International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 9, September- 2014

Multi Layer Security for MIMO Wiretap System

Dency Jose
PG Scholar, Communication Engineering
Amal Jyothi College of Engineering
Kanjirappally, India

Darsana P
Assistant Professor
Amal Jyothi College of Engineering
Kanjirappally, India

***Abstract*—The broadcast nature of physical medium makes security an important concern in wireless communication. This work proposes a cross layer security approach for Gaussian multiple-input-multiple-output (MIMO) wiretap channel. Here, RSA algorithm is used along with a physical layer dependent transmitter and receiver filter design. The transmit and receive filters are designed with an objective to minimize the mean-square error (MSE) between authenticated parties, while ensuring that the eavesdropper MSE goes beyond a certain level. The power constraint is also taken into account and optimal filters are designed through the solution of convex optimization problems. The performance of zero forcing (ZF) and Wiener filters at eavesdropper receiver is analyzed for the case when legitimate receiver uses ZF filters, under degraded and non-degraded channel conditions. We also assume that the channel state information (CSI) is known to all other parties. The filter coefficients at legitimate receiver are then used to obtain the two prime numbers required for key generation at the initial stage of RSA algorithm. Performance of the system is analyzed by plotting BER vs SNR values and using numerical simulations.**

***Keywords*—MIMO, ZF filters, wiener filetr,RSA, secrecy.**

I. INTRODUCTION

Wireless communication is the fastest growing segment of the communication industry. The broadcast nature of the physical medium allows unauthorized receivers located within the transmission range to observe the signals sent by the transmitter to a legitimate receiver and intercept it. Thus the security aspect has to be given proper importance in communication systems. Here, we consider passive eavesdropping by active users of the network.

In order to ensure secure data transmission, a wide variety of methods are adopted till date. The widely developed area of private and public key cryptography is commonly used to provide computational security. [1] But, these methods are independent of the physical nature of the medium. Thus another area of research called physical layer security emerged, which exploit physical phenomena occurring at the PHY layer to enable secret communication. These techniques exploit available channel state information and use proper coding and transmit precoding schemes to ensure security.

Physical layer security for communications was first proposed by Wyner in [2]. Wyner introduced the concept of wiretap channel and assumed that eavesdropper channel is a degraded version of the main channel (i.e; main channel has a better signal-to noise ratio (SNR)) and the wiretapper knows the codebook used by the transmitter. Secrecy is achieved by using a randomized coding scheme where the information is hidden in the additional noise seen by the eavesdropper Csizar and Korner generalized Wyner's work by considering a non degraded version of the wiretap channel [3].

In [4] the authors considered a scenario of Gaussian wiretap channel, where the main and the eavesdropper channels are additive white Gaussian noise (AWGN) channels. The impact of these works was limited initially because of the difficulty in designing secrecy achieving codes for wiretap channels, with realizable encoding- decoding complexity. Also, such codes are known only in certain scenarios. For eg; Low-density parity check (LDPC) codes can be used only when the main channel is noiseless and the eavesdropper channel is a binary erasure channel. [5]

A study involving multiple antenna channels was first proposed by Hero in [6]. He showed that space-time signal processing techniques can be used to achieve secure communication for wireless links. A lot of research was also done in applying signal processing techniques to enlarge the channel quality difference between the main and the eavesdropper channels.

If the channel state information (CSI) is perfectly known at all nodes, then optimal beamforming methods can be used to achieve secrecy in [7] which are based on the general singular value decomposition (GSVD) of the main and eavesdropper channel matrices. Artificial noise schemes were later proposed by Goel and Negi [8], in which only the statistics of eavesdropper channel is known to the transmitter. But, it does not exploit the spatial multiplexing ability of MIMO systems and might lead to limited security gains.

In [9] a cross layer security scheme for MIMO STBC system has been proposed. It combines higher layer cryptographic methods with physical layer techniques to enhance security. Motivated from this work, we propose another cross layer approach to enhance security in MIMO wiretap scenario.

