randomly picks up ξ blocks of data symbols, where $\xi = [L/\gamma]$, from M_k for encryption. Fig 3.3 illustrates that for each chosen data symbols block that begins with the i^{th} data symbol, the corresponding $(i + j)^{th}$ data symbol vector $m_{k,i+j}$ is added with the j^{th} key symbol vector $Key_{k,\ j}$ to generate an encrypted data symbol given as:

$E_{Key_{k,\ j}}(m_{k,i+j}) = Key_{k,\ j} + m_{k,i+j}$

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 Key_{k+1} for the next data packet is generated from the data symbols which are 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. 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.

B.MIO Encryption

We first consider that legitimate transmitter A is about to send N data packets to legitimate receiver B. As shown in Fig.1, for each data packet, it goes through the MIO encryption process by two

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 7
July 2017

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.

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 succeeding 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.

C.M IO Decryption

When the encrypted symbols arrive at the legitimate receiver through the wireless channel the receiver would conduct the MIO

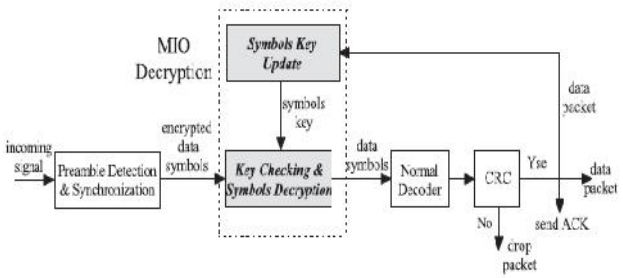

Fig 2. MIO Decryption process at legitimate receiver

decryption process in two steps: key checking and symbol decryption and symbols key update at the receiver.

1) *Key Checking & Symbols Decryption:* Upon receiving signals by the legitimate receiver, 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))*, the received encrypted symbol $y_{k,i+j}$ can be represented as:

$$y_{k,i+j} = H \cdot \hat{} \cdot EKeyk, j\ (mk,i+j\ ) + w_{k,i+j}$$

Where, H and $w_{k,i+j}$ denote the wireless channel coefficient and

Gaussian noise, respectively. The decrypted data symbol $\hat{}_{k,i+j}$ can be

computed as:

$$\hat{}_{k,i+j} = y_{k,i+j} - H \cdot \hat{} \cdot Keyk, j$$

$$= H \cdot \hat{} \cdot mk,i+j + wk,i+j$$

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 (1) 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 (2) the receiver cannot precisely determine whether the received symbols are the packet's data symbols at the physical layer during the wireless communications.3 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*. 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. 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 to calculate

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 7
July 2017

the clean data symbols in each block. We call this *symbols decryption.*

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 so that the channel coefficient and the noise can be filtered out. After decoding the digital bits, receiver B will check if the packet P_k is correct through cyclic redundancy check (CRC). If the received data packet is correct, the packet acknowledgment will be sent back to transmitter A and this disadvantage of low security level and high complexity. These problems can be overcome by using adaptive LFSR protocol based key generation unit.

