RESEARCH ARTICLE OPEN ACCESS

Secure Communication in Low Snr Regime Over Fading Channels in Mimo

K. Rajesh*, K. V. Lalitha Bhavani**
*M.Tech (Digital Electronics And Communication Systems) Student, AITAM College, Tekkali in India.
**Associate Professor in ECE Department, AITAM College, Tekkali in India.

ABSTRACT
In this work we consider MIMO fading channels and characterize the reliability function in the low-SNR regime as a function of the number of transmit and receive antennas. For the case when the fading matrix H has independent entries, we show that the number of transmit antennas plays a key role in reducing the peakiness in the input signal required to achive the optimal error exponent for a given communication rate. Further by considering a correlated channel model, we show that the maximum performance gain is achieved when the entries of the channel fading matrix are fully correlated. The results we presented in this work in the low- SNR regime can also be applied to the finite bandwidth regime.
Keywords: MIMO, Bandwidth Allocation, Fading, Low SNR

I. INTRODUCTION

The use of multiple antennas at the transmitter and receiver in wireless systems, popularly known as MIMO (multiple-input multiple-output) technology, has rapidly gained in popularity over the past decade due to its powerful performance-enhancing capabilities. Communication in wireless channels is impaired predominantly by multi-path fading. Multi-path is the arrival of the transmitted signal at an intended receiver through differing angles and/or differing time delays and/or differing frequency (i.e., Doppler) shifts due to the scattering of electromagnetic waves in the environment. Consequently, the received signal power fluctuates in space (due to angle spread) and/or frequency (due to delay spread) and/or time (due to Doppler spread) through the random superposition of the impinging multi-path components. This random fluctuation in signal level, known as fading, can severely affect the quality and reliability of wireless communication. Additionally, the constraints posed by limited power and scarce frequency bandwidth make the task of designing high data rate, high reliability wireless communication systems extremely challenging.

MIMO technology constitutes a breakthrough in wireless communication system design. The technology offers a number of benefits that help meet the challenges posed by both the impairments in the wireless channel as well as resource constraints. In addition to the time and frequency dimensions that are exploited in conventional single-antenna (single-input single-output) wireless systems, the leverages of MIMO are realized by exploiting the spatial dimension (Provided by the multiple antennas at the transmitter and the receiver).

The advantages of multiple-input multiple-output (MIMO) systems have been widely acknowledged, to the extent that certain transmit diversity methods (i.e., Alamouti signaling) have been incorporated into wireless standards. Although transmit diversity is clearly advantageous on a cellular base station, it may not be practical for other scenarios. Specifically, due to size, cost, or hardware limitations, a wireless agent may not be able to support multiple transmit antennas. Examples include most handsets (size) or the nodes in a wireless sensor network (size, power).

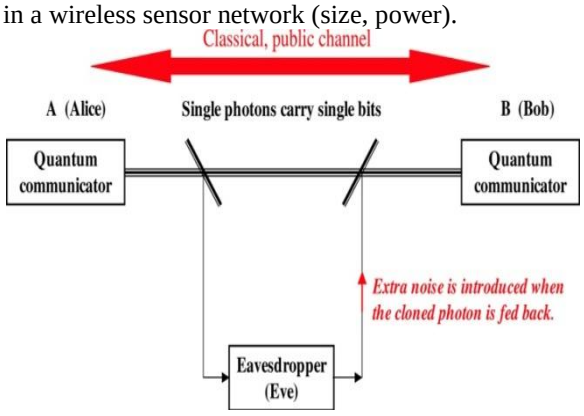

Fig.1:secure communication system

We consider the secure transmission of information over an ergodic fading channel in the presence of an eavesdropper. Our eavesdropper can be viewed as the wireless counterpart of Wyner's wire tapper. The secrecy capacity of such a system is characterized under the assumption of asymptotically long coherence intervals. We first consider the full channel state information (CSI)

case, where the transmitter has access to the channel gains of the legitimate receiver and the eavesdropper. The secrecy capacity under this full CSI assumption serves as an upper bound for the secrecy capacity when only the CSI of the legitimate receiver is known at the transmitter, which is characterized next. In each scenario, the perfect secrecy capacity is obtained along with the optimal power and rate allocation strategies. We then propose a low-complexity on/off power allocation strategy that achieves near-optimal performance with only the main channel CSI. More specifically, this scheme is shown to be asymptotically optimal as the average signal-to-noise ratio (SNR) goes to infinity, and interestingly, is shown to attain the secrecy capacity under the full CSI assumption. Overall, channel fading has a positive impact on the secrecy capacity and rate adaptation, based on the main channel CSI, is critical in facilitating secure communications over slow fading channels.