The transmit and receive filters are designed with an objective to minimize the mean square error (MSE) between authenticated parties. The design also takes into consideration the fact that the eavesdropper MSE should go beyond a certain level and the transmitted power is constrained. This

sets a convex optimization problem for a scenario where CSI is assumed to be known to all parties. Once the transmit and receive filters are designed, the legitimate receiver filter is used to obtain the two prime numbers required for key generation at the initial stage of RSA algorithm. Later the public key of authorized receiver is produced using these numbers and are made known to all parties in communication. The RSA encrypted data can provide an enhanced security along with physical layer dependent filter designs.

The rest of the paper is arranged as follows: section II formulates the problem. A brief introduction into the optimal filter design is given in section III. Section IV describes the proposed system. Finally simulation results are shown in section V.

II. PROBLEM STATEMENT

The wiretap scenario can generally be modelled as a scenario where Alice, the transmitter needs to communicate to an authorized receiver Bob in presence of an eavesdropper Eve. The eavesdropper is expected to be passive i.e; it just overhears the conversation without trying to interfere in it. Consider a MIMO scenario where m, n_M, n_E represents the number of antennas at transmitter, legitimate receiver and eavesdropper side. In this work we consider a 2x2 MIMO channel where m, n_M, n_E are all equal to two, as shown in Fig. 1 [10].

Let X be an m-dimensional vector of independent, transmit symbols. H_M and H_E denote the main channel and eavesdropper channel matrices. The n_m x m matrix H_M and n_E x m matrix H_E, represents the gains from the input of main and eavesdropper channels to their respective output. The m × m matrix H_T denotes the transmit filter of Alice.

The signal passing through the channel is also affected by the Gaussian noise present in the channel. The noise present in the main and eavesdropper channels are modelled as N_M and N_E, which are n_m and n_E dimensional Gaussian random vectors with identity covariance matrix and zero mean. Thus Bob and Eve observe their input signal as a combination of channel and filter matrices along with the noise present in the system.

Thus the receive symbols can be represented as n_m and n_E dimensional vectors Y_M and Y_E. The received signals at the input of Bob and Eve is given by,

$$Y_M = H_M H_T X + N_M \quad (1)$$

$$Y_E = H_E H_T X + N_E \quad (2)$$

The input symbol vector is estimated by Bob and Eve as,

$$\hat{X}_M = H_{RM} Y_M \quad (3)$$

$$\hat{X}_E = H_{RE} Y_E \quad (4)$$

where the m ×n_m matrix H_{RM} and the m xn_E matrix H_{RE} represents the corresponding receive filters of Bob and Eve.

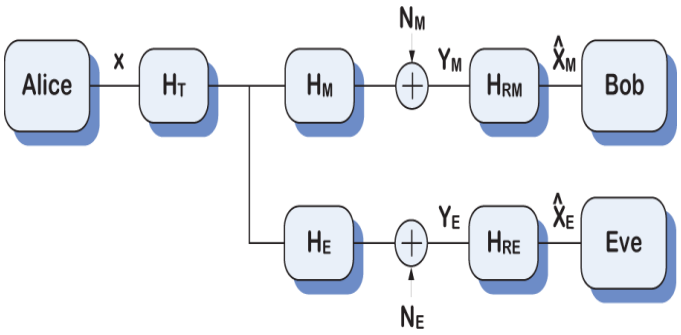

Fig. 1 A Model for MIMO Gaussian Wiretap Channel

Our objective is to minimize the MSE between transmitter and authorized receiver keeping the MSE between transmitter and eavesdropper above a certain threshold. We also consider a power constraint that the transmitted power should be less than or equal to the average power (P_{avg}). Thus this can be modelled as an optimization problem where the objective function is written as:

$$\min MSE_M = \varepsilon[||X - \hat{X}_M||^2] \quad (5)$$

subject to the security constraint:

$$\min MSE_E = \varepsilon\left[\left||X - \hat{X}_E\right|\right|^2] \geq \gamma \quad (6)$$

and to the total power constraint:

$$\mathrm{tr}(H_T H_T^{\dagger}) \leq P_{avg} \quad (7)$$

where $\varepsilon(.)$ represents the expectation operator and $(.)^{\dagger}$ represents the hermitian transpose. Here, as all the matrices are real, hermitian transpose equals to simple transpose.

