# An Efficient Security Method Based on Exploiting Channel State Information (CSI)

Jehad M. Hamamreh*, Haji M. Furqan*, Zain Ali†, and Guftaar Ahmad Sardar Sidhu†
*College of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey, 34810
†Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, Pakistan

***Abstract*—A channel amplitude quantization method that can effectively quantize the channel response using just one single threshold value is proposed in order to extract a random manipulating sequence with good secrecy properties. Specifically, a Time Division Duplex (TDD) wireless system is considered over independent identical distributed (i.i.d.) Rayleigh fast fading channel, where potential passive eavesdroppers (Eves) can only estimate their own channel and have no knowledge about CSI between legitimate communication parties. The transmitter (Alice) is only aware of the CSI of the legitimate user (Bob). Particularly, the proposed security technique takes the bits of the transmitted data packets and manipulate them with a logical vector that characterizes the channel randomness based on the estimated CSI gain. The process of manipulation is implemented on a bit level basis using an XOR operation exactly before modulation process. The same XOR operation is implemented after demodulation process on the detected bits to extract the concealed bits. The obtained simulation results show that the employment of such mechanism can ensure data confidentiality. Furthermore, the simulation results are extended to include the effect of the selected quantization threshold on the BER performance of Eve as well as the amount of information leakage to its side. It is shown that security gap region between Bob and Eve is made very large over all expected Signal to Noise ratio (SNR) values despite the small degradation in the bit error rate (BER) performance of Bob because of the expected channel estimation errors due to noise.**

## I. Introduction

The proliferation of wireless devices creates a surge in data communication over wireless media. This wirelessly transferred data is becoming more and more important to its own generators since it includes personal information or even sensitive financial data contents about its owners. Users want their data to be sent confidentially and securely even in wireless systems. However, because of the broadcast nature of wireless signals, the security task is getting harder and more challenging than before. As a result, well advanced security techniques have to be designed and developed to address this issue. Traditionally, confidentiality has been tackled by using cryptography-based methods as shown in Shannon's work [1].

However, recently developed and advanced decryption methods supported by very powerful processing and computing devices disclose the weakness of this kind of approaches. Additionally, the trends of future wireless systems toward decentralized and asynchronous network infrastructure make the key sharing method alongside the required key management process extremely difficult. So, Physical layer security (PHY security) arises as a promising method to achieve additional protection along with the conventional cryptography based methods. In Wyner's paper [2], it was demonstrated that confidential communication between trusted users is possible without even sharing a secret key if the eavesdropper's channel is a degraded version of the legitimate receiver channel. Thus, PHY security was achieved at that time using secrecy codes generated randomly by channel dependent stochastic encoders. Inspired by the same paper [2], the secrecy capacity from an information theoretic point of view has been studied for various wireless fading channel scenarios [3]-[9]. Signal processing security techniques that are based on exploiting specific features of the transmitted waveform such as OFDM, have also been proposed for PHY security [10-12]. Artificial noise alongside Multiple Input Multiple Output (MIMO) systems are also investigated for security as shown in [13-15].

Additionally, beam-forming MIMO based security procedures, that take into account the effect of imperfect channel estimation on the secrecy capacity, have been examined in [16-18]. Other studies analyzed middle situations in which partial Channel State Information (CSI) knowledge is available from all parties [19]-[23]. Particularly, in [22], [23], two concurrent and independent works stated similar information theoretic based conclusions regarding the advantages of CSI availability at the transmitter, where authors of [23] studied the secure message rates and secret-key rates that can be obtained if there is only partial CSI over ergodic fading channels with known statistics. However, most of the previously mentioned security techniques depend on designing secrecy codes or on exploiting the availability of a certain degree of freedom available in frequency, time, space, or code domain, while some others are specific for particular systems such as OFDM. Despite of all these constrains, still security can be provided by exploiting the CSI knowledge at the legitimate parties to extract secret keys from the channel response [24]. For more details on the existing methods used for extracting secret keys, interested readers can refer to [24] and [25] and the references therein.

