Privacy Security of Multiuser on Multilevel System using XOR

Siji P.Raj
(Dept. of Computer Science and Engineering, Mahatma Gandhi University, Kerala, India)

Abstract: *Privacy security of multiuser on multilevel system is considered in this work. On communication there is a chance for the eavesdropper's to secretly listen to the conversation. In order to confuse the eavesdropper's, the transmitter sends information signal to both the receiver and eavesdropper. But the orginal message is send to the receiver and the information signal which looks same as the original message is send to the eavesdropper. The existing system says that if the eavesdropper is of lower quality than the transmitter that is transmitter having higher quality then it is easy for the transmitter to avoid the interface and send the information safely. Client send the original message to the user at the same time the fake message or artificial message which is same as the original message is send to the eavesdropper. The original message which is sending to the client is cleaned before reaching to the recipient. In the previous work there is a chance for the eavesdropper's to view the message and add any noise to the orginal data. It is not secure so in the enhancement of work I encrypted the original message and send to the receiver . The message which looks same as the original message is send to the eavesdropper .Since the orginal message is encrypted it is not viewed by the eavesdropper. The receiver then obtained the original message which is in the encrypted form is decrypted by using XOR system.*

Index terms: *Multi User Multi Eavesdropper (MUME), secrecy capacity, channel state information (CSI), passive eavesdropper, XOR system.*

I. Introduction

Securities in wireless communication have gained much prominence in recent years. During the communication there may occur chance to create security problems. In between the conversation of multiuser the eavesdropper who is secretly listening to the conversation of others or who gain an unauthorized access to the communication may create noise or view the message. Here the secret information is viewed by a third party who is an eavesdropper so that the information channel is not secure. The communication become secret only if the eavesdropper cannot view the orginal information. For that the original message should be encrypted. The fake information which looks same as the encrypted message is send to the eavesdropper. Existing system says that a non –zero security capacity will be obtained only if the eavesdropper's channel capacity is less than that of receivers channel capacity. During multi-user communication common message to seat to both the receiver and secret message is send to only one of them. It is not a good way of communication because only one user gets the original data. In my work I extend the idea to multi-user communication. Here both the users can get the original message simultaneously [2]. When channel capacity of the transmitter is less than that of the eavesdropper then security at that time is less. That means there may have more chance for the occurrence of interference. To avoid the unauthorized access of the eavesdropper, [3] the transmitter send signal to the null-space of the channel of eavesdropper this is none by transmitter. The passive eavesdropper that is only secretary listening to the private conversation of others not adding any artificial data to the original data, this concept is difficult to implement. So in my work this problem is overcome and proposes a scheme without using any change in the channel state information(CSI).***Channel state information*** or channel status information (CSI) means the information which represents the state of a communication link from the transmit source to the receiver source.

To obtain secure communication various physical layer techniques have been proposed even if the receiver's channel is worse than the eavesdropper's channel. The major technique is to use the artificial noise in order to confuse the eavesdropper's. The transmitter sends the original signal which is in the encrypted form. The message is encrypted in order for the security of message that is to be transmitted at the receiver in the original form which is same as the information send by the receiver. The eavesdropper views the information send by the transmitter to confuse the eavesdropper. The transmitter sent another message which is same as the original message to the eavesdropper. This method can be divided into 2 types. First is the (i) trust friend model, this model consists of two base stations and these base stations are connected by the backbones like optical fiber. Here any one of the base station transmit interfering signal to the other base station in order to secure the uplink communication .The next method is the (ii) helper-relay model, in this model codeword's will be send with the original message. Section II details about the existing methodology and Section III address the related work regarding the proposed methodology.

II. Existing system

The existing system uses the concept of single-user. In order to avoid the eavesdropper's some techniques are used. First method is 1) the use of multiple antennas- to receive the information safely. Multiple antennas helps to transmit the information simultaneously to multiuser It is a good method but there may have chance for the interference. The other method is that 2) the use of artificial noise by the transmitter in order to confuse the eavesdropper. Here the original message is sending to the receiver at the same time artificial information is sending to the receiver. The disadvantage of this is there is no any security will apply to the original message. The system model for the use of multiple antenna is that Alice send message to different user Bob 1, Bob 2 and Bob j each having multiple antennas and send the message by removing all artificial noise created by the eavesdropper Eve k. Antennas receive only particular frequencies. This communication is done using local area networks. The disadvantage of this is this is difficult for implementing in the longer distance. In this system the transmitter send original message to the receiver at the same time the fake message is send to the eavesdropper. Here the original message has not secured so it is enhanced with the concept of XOR system.