III. OPTIMAL FILTER DESIGN

The filters are designed for two different scenarios. In scenario one, we assume that the legitimate receiver and eavesdropper use zero forcing filters (ZF). In the second scenario, the eavesdropper is assumed to use a wiener filter while the legitimate receiver uses zero forcing filter itself.

Scenario 1: When both receivers use ZF filters.

In this scenario, the ZF constraints are satisfied and are given by:

$$H_{RM} H_M H_T = I \quad (8)$$

$$H_{RE} H_E H_T = I \quad (9)$$

Thus the receive filters at Bob and Eve are designed as:

$$H_{RM}^{*} = (H_T^{\dagger} H_M^{\dagger} H_M H_T)^{-1} H_T^{\dagger} H_M^{\dagger} \quad (10)$$

$$H_{RE}^{*} = (H_T^{\dagger} H_E^{\dagger} H_E H_T)^{-1} H_T^{\dagger} H_E^{\dagger} \quad (11)$$

Thus the main channel and eavesdropper channel MSEs are given by:

$$\mathrm{MSE}_M = \varepsilon\left[\left||X - H_{RM} Y_M\right|\right|^2] = \mathrm{tr}\{(H_T^{\dagger} H_M^{\dagger} H_M H_T)^{-1}\} \quad (12)$$

$$\mathrm{MSE}_E = \varepsilon\left[\left||X - H_{RE} Y_E\right|\right|^2] = \mathrm{tr}\{(H_T^{\dagger} H_E^{\dagger} H_E H_T)^{-1}\} \quad (13)$$

Thus the optimization problem takes a new form as:

$$\min H_T \text{ in } \mathrm{tr}\{(H_T^{\dagger} H_M^{\dagger} H_M H_T)^{-1}\} \quad (14)$$

subject to the constraints:

$$\mathrm{tr}\{(H_T^{\dagger} H_E^{\dagger} H_E H_T)^{-1}\} \geq \gamma \quad (15)$$

and

$$\mathrm{tr}(H_T H_T^{\dagger}) \leq P_{avg} \quad (16)$$

also, $H_T H_T^{\dagger} \succ 0$.

The solution of this problem can be solved by using KKT optimality conditions. The solution of this problem and filter performance is analyzed in [10].

Scenario 2: When legitimate receiver uses ZF filter and eavesdropper uses wiener filter.

The receive filter at Eve is given by:

$$H_{RE}^{*} = H_T^{\dagger} H_E^{\dagger} \ (I + H_E H_T H_T^{\dagger} H_E^{\dagger})^{-1} \qquad (16)$$

Thus another optimization problem is set, similar to (14)-(16). The solution of that optimization problem and the transmit filter design are given in [10].

We have incorporated the common cryptographic procedures along with this physical layer dependent filter designs to increase the overall security of the system.

IV. PROPOSED SYSTEM

A cross layer security scheme for 2 x 2 narrow band MIMO wiretap system is designed with an assumption that perfect channel knowledge is available at all network nodes. As the first step the MSE threshold is chosen transmit filter designed based on design procedures specified in section III. The receiver filter is then designed using transmit filter knowledge. The receive filter coefficients at legitimate receiver is then used to generate the two prime numbers required at the initial stage of RSA cryptographic algorithm.

The input message from Alice consists of a long string of characters. They are converted to their corresponding ASCII code which is required for RSA encryption. This message sequence is then encrypted using public key of Bob available to all network users. The cipher text has to be converted to a format, suitable for transmission through a MIMO channel. Appropriate message reshaping is done and messages are converted to bits required for transmission through the channel.