In this paper, different from the existing methods that use multiple quantization thresholds [24], we propose a channel amplitude based-quantization method that can effectively quantize the channel response using just one **single** threshold value in order to extract a random manipulating sequence with good secrecy properties. This results in making the random sequence extraction process faster (i.e., less delay, less processing time, and minimal energy consumption), simpler (i.e., less complexity with negligible overhead), and self-

0-7695-6347-3/17/$31.00 ©2017 IEEE
DOI 10.1109/FIT.2017.00058

dependent as it does not require sharing the value of the selected quantization threshold publicly. These advantages can make the proposed method attractive and good candidate for Internet of Thing (IoT) devices. This paper also shows that by using just a single properly selected threshold, a random vector with good entropy can be extracted from fast fading channels. The effect of the selected channel-based quantization threshold on both the secrecy gap and eavesdropper's BER performances are investigated and quantified. The optimal selected threshold that gives the best secrecy performance is found to be equal to the mean of the channel variation (realization) vector. Accordingly, the bits of the data packets are manipulated before transmission with the corresponding threshold-based manipulating random vector extracted from the channel. The process of manipulation is performed using an XOR operation, implemented on a bit level basis directly before modulation process.

Our results clearly prove that the employment of such mechanism can significantly ensure data confidentiality. Additionally, since the operation of this method highly depends on the channel, the simulation results are extended to include the effect of imperfect channel estimation on the performance of both Bob and Eve as well as the effect of the selected threshold on the BER performance of Eve. It is shown that the security gap between Bob and Eve is kept very high even though there is a small BER degradation at Bob because of channel estimation errors due to noise. These errors are normal and expected observations even without using our proposed security method. It is worth mentioning that we have used in this paper a simple communication system to prove the concept of the method, however, this technique can be applied for any communication system such as Orthogonal Frequency Division Multiplexing (OFDM), Code Division Multiple Access (CDMA) to provide approximately perfect (i.e. secrecy capacity equals Shannon capacity) secure communication systems over fading channels.

## II. SYSTEM MODEL AND PRELIMINARIES

A communication system scenario as drawn in Fig.1 is examined in this study. A trusted sender, Alice, conveys data packets (messages) to legitimate receiver, Bob. The message $x(n)$ is transmitted over a discrete time wireless multipath Rayleigh fast fading channel whose baseband received signal at Bob's side is given in (1), where $h_b(n)$ is time-varying complex gain of one tap channel and $w_b(n)$ is the zero-mean complex additive white Gaussian noise (AWGN). An eavesdropper, Eve, tries to eavesdrop the signal transmitted by Alice. Similarly, the signal captured by Eve is given in (2) where $h_e(n)$, and $w_e(n)$ are the complex channel response, and AWGN of eavesdropper channel, respectively.

$$y_b(n) = h_b(n) * x(n) + w_b(n), \quad (1)$$

$$y_e(n) = h_e(n) * x(n) + w_e(n). \quad (2)$$

Packet based transmission is considered where each packet constitutes $N$ information symbols. The duration of a symbol is on the order of the channel coherence time; so, the fading gain varies from one symbol to the next.

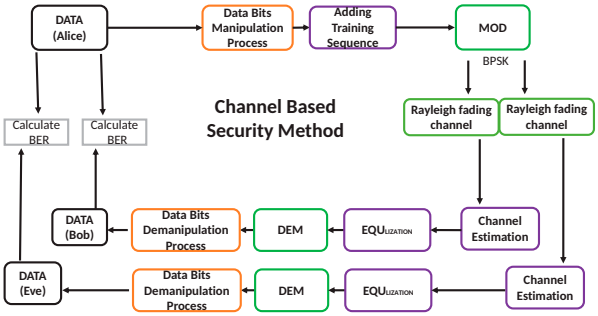



Fig. 1. System model considered in this work.

Packets consist of Q-size cyclic redundancy check (CRC) as well as the main packet of size N. We assume the channel fading coefficients are i.i.d. over the conveyed symbols during one transmission packet. Multipath response of the main channel, $h_b(n)$, is assumed to be known by the legitimate users Alice and Bob. This can be realized by utilizing the channel reciprocity in TDD systems. Since Eve is a passive node, we assume that Alice has no information about CSI for the eavesdropper channel, $h_e(n)$. This practical assumption is also inspired by the results that additional knowledge of eavesdropper channel does not provide gain in terms of secrecy in fading channels [5]. As a final notice, we assume that Eve has no information about the main channel because the wireless channel response is unique to the locations of the transmitter and receiver as well as the environment. Therefore, $h_b(n)$ and $h_e(n)$ are uncorrelated, where multipath components decorrelate from one transmit-receive path to another if the paths are detached by the order of an RF wavelength or more.

