© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Investigation of Physical Layer Security Method in Cooperative Communication

Krishna Zalavadiya[1], Dimple Agrawal[2]

[1]PG student in Electronics and Communication Silver Oak college of Engineering and Technology, Ahmedabad, Gujarat, India

[2]Assistant Professor in Electronics and Communication Silver Oak College of Engineering and Technology, Ahmedabad, Gujarat, India

ABSTRACT

Wireless communication system have broadcast nature which limits performance in terms of security and privacy. Physical layer security is meant to provide secure communication and having legitimate user to successfully obtain secure information. The work in present paper is to investigate various methods developed for enhancing physical layer security starting from Shannon's wire-tap model in 1949 to recent multiple input multiple output based security models.

Keywords: Artificial fast fading, wiretap, ciphering, physical security, MIMO-OFDM, secrecy rate

I. INTRODUCTION

In wireless channel because of the broadcast nature, the main issue is privacy and security. Secrecy play main role in the wireless communication. Mainly security issue in the military as well as in the homeland. Theirs main aim is to secure communication in anyhow. In which data of source is only reached at the legitimate receiver not at eavesdropper. If unfortunately that data reached at eavesdropper then they cannot decode it [1]. When data is transmitted from source at that time so many receivers were presented, in that all some are legitimate receivers and others are malicious receivers. Legitimate receiver can decode data easily but malicious can't decode it. To do this we want to encrypt data at the transmitter side. In encryption original data has added with some code and reverse process is done at the receiver which is called as the decryption. With this we prevent data leakage. Now a days to do secure communication trend of physical layer security is in major concern [4]-[9].

For proper wireless communication we want to change characteristic of a physical channel. The number of research works on physical layer security has increased exponentially over the last few years. This number is certainly growing with the emergence of decentralized networks and deployment of 5G and beyond wireless communication system. So many difference between physical layer security and other higher layer cryptography. Do work on higher layer, computational complexity is increases because of the fluctuation in wireless channel. Now we learn different models used for enhancing secrecy. First we see introduction in which, what is physical layer security (PLS) and why we are doing PLS? This paper is based on the survey that's why in next section see the existing techniques for the security. Then after we take a comparative analysis of the techniques and conclusion. Mainly there are two parts to do security on the physical layer 1) information theoretic 2) signal processing. Here we discuss on the base of information theoretic analysis.

II. EXISTING METHODS FOR PHYSICAL LAYER SECURITY

There are many techniques which are used to a safe communication in between the environment of eavesdropper. Information theoretic security dates back to Shannon's pioneer work in 1948.

Shannon's Cipher Model (1948)

Claude Elwood Shannon was an American mathematician, electrical engineer and cryptographer known as "the father of Information Theory". His first founded landmark paper, "A Mathematical Theory of Communication" that he published in 1948[11]. Which model is known by "Shannon's Cipher Model". His consideration is to transfer data from transmitter to legitimate receiver in presence of passive eavesdropper. Shannon's mode consider noise less atmosphere that means ideal case. He says that with the help of this we get identical observation at the eavesdropper and legitimate receiver on the base of information theoretic level. Shannon's shows that legitimate parties can do secure communication with secret key. This secret key is added with the original message and then transferred, at the receiver we can decrypt that message with the help of same key. Here transmitter and receiver both are fixed and with this method only get information at receiver not at eavesdropper. Here we see the Shannon's cipher model in Figure 1.