The symbol vector is modulated using QPSK modulation scheme. The modulated vector is of the form of a 2 X 1 vector. The transmit vector is first transmitted through the transmitter filter before passing through the communication channel. The signal reaching the receiver side has a combined effect of transmit filter, transmission channel and the noise added to the symbol while transmission. The received signal is first passed through the corresponding receive filter. These symbols are demodulated and bit error rate (BER) is calculated. From bit format, the symbols are first converted to ASCII format and then to the original message format. These steps are summarized in Fig 2.

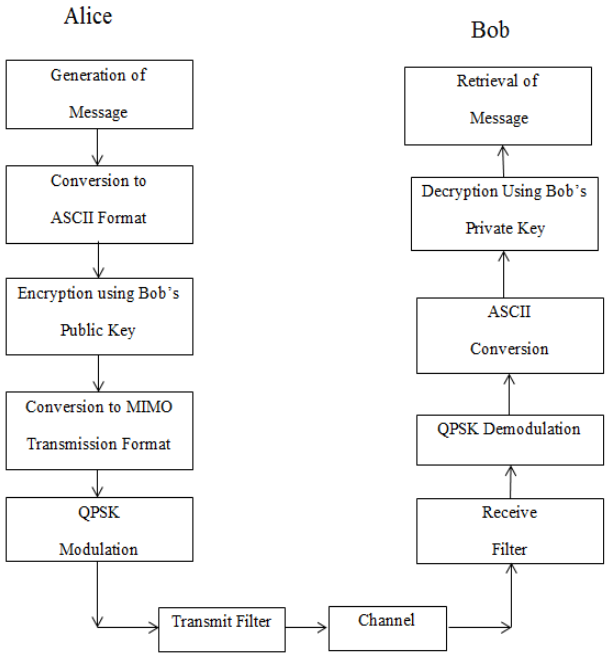

Fig 2. The proposed method

V. SIMULATON RESULTS

The performance of the proposed system are analyzed using SNR vs. BER curve. Simulations were performed in MATLAB. The results are shown in Figures 3, 4 and 5.

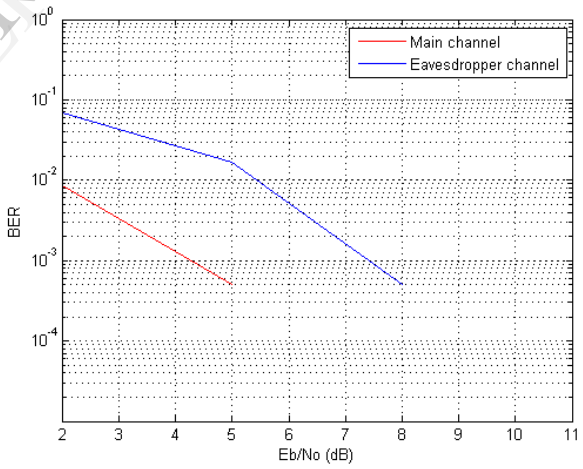

Fig 3. BER Vs SNR plot when legitimate receiver uses ZF filter and eavesdropper uses wiener filter in a degraded scenario.

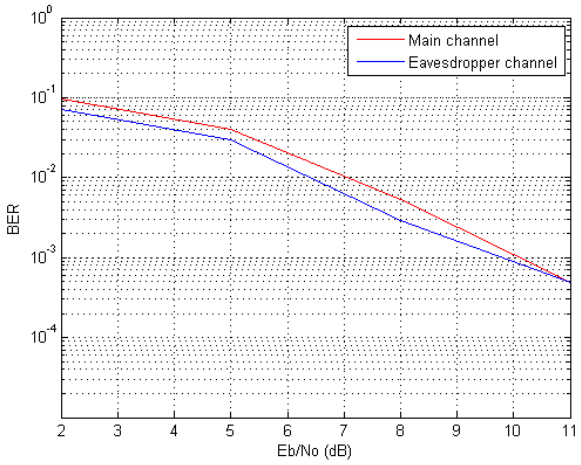

Fig 4. BER Vs SNR plot when legitimate receiver uses ZF filter and eavesdropper uses wiener filter in a non degraded scenario.