II. CHANNEL MODEL

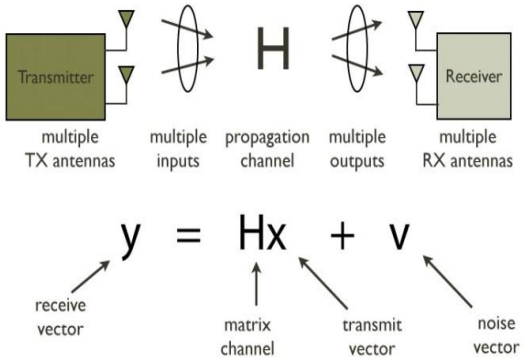

Fig.2.Channel Model

MIMO is the use of multiple antennas at both the transmitter and receiver to improve communication performance. It is one of several forms of smart antenna technology. Note that the terms input and output refer to the radio channel carrying the signal, not to the devices having antennas. New techniques, which account for the extra spatial dimension, have been adopted to realize these gains in new and previously existing systems.

MIMO technology has attracted attention in wireless communications, because it offers significant increases in data throughput and link range without additional bandwidth or increased transmit power. The use of multiple dimensions at both ends of a communication link offers significant improvements in terms of spectral efficiency and link reliability.

We consider a MIMO channel model and assume that the transmitter, legitimate receiver, and eavesdropper are equipped with *nT* , *nR*, and *nE* antennas, respectively. We further assume that the channel input-output relations between the transmitter and legitimate receiver, and the transmitter and eavesdropper are given by

$y_m = H_m x + n_m$, $y_e = H_e x + n_e$,

where, **x** denotes the *nT* ×1–dimensional transmitted signal vector. *nR*×1–dimensional $\mathbf{y}_m$ and *nE* ×1–dimensional $\mathbf{y}_e$ represent the received signal vectors at the legitimate receiver and eavesdropper, respectively. Moreover, $\mathbf{n}_m$ with dimension *nR*×1 and $\mathbf{n}_e$ with dimension *nE* × 1 are independent, zero-mean Gaussian random vectors. The signal-to-noise ratio is defined as,

$$SNR = \frac{P}{n_R N_m}$$

the channel models, H_m is the *nR* × *nT* – dimensional channel matrix between the transmitter and legitimate receiver, and H_e is the *nE* × *nT* – dimensional channel matrix between the transmitter and eavesdropper.

III. SECRECY IN THE LOW-SNR REGIME

The channel matrices H_m and H_e are fixed for the entire transmission period and are known to all three terminals. The assumption of perfect channel knowledge can be justified in scenarios in which a base station, which knows the channels of the users, attempt to transmit confidential messages to a user and hence treat the other users as eavesdroppers.

In this paper, we concentrate on the low-SNR regime. In this regime, the behavior of the secrecy capacity can be accurately predicted by its first and second derivatives with respect to SNR at SNR = 0:

$$C_S(SNR) = \dot{C}_S(0)SNR + \frac{\ddot{C}(0)}{2}SNR^2 + o(SNR^2)$$

$$\frac{E_b}{N_{0\cdot s,\min}} = \frac{\log 2}{\dot{C}_S(0)}$$

$$S_0 = \frac{2\left[\dot{C}_S(0)\right]^2}{-\ddot{C}_S(0)}$$

N_0 *s*, min denotes the minimum bit energy required for reliable communication under secrecy constraints (or equivalently minimum energy per secret bit), and S_0 denotes the wideband slope which is the slope of the secrecy capacity in bits/dimension/(3 dB) at the point $E_b/N_{0\ s,\min}$.

3.1.1 FIRST AND SECOND DERIVATIVES OF THE SECRECY CAPACITY

We determine the first and second derivatives of the secrecy capacity at SNR = 0, and provide a second-order approximation to the MIMO secrecy capacity in the low-SNR regime. Through this analysis, we quantify the impact of

secrecy constraints on the performance. We identify the optimal transmission strategies in the low-SNR regime. In particular, we determine that transmission in the maximal-eigenvalue eigenspace of a certain matrix that depends on the channel matrices is second-order optimal. In the case in which the maximum eigenvalue is distinct, beamforming is shown to be optimal.