Additionally, single antenna is considered to be used by all communication parties (Bob, Alice and Eve). In order to perform the proposed security method, the knowledge of the uplink fading channel is required in order to obtain fading gains over each single transmitted symbol. This can be estimated using the downlink channel in the TDD systems since these systems use the same carrier frequency for both uplink and downlink channels. The TDD can flexibly assign the limited channel resources to uplink and downlink. Another advantage of TDD is that channel reciprocity, which means that fading is highly correlated between the uplink and downlink due to the use of the same carrier frequency. These feasible assumptions facilitate the implementation of our proposed security technique.

## III. THE PROPOSED SECURITY TECHNIQUE

Many physical security methods have been proposed in the literature, in which, most of them rely on the existence of a certain degree of freedom in signal domains such as space, code, time or frequency. These domains are exploited and used to design secure systems based on the characteristics of the observed channel between the legitimate communication

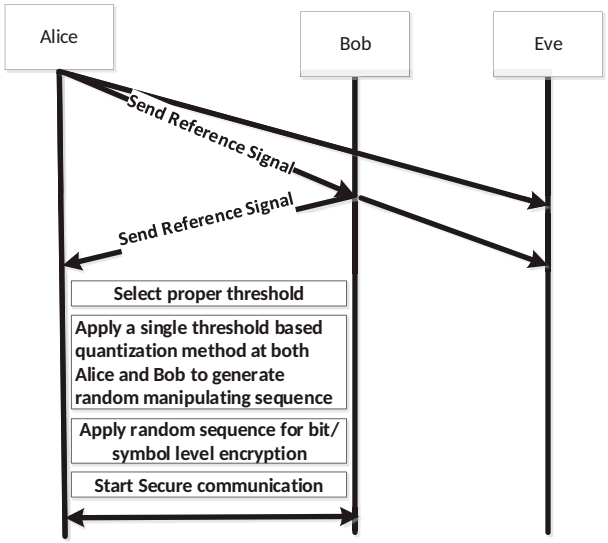



Fig. 2. Signaling process of proposed method.

parties. It has been noticed that the more degree of freedom we have, the more secure the designed system will be. Unfortunately, despite the effectiveness of such approaches, their obtained secrecy rate is limited and very small and usually providing a certain secrecy rate at the cost of sacrificing the precious telecommunication resources such as power and bandwidth. On the other hand, secrecy capacity of fast fading channels under imperfect CSI estimation at the transmitter has been studied in [22], [23]. However, in the previous works, the source of security was based on using Wyner codes, while in our proposed security method the knowledge of the instantaneous CSI at the transmitter is the kernel of the developed security method. The CSI of i.i.d fading Rayleigh channel is considered to be the main cause of randomness. As stated in the aforementioned section (system model), the main CSI between the transmitter and the trusted receiver can't be obtained by eavesdroppers since there is no CSI feedback about the channel status in TDD system; instead, channel reciprocity property of TDD systems is implemented to know uplink channel from the downlink one. Since our security technique is based on the CSI knowledge of the trusted receiver at the transmitter, we consider from the beginning the effect of channel estimation errors on the security performance of our proposed method. Channel estimation based results are then compared with the theoretical performance when perfect channel estimation assumption is adopted in the model. We also assume that the primary cause for channel estimation errors is the AWGN, where the adopted system is considered to be error free of both inter-symbol interference (ISI) and inter-carrier interference (ICI) since there are enough guard time period between the transmitted symbols and at the same time sufficient guard band between the assigned sub-carriers.