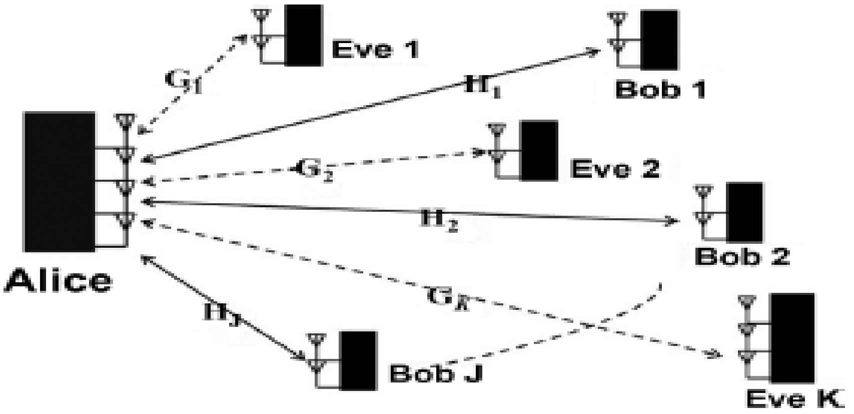

Fig. 1. Multi-user multi eavesdrop system model

Most of the previous papers are all concentrating on the single user system. But in modern communication system multi-user were communicating and same as the eavesdropper's. Eavesdroppers also not appear as single, but they appear are cooperating. This cooperation of eavesdropper's will severely affect the performance of the system. This performance depends on the quality of the transmitter and receiver. Also it is connected with multiple antennas at the side. The secrecy rate obtained while using antennas and single-user is of different. The transmitter has to send different messages to the different receiver. During the transmission of the message, there is a chance for the cause of co channel interference. This co channel interference (CCI) need to be minimize at the same time the transmitters should be hide from the viewing of eavesdropper's. For that various methods are used. Our aim is that any of the authorized users will not be trapped by the eavesdropper's. One of the methods is (i) the SVD method. In this method, decomposition is done at each user's channel but not suppress the interference caused by other user. Here the interference of their own message is only suppressed. One of the disadvantages of this method is here only single-user communication is concentrating but in modern wireless communication multiuser system is considered, so if their own message is only considered then the interferences caused by the other user in the same channel will affect all other users also. Second is the ZF beam forming method? In this method, all the transmitted is kept in the null space of the receiver. In these two methods ZF method is better and simple but it is difficult to implement.

According to the drawback of the previous method, an alternative approach is proposed in this method, that may take the concept from SVD method and ZF beam forming method. It can increase the secrecy rate and the performance of the system. So that privacy communication between multi-users can take place.

III. System model

X is the transmitted signal. Uj is the information signal user j (Uj). V denotes the artificial noise to interfere the eavesdropper's. Then the signals received at the Bob and eavesdropper k is as follows

Bob j : $\boldsymbol{Y}_j = \mathbf{H}_j\mathbf{X} + \mathbf{N}_j^B$, for j = 1,…..,$\boldsymbol{J}$,
Eve k : $\boldsymbol{Z}_k = \boldsymbol{G}_k\mathbf{X} + \mathbf{N}_k^E$, for k = 1,…..$\boldsymbol{K}$,

Where Hj is the channel matrix between the transmitter and Bob j and Gk is the channel matrix between the transmitter and eavesdropper and eavesdropper k. Hj and Gk are the channel matrix. Our aim is to transmit message from Alice to Bob secretly without any interference or any eavesdropper. We try to reduce all the co channel interference created and to reach the message from Alice to Bob without viewing by any of the eavesdropper. We make sure that none of the eavesdroppers will wiretap the communication between Alice to Bob.

