Enhancing Physical Layer Security of OFDM Systems Using Channel Shortening

Haji M. Furqan*, Jehad.M. Hamamreh*, and Huseyin Arslan*§
*School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey, 34810
§Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620

***Abstract*—This work presents a simple, spectral and power efficient scheme for providing secure OFDM communication system using channel shortening. The basic concept is to utilize a channel shortening technique, whose design is based on the channel of the legitimate user (Bob), in such a way that the length of the effective channel is made equal to or less than the cyclic prefix (CP) at Bob only, while the length of the effective channel at the illegitimate receiver (Eve) is greater than CP. Thus, this causes inter-symbol-interference (ISI), loss of orthogonality, and overall performance degradation at Eve. The simulation results show that the presented technique can provide a significant BER performance gap between Bob and Eve, and can provide Quality of Service (QoS) based security. The design is shown to be robust against channel imperfections and can provide spectral and power efficiency beside enhancing security.**

I. Introduction

Due to the broadcast characteristics of wireless communication services, it is inherently vulnerable to eavesdropping and spying. Thus, designing effective and efficient security techniques is one of the most crucial requirements [1]. The conventional security techniques are mainly focused on cryptography, but they are not sufficient due to their high complexity in key's establishment and management, especially for future decentralized network [2]. Nowadays, physical layer security (PLS) techniques have drawn a lot of attention due to their ability to solve the challenges in the conventional encryption-based techniques. The PLS techniques provide security by means of exploiting the impairments of the wireless channel, such as noise, fading and interference, etc.

Among the many emerging PLS fields, securing OFDM transmission has become one of the most important areas of PLS research [2]. This is due to the fact that OFDM is the most popularly used technique in current and for future wireless systems because of its high spectral efficiency, and ability to combat frequency-selective fading channels [2]. In the literature, a lot of PLS techniques have been proposed to secure OFDM. These techniques include: a) secret key generation [3], b) artificial noise (AN) [4], c) signal feature suppression[5], and d) channel based adaptive transmission, such as adaptive power allocation and pre-equalization based on Bob's channel for PLS [6].

978-1-5386-3531-5/17/$31.00

In OFDM, to combat multipath fading effects of the channel, a cyclic prefix (CP) is inserted between OFDM blocks [7]. The CP ensures immunity to multipath effect only if the length of the channel delay spread is less than or equal to the CP. Otherwise, it will destroy the orthogonality of subcarriers and will cause ISI. However, the length of channel delay spread is very long for certain outdoor multipath channels. Thus, they require longer CP, causing more spectral and power efficiency loss [8].

To avoid this efficiency loss due to longer CP, one solution is to reduce the length of effective channel by means of channel shortening (CS) [7]. In the literature, a lot of techniques have been proposed in order to design coefficients of the channel shortening filter by using time or frequency domain characteristics of the channel. The proposed methods in [7]-[9] tried to shorten the channel on the basis of its time domain characteristic. These techniques try to maximize the energy inside the window that contains $V+1$ consecutive samples of the channel, where V is CP length. In [10], a method of CS is proposed, in which the channel is shortened by removing the zeros of an all-zero wireless system model with the help of series of cascaded feedback filters. The proposed techniques in [11-13] exploit frequency domain characteristics of channel to design filter coefficients. These techniques attempt to maximize sub-channel Signal to Interference and Noise Ratio (SSINR) to enhance the data rate. The above mentioned techniques require training sequence for CS operation and in order to avoid transmission of training sequence, blind CS base schemes have been proposed [14].

In the literature, CS techniques are mainly applied at receiver side, and only a few studies reported its use at the transmitter. To the best of the authors' knowledge, no work has been reported to use CS technique for PLS. Therefore, in this study, a simple approach to provide PLS by using CS is presented. More specifically, the basic idea is to use smaller CP, and apply CS method at transmitter side, and design the equalizer coefficients in such a way that the effective channel for Bob does not cause ISI, while effective channel for Eve causes

ISI. Although CS at the transmitter looks similar to pre-equalization but they are different, because in CS the channel is shortened in time domain, while in pre-equalization, the amplitude and phase of the channel are equalized in frequency domain [7], [8]. Thus, CS has lower peak to average power (PAPR) and is more robust to channel estimation errors as compared to pre-equalization [7]. It is shown by simulation results that the use of smaller CP and CS schemes with respect to Bob's channel at transmitter can provide QoS based security. The rest of the paper is organized as follows: The system model is presented in Section II, followed by the proposed approach for using CS for security in Section III. Section IV presents simulation results, and the paper is concluded in Section V.

