ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

An Efficient SNR Estimation Scheme For Secure Communication Over Fading Channel

A.Leelavathi[1], P.Venkata Lakshmi[2], K.Madhavi[3]

Senior Asst. Professor, Department of ECE, DIET, Anakapalli, A.P., India[1]

Department of ECE, DIET, Anakapalli, A.P., India[2]

Asst. Professor, Department of ECE, DIET, Anakapalli, A.P., India[3]

Abstract: Secure transmission of confidential messages is a critical issue in communication systems and especially in wireless systems due to the broadcast nature of wireless transmissions.In order to address the two critical issues of security and energy-efficiency jointly, we study the secrecy capacity in the low-SNR regime. It is worthwhile to note that operation at low SNRs, in addition to improving the energy efficiency, is beneficial from a security perspective as well.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. It is very important to estimate the signal to noise ratio (SNR) of received signal and to transmit the signal effectively for the modern communication system. The performance of existing non-data-aided (NDA) SNR estimation methods are substantially degraded for high level modulation scheme such as M-ary amplitude and phase shift keying (APSK) or quadrature amplitude modulation (QAM).As an Extension we propose a SNR estimation method which uses zero point auto-correlation of received signal per block and auto/cross- correlation of decision feedback signal. Finally, the impact of fading is investigated, and the benefits of fading in terms of energy efficiency are shown.

Keywords: Secrecy capacity, QAM, SNR, MIMO

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., Alamoutisignaling) 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).

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. In this work, we quantify these increased energy costs and address the tradeoff between secrecy and energy efficiency. It should also be noted that since practical codes for the MIMO wiretap channel have not been identified yet, the results presented in this paper represent the ultimate limits and are mostly of theoretical interest.

Expressions for the first and second derivatives of the secrecy capacity with respect to SNR at SNR = 0 are derived. Transmission strategies required to achieve these derivatives are identified. Energy efficiency is analyzed by finding the minimum bit energy required for secure and reliable communications, and the wideband slope. Increased bit energy requirements under secrecy constraints are quantified. Finally, the impact of fading is

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

investigated, and the benefits of fading in terms of energy efficiency are shown.

II. LITERATURE SURVEY ON THE EXISTING SYSTEM

In the existing system, the transmission security from an information-theoretic point of view, and identified the rate equivocation region and established the secrecy capacity of the discrete memoryless wiretap channel in which the wiretapper receives a degraded version of the signal observed by the legitimate receiver. The secrecy capacity for the most general case in which arbitrary numbers of antennas are present at each terminal has been established. For unfaded and fading Gaussian channels subject to average input power constraints, energy efficiency improves as one operates at lower SNR levels, and the minimum bit energy is achieved as SNR vanishes. In [2] considers a general linear vector Gaussian channel with arbitrary signaling and pursues two closely related goals: i) closed-form expressions for the gradient of the mutual information with respect to arbitrary parameters of the system, and ii) fundamental connections between information theory and estimation theory. Generalizing the fundamental relationship recently unveiled by Guo, Shamai, and Verdu´ we show that the gradient of the mutual information with respect to the channel matrix is equal to the product of the channel matrix and the error covariance matrix of the best estimate of the input given the output. Gradients and derivatives with respect to other parameters are then found via the differentiation chain rule.

The fading broadcast channel with confidential messages (BCC) is investigated in [3], where a source node has common information for two receivers (receivers 1 and 2), and has confidential information intended only for receiver 1. The confidential information needs to be kept as secret as possible from receiver 2. The broadcast channel from the source node to receivers 1 and 2 is corrupted by multiplicative fading gain coefficients in addition to additive Gaussian noise terms. The channel state information (CSI) is assumed to be known at both the transmitter and the receivers. The parallel BCC with independent sub channels is first studied, which serves as an information-theoretic model for the fading BCC. The secrecy capacity region of the parallel BCC is established, which gives the secrecy capacity region of the parallel BCC with degraded sub channels. The secrecy capacity region is then established for the parallel Gaussian BCC, and the optimal source power allocations that achieve the boundary of the secrecy capacity region are derived. In particular, the secrecy capacity region is established for the basic Gaussian BCC. The secrecy capacity results are then applied to study the fading BCC. The ergodic performance is first studied. The ergodic secrecy capacity region and the optimal power allocations that achieve the boundary of this region are derived. The outage performance is then studied, where a long-term power constraint is assumed. The power allocation is derived that minimizes the outage probability where either the target rate of the common message or the target rate of the confidential message is not achieved. The power allocation is also derived that minimizes the outage probability where the target rate of the confidential message is not achieved subject to the constraint that the target rate of the common message must be achieved for all channel states. In [4] considers the transmission of confidential data over wireless channels. Based on an information-theoretic formulation of the problem, in which two legitimates partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi-static fading channel, the important role of fading is characterized in terms of average secure communication rates and outage probability. Based on the insights from this analysis, a practical secure communication protocol is developed, which uses a four-step procedure to ensure wireless information-theoretic security: (i) common randomness via opportunistic transmission, (ii) message reconciliation, (iii) common key generation via privacy amplification, and (iv) message protection with a secret key. A reconciliation procedure based on multilevel coding and optimized low-density parity-check (LDPC) codes is introduced, which allows to achieve communication rates close to the fundamental security limits in several relevant instances. Finally, a set of metrics for assessing average secure key generation rates is established, and it is shown that the protocol is effective in secure key renewal-even in the presence of imperfect channel state information.