In the normal multi-user multi-eavesdrop system during communication different message reaches to different user at different manner. Select each user according to any specific criteria and make each user into consideration. So that we can assure that our message will not be wiretapped by any one. By this method the secrecy rate of the system is identified either by finding the best transmission pair or the total rate gap between Bobs and Eavesdropper. The difference between the current rate and the rate to which it could adjust on an ARM. Another one method is also proposed for finding the secrecy rate transmission which is termed as Absolute Secrecy Rate. The absolute Secrecy rate is always lower than the obtained secrecy rate.

IV. Precoders design at multi-user multi eavesdrop system according to ISDF

Before each transmission from Alice the data has been processed. **Pre-coding** is a generalization of beam forming to support multi-stream (or multi-layer) transmission in multi-antenna wireless communications. In conventional single-stream beam forming, the same signal is emitted from each of the transmit antennas with appropriate weighting (phase and gain) such that the signal power is maximized at the receiver output. When the receiver has multiple antennas, single-stream beam forming cannot simultaneously maximize the signal level at all of the receive antennas.[1] In order to maximize the throughput in multiple receive antenna systems, multi-stream transmission is generally required. After that these data is moved into the MIMO channel with the artificial noise. The main emphasis with this work is to make the pre coders which is denoted as Wl for l=1, 2, J and W. In electrical engineering, computer science and information theory, **channel capacity** is the tightest upper bound on the rate of information that can be reliably transmitted over a communications channel. By the noisy-channel coding theorem, the channel capacity of a given channel is the limiting information rate (in units of information per unit time) that can be achieved with arbitrarily small error probability. Information theory, developed by Claude E. Shannon during World War II, defines the notion of channel capacity and provides a mathematical model by which one can compute it. The key result states that the capacity of the channel, as defined above, is given by the maximum of the mutual information between the input and output of the channel, where the maximization is with respect to the input distribution.

Using this method each user keep their data on their own channel space so that each user can gain maximum channel gain. Here each user their data in their own channel but we use another one method in which each user can kept their data on another users channel space. This method is called block diagonization method. In this different users can keep their data on the different null space of the different channel. Other than this method two more method is also used named as Dirty Paper Coding and ZF beam forming. In telecommunications, dirty paper coding (DPC) is a technique for efficient transmission of digital data through a channel subjected to some interference known to the transmitter. The technique consists of pre coding the data in order to cancel the effect caused by the interference. To explain where the term 'dirty paper coding'[1] comes from, imagine a paper which is partially covered with dirt that is indistinguishable from ink. The theorem says that if the writer knows where the dirt is to start with, she can convey just as much information by writing on the paper as if it were clean, even though the reader does not know where the dirt is. In this case the dirt is interference, the paper is the channel, the writer on the paper is the transmitter, and the reader is the receiver. In information-theoretic terms, dirty-paper coding achieves the channel capacity, without a power penalty and without requiring the receiver to gain knowledge of the interference state. Zero-forcing (or Null-Steering) precoding is a spatial signal processing by which the multiple antenna transmitter can null multiuser interference signals in wireless communications. Regularized zero-forcing precoding is enhanced processing to consider the impact on a background noise and unknown user interference,[1] where the background noise and the unknown user interference can be emphasized in the result of (known) interference signal nulling. In particular, Null-Steering is a method of beam forming for narrowband signals where we want to have a simple way of compensating delays of receiving signals from a specific source at different elements of the antenna array. In general to make use of the antenna arrays, we better to sum and average the signals coming to different elements, but this is only possible when delays are equal. Otherwise we first need to compensate the delays and then to sum them up. To reach this goal, we may only add the weighted version of the signals with appropriate weight values. We do this in such a way that the frequency domain output of this weighted sum produces a zero result. This method is called null steering. The generated weights are of course related to each other and this relation is a function of delay and central working frequency of the source.

The message is only decoded only if the maximum transmission stream of data is send simultaneous. Within the same frequency of Alice different co channel Bobs with multiple antennas will communicate. With Multiple User multiple Eavesdropper several antennas are connected together. This is very difficult to implement and transmit the data with applying security for that we use different security measures. In this scenario transmission schemes are designed. During the communication system of wireless security, in null space of the channel coding matrix is applied to the channel matrix Hj. This space is also termed as the selection space. If smaller is the matrix rank Hj, then larger is the pre coding selection space.