II. SYSTEM MODEL AND PRELIMINARIES

Our system model consists of a legitimate transmitter (Tx), called Alice, that wants to have a secure communication with a legitimate receiver (Rx), called Bob, in the presence of a passive eavesdropper, called Eve, as presented in Fig. 1. The notations $h_b(h_{ab})$ and $h_e(h_{ae})$ denote slow varying rayleigh fading coefficients from source to destination and source to Eve, respectively, while n_{bk} and n_{ek} represent additive white Gaussian noise (AWGN) at source to destination and source to Eve, respectively. Channel reciprocity property is also adopted, where the channel from Alice to Bob can be estimated from the channel of Bob to Alice in TDD system, i.e. $h_{ab} = h_{ba}$.

III. PROPOSED APPROACH TO USE CS FOR SECURITY

Consider a simplified OFDM based model with channel shortener,$w(n)$, as presented in Fig 1. At the Tx, the total number of modulated symbols in one block is N, that also represents the utilized frequency spectrum. Thus, the frequency domain of each OFDM symbol can be represented as $X = [X_0 \;\; X_1 \;\; ..... \;\; X_{N-1}] \in C^{[N\times 1]}$. These blocks are then passed through an IFFT process, which maps the frequency domain data symbols to time domain points represented by $x = [x_0 \;\; x_1 \;\; ... \;\; x_{N-1}] \in C^{[N\times 1]}$. To avoid ISI, a CP of length V is inserted at the beginning of the block. The resultant signal is then passed through time domain channel shortener, $w(n)$, as presented in Fig. 1. Finally, the signal is transmitted through the channel, and reaches to both Bob and Eve. The output of linear time-invariant wireless OFDM with respect to Bob's channel without $w(n)$ is given by

$$y_b(n) = h_b(n) * x(n) = \sum_{k=0}^{L-1} h_b(k)x(n-k). \qquad (1)$$

We can re-write the above equation as follows

$$y_b(n) = h_{b0}x(n) + \sum_{k=1}^{v} h_b(k)x(n-k) + \sum_{k=v+1}^{L-1} h_b(k)x(n-k). \qquad (2)$$

The output of linear time-invariant wireless OFDM with respect to Eve's channel without $w(n)$ is given by

$$y_e(n) = h_e(n) * x(n) = \sum_{k=0}^{L-1} h_e(k)x(n-k) \qquad (3)$$

The above equation can be reformulated as

$$y_e(n) = h_{e0}x(n) + \sum_{k=1}^{v} h_e(k)x(n-k) + \sum_{k=v+1}^{L-1} h_e(k)x(n-k). \qquad (4)$$

The first term at the right side of equation (2) and (4) is the desired term for Bob and Eve, respectively, while the second and third terms in both equations are the undesired ones. The second term can be handled by CP, while the third term causes ISI. More specifically, if the channel length is equal to or less than CP then CP can remove ISI completely but if the channel length is greater than CP then it causes ISI. This is the basic principle that is used for CS based security concept.

To avoid efficiency loss due to longer CP, smaller CP is preferred with channel shortening techniques. In the literature, majority work is based on channel shortening techniques at receiver side and no work has been reported related to PLS based CS. Therefore, in this work, CS techniques are applied in such a way that they not only provide spectral and power efficiency, but also provide QoS based security. Our idea can be applied by using two approaches:

(A) Approach 1: Shortening based on Bob's and Eve's channels.
(B) Approach 2: Shortening based on Bob's channel only.

A. Approach 1: Shortening based on Bob's and Eve's channels

We use smaller CP and apply CS technique at the transmitter by designing $w(n)$ with respect to channel of both Bob and Eve, simultaneously. More specifically, the filter coefficients $w(n)$ are designed in such a way that the energy of the effective channel at Bob, $h_{effb} = w(n) * h_b(n)$, gets concentrated in a window of $V+1$ consecutive samples of effective channel, while the energy of effective channel at Eve, $h_{effe} = w_b(n) * h_e(n)$, gets concentrated out of window of length $V+1$. In this way, CP is enough for Bob, while CP is not enough for Eve, so ISI is caused at Eve.