To generate and apply shared manipulating vector using proposed method, Alice and Bob perform the following main steps:

(A) Estimation of the complex channel coefficients vector.
(B) Selection of threshold.
(C) Generation of manipulating vector.
(D) Application manipulating vector

The details of the main steps are as follows:

### *A. Estimation of the complex channel coefficients vector*

Firstly, before the communication process starts, a set of already known training sequence is sent via i.i.d. Rayleigh fast fading channel to the intended receiver, that in turn estimates the instantaneous channel gain over each symbol by dividing the received training symbols on the already known ones at the receiver as presented in Fig. 2. The estimated downlink channel is then used to estimate the CSI gain at the transmitter using the channel reciprocity property applied in TDD systems, thus, there is no way for Eve to know the CSI between Alice and Bob. This assumption coincides with the practical situation. Generally speaking, the estimated available CSI at the transmitter after the training process is as close as the one used for equalization at the receiver side.

### *B. Selection of threshold*

One of the most critical step in this algorithm is the selection of proper threshold $\xi$. The reason behind this is that, although Bob and Eve have different channels with respect to Alice, the amount of randomness of the generated manipulating vector and information leakage to Eve can be significantly impacted by the selected threshold. Through computer simulations, it is observed that the best threshold is that one which is selected with respect to the mean of the amplitude of the considered fading channel distribution. In other words, if the threshold is equal to the mean of the estimated channel amplitude sequence, then the manipulating vector will provide a complete confusion to Eve, while selecting different threshold values leads to leakage of information to Eve. The effect of threshold on the BER performance of Eve is presented in the simulation results section.

### *C. Generation of manipulating vector*

After proper selection of threshold with respect to the estimated channel gain (i.e. $\alpha(n) = |h_b(n)|$), the manipulated vector is constructed based on comparison of received channel gain vector values with the threshold. More specifically, the obtained amplitude gain value caused by the channel over each single symbol is compared with this threshold, then a conditional if clause statement is implemented to check if $\alpha(n) > \xi$ or not. A new vector called $\beta(n)$ is defined and created to store the resulted logical bit value of the performed conditional operation. The bit value is set to one (1) when the condition is met and zero (0) elsewhere. By doing so, the existed randomness in the channel between Alice and Bob is completely mapped into a vector of digital values (zeros and ones) that can be used in the digital processing domain for different purposes including enhancing the reliability of communication systems. Specifically, in this work, we use it for security purposes.

### D. Application manipulating vector

*1) At Transmitter side:* At transmitter side, the net raw information bits $N_I$, which are divided into packets of fixed number of bits attached with CRC followed by interleaving or encoding processes, reach the modulator (bit mapper) as coded bits $N_C$. These coded bits $N_C$ are manipulated (by using manipulating vector generated in previous step) exactly before they are mapped onto a constellation $S$ to obtain $N$ modulation symbols $(s_1, ..., s_N)$. The manipulation can be done at symbol level or at bit level but in this work we are applying manipulating vector at bit level. The manipulation process in this work is done by performing an XOR operation with the previously obtained vector $\beta(n)$ that includes and represents the randomness of the channel in a digital manner. The resulted manipulated bits shape the new vector that is going to be modulated. Finally, the $N$ modulation symbols are conveyed to the destination.

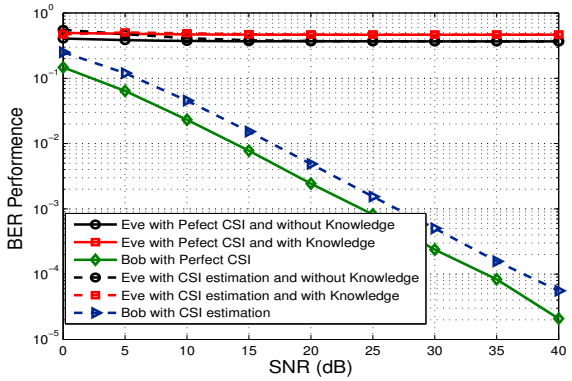



Fig. 3. Simulation Performance Result of the Proposed Security Method (Threshold $\xi$=1).

*2) At Receiver side:* Looking at the receiver side, simply and briefly, the same process implemented at transmitter is done at the receiver since the channel is available at both sides. At the receiver side, the reverse process is performed according to the available estimated CSI gain, where the same XOR operation is implemented after demodulation process on the detected bits to get the concealed bits. For Bob who has the same estimated CSI as Alice, will be able to decode the data correctly since the created logical random vector is same as the one made at the transmitter, whereas, Eve has completely different logical vector, so even if she is aware of the technique, she will detect wrong bits that degrade the BER behaviour. Note that Eve will have different logical vector because of different location and due to properly selected threshold by legitimate parties. Simulation results prove that the use of this security method provides a very high secrecy performance gain where the BER gap region between Bob and Eve is made very large over all SNR values.