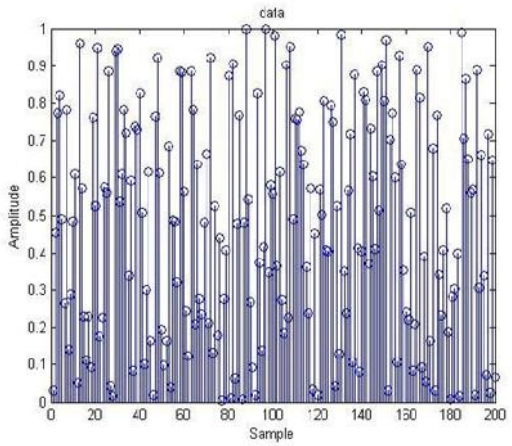

Fig 3. Input data

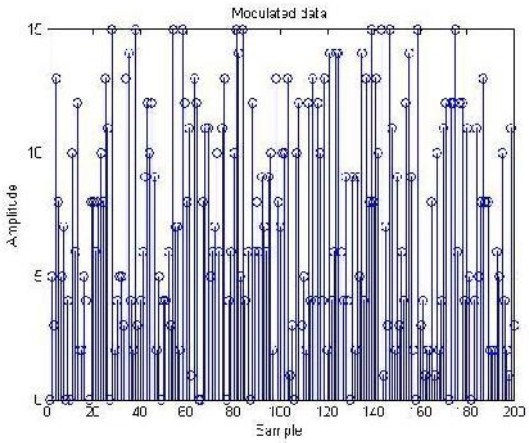

Fig 4. Modulated data

acknowledgment 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. In the MIO decryption process, after filtering noises and channel coefficients, the digital bits which are mapped into the data symbols for the key updating are exactly the same as those for the transmitter. In existing method, there is

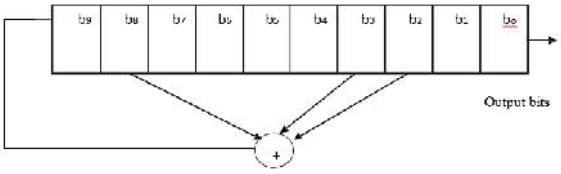

Fig 5. Block diagram of Linear Feedback Shift Register

III LFSR PROTOCOL

The input bit of the linear feedback shift register (LFSR) is a linear function of its previous state. The only linear functions of single bits are XOR and inverse-XOR; thus it is a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value. The sequence of values produced by the register is completely determined by its current (or previous) state, since the operation of the register is deterministic and the initial value of the register is called the seed. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. The sequence of bits produced with a well-chosen feedback function in LFSR, appears random and has a very long cycle [5].

One of the two main parts of an LFSR is the shift register (the other is the feedback function). A shift register shifts the contents within the register or out of the register into adjacent positions. The position on the other end is left empty unless some new content is shifted into the register. When the clock that forms one of the

input to a shift register changes state from one to zero, a shift occurs in the register. A shift register can shift its contents in either direction depending on how the device is designed. The bit on the far right end of the shift register is moved out of the register when a shift occurs. This end bit position is often referred to as the output bit. After a shift, the bit on the left end of the shift register is left empty unless a new bit is put into it.

The random number generator using Linear Feedback Shift Register generates different patterns of random numbers. Here we get perfect randomness. In a less amount of time, the LFSR can generate different patterns. This is mainly useful for security purpose. The main applications are circuit testing, cryptography and also data encryption. Because of getting good randomness these are very much useful for security purpose. In the above figure we have taken the initial seed to generate different random numbers. From the initial seed only it starts to generate the different patterns to get the randomness and is very useful for security purpose [7].

IV ENERGY RATIO APPROACH

The performance of the proposed algorithm is evaluated using an efficient detector, named energy ratio detector (ERD), by exploring the asymmetry of received signal power levels at the transmitter and the legitimate receiver when there exists a pilot spoofing attack. It provides a great chance for an intelligent eavesdropper to attack the training phase by sending the same pilot signal as that of the legal receiver and act as a normal receiver during the data transmission phase. If the eavesdropper can successfully synchronize its transmission with that of the legal receiver, the transmitter would be spoofed. A pilot spoofing attack could lead to the information leakage to the active eavesdropper and also decrease the legitimate channel rate considerably.

A three-component system model is considered: one transmitter (Alice), one legitimate receiver (Bob) and one active eavesdropper (Eve). Alice is equipped with M ($M \geq 2$) antennas and both Bob and Eve are single-antenna users [6].

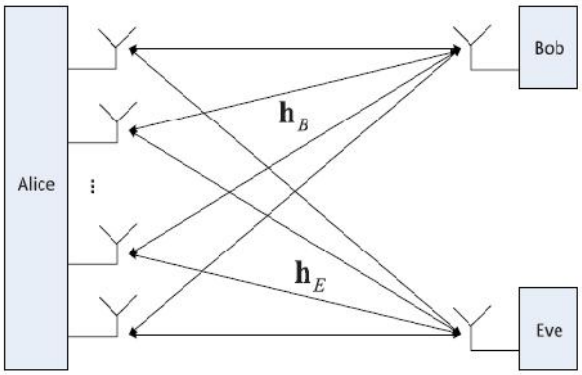

Fig 6.Communication system model

Our detection method mainly includes two phases: first, the legitimate receiver (Bob) sends the assigned pilot signal to the transmitter (Alice) via uplink channel, and Alice estimates the channel based on the samples of the signal; second, Alice calculates the received signal power, modulates that as a data signal and broadcasts it via downlink channel. Bob demodulates the data and calculates the power of his received signal. Bob then decides whether the system is under pilot spoofing attack or not by comparing the two power levels. Note that Alice utilizes the same power to broadcast the data as that of Bob used for sending the pilot signal [6].