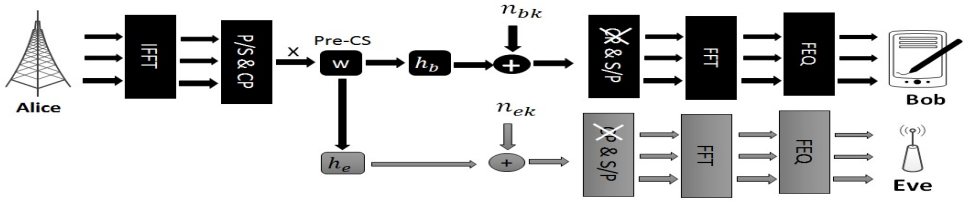


Fig. 1. System Model.

B. Approach 2: Shortening based on Bob's channel only

We use smaller CP and apply CS technique at the transmitter by designing $w(n)$ with respect to the channel of Bob only. In this approach, $w(n)$ are designed in such a way that the energy of the effective channel at $h_{effB} = w(n) * h_b(n)$ gets concentrated in the window of length $V + 1$ while the energy of tails around it get minimized out of window.

Both of the above mentioned approaches can provide QoS based security. It should be noted that the first approach can provide more security, but it requires channel state information of Eve which is not always available. Thus, in this work, we focus on the second approach. To show the effectiveness of second approach, we design CS coefficients by using two channel shortening techniques based on Bob's channel and we apply them at the transmitter side. As the coefficients are designed with respect to Bob's channel, this approach not only provides spectral and power efficiency but also QoS based security. These techniques are as follows:

1) Maximum shortening SNR (MS-SNR)-based CS.
2) Z-Transform (ZT)-based CS.

1) Maximum shortening SNR (MS-SNR)-based CS: The MS-SNR-based technique [7] helps to design equalizer coefficients such that the maximum energy lies just in a portion of the effective channel that is less than or equal to $V + 1$. Let us suppose H_b is the Toeplitz matrix for h_b and $h_{effb} = H_b w$ is the effective channel after passing through equalizer. Let us suppose $p_{winb} = H_{winb} w$, represents a window of $V + 1$ consecutive samples of h_{effb} where we want to concentrate maximum energy and $p_{wallb} = H_{wallb} w$ represents the remaining $L+t-V-2$ samples, where L is the length of channel, t is length of effective channel, V is CP length and H_{winb} & H_{wallb} are parts of H_b corresponding to p_{winb} and p_{wallb}, respectively.

We can define MS-SNR problem as to "maximize $||p_{winb}||$ subject to the constraint $||p_{wallb}|| = 1$" . The problem can be defined as

$$\max_{w}(w^T B w) \quad subject\ to \quad w^T A w = 1, \tag{5}$$

$$A = H_{wallb}^T H_{wallb}, \quad B = H_{winb}^T H_{winb}. \tag{6}$$

The solution of the above equation leads to the equalizer coefficients $w(n)$ that satisfy the generalized eigenvector problem given as