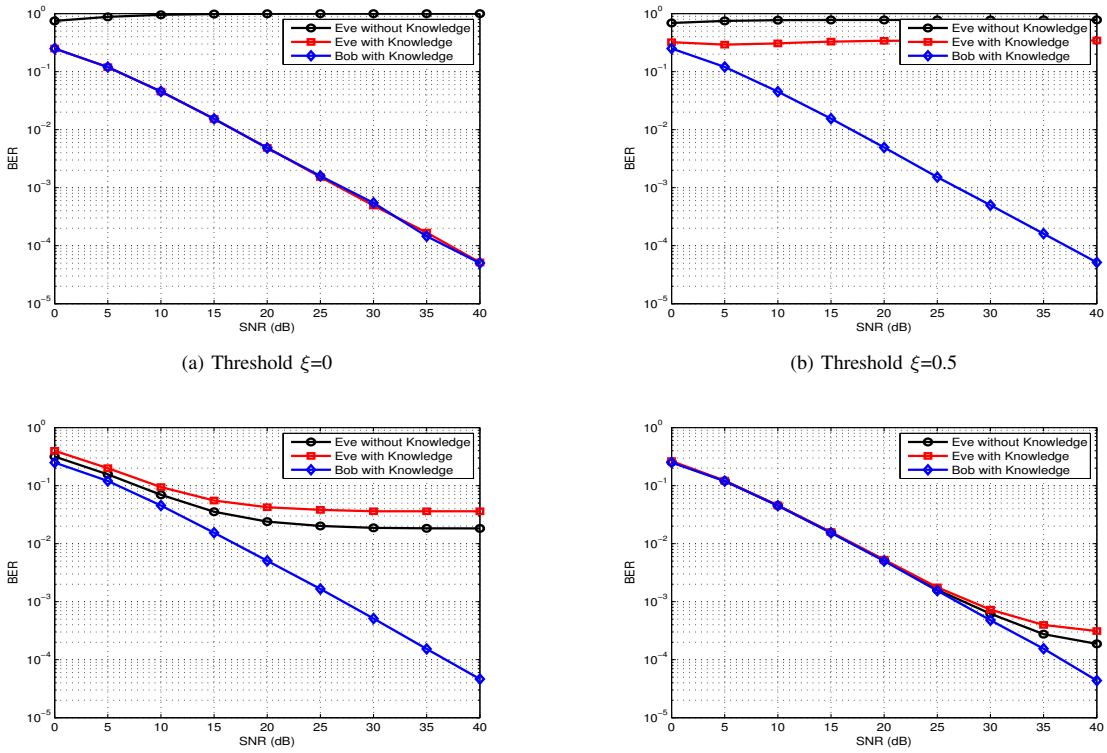
It should be noted that this security algorithm is implemented just before the communication process starts, and it can be renewed at any time the transmitter and receiver agree on to keep refreshing the source of security and make it as strong as possible. One important point that should be emphasized here is that this security training process should be implemented with sufficient high power to combat the effect of noise on the estimation errors so that the detected secret vector is as immune, robust and error-free as possible.

## IV. Simulation Results

The effectiveness of the developed security technique is characterized by the BER performance verses average SNR for both Bob and Eve. A simple communication system based on packet transmission is simulated, the packet size is equal to 432 bits with additional 32 CRC bits appended to the packet for the sake of error detection and a training sequence is also added to the original manipulated bits. Channel estimation using a training sequence is performed at both Bob and Eve as previously stated, from the estimated CSI gain at the transmitter, a vector of logical bits representing the randomness of the main channel is created by performing logical comparison with a proper selected threshold $\xi$, then the vector is used to manipulate data bits using an XOR operation, finally BPSK is used to modulate the manipulated data bits.