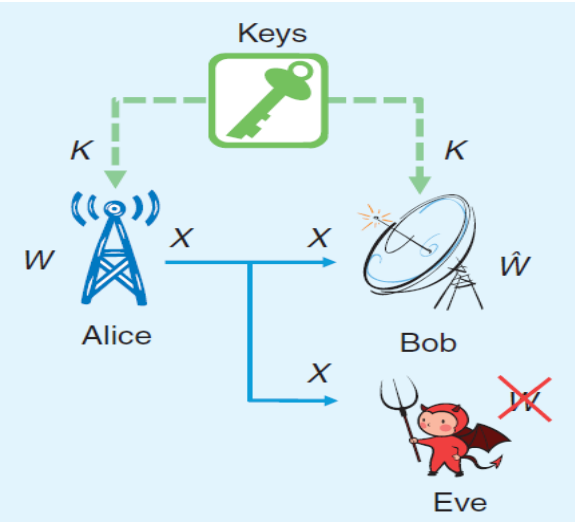

Figure 1. Shannon's Cipher Model [13]

In this figure W is original signal which is transfer from transmitter (Alice) to legitimate receiver (Bob). Secret key is used to encrypt the data. In Shannon's One Time Pad (OTP) approach original data W XORing with secret key K and then that encrypted data X will transmitted at the Alice. That same data is reached at the Bob as well as Eve. Bob has secret key that's why they again XORing of received data and secret key K. after this process Bob get original data but Eavesdropper haven't secret key, because of this it cannot decode the data. Shannon's shows that each key is used only for one time that's why its name is one time pad. With this we do a reliable communication. Size of secret key is always more than the original signal, which is often too costly to implement efficiently [13].

Wyner's Wire-Tap Channel (1975)

To overcome limitations of the Shannon's model public key cryptography is introduced. In a 1975 paper, Dr. Aaron D. Wyner introduced the "wire-tap channel", showing how one could obtain "perfect secrecy" when a receiver enjoys a better channel than does the wire-tapping opponent. In order to get rid of some of the hard problems, we have to change our conventional way of information theoretic security with computation based security. By accommodation such technique could be easily able to solve some the rigid problems such as factoring, logarithms which used to take a large amount of time but now such algorithms could be solve in appreciably very less amount of time. This all factors could help the communication sector to overcome all the adversaries to become successful [14], [15]. Wyner who develop a wire-tap channel and create a perfectly secure communication without use of secret keys. Wyners shows that if the wiretapper channel has degraded version of the main channel then the source and destination can exchange perfect secure communication with nonzero rate [4]. While the eavesdropper cannot get information from its observation. Achievable secrecy rate is called when the rate at which information can transmitted by transmitter and received at intended receiver is

secretly. Secrecy capacity is called as the maximal achievable secrecy rate. Then after in [5] secrecy capacity of scalar Gaussian wire-tap channel was analyzed. In [6] wyner shows the transmission of confidential message over the broadcast communication. Model of Wyner's wire-tap channel is shown in Figure 2.

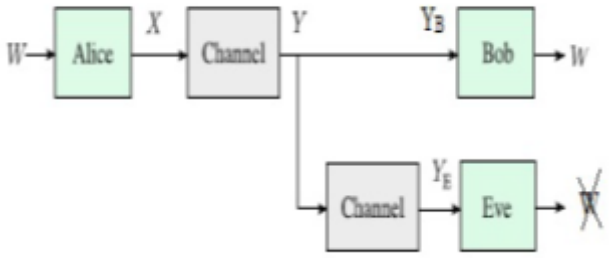

Figure 2. Wyner's Wire-Tap Channel [12]

Here in this figure original signal W is transmitted by the transmitter (Alice) that transmitted signal X is reached at the Bob as Y_B and at Eav as Y_E because of wireless communication. Bob can easily decode the message but eavesdropper cannot decode it because of key, here public key is used. To understand secrecy capacity we take some assumptions, where source input is X and intended destination output is Y and Eav output is Z. then the secrecy capacity (C_S) is given by

$$C_S = \max [I(X; Y) - I(X; Z)]$$

That means signal transmit over main channel to wire-tap channel is called as secrecy capacity [1].

