ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 5, March 2017

National Conference on Advanced Computing, Communication and Electrical Systems - (NCACCES'17)

24th - 25th March 2017

Organized by

C. H. Mohammed Koya
KMEA Engineering College, Kerala- 683561, India

Secret Communication Using Random Masked Beamforming

Simitha Shakkeer J. [1], Aparna Salil. [2]

P.G. Student, Department of Communication Engineering, KMEA Engineering College, Cochin, Kerala, India[1]

P.G. Student, Department of Communication Engineering, KMEA Engineering College, Cochin, Kerala, India[2]

ABSTRACT: Communication over wireless medium is vulnerable to eavesdropping. Thus, for secure communications, signals are needed to be encrypted and actively employ various approaches in cryptography. Here random masked beamforming method is used. A positive secrecy rate is achieved by the generation of an artificial noise(AN), which degrade the eavesdropper channel. This approach is referred to as random masked beamforming. Without knowing instantaneous channel state information (CSI) of an eavesdropper random masked beamforming can generate artificial jamming signals. Turbo channel encoder and decoder can be used for channel coding to detect and correct errors. Integrate amplify and forward relay network, and use transmission rate based jammer for enhance the secrecy rate. Using SINR select the best relay and do jamming for the rest of relays so that secrecy rate can be increased. Comparison between the beamforming method and transmission rate based jammer method with beamforming is considered. Here, instantaneous secrecy rate is considered.

KEYWORDS: Secure communication, Random masked beamforming, Artificial noise, Turbo channel encoder

I. INTRODUCTION

Communication over wireless medium is vulnerable to eavesdropping. A passive eavesdropper within the range of a wireless transmission obtains the transmitted information without the risk of detection. Thus, for secure communications, signals are needed to be encrypted. Encryption can be used to ensure confidentiality. Even when encryption is available, there are possibilities of eavesdropping. As a result, there is recently interest in the use of physical layer mechanisms to increase the secrecy in wireless communications systems. The secrecy in data transmissions is the major issue in wireless communication systems, where the broadcast characteristic of this medium makes it difficult for preventing eavesdropping. Traditional key-based cryptography is based on the eavesdropper who has a limited computational resource. These algorithms ensure that without the knowledge of the secret key it is infeasible to recover the encrypted data.

Broadcast nature of the wireless medium has given it a much more popularity and is easily accessible. This ease of accessibility makes it easy to overhear communication over this medium, thus there is need for privacy concerns. Secrecy is considered in three nodes; the transmitter, the receiver and an eavesdropper. Considering the secret communication from the transmitter to the receiver, over a wireless channel, where a passive eavesdropper is present, transmitter wants to transmit the secret message to a intended receiver, such that the eavesdropper is unable to translate it. The eavesdropper is assumed to be passive, so its location, and its presence will be not known to the transmitter.

Shannon had given a theoretical foundation for the study of secret communication and proved that when the secret key is at least as large as the secret message, the perfect secrecy achieved. However, this result was based on the assumption that the eavesdropper has access to all information as the receiver, except the secret key. Later, considered a situation where the receiver and an eavesdropper have separate channels then showed that secret communication is possible when eavesdropper's channel has a smaller capacity than that of receiver's channel. The eavesdropper's channel will be a degraded version of the receiver's channel. The paper also defined the term 'secrecy capacity' [1], which is the maximum rate at which the transmitter can efficiently communicate a secret message to the intended receiver, without eavesdropper able to decode it. However, if the eavesdropper is having a better channel than receiver to the transmitter, then the secrecy capacity is zero, means that secrecy cannot be guaranteed.

Information theoretic secrecy to the channel models with single transmitter, single receiver, and single wiretapper was mapped out by Wyner, Csiszar and Korner, and Leung-Yan-Cheong and Hellman. Wyner introduced the wiretap channel where it is assumed that the received signal by the wiretapper will be a degraded version of signal received by genuine receiver [2]. For that model, Wyner established a secrecy capacity region, which is defined as a region of all simultaneously achievable rates and also equivocation-rates. Jinho Choi et al. used a beamforming approach which induces jamming signals to avoid eavesdropping from a transmitter having an antenna array. With this masked beamforming, to guarantee a certain instantaneous secrecy rate, robust beamforming problems with [3] the constraint that deals with the eavesdropper channel's uncertainty is formulated and then found the solutions. Amitav Mukherjee et al. investigated the methods for lowering the likelihood that, a message transmitted between two multi-antenna nodes is interrupted by an undetected eavesdropper [4]. Satashu Goel, and Rohit Negi, investigated the problem of secret communication in a fading environment, in the presence of passive eavesdroppers [5]. The eavesdroppers were assumed to know the channel state information of all the channels and they were allowed to collude. Wei-Cheng Liao et al. established a secret transmit beamforming approach using a QoS- oriented perspective [6]. Lun Dong et al. proposed cooperating relays for improving the performance of secure wireless communications in presence of one or more wiretappers [7].

This paper is organized as follows: Section II describes the related work in which random masked beam forming and transmission rate based jammer method are explained. Section III presents experimental results showing the selection of the best relay, comparison of the performance of secrecy capacity with relay and with beamforming. Finally section IV presents the conclusion.

II. RELATED WORK