How much information will be leaked to Eve after implementing the ERD is considered under study. If Eve utilizes larger power to attack Alice and Bob, it could obtain higher information rate from the illegitimate channel and further decrease the information rate of the legitimate channel. However, using larger *Pe* highly increases Eve's risk of being detected by Bob. Obviously, there exists a trade- off between the achieved information rate and probability of being detected [9].

V PERFORMANCE EVALUATION

In existing method, there is disadvantage of low security level and high complexity. These problems can be overcome by using adaptive LFSR protocol based key generation unit. LFSR is an acronym for Linear Feedback Shift Register. The majority of encryption models that aims at preventing intruders from hacking mobile communication networks use stream coding based on linear feedback shift registers (LFSR). LFSR protocol when compared to existing

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 7
July 2017

method gives high security and low complexity. Performance of the proposed algorithm is evaluated using an efficient detector, named energy ratio detector (ERD), by exploring the asymmetry of received signal power levels at the transmitter and the legitimate receiver when there exists a pilot spoofing attack.

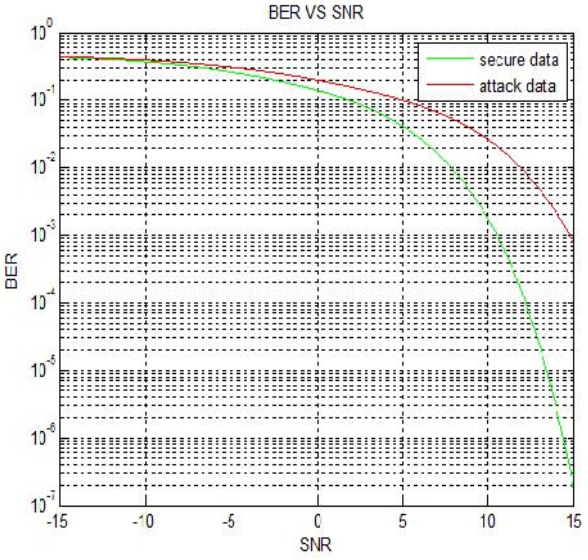

Fig 7. SNR v/s BER

VI DISCUSSION

The results for performance evaluation of the proposed method in terms of detection probability and information leakage have been obtained. The SNR vs BER graph (fig.7) shows the BER is low for secure data and is high for attack data. The proposed method gives the channel coefficients as same as that of the actual channel estimation (fig.8). The detection probability is high; approximate Pd =1(fig.9),for increase in the eavesdropper power Pe. The information leakage is high (0.5) for existing method. Compared to this, the proposed method gives a lower value which reaches zero as Pe increases (fig.10).