The modulated symbols are sent over i.i.d. Rayleigh fast fading channel. Fig. 2 depicts the BER performance when $\xi = 1$ for both Bob and Eve considering two cases with perfect CSI and with estimated CSI, the green solid line represents the performance of Bob when perfect channel estimation is assumed, whereas the intermittent blue line represents Bob's performance when channel estimation error is taken into account. The obtained results for Bob under the implementation of the proposed security method exactly coincides with the ones found in the literature under channel estimation [26]. This proves that the developed security method has no side effects on the BER performance of targeted users, instead it completely deteriorates the ability of malicious eavesdroppers to decode the received bits correctly. Particularly, in both cases whether Eve is aware of the manipulation process (i.e. Eve has pre-knowledge of the used algorithm) or not, she is going to experience a very bad BER as shown in Fig. 2. A very important observation should be taken into account that the BER plots exhibited in Fig. 2 are only obtained when $\xi = 1$, which is the best and optimum value for the selected threshold and is highly affected by the PDF of the amplitude (gain) of the considered fading channel.

In Fig. 3, we test the exact effect of the selected threshold $\xi$ on the BER of Eve, that changes dramatically as $\xi$ varies. Specifically, four different values are tested to show this impact. Fig. 3.(a) presents performance for $\xi = 0$ such that Eve's BER takes two curves based on her awareness of the algorithm or not. The black curve in Fig. 3.(a) exhibits the performance for the case in which Eve has no knowledge about the used method, where she sees a very bad BER (constant unity and full error rate over all SNRs). However, if she already knows the algorithm and uses her estimated channel in decoding process then its performance (drawn in red color) matches Bob's BER (drawn in blue color). The




(a) Threshold $\xi$=0

(b) Threshold $\xi$=0.5

(c) Threshold $\xi$=2

(d) Threshold $\xi$=3

Fig. 4. BER Performance of the proposed security technique for BPSK Modualtion in i.i.d Rayleigh Fading Channel with CSI Estimation at different values for the selected threshold.

main reason behind this is that the shape of the amplitude fad gain of the observed channel (i.e. PDF of the channel), which is, in our case, considered to be Rayleigh fading and has an amplitude of fading gain ranging from 0 to 3.5 with maximum probability (highest PDF peak) at amplitude gain equals 1. Therefore, at $\xi = 0$, all the transmitted bits are going to be manipulated using the adapted XOR operation, which means that if Eve is aware of this, she will use her channel to de-manipulate the received data bits and get the correct ones although her estimated CSI is different from Bob, but at the end, the amplitude gain is always greater than the set threshold $\xi = 0$. This leads to manipulating all the bits and removes randomness of the method totally. Such situation should be avoided by staying away from setting and selecting such a threshold. The rest of the cases in Fig. 3, cases (b), (c) and (d) are plotted for $\xi = 0.5$, $\xi = 2$, $\xi = 3$, respectively.

It should be noted that as the value of threshold increases, the degradation in the BER performance of Eve increases firstly for both cases until certain threshold and then the degradation in BER of Eve decrease. More specifically, the information leakage decreases as the value of threshold increases until optimum threshold and then it increases. The reason is that threshold is controlling the randomness of the manipulating vector. The best threshold value is found by simulation to be when $\xi = 1$ since it results in a complete random process as presented in Fig. 2.

## V. Conclusion

A new PHY layer security method is designed based of channel randomness and quantization threshold selection. The proposed method requires no CSI knowledge of the eavesdroppers; instead, it only relies on CSI knowledge of the legitimate users at the transmitter, where potential passive eavesdroppers can only estimate their own channel and have no knowledge about CSI between legitimate communication parties since channel reciprocity property of TDD systems is used in channel estimation instead of exchanging feedback signaling about the channel. Particularly, a logical vector, that reflects the channel randomness based on the estimated CSI gain, is created in order to be manipulated with the bits of the transmitted data packets. The process of manipulation is implemented on a bit level basis exactly before modulation process using an XOR operation. The same XOR operation is implemented after demodulation process on the detected bits to extract the concealed bits.

The obtained results demonstrate that the deployment of such mechanism can significantly ensure complete data confidentiality in fading channels, where security gap region between Bob and Eve is made very large over all observed SNR values. It is also deduced that the developed security

algorithm has no side effects on the performance of targeted users. Future work will involve extending the proposed security technique to different fading channel scenarios, and various communication systems setups with different MIMO configurations so that exact performance results for both Bob and Eve can be provided.