A. Designing of Precoders

Here the designing of pre coders for Bobs on ISDF is stated. The pre coders were designed for stating the ISDF method with the corresponding users own channel matrix so that the performance will be severely affected. A new model is proposed in order to solve this problem; this is designed according to the previously designed pre coders. This can increase the SDF directly, when each pre coder is design directly also it is called as increasing security degree of freedom. By this method, we can directly increase the degree of freedom. Consider an example. Alice selects a pre coder for Bob 1 then select another pre coder for Bob2 but these Bobs could not know about the pre coders signal. Like wise Bob3 could not see the signal intended to Bob1 and Bob2. The Bobs can see the signal of each other as the interference. Only a single stream of data is send to the receiver in the existing system but in the proposed system, we extend the idea to the multiple streams of data. Through the equivalent channel the data is transmitted. If water filling (WF) method is used, then the secrecy rate can be increased. For that uniformly the power is allocated to the each user j.

V. Security using XOR

A new algorithm XOR is described in order for the security analysis. Like as key management. Security protocols aim at the secure communication over the internet. For addressing the problem of security, a new class of protocols is used. Here the data is encrypted before sending it to the receiver same as decrypt. Encipher rule allows the data key to encrypt the plain text. Decipher allows the data key for the encryption of messages. Key export allows the encrypting key for transporting to another space. By using functional symbols we represent cryptographic primitives. The representation of XOR consists of of XOR term which is encoded as a binary string. This is assigned as a finite set of atoms. Let us consider an example: The ordered set of base atoms is as follows: KM, KP, KEK, IMP, EXP, DATA, PIN, This representation of KEK_PIN_DATA is as

```
                 KM KP KEK IMP EXP DATA PIN
KEK_PIN_DATA -> 0  0   1    0    0    1    1
                                |
                               19
```

Thus KEK_PIN_DATA is represented by the decimal integer 19. we still get the same integer - so our representation effectively normalises the term with respect to the properties of XOR. Notice further that if we have two terms x1 and x2, that are represented by integers l and m, then the integer representing x1_x2 is just l _m. So, we represent XOR using XOR, which is an attractive feature of the representation. For example, we can write the intruder rule x1, x2 ! x1 _ x2 as l,m ! l _ m For encryption terms, which consist of one XOR term encrypted by another, we simply shift the bits of the integer representing the message term n places to the left (where n is the number of base terms), and add the integer representing the key. We obtain a unique number in the range 0 . . . 22n for each encryption term. For example, the term {|KEK_PIN_DATA|}KM_DATA is represented by

```
KM KP KEK IMP EXP DATA PIN
 0  0   1    0    0    1    1
                                ---→2498
KM KP KEK IMP EXP DATA PIN
 1  0   1    0    0    1    1
```

VI. Artificial noise for secret communication

The key idea of this paper is that the transmitter can use multiple antennas to add artificially generated noise to the information signal, such that it lies in the null space of the receiver’s channel. Thus, the receiver’s channel nulls out the artificial noise and hence the receiver remains unaffected by the noise. The information signal is transmitted in the range space of the receiver’s channel, while the artificial noise is created in the null space, and thus, there is a clean separation between the two. The null and range spaces of the eavesdropper’s channel will, in general, be different from those of the receiver’s channel. Thus, the eavesdropper’s channel will be degraded because some component of the artificial noise will lie in its range space. An increase in the number of receiver antennas affects two aspects of secrecy capacity, the MIMO capacity and the ability to produce artificial noise. Intuitively, the more the number of receive antennas, more the number of ‘parallel’ channels that can be created between the transmitter and the receiver, leading to capacity gain. However, more receive antennas reduces the number of dimensions available for generating artificial noise, limiting the ability to degrade the eavesdropper’s channel. These two opposing effects suggest that there may be interesting trade-offs to be made between them. Assuming that NR · NT and that Hk is full rank (i.e. has rank NR), NR dimensions can be used for information transmission while NT ¡ NR dimensions can be used to create artificial noise. The eavesdropper can use NE. dimensions to receive information, of which some, or all, may be degraded by artificial noise. We need to study the variation of secrecy capacity with NT , NR and NE. The effect of number of transmit antennas on secrecy capacity was shown in [1]. In this paper, we investigate the effect of multiple receive antennas and multiple colluding eavesdroppers (represented by NE > 1) on secrecy capacity.