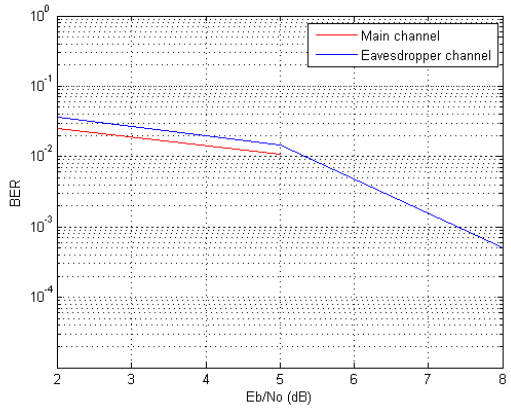

Fig 5. BER Vs SNR plot for main and eavesdropper channels when ZF filters at both receivers in non degraded scenario

It can be seen that the BER of eavesdropper channel is always greater than that of main channel, when eavesdropper channel is degraded with respect to main channel. Although the BER of main channel is higher than that of eavesdropper in a non- degraded scenario, the transmit and receive filters considerably reduce the BER at higher values of SNR. In such a scenario RSA algorithm provides an additional layer of security as the legitimate receiver can only decode the encrypted message. The BER Vs SNR values of various scenarios are described in Tables 1 and 2.

TABLE 1: MSE VS BER FOR SCENARIO 1

Main receiver uses-ZF filter and Evasdropper uses Wiener Filter $\gamma = 1.2$					
Degraded Channel			Non-Degraded Channel		
SNR	Main Channel	Eavesdropper Channel	SNR	Main Channel	Eavesdropper Channel
2	0.0086	0.0683	2	0.0979	0.0703
5	0.0005	0.0167	5	0.0402	0.0296
8	0	0.0005	8	0.0053	0.0029
11	0	0	11	0.0005	0.0005

TABLE 2: MSE VS BER FOR SCENARIO 2

Both receiver uses ZF filter ($\gamma = 1.5$)		
SNR	Main Channel	Eavesdropper Channel
2	0.0142	0.0263
5	0.0071	0.0086
8	0	0

CONCLUSION

A cross layer security system is designed for a 2 X 2 narrow band MIMO wiretap channel. The transmit and receive filters are designed from an estimation theoretic point of view and is dependent on the physical nature of the medium. This design minimizes the MSE between the transmitter and legitimate receiver and ensures that the MSE of the eavesdropper remains above a threshold. The transmit filter is designed on the assumption that it knows the type of filter used at the receiver sides. The implementation of RSA algorithm along with this design provides an additional layer of security. The simulation results show the BER vs SNR graphs and validate the study done.

REFERENCES

[1] William Stallings ``Cryptography and Network Security, Principles and Practice", Fifth edition, PEARSON Education.
[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, no. 3, pp. 339-349, May 1978.
[4] S. K. Leung-Yan-Cheong and M. E. Hellman ``The Gaussian Wiretap Channel", IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451-456, Jul. 1978.
[5] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin ``Applications of LDPC Codes to the Wiretap Channel", IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933-2945, Aug. 2007.
[6] A. Hero ``Secure Space-Time Communication", IEEE Trans. Inf. Theory, vol. 49, no. 12, pp. 3235-3249, Dec. 2003.
[7] A. Khisti,G. Wornell ``Secure Transmission with Multiple Antennas-Part II: The MIMOME Wiretap Channel," IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.
[8] S. Goel , R. Negi ``Guaranteeing Secrecy using Artificial Noise," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, Jun. 2008.
[9] HongWen, Guang Gong, Shi-Chao Lv, Pin-Han Ho ``Framework for MIMO Cross Layer Secure Communication Based on STBC," Springer Science+Business Media, Telecommun Syst (2013) 52, pp. 2177-2185.
[10] Hugo Reboredo, Joao Xavier and Miguel R. D. Rodrigues ``Filter Design with Secrecy Constraints: The MIMO Gaussian Wiretap Channel", IEEE Trans. on Signal Processing, vol. 61, no. 15, August 2013.