## REFERENCES


[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, pp. 1355–1387, 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, pp. 339–348, May 1978.

[4] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, 2008.

[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, pp. 4687–4698, Oct. 2008.

[6] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," IEEE Trans. Inf. Theory, vol. 54, pp. 2453–2469, June 2008.

[7] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," IEEE Trans. Inf. Theory, vol. 55, pp. 4033–4039, Sept. 2009.

[8] J. Li, "On ergodic secrecy rate for Gaussian MISO wiretap channels," IEEE Trans. Wireless Commun., vol. 10, pp. 1176–1187, Apr. 2011.

[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I,II:The MISOME wiretap channel," IEEE Trans. Inf. Theory, vol. 56, pp. 3088–3104, July 2010.

[10] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," IEEE J. Sel. Areas Commun., Special Issue on Signal Proc. Techn. for Wireless Phys. Layer Security, vol. 31, pp. 1864–1874, Sept. 2013.

[11] Z. E. Ankarali, M. Karabacak, H. Arslan, "Cyclic Feature Concealing CP Selection for Physical Layer Security," IEEE Military Communications Conference (MILCOM), Baltimore, Maryland, Oct. 6-8, 2014.

[12] E. Guvenkaya, H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," Communications Workshops (ICC), 2014 IEEE International Conference on , vol., no., pp.813–818, 10-14 June 2014

[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun., vol. 7, pp. 21802189, June 2008.

[14] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," IEEE Trans. Signal Proc., vol. 59, pp. 1202–1216, Mar. 2011.

[15] J. Zhu, R. Schober and V. k. Bhargava, "Secure transmission in multi-cell massive MIMO systems," Globecom Workshops (GC Wkshps), 2013 IEEE, pp.1286–1291, 9-13 Dec. 2013

[16] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," IEEE Trans. Signal Processing, vol. 59, no. 1, pp. 351361, 2011.

[17] L. Chenxi, G. Geraci, N. Yang, Y. Jinhong and R. Malaney, "Beamforming for MIMO Gaussian wiretap channels with imperfect channel state information," Global Communications Conference (GLOBECOM), 2013 IEEE, pp.3253,3258, 9-13 Dec. 2013

[18] C. Xiaoming, Y. Chau and Z. Zhaoyang, "Exploiting large-scale MIMO techniques for physical layer security with imperfect channel state information," Global Communications Conference (GLOBECOM), 2014 IEEE, pp.1648-1635, 8-12 Dec. 2014

[19] L. Pin-Hsun, E. Jorswieck, "On the fading Gaussian wiretap channel with statistical channel state information at transmitter," Communications and Network Security (CNS), 2014 IEEE, pp.121 - 126, 2014

[20] Z. Rezki, B. Alomair, and M. S. Alouini, "On the secrecy capacity of the MISO wiretap channel under imperfect channel estimation", Global Communications Conference (GLOBECOM), 2014 IEEE, pp.1602 - 1607, 2014

[21] M. R. Bloch, J. N. Laneman, "Strong Secrecy From Channel Resolvability", IEEE Transactions on Information Theory, vol.59, no.12, pp.8077-8098, Dec. 2013

[22] M. R. Bloch and J. N. Laneman, "Exploiting Partial Channel State Information for Secrecy over Wireless Channels," IEEE Journal on Selected Areas in Communications, vol.31, no.9, pp.1840-1849, September 2013

[23] Z. Rezki, A. Khisti and M.-S. Alouini, "On the Secrecy Capacity of the Wiretap Channel With Imperfect Main Channel Estimation", IEEE Transactions on Communications, vol. 62, no. 10, pp. 3652 - 3664, Oct. 2014.

[24] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on Channel Reciprocity Based Key Establishment Techniques for Wireless Systems," Wireless Networks, vol. 21, no. 6, pp. 1835-1846, 2015.

[25] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret Key Generation Using Channel Quantization with SVD for Reciprocal MIMO Channels," in 2016 International Symposium on Wireless Communication Systems (ISWCS), Sept 2016, pp. 597-602.

[26] Y. Chi-Hsiao, "Effects of Channel Estimation Error on the BER Performance of OFDM Systems in Multipath Rayleigh Fading Channels," IEEE Vehicular Technology Conference, pp.1097-1101, 2007