VII. Simulation results

We compute the lower bound on average secrecy capacity Csec under a power constraint of P0. It is compared with the average capacity of the transmitter-receiver link (without secrecy requirements) under the same power constraint. The difference between the two (C -Csec) is an upper bound on the loss in capacity because of the secrecy requirement. Further, given an outage capacity Coutage, we compute the outage probabilities PrfCsec < Coutageg, hoping that low outage probabilities can be achieved. The effect of the number of transmit antennas (NT) on secrecy capacity was considered in [1]. In this paper, the effect of the number of antennas at the receiver (NR) and the eavesdropper (NE) is considered, while keeping the number of transmit antennas (NT) fixed. In the following discussions, references to average secrecy capacity should be interpreted to be the lower bound Csec.

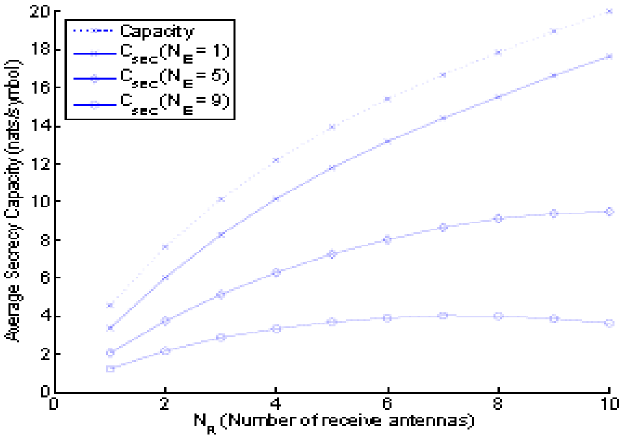

Fig. Average secrecy capacity

The average secrecy capacity and outage probability are computed using Monte Carlo simulations. For each given Hk, its SVD is computed. The singular values of Hk are used to find the optimal covariance matrix Qr as the waterfilling solution (with fixed Pinfo). The null space matrix, obtained from the SVD, determines the subspace (of dimension NT -NR) in which artificial noise is produced (with power P0 -Pinfo). The average secrecy capacity is computed by averaging over various realizations
of Hk and Gk. The optimal Pinfo is found by performingan exhaustive line search.

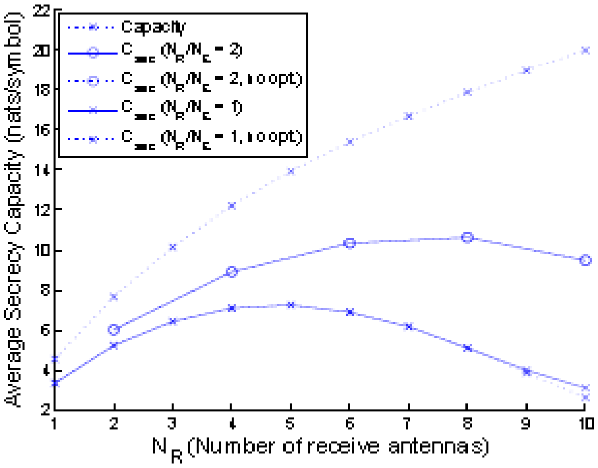

Fig. Average secrecy capacity

Figures 2 and 3 show that the average capacity of the link between the transmitter and the receiver is an upper bound on the average secrecy capacity between them. The former is independent of NE and its behavior is given by the standard results for MIMO channels [6]. The gap between capacity and secrecy capacity represents the loss in capacity because of the secrecy requirement. The loss in capacity occurs because of two reasons. Firstly, only part of the power P0 is used for the information bearing signal (Pinfo) while the rest of the power (P0 ¡ Pinfo) is used for creating artificial noise. This reduces the mutual information I(Z; S) between the information signal and the signal received by the receiver. Secondly, the amount of information that the eavesdropper gains about the information bearing signal I(Y; S) reduces secrecy capacity, based on (7). The results with no optimization are plotted using dotted lines while those with optimization are plotted using solid lines.