Relay Beamforming Technique

In olden days the work on Physical layer security is based on single antenna system were Absent Feedback scheme was shown, If the channel between source and eavesdropper is better than the channel between source and destination, secrecy rate is typically zero [4],[5]. After some time to overcome this problem one newer technology is established, in which multiple antennas are used to transmit and receive the signal. In this system there are three phases, i) Multiple-Input-Multiple-Output (MIMO) [16]-[20] ii) Single-Input-Multiple-Output (SIMO) [21] iii) Multiple-Input-Single-Output (MISO) [22]-[23] systems. To implement this system costing is very high as well as the size is so higher. Because of this limitations multiple antennas may not be available at network nodes. After seeing this scenario node cooperation is an effective way to enable single antenna node to operate as a multiple antenna system. Here we consider a scenario in which source communicates with destination with the help of number of relays in presence of multiple eavesdroppers. Each node has single antenna which is omnidirectional and global channel state information (CSI) is achievable. Beamforming is used in relay system to improve the received signal-to-noise ratio (SNR) at the legitimate receiver. To establish this type of system from the traditional system without security concerns is to exploit the magnitudes and phases of the relay to destination channels and accordingly adjust the transmit powers and phases of the signals that are to be transmitted from several relays bearing a common message, so as to combine the signals at the destination contractively [25]. If relay system wants to consider as a security concern then it need to exploit the channel information of eavesdropper as well as intended receiver and the objective is no longer the received signal to noise ratio at the legitimate receiver. Relay beam forming model is shown in Figure 3.

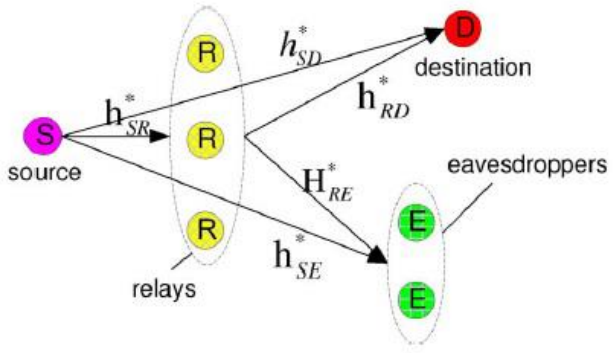

Figure 3. Illustration Of Relay Model [1]

To understand this concept we study 3 cooperative schemes that improve the total transmit power at the source and increase the achievable secrecy rate. Three cooperative schemes are i) Decode and Forward (DF)

ii) Amplify and Forward (AF) iii) Cooperative Jamming (CJ).

In Decode and Forward method source transmits encoded signal to relays, each relay decode the signal then again re-encode that weighted version of signal and after improving the signal power they transmit signal in the atmosphere, here signal can cover more distance and reached at the receiver. If any problems are occur in the signal that is recover at the relays because of the decoding process. In Amplify and Forward method first the encoded data is reached at the relays. This time data is not decoded by the relays but they only amplify the signal that's why they bust the signal and then transmitted after some distance data catch by the receiver. Here if any mistakes are presented in the transmitter that same mistakes is reached at the receiver. In Co-operative jamming system source transmits the encoded signal and relays transmit weighted jamming signals because of the confusion at receiver. Legitimate receiver can catch the signal, because of the decoding process it can judge the feck data or original encoded signal but malicious receiver cannot judge. With this process can protect the data from the eavesdropper. We find the perfect value of the source power after obtaining the relay weights for a fixed source power. However beamforming scheme offers secure communications by decreasing the signal-to-noise power ratio (SNR) of an eavesdropper. Since, the beamforming scheme need the channel state information between a transmitter and an eavesdropper, it is rather impractical.

Transmit Antenna Selection

As a more practical scheme then the beam forming scheme is Transmit Antenna Scheme (TAS). Limitation of the beamforming method is overcome by the TAS process. In this process we didn't required CSI between source and eavesdropper. We find the secrecy when transmitter has multiple antenna with single RF chain, legitimate receiver has single antenna device and eavesdropper has multiple antenna. We develop close form expressions for the secrecy outage probability. Here we get higher level security to increase number of antenna at Alice. To comparing both single RF chain and multiple RF chain, we get more advantages in single chain. Like reduced cost, complexity, power consumption and size. Some limitation of this scheme is that Alice has not the knowledge of CSI between Alice and Bob as well as Alice and Eav. Therefore secrecy is not guaranteed it is only probabilistic treatment of secrecy capacity [8].