$$Bw = \lambda A w. \tag{7}$$

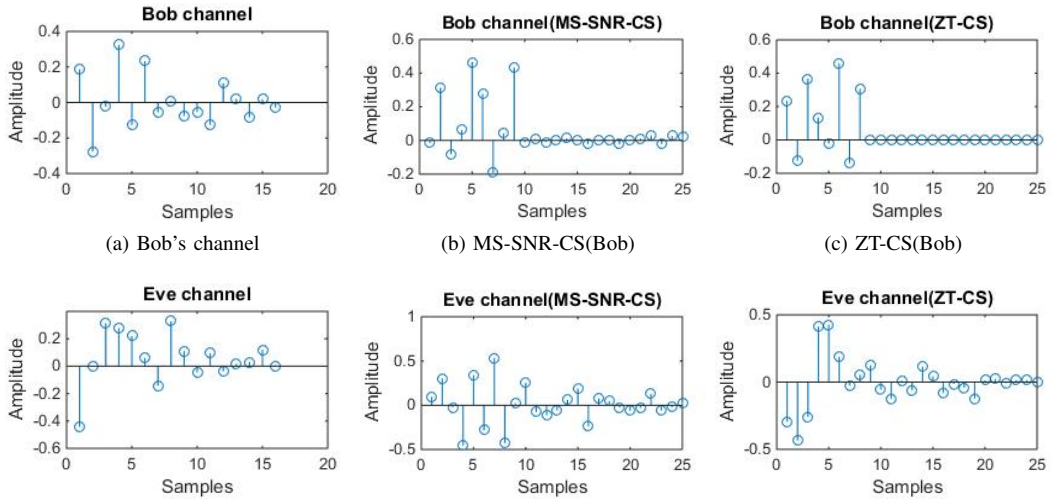
The solution of the above problem for $w(n)$ will be the generalized eigenvector corresponding to the largest generalized eigenvalue λ. Alternatively, we can also define MS-SNR problem as to "minimize $||p_{wallb}||$ subject to the constraint $||p_{winb}|| = 1$". The solution for $w(n)$ will be the generalized eigenvector corresponding to the smallest generalized eigenvalue $\bar{\lambda}$.

2) Z-Transform (ZT) based CS: The impulse response of wireless channel can be represented as a finite impulse response (FIR) filter thus it has only zeros. In this method the channel is shortened by removing zeros of wireless channel with the help of series of cascaded feedback filters. In order to derive filter coefficients based on Bob's channel, we apply Z-transform on both sides of equation (1) and then simplify it by using partial fraction as follows

$$H_b(z) = \frac{Y_z}{X_z} = h_0 \prod_{k=0}^{L-2} (1 - r_k z^{-1}), \tag{8}$$

where r_k is the root (also know as the zero) of H(z). The inverse of the factor "$(1 - r_k z^{-1})$" is stable and causal if the zero "r_k" is inside unit circle, which ensures that the system $a_k(z) = 1/(1 - r_k z^{-1})$ and $H_b(z) a_k(z)$ are both causal and stable. Thus, the zeros of channel can be canceled by using $a_k(z) = 1/(1 - r_k z^{-1})$, that can be implemented by using feedback with lower complexity, such that one zero of channel can be canceled by one feedback filter. In order to cancel e taps of channel, we require e feedback filter. Thus, CS based shortener $w(n)$ consists of series of cascaded feedback filters $a_k(z)$.

From the above mentioned techniques, the coefficients for CS based techniques are calculated based on Bob's channel and applied at the transmitter. Finally, the signal passes through h_b and h_e and reaches to Bob and Eve. After reception of signals, each of them will first discard the CP and then perform FFT process. After that, both receivers will apply frequency domain equalization. The effective channel at Bob, $h_{effb(n)} = h_b(n) * w(n)$, does not cause ISI because CP is enough to combat ISI. The effective channel at Eve, $h_{effe(n)} = h_e(n) * w(n)$, causes ISI because CP is not enough at Eve. It should



(a) Bob's channel (b) MS-SNR-CS(Bob) (c) ZT-CS(Bob)

(d) Eve's channel (e) MS-SNR-CS(Eve) (f) ZT-CS(Eve)

Fig. 2. Channel at Bob and Eve with MSSNR-CS and ZT-CS

be noted that the proposed security scheme can easily be implemented by using USRP-devices controlled by LabVIEW or MATLAB [16].

IV. Simulation Result

In this section, the channel impulse response (CIR) at Bob and Eve before and after CS techniques as well as the simulation results using bit error rate (BER) as a metric [3], [15] are presented to analyze the effectiveness of the proposed method. The basic simulation parameters are presented in Table 1. In Fig. 2 CIR at Bob and Eve before and after the channel shortening techniques is presented. Fig. 2.a, 2.b and 2.c present the CIR at Bob before shortening, Bob with MS-SNR-based CS and Bob with ZT-based CS, respectively. It should be noted that MS-SNR-based CS algorithm concentrates maximum energy of effective channel in window of $V+1$ length as much as possible, and minimizes energy out of window as much as possible, but there is still some leakage outside the window that causes some ISI. On the other hand, ZT-based algorithm can eliminate ISI completely as compared to MS-SNR and there is negligible leakage.