Secrecy rate expression given by

$$I_S(SNR) = \frac{1}{n_R}\left[\log\det\left(I + \frac{1}{N_m}H_m K_x H_m^{+}\right) - \log\det\left(I + \frac{1}{N_e}H_e K_x H_e^{+}\right)\right]$$

The first derivative of the secrecy capacity in with respect to SNR at SNR = 0.

$$\dot{C}_S(0) = [\lambda_{\max}(\phi)]^{+} = \begin{matrix}\lambda_{\max}(\phi) \ if\ \lambda_{\max}(\phi) > 0 \\ 0 \ else\end{matrix}$$

In the absence of secrecy constraints, the first and second derivatives of the MIMO capacity at SNR = 0.

$$\dot{C}_S(0) = \left[\lambda_{\max}(H_m^{+}H_m)\right]$$

and $\ddot{C}(0) = -\frac{n_R}{l}\lambda^2_{\max}(H_m^{+}H_m)$

Where, l is the multiplicity of $\lambda_{\max}(H_m^{+}H_m)$

Hence, the first and second derivatives are achieved by transmitting in the maximal-eigenvalue eigenspace of $H^{\dagger}{}_m H_m$, the subspace in which the transmitter-receiver channel is the strongest.

If there are secrecy constraints, we should at low SNRs transmit in the direction in which the transmitter-receiver channel is strongest with respect to the transmitter-eavesdropper channel normalized by the ratio of the noise variances.

3.1.2. MINIMUM ENERGY PER SECRET BIT

In this section, we study the energy required to send information both reliably and securely. In particular, we investigate the minimum energy required to send one secret bit. Before identifying the minimum energy per secret bit, we first show that the secrecy capacity is concave in SNR. The secrecy capacity C_s achieved under the average power constraint $E\{||x||^2\} \le P$ is a concave function of SNR.

The energy per secret bit normalized by the noise variance at the legitimate receiver is defined as

$$\frac{E_b}{N_0} = \frac{SNR}{C_S(SNR)}\log 2$$

$$\frac{E_b}{N_0} = \lim_{SNR \to 0}\frac{SNR}{C_S(SNR)}\log 2 = \frac{\log 2}{\dot{C}_S(0)}$$

The minimum bit energy in the absence of secrecy constraints, the minimum bit energy per secret bit is calculated. Secrecy constraints lead to an increase if the minimum energy requirements. We also note that the energy cost of secrecy increases as secrecy rates increase.

We plot the secrecy rates in bits/s/Hz/dimension as a function of the energy per secret bit under the same assumptions and channel model. We see, as predicted, that the minimum bit energy is attained in all cases as SNR and hence rates approach zero. While the minimum bit energy is Eb/N_0=-6.01dB in the absence of secrecy constraints, the minimum bit energy per secret bit is $Eb/N_{0\ s,min}$=-3.71Db.

IV. THE IMPACT OF FADING

Assume that the channel matrices H*m* and H*e* are random matrices, whose components are stationary and ergodic random variables, modeling fading in wireless transmissions. We again assume that realizations of these matrices are perfectly known by all the terminals. As discussed fading channel can be regarded as a set of parallel sub channels each of which corresponds to a particular fading realization. Hence, in each sub channel, the channel matrices are fixed similarly as in the channel model considered in the previous section. It is shown that having independent inputs for each sub channel is optimal and the secrecy capacity of the set of parallel sub channels is equal to the sum of the capacities of sub channels. Therefore, the secrecy capacity of fading channels can be found by averaging the secrecy capacities attained for different fading realizations.