Artificial Noise

In practical transmitter cannot get CSI of eavesdropper at all time. The secrecy capacity of MISO wiretap channel has been investigated when statistical channel state information of eavesdropper is available. When Eav's CSI is completely absent, AN scheme has been proposed for MISO and MIMO systems to improve the secrecy rate, and continued cooperative jamming scheme. The AN scheme recover the limitation of the CSI scheme that to cope with the passive eavesdropper. It gives the degraded version of SNR of an eavesdropper. In this process transmitter add AN code with the original information. That code is removed at the legitimate receiver and they get information. This scheme offers multiple antenna at transmitter is more than the eavesdropper. But if number of antenna at eavesdropper is more or twice the Alice's antenna then eavesdropper can trace information signal and effect of AN scheme is failed. Because of the multiple antenna, it's very costly. This all work is assumption that eavesdropper know CSI of itself that's why it can detect the intercepted signal coherently. This assumption is valuable for some situations. In that firs the sample signal is transmitted by transmitter for the legitimate receiver to design the channel coefficient as well as synchronize the sampling time and frequency. Against this the Artificial Fast Fading (AFF) has been proposed.

Artificial Fast Fading

The Artificial Fast Fading scheme causes the effect of pseudo fast fading to the received signal of an eavesdropper without affecting the received signal of

a legitimate receiver. This can be achieved by multiplying the signal to be transmitted by an intentional random weight which is called the AFF weight. AFF weight is generated to be canceled out by the CSI between an Alice and a Bob while processing the random property. Since the signal detection under a fading channel generally results in a lower performance then that under a noise only channel, the AFF scheme is effective in improving the secrecy. In [27] the AFF scheme is considered for single stream transmitter. For cancelling the AFF weight by the CSI between a transmitter and a legitimate receiver, it is required that the system has Multiple Input Single Output (MISO) architecture. Thus the AFF scheme has been developed in a MISO system in [27]. In AFF scheme with MISO system is shown in Figure 4.

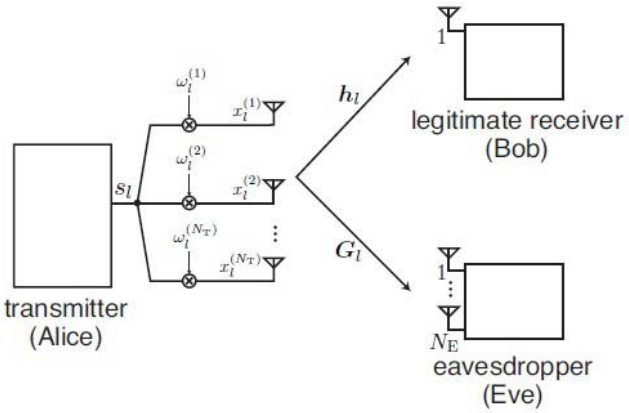

Figure 4. Miso-Ofdm System With An Eavesdropper [32]

Here in this system transmitter Alice transmits encoded signal. Original signal added with the AFF weighted signal then converted signal is transmit by the antenna. Alice and Eve has multiple antenna but Bob has only one antenna. In this system weighted code and channel state information made unity then and then that receiver get that data. With the help of this can judge legitimate receiver.

Artifical Fast Fading With Mimo-Ofdm System

Meanwhile, modern wireless communication systems mostly use Multiple Input Multiple Output (MIMO) architecture. By transmitting multiple data streams at a time, system attains a larger capacity. Here, we propose an AFF generation scheme for MIMO-OFDM systems.