We consider the secure transmission of information over an ergodic fading channel in the presence of an eavesdropper [5]. Our eavesdropper can be viewed as the wireless counterpart of Wyner's wiretapper. 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.

III. FADING CHANNELS

A. *All Rayleigh fading*

Rayleigh fading is a statistical model for the effect of a propagation environment on a radio signal, such as that used by wireless devices.Rayleigh fading models assume

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

that the magnitude of a signal that has passed through such a transmission medium (also called a communications channel) will vary randomly, or fade, according to a Rayleigh distribution, theradial component of the sum of two uncorrelated Gaussian random variables.Rayleigh fading is viewed as a reasonable model for tropospheric and ionospheric signal propagation as well as theeffect of heavily built-up urban environments on radio signals. Rayleigh fading is most applicable when there is no dominant propagation along a line of sight between the transmitter and receiver. If there is a dominant line of sight, Rician fading may be more applicable.

B. *The model*

Rayleigh fading is a reasonable model when there are many objects in the environment that scatter the radio signalbefore it arrives at the receiver. The central limit theorem holds that, if there is sufficiently much scatter, the channelimpulse response will be well-modelled as a Gaussian process irrespective of the distribution of the individualcomponents. If there is no dominant component to the scatter, then such a process will have zero mean and phaseevenly distributed between 0 and 2π radians. The envelope of the channel response will therefore be Rayleighdistributed. Calling this random variable, it will have a probability density function: where. Often, the gain and phase elements of a channel's distortion are conveniently represented as a complex number. In this case, Rayleigh fading is exhibited by the assumption that the real and imaginary parts of the response are modelled by independent and identically distributed zero-mean Gaussian processes so that the amplitude of the response is the sum of two such processes.

$$p_R(r) = \frac{2r}{\Omega} e^{-r^2/\Omega}, \; r \geq 0$$

The normalized autocorrelation function of a Rayleigh faded channel with motion at a constant velocity is a zeroth-order Bessel function of the first kind:

$$R(\tau) = J_0(2\pi f_d \tau)$$

At delay when the maximum Doppler shift is. The autocorrelation function of the Rayleigh fading channel shown above with 10 Hz maximum Doppler shift is shown in the figure. It is periodic in delay and its envelope decays slowly after the initial zero-crossing.

IV. RESULT AND DISCUSSION

We present simulation results for the secrecy rates and energy per secret bit, and in order to analyze the energy efficiency, we have determined the minimum bit energy required for secure and reliable communications in the presence of an eavesdropper. We have shown that secrecy in general increases the bit energy requirements. We have also noted that the suboptimal choices of transmission strategies can incur additional energy penalties. Numerical results are provided to illustrate the theoretical findings. Following the analysis for the fixed channel, we have investigated the low-SNR secrecy capacity in the presence of fading. We have demonstrated the benefits of fading in terms of energy efficiency.