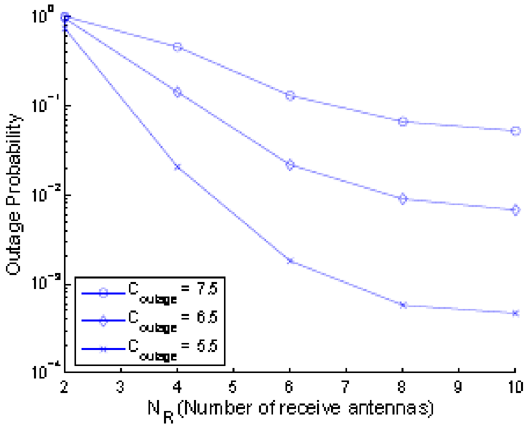

Fig: Outage Probability

Figure 4 shows the effect of the eavesdropper's distance from the transmitter, on the average secrecy capacity. The variation in eavesdropper's distance was modeled by varying the per antenna SNR at the eavesdropper P0=¾2 e , which in turn was achieved by varying ¾2 e . The per antenna SNR at the receiver was kept fixed at 10 dB and 20 dB, for two different cases. Figure 4 shows that when the eavesdropper's distance from the transmitter is much larger than that of the receiver (i.e. when the eavesdropper's SNR is low), the average secrecy capacity is close to the average capacity, as expected. As the eavesdropper comes closer to the transmitter, the average secrecy capacity reduces. However, instead of becoming arbitrarily small, it ultimately approaches a floor. Thus, even if the eavesdropper is very close to the transmitter, secret communication at non-trivial rates is possible.

VIII. Conclusion

We propose a Secure communication in the multiuser and multi-eavesdropper (MUME) scenario for the police department. Main aim is to provide security for the data passed from the police head office to sub offices or users without data leakage. The administrator is the authority who manages the system and will verify the registered user for monitoring. Users needs to register for posting complaints and check status of case Police officers can register in this site to avail features like case detail, criminal detail and case search For better and secure data transfer between the head office and sub offices, we are implementing the paper concept in messaging part of the project. The messaging part, simultaneously transmits an information-bearing signal to the intended receivers and artificial noise to confuse the eavesdroppers.

References

[1]. R. Negi, S. Goel, "Secret Communication using Noise," To appear in Proceedings VTC Fall '05, Sept. 2005.

[2]. I. Csiszar, J. Korner, "Broadcast Channels with Confidential Messages," IEEE Trans. Info. Theory, pp. 339-348, May 1978.

[3]. U. M. Maurer, "Unconditionally Secure Key Agreement and the Intrinsic Conditional Information," IEEE Trans. Info. Theory, pp. 499-514, March 1999.

[4]. A. E. Hero, "Secure Space-Time Communication," IEEE Trans. Info. Theory, pp. 3235-3249, Dec. 2003.

[5]. H. Koorapaty, A. A. Hassan, S. Chennakeshu, "Secure Information Transmission for Mobile Radio," IEEE Trans. Wireless Communications, pp. 52-55, July 2003.

[6]. G. J. Foschini, D. Chizhik, M. J. Gans, C. Papadias, R. A. Valenzuela, "Analysis and performance of some basic spacetime architectures," IEEE J. Select. Areas Commun., Special Issue on MIMO Systems, pt. I, vol. 21, pp. 303-320, Apr. 2003.

[7]. X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in Proc. IEEE ITW, Porto, Portugal, May 2008, pp. 164–168.

[8]. L. Lai and H. E.Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[9]. R. Negi and S. Goel, "Secret communications using artificial noise," in Proc. IEEE VTC, Dallas, TX, USA, Sep. 2005, pp. 1906–1910.

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

[11]. A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in Proc. IEEE ICASSP, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[12]. A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in Proc. IEEE ICASSP, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[13]. G. Geraci, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates formulti-user MIMO linear precoding," in Proc. 8th Int. Symp. on Wireless Commun. Syst. (ISWCS), Aachen, Germany, Nov. 6–9, 2011, pp. 286–290.

[14]. E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," IEEE Trans. Inf. Theory, vol.57, no. 4, pp. 2083–2114, Apr. 2011.

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

[16]. Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," in Proc. 45th Annu. Allerton Conf. Commun., Control and Computing, Monticello, IL, USA, 2007.