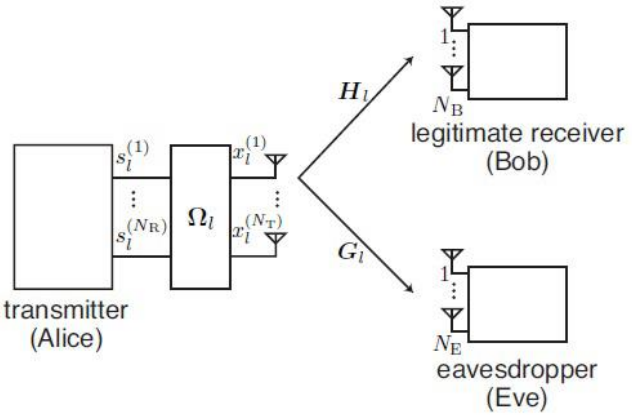

Figure 5. Mimo-Ofdm System With An Eavesdropper [32].

The proposed AFF weight matrix and the cancelling weight matrix. Simulation results show that the AFF produced by our AFF generation scheme is successfully cancelled out at legitimate receiver. Moreover the MIMO-OFDM system using our proposed AFF scheme is shown to provide a larger mutual information at the legitimate receiver then the MISO-OFDM system using the existing AFF scheme [32]. In [32], proposed a frequency domain AFF generation scheme for MIMO-OFDM systems employing spatial multiplexing. The proposed AFF matrix is composed by stacking the random weight matrix and the canceling weight matrix. The AFF produced by our AFF generation scheme is successfully cancelled out ae the legitimate receiver, while causing the pseudo fading effect at the eavesdropper. When the multiple streams are transmitted, the mutual information of the system is increased along with the number of transmitted streams. Therefor the proposed scheme is effective for improving the secrecy rate of MIMO-OFDM system [32].

Cooperative Jamming

In wireless communication so many transmitters and receivers to accept and release data signal. To keep reliable communication only Alice and Bob can

communicate, all other must be silent as the signals they transmit will cause interference at Bob. When security is an added concern independent transmitters can increases the secrecy rate of a given transmit receiver pair by transmitting signals. This system first shown in [33] then in [34] and [35], cooperative jamming is work on this concept to protect data from the eavesdropper. One interpretation of this fact has to do with the relative nature of secure communications and the fact that the achievable throughput in secrecy is equal to the difference in the rates of the legitimate channel, and eavesdropper's channel. Model of cooperative jamming signal is shown in Figure 6.

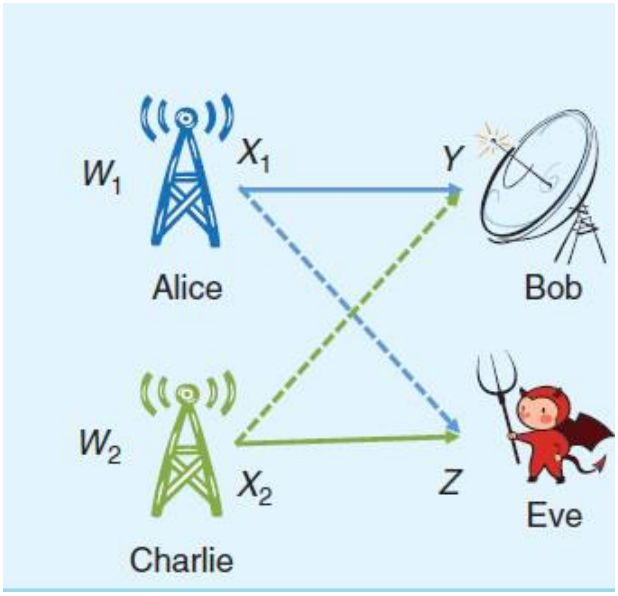

Figure 6. A Multiple Access Wiretap Channel

Cooperative jamming was originally proposed for a multiple access wiretap channel, where multiple legitimate users wish to have simultaneous secure communications with a legitimate receiver in the presence of eavesdropper. Here in this figure, Alice and Bob are legitimate transmitter-receiver, Charlie also wish to transmit data to Bob simultaneously in the presence of Eav. To maximize the sum secrecy rate of the system, a user Charlie who has stronger connection to the eavesdropper then to the Bob should cease sending message carrying signals and instead help by sending Independent Identically Distributed (IID) Gaussian noise signals. Since Charlie has a stronger channel gain to Eav then to Bob, his jamming is more detrimental to Eav than Bob, thus increasing Alice's achievable secrecy rate.