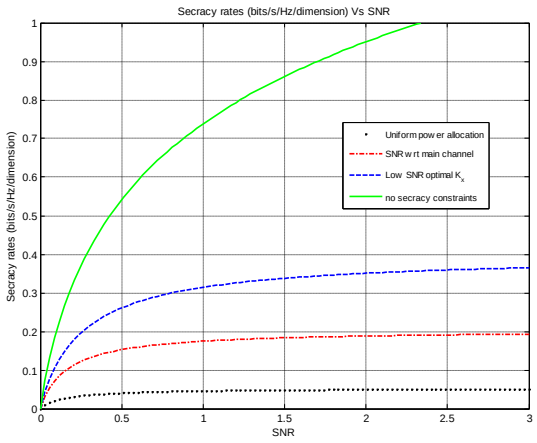

Fig.1 Secrecy rates in nats/s/Hz/dimension vs. SNR

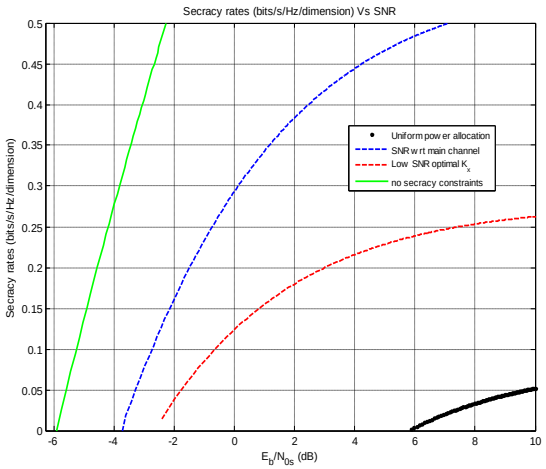

Fig.2 Secrecy rates in bits/s/Hz/dimension vs. energy per secret bit

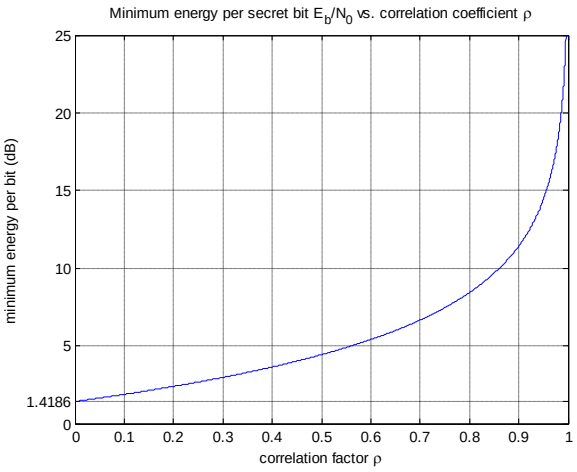

Fig.3Minimum energy per secret bit $E_b/N_{0\ min}$, vs. Correlation coefficient ρ.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

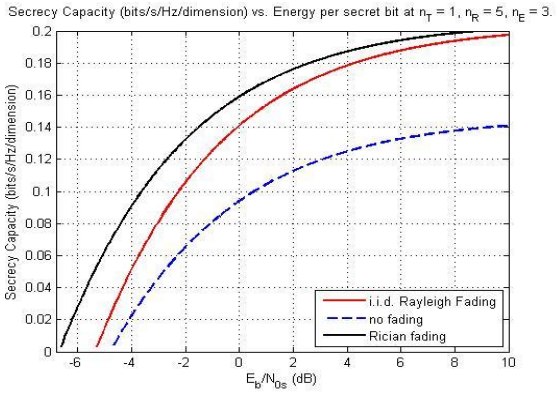

Fig .4 Secrecy capacity in bits/s/Hz/dimension vs. energy per secret bit $E_b/N_{0\,s}$ when n_T= 1, n_R= 5, and n_E= 3.

V. CONCLUSION

In order to analyze the energy efficiency, we have determined the minimum bit energy required for secure and reliable communications in the presence of an eavesdropper. We have shown that secrecy in general increases the bit energy requirements. We have also noted that the suboptimal choices of transmission strategies can incur additional energy penalties. Numerical results are provided to illustrate the theoretical findings. Following the analysis for the fixed channel, we have investigated the low-SNR secrecy capacity in the presence of fading. We have demonstrated the benefits of fading in terms of energy efficiency.

REFERENCES

[1] EzioBiglieri, Robert Calderbank, Anthony Constantinides, Andrea Goldsmith, ArogyaswamiPaulraj, H. Vincent Poor ,"MIMO Wireless Communications," Vol.2, Cambridge Press
[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, pp. 1355–1367, Oct. 1975
[3] 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.
[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages, IEEE Trans. Inf. Theory, vol. 3, pp. 339–348, May 1978.
[5] Special issue on information-theoretic security, IEEE Trans. Inf. Theory, vol. 54, no. 6, June 2008.
[6] A. O. Hero, "Secure space-time communication," IEEE Trans. Inf. Theory, vol. 49, pp. 3235–3249, Dec. 2003.
[7] Z. Li, W. Trappe, and R. D. Yates, "Secret communication via multiantenna transmission," 2007 Conf. Inf. Sciences Syst..
[8] 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.

BIOGRAPHIES

A.Leelavathi completed her M.Tech and currently working as Sr.Asst.Professor in the Department of ECE, Dadi Institute of Engineering and Technology, Anakapalli, AP, India

Poothi Venkata Lakshmi completed her graduation and currently is an M.Tech scholar in the Department of ECE, Dadi Institute of Engineering and Technology, Anakapalli, AP, India

K.Madhavi completed her M.Tech and currently working as Assistant t.Professor in the Department of ECE, Dadi Institute of Engineering and Technology, Anakapalli, AP, India