We assume that the transmitter is subject to a short-term power constraint. Hence, for each channel realization, the same amount of power is used and we have tr (Kx) ≤ P. With this assumption, the transmitter is allowed to perform power adaptation in space across the antennas, but not across time. Under such constraints, it can easily be seen from the above discussion that the average secrecy capacity in fading channels is given by

$$C_s = \frac{1}{nR}EH_m, H_e\left\{\begin{matrix}max \\ K_{x\ge 0} \\ tr(K_x \le P)\end{matrix}\log\det\left(I + \frac{1}{N_m}H_m K_x H_m^{+}\right) - \log det\left(I + \frac{1}{N_e}H_e K_x H_e^{+}\right)\right\}$$

The first derivative of the average secrecy capacity with respect to SNR = $P/n_R N_m$ at SNR = 0

$$\dot{C}_s(0) = \mathbb{E}_{\mathbf{H}_m,\mathbf{H}_e}\{[\lambda_{\max}(\mathbf{\Phi})]^{+}\}$$

The second derivative of the average secrecy capacity at SNR = 0 is given by

$$\ddot{C}_s(0) = -n_R\mathbb{E}_{\mathbf{H}_m,\mathbf{H}_e}\left\{\min_{\substack{\{\alpha_i\} \\ \alpha_i\in[0,1]\ \forall i \\ \sum_{i=1}^{l}\alpha_i=1}}\sum_{i,j=1}^{l}\alpha_i\alpha_j\left(|\mathbf{u}_j^{\dagger}\mathbf{H}_m^{\dagger}\mathbf{H}_m\mathbf{u}_i|^2 - \frac{N_m^2}{N_e^2}|\mathbf{u}_j^{\dagger}\mathbf{H}_e^{\dagger}\mathbf{H}_e\mathbf{u}_i|^2\right)1\{\lambda_{\max}(\Phi)>0\}\right\}$$

Above, we have assumed that the fading coefficients h_m and h_e are independent. Next, we demonstrate that the gains are still observed even if the channel coefficients are correlated. We again

assume that hm and he are zero-mean, circularly symmetric Gaussian random variables with $E\{|h_m|^2\} = E\{|h_e|^2\} = 1$. Let us denote $z_m = |h_m|^2$ and $z_e = |h_e|^2$. Using the bivariate Rayleigh probability density function given in, we can easily obtain the bivariate exponential density as

The minimum energy per secret bit is plotted as a function of the correlation coefficient ρ. When $\rho = 0$ and hence the channel coefficients are independent, we

$$\frac{E_b}{N_{0\,s,min}} = \frac{\log 2}{\left[\frac{N_e}{N_m + N_e}\right]} = 1.419dB$$

As the correlation increases, the minimum bit energy value increases. However, note that the bit energy values are finite unless there is full correlation. Note further that if there were no fading, we would have

$$\frac{E_b}{N_{0\,s,min}} = \frac{\log 2}{\left[1 - \frac{N_m}{N_e}\right]^+} = inf$$

The minimum energy per secret bit, which is attained as SNR vanishes, are discussed. In general, fading is beneficial in terms of energy efficiency at nonzero SNR levels as well. This is demonstrated. In this figure, we plot the secrecy capacity when $n_T = 1$, $n_R = 5$, and $n_E = 3$. We consider two scenarios: no fading and i.i.d. Rayleigh fading. In the case in which there is no fading, we assume that the channel coefficients are all equal to 1. In the fading scenario, we assume that the channel vectors hm and he consist of independent and identically distributed, zero-mean Gaussian components each with unit variance, i.e., $E\{|h_{m,i}|^2\} = 1$ and $E\{|h_{e,i}|^2\} = 1$ for all i. We additionally assume that hm and he are independent of each other. Note that under these assumptions, $||h_m||^2$ and $||he||^2$ are independent chi-square random variables with $2n_R$ and $2n_E$ degrees of freedom, respectively. In Fig. 4, we observe that better performance is achieved in the presence of fading. Indeed, energy gains tend to increase at higher values of secrecy capacity. For instance, when C_s = 0.14 bits/s/Hz/dimension, we have a gain of approximately 8 dB in $Eb/N_{0\,s}$. Note that this is a substantial improvement in energy efficiency

4.1 SIMULATION RESULTS

The two critical issues of security and energy-efficiency jointly, we study the secrecy capacity in the low-SNR regime. The operation at low SNRs, in addition to improving the energy efficiency, is beneficial from a security perspective as well. In the low-SNR regime, either the transmission power is small or the bandwidth is large. In either case, we have low probability of intercept as it is generally difficult for an eavesdropper to detect the signals in this regime.