TABLE I
System parameters

Modulation	QAM
Channel	Rayleigh fading channel
Channel length h_e	16
FFT size	64
CP length (required)	16
CP length (used)	8

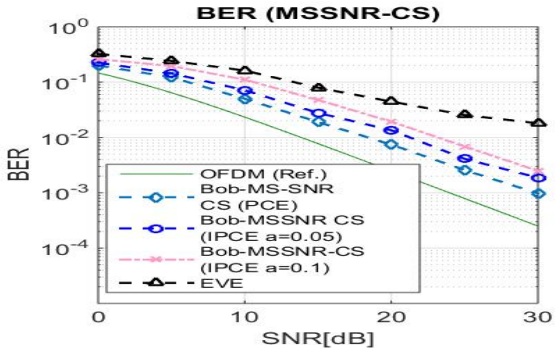


Fig. 3. BER performance for MS-SNR-CS.

On the other hand, Fig. 2.d, 2.e and 2.f show the CIR at Eve before shortening, Eve with MS-SNR-based CS and Eve with ZT-based CS, respectively. It is observed that MS-SNR and ZT-based CS algorithm do not help too much to Eve to concentrate energy inside window of $V+1$ because $w(n)$ is designed based on Bob's channel which is different from Eve's channel due to spatial decorrelation nature of the wireless channel. Thus, Eve will suffer from the leakage in window out of $V+1$ and CP will not be enough for Eve.

In Fig. 3 and Fig. 4, simulation results are shown by using BER as a metric. In all simulations, the effect of imperfect channel estimation that may occur due to possible noise, interference etc. is taken into account. The imperfectly estimated channel at Alice and Bob can be modeled by adding intentional errors $(\Delta h_{T/R})$ to the perfect channel (h_b) at both the transmitter and receiver and is given by $h_{T/R} = h_b + \Delta h_{T/R}$, where Δh is modeled as an independent complex Gaussian noise vectors with zero mean and error variance $\sigma^2 = a \times 10^{\frac{-SNR_{dB}}{10}}$, where a represents different estimation qualities [15], [16].

In Fig. 3 and Fig. 4 the BER performance at Bob

and Eve for MS-SNR and ZT-based CS algorithm is presented. The results show BER performance at Bob under different estimation qualities with a=0 (perfect estimation), a=0.05 and a=0.1. It is shown in both cases that there is some degradation due to imperfect channel estimation. However, this degradation can be overcome by using training sequence of longer length and by using higher power. Furthermore, Fig. 3 and Fig. 4 also present performance of conventional OFDM (OFDM-Ref.) for comparison. In OFDM-Ref. no CS is applied and longer CP corresponding to channel length (L) is used. It is shown that the performance of ZT-based CS is approximately same as OFDM-Ref., while there is a small degradation in the performance of MS-SNR based CS as compared to both ZT-based and OFDM-Ref. The reason is that although MS-SNR-based CS algorithm concentrate the energy of effective channel in window of $V+1$ as much as possible but there is still some leakage as presented in Fig. 2.b. Moreover, Fig. 3 and

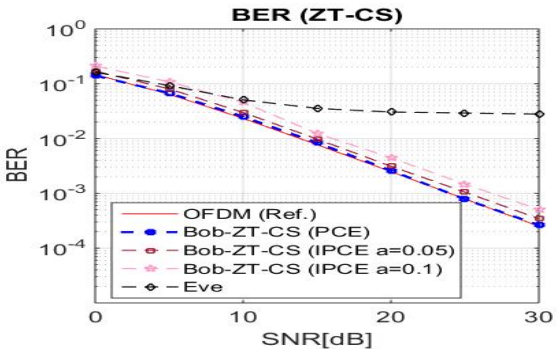


Fig. 4. BER performance for ZT-CS.

Fig. 4 also present performance for Eve. It is observed that there is a BER performance degradation at Eve for both MS-SNR and ZT based CS. The reason is that the equalizer coefficients $w(n)$ are designed based on Bob channel and $w(n)$ will not help Eve to shorten its channel and thus the effective channel causes ISI. The BER performance at Eve is greater than 10^{-2}, which can provide QoS based security [15]. More specifically, it can secure voice communication between legitimate parties as per LTE [15]. Hence, our algorithm can provide QoS based security.