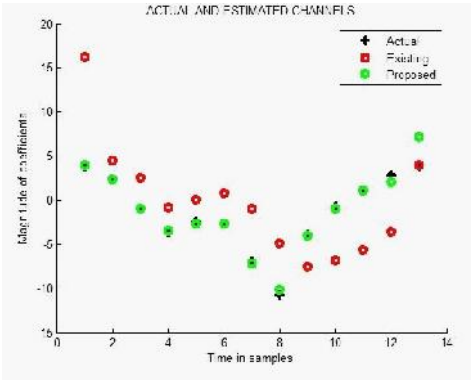

Fig 8. Actual & Estimated channels for actual, existing and proposed method

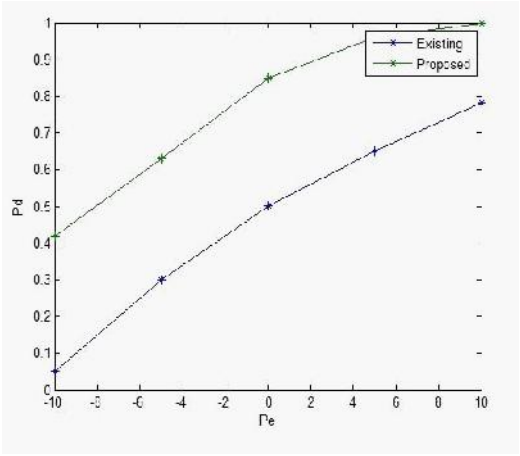

Fig 9. Detection probability v/s eavesdropper power

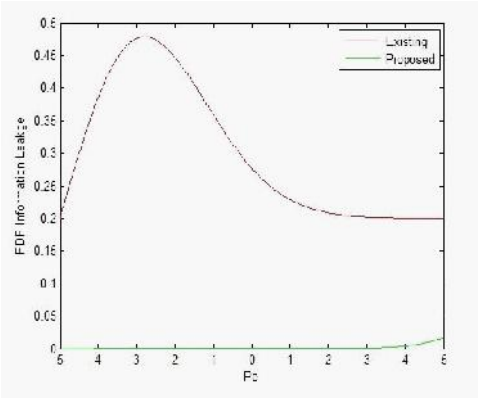

Fig10. Information leakage

VII CONCLUSION

The basic idea of this work is to enhance the security in wireless communication using dynamic updating of symbols key. Multiple Inter-symbol Obfuscation is a method for transferring the data and it provides security in wireless network. LFSR protocol when used for key generation reduces

complexity. Energy ratio approach gives the performance evaluation of the new method in terms of detection probability and information leakage. Numerical results validated the accuracy of the theoretical analysis and also proved that the ERD could protect the legitimate users from the Eavesdroppers attack efficiently.

REFERENCE

[1] Tao Xiong, Wei Lou, Jin Zhang and Hailun Tan,*"MIO: Enhancing Wireless Communications Security through Physical Layer Multiple Inter-Symbol Obfuscation*", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, August 2015. [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. 956962.

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

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

[5] Nitin Kaul and Shikha, *"Algorithm for Text Data Encryption by Position Swapping based on LFSR Pseudorandom Key Generation"*, International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 5, April 2015.

[6] Qi Xiong, Ying-Chang Liang, Kwok Hung Li, and Yi Gong, *"An Energy-Ratio-Based Approach for Detecting Pilot Spoofing Attack in Multiple-Antenna Systems"*, IEEE Transactions On Information Forensics And Security, Vol. 10, No. 5, May2015.

[7] M. Sahithi and B. Murali Krishna, *"Implementation of Random Number Generator Using LFSR for High Secured Multi Purpose Applications", International Journal of Computer Science and Information Technologies*, Vol. 3 (1), 2012, 3287-3290.

[8] J. Yang, Y. Chen, W. Trappe, and J. Cheng, *"Detection and localization of multiple spoofing attackers in wireless networks", IEEE Trans. Parallel Distributions, Syst.*, vol. 24, no.1, pp. 44–58, Jan. 2013.

[9] 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 Communication*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[10] M. Bloch, J. Barros, M. Rodriguez, and S. McLaughlin, *"Wireless information-theoretic security", IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[11] Subhra Mazumdar and TannishthaSom, *"Data Encryption with Linear Feedback Shift Register"*, International Journal of Scientific & Engineering Research, Volume3, Issue6, June- 2012.

[12] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, *"Channel based detection of Sybil attacks in wireless networks"*, IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 492– 503, Sep.2009.

[13]I. Csiszár and J. Körner, *"Broadcast channels with confidential messages"*, IEEE Trans.Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[14] S. M. Bellovin and M. Merritt, *"Encrypted key exchange: Password based protocols secure against dictionary attack"*, in Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy, May 1992, pp.72–84. [15] M. L. Jorgensen, B. R. Yanakiev, G. E. Kirkelund, P. Popovski,
H. Yomo, and T. Larsen, *"Shout to secure: Physical-layer wireless security with known interference"*, in Proc. IEEE GLOBECOM, Nov. 2007, pp.33–38.