We consider a general multiple-input and multiple-output (MIMO) channel model and identify the optimal transmission strategies in the low-SNR regime under secrecy constraints. Since secrecy capacity is in general smaller than the capacity attained in the absence of confidentiality concerns. Energy per bit requirements increase due to security constraints.

This work, quantify these increased energy costs and address the tradeoff between secrecy and energy efficiency. The fundamental benchmarks with which the performance of practical systems can be compared, and to obtain design guidelines for energy-efficient and secure communication.

Observation 1: When nT=3,nR=3,nE=3; Here the Fig.3. shows that secrecy rates comparison with reference to signal to noise ratio.

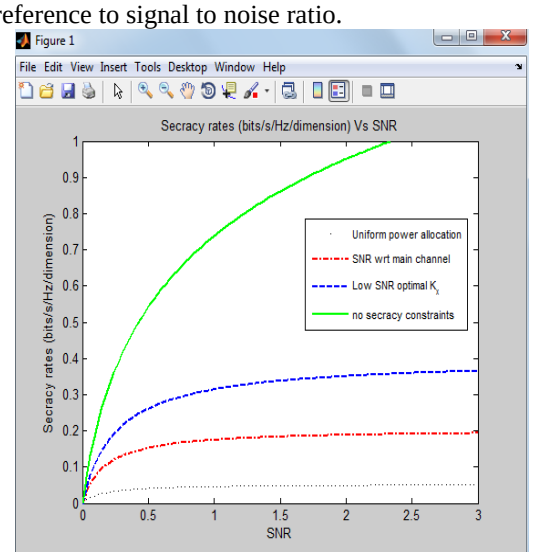

Fig.3: Secrecy rates in nats/s/Hz/dimension vs. SNR.

Observation 2: Where power allocation at low SNR condition; Here the Fig.4. shows secrecy rates comparison with reference to energy per secret bit and also power allocation scheme in a network.

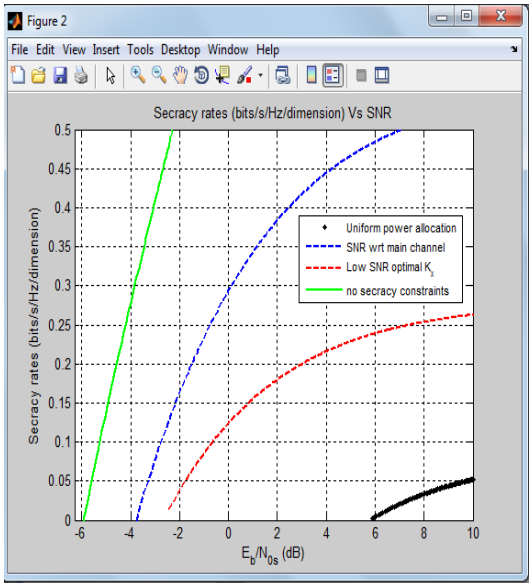

Fig.4: Secrecy rates in bits/s/Hz/dimension vs. energy per secret bit

Observation 3: Minimum energy per bit Vs correlation coefficient; Here the Fig.5. shows that minimum energy calculation with reference to correlation coefficient and the energy levels depends on correlation coefficient.

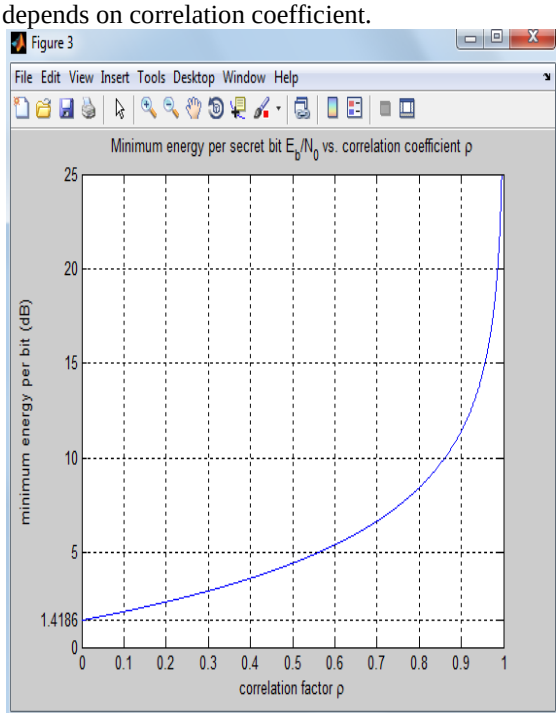

Fig. 5. Minimum energy per secret bit $E_b/N_{0\ min}$s vs. correlation coefficient □

Observation 4: When nT=1,nR=5,nE=3; Comparison of different fading channels with no fading; Here the Fig.6. shows that comparison of different fading channels and no fading condition in a network.