V. Conclusion

In this work, a practical spectral and power efficient security method is presented that is based on channel shortening. Channel shortening equalizer coefficients are designed based on Bob's channel and CS is used at transmitter in such a way that the effective channel ensures no ISI at Bob, while causing ISI and performance degradation at Eve, thus, QoS based security can be provided. The simulation results are given for both perfect and imperfect channel estimation to demonstrate the effectiveness and robustness of the proposed algorithm. The proposed scheme can provide QoS based security and can successfully secure voice communication between legitimate parties. The idea can be extended to provide security to any single carrier or multi carrier CP based system.

Acknowledgment

This work has been supported by The Scientific Research Council of Turkey (TUBITAK) under grant No. 114E244.

References

[1] H. M. Furqan, J. M. Hamamreh and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *International Symposium on Wireless Communication Systems (ISWCS)*, Poznan, pp. 597–602, 2016

[2] J. M. Hamamreh and H. Arslan, "Secure Orthogonal Transform Division Multiplexing (OTDM) Waveform for 5G and Beyond," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1191–1194, May 2017

[3] H. Li, X. Wang, and J. Y. Chouinard, "Eavesdropping-Resilient OFDM System Using Sorted Subcarrier Interleaving," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 2, pp. 1155–1165, Feb. 2015.

[4] H. Qin, Y. Sun, T. H. Chang, X. Chen, C.Y. Chi, M. Zhao, and J. Wang, "Power Allocation and Time-Domain Artificial Noise Design for Wiretap OFDM with Discrete Inputs," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[5] Z. E. Ankaral, M. Karabacak, and H. Arslan, "Cyclic feature concealing cp selection for physical layer security," in *IEEE Military Communications Conference (MILCOM)*, Baltimore, pp. 485–489, Oct 2014,

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", IEEE Commun. Surv. Tutorials, vol. 16, no. 3, pp. 1550–1573, 2014.

[7] P. J. W. Melsa, R.C. Younce and C.E. Rohrs, "Impulse response shortening for discrete multitone transceivers," *IEEE Trans. Commun.*, vol. 44, pp. 1662–1672, Dec. 1996.

[8] J. S. Chow and J. M. Cio, "A Cost-Effective Maximum Likelihood Receiver for Multicarrier Systems," in *Proc. IEEE Int. Conf. on Comm.*, vol. 2, pp. 948–952, June 1992.

[9] S. Celebi, "Interblock interference (IBI) minimizing time-domain equalizer (TEQ) for OFDM," *IEEE Signal Process. Lett.*, vol. 10, pp. 232–234, Aug. 2003.

[10] P. Zhang and J. Qin, "A simple channel shortening equalizer for wireless TDD-OFDM systems," in *IEEE International Conference on Wireless Communications, Networking and Information Security*, Beijing, China, pp. 83–86, 2010.

[11] N. Al-Dhahir and J. M. Cio, "Optimum finite-length equalization for multicarrier transceivers," *IEEE Trans. Commun.*, vol. 44, pp. 56–64, Jan. 1996.

[12] G. Arslan, B. Evans and S. Kiaei, "Equalization for discrete multitone transceivers to maximize bit rate," *IEEE Trans. Signal Processing*, vol. 49, pp. 3123–3135, Dec. 2001.

[13] K. Vanbleu, G. Ysebaert, G. Cuypers, M. Moonen and K. V. Acker, "Bitrate-maximizing time-domain equalizer design for DMT-based systems," *IEEE Trans. Commun.*, vol. 52, no. 6, pp. 871–876, June 2004.

[14] R. K. Martin, J. Balakrishnan, W. A. Sethares and C. R. Johnson, "A blind adaptive TEQ for multicarrier systems," *IEEE Signal Process. Lett.*, vol. 9, pp. 341–343, Nov. 2002.

[15] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY Layer Security Design Using ARQ with MRC and Adaptive Modulation," *IEEE Wireless Commun. Netw. Conf. (WCNC)*, pp. 1632–1638., Apr. 2016

[16] H. M. Furqan, Jehad. M. Hamamreh, H. Arslan, "Secure reliable communication using untrusted Switchable Decode and forward relay for power efficient system," *International Wireless Communications and Mobile Computing Conference (IWCMC)*, Spain, pp. 1–1, 2017.