III. COMPARITIVE ANALYSIS

Shannon's Chipher Model

Adv. Private Key is used. One time pad requires, that's why we get perfect secrecy.

Dis. Secret key length should be as large as the size of the message which is often too costly to implement efficiently.

Wynner's Wire-Tap Model

Adv. Public key cryptography. Assume that wire-tap channel gets degraded version of the main channel, designer attempts to build the encoder-decoder in such a way as to maximize the transmission rate R and the equivocation d of the data as seed by the wire-tapper.

If equivocation is equal to entropy of the data source, then that transmission is accomplished in perfect secrecy.

Result imply that there exist secrecy capacity is greater than 0, such that reliable transmission at rate up to secrecy capacity is possible in approximately perfect secrecy.

Dis. Tread off curve between transmission rate and equivocation.

Csiszar And Corner

Adv. When the eavesdropper isnot degraded with respect to the legitimate user, information theoretically secure communication between the legitimate user is possible by exploiting the inherent channel is degraded.

Relay Beamforming

Adv. Beam forming scheme offers secure communication by reducing the signal to noise power ratio (SNR) of an eavesdropper.

Dis. BF scheme requires the channel state information (CSI) between a transmitter and eavesdropper, it is rather impractical.

Transmit Antenna Selection

Adv. Requires only the CSI between a transmitter and legitimate user, it can cope with a passive eavesdropper.

Dis. TAS does not always degraded the demodulation performance of the eavesdropper.

Artificial Noise Scheme

Adv. It proposed to cope with a passive eavesdropper, it degrades the SNR of the eavesdropper.

Dis. If the eavesdropper increases the number of receive antennas to improve the received SNR the effect of AN is mitigated at the eavesdropper.

Artificial Fast Fading

Adv. It is effective in improving the secrecy.

Dis. AFF scheme is considered for single-stream transmission for cancelling the AFF weight by the CSI between a transmitter and legitimate receiver, it is required that the system has multiple-input single-output architecture.

Artificial Fast Fading With Mimo

Adv. Transmit multiple data streams at a time, system attain a larger capacity.

Cooperative Jamming

Adv. Gives more reliability.
Increase secrecy rate.

IV. REFERENCES

[1]. Lun Dong, member, IEEE, Zhu Han, senior member, IEEE, Athina P. Petropulu, fellow, IEEE, and H. Vincent Poor, fellow, IEEE "Improving wireless physical layer security via cooperating relays" IEEE transactions on signal processing, vol. 58, no. 3, march 2010

[2]. W. K. Harrison, and S. W. McLaughlin, "Physical-layer security: combining error control coding and cryptography," Proc. IEEE ICC, pp. 1–5, Jun. 2009.

[3]. C. Shin, R. W. Heath, and E. J. Powers, "Blind channel estimation for MIMO-OFDM system," IEEE Trans. Wireless Commun., vol. 56, no. 2, pp. 670–685, Mar. 2007.

[4]. A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[5]. S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," IEEE Trans. Inf. Theory, vol. 24, pp. 451–456, Jul. 1978.

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

[7]. A. Khisti, G. W. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," Proc. IEEE ISIT, pp. 524–528, July 2008.

[8]. H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," IEEE Signal Process. Lett, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[9]. N. Yang, P. L. Yeoh, M. Elkashlen, R. schober, and I. B. Collings, "Secure transmission via transmit antenna selection in MIMO wiretap channels," Proc. IEEE GLOBECOM 2012, pp. 789–794, Dec. 2012.

[10]. Yu Kozai and Takahiko Saba" an artificial fast fading generation scheme for physical layer security of MIMO-OFDM systems" dept. of computer science, Chiba Institute of Technology, 2-17-1 tsudanuma, narashino, chiba 275-0016 japan,2015 IEEE.