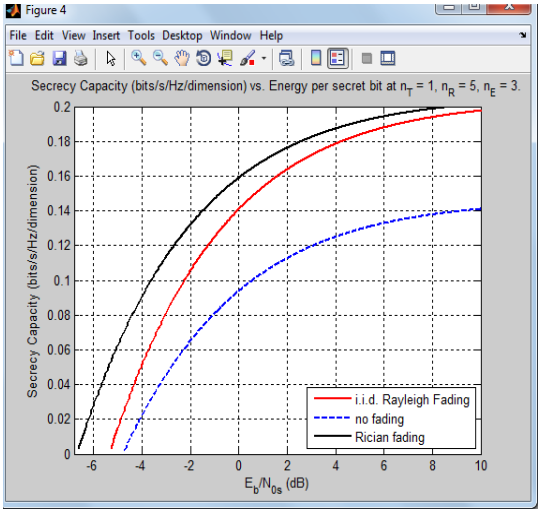

Fig.6: Comparison of different fading channels with no fading channel

V. CONCLUSION

In this paper, we investigated the tradeoff between communication rate and average probability of decoding error for a non-coherent multiple antenna fading in a low-SNR regime. We started with the assumption that the fading matrix H has i.i.d.entries. In this regime, we showed that using M transmit antennas and N receive antennas allow us to realized a performance gain of N and peakiness gain M. When both the average and peak power are constrained, having large M can improve both the channel capacity and the low-SNR reliability function. In the low-SNR regime, channel correlation can actually improve the channel performance. In the extreme case where the fading is fully correlated, in the sense that the entries of the fading matrix H are either identical or differ by a phase shift, we can achieve a performance gain of M N. Thus, the advantage of having multiple antennas is best realized when we have fully correlated fading channels. This suggests that the antennas should be placed close together in the low-SNR regime.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1367, Oct. 1975

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, July 1978.

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

[4] Special issue on information-theoretic security, *IEEE Trans. Inf. Theory*, vol. 54, no. 6, June 2008.

[5] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, pp. 3235–3249, Dec. 2003.
[6] Z. Li, W. Trappe, and R. D. Yates, "Secret communication via multiantenna transmission," *2007 Conf. Inf. Sciences Syst.*.
[7] S. Shafiee, N. Liu, 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, Sep. 2009.
[8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.
[9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO Wiretap channel." Available: http://arxiv.org/abs/0710.1920.
[10] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2547–2553, June 2009.
[11] S. Verdú, "Spectral efficiency in the wideband regime," *IEEE Trans. Inf. Theory*, vol. 48, pp. 1319–1343, June 2002.
[12] D. P. Palomar and S. Verdú, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 52, pp. 141– 154, Jan. 2006.
[13] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470–2492, June 2008.
[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, June 2008.
[15] 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.
[16] M. El-Halabi, T. Liu, and C. Georghiades, "On secrecy capacity per unit cost," in *Proc. 2009 IEEE Internation Symp. Inf. Theory*, pp. 2301–2305.
[17] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1999.
[18] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
[19] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*. Wiley-Interscience, 2005.

K.Rajesh Obtained B.Tech degree from D.M.S.S.V.H.College of Engineering at Matchilipatnam in Andhrapradesh under Acharya Nagarjuna University Guntur in INDIA and M.Tech student in AITAM College Tekkali in Srikakulam district Under JNTU Kakinada in India. His area of interest is Communication Systems.

Smt K.V.Lalitha Bhavani, Received the B.E(ECE) from GITAM College of Engineering at Visakapatnam in Andhrapradesh Under Andhra University Visakapatnam in India and M.TECH (VLSI system design) from AITAM college Tekkali in Srikakulam district Under JNTU Kakinada in India.She is an Associate Professor in the Department of ECE, AITAM College Tekkali in India. Areas of interest are Communication systems signal and image processing.