[11]. C. E. Shannon, "communication theory of secrecy systems", bell system technical journal, vol. 28, pp. 656-715, Oct. 1949

[12]. Amal Hyadi, (student member, IEEE), Zouheir Rezki, (senior member, IEEE), and Mohamed-slim Alouini, (fellow, IEEE)." An overview of physical layer security in wireless communication systems with CSIT uncertainty" 2169-3536 2016 IEEE. Translations and content

[13]. Raef Bassily, Ersen Ekrem, Xiang He, Ender Tekin, Jianwei Xie, Matthieu R. Bloch, Sennur Ulukus, and Aylin Yener, "Cooperative Security at the Physical Layer" IEEE signal processing magazine September 2013

[14]. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[15]. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976

[16]. O. Hero, "Secure space–time communication," IEEE Trans. Inform. Theory, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[17]. A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," IEEE Trans. Inf. Theory, Aug. 2007. [Online]. Available: http://arxiv.org/abs/0708.4219, submitted for publication.

[18]. R. Negi and S. Goelm, "Secret communication using artificial noise," in Proc. IEEE Vehicular Tech. Conf., Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.

[19]. F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, Oct. 2007 [Online]. Available: http://aps.arxiv.org/abs/0710.1920, submitted for publication.

[20]. T. Liu and S. Shamai, "A note on the secrecy capacity of the multi-antenna wiretap channel," IEEE Trans. Inf. Theory, Nov. 2007 [Online]. Available: http://arxiv.org/abs/0710.4105, submitted for publication.

[21]. P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in Proc. IEEE Int. Symp. Inf. Theory, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[22]. Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in Proc. 41st Conf. Information Sciences Systems, Baltimore, MD, Mar. 2007

[23]. S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in Proc. IEEE Int. Symp. Inf. Theory, Nice, France, Jun. 2007.

[24]. V. Havary-Nassab, S. Shahbazpanahi, A. Grami, and Z. Luo, "Distributed beamforming for relay networks based on second-order statistics of the channel state information," IEEE Trans. Signal Process. vol. 56, no. 9, pp. 4306–4316, Sep. 2008.

[25]. R. Mudumbai, d. Richard, Upmanyu Madhov, h. Vincent poor, "Distributed transmit beamforming: challenges and recent progress", IEEE communications magesins

[26]. Yindi Jing, Hamid Jafaekjani, "Network beamforming using relays with perfect channel information", IEEE transactions on information theory.

[27]. H. M. Wang, T. Zheng, and X-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading," IEEE Trans. Wireless Commun., vol. 14, no. 1, pp. 94–106, Jan. 2015.

[28]. G. B. Giannakis, J. M. Mendel, "Identification of nonminimum phase systems using higher order statistics", IEEE transaction on Acoustics, speech, and signal processing

[29]. Lang tong, Guanghan Xu; T. Kailath, "Blind identification and equalization based on second-order statistics: a time domain approach" IEEE transactions on Information theory

[30]. Xiaohua Li, E.P. Ratazzi, "MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks" Military Communications Conference,2005, MILCOM 2005,IEEE

[31]. Xiaohua Li and Juite Hwu, E. Paul Ratazzi, "Using antenna array redundancy and Channel Diversity for Secure Wireless transmissions" Journal of Communications, Vol. 2, No. 3, May 2007

[32]. Yu Kozai and Takahiko Saba" An artificial fast fading generation scheme for physical layer security of MIMO-OFDM systems" dept. of computer science, chiba institute of technology, 2-17-1 tsudanuma, narashino, chiba 275-0016 japan,2015 IEEE.

[33]. Ender Tekin and Aylin Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy" 44th Annual Allerton Conference

[34]. Ender Tekin, Aylin Yener, "the general Gaussian Multiple-access and Two-way wiretap Channels: Achievable Rates and Cooperative Jamming" IEEE Transactions on Information Theory

[35]. E. Tekin, "The multiple access wire-tap channel: wireless secrecy and cooperative jamming" Information theory and application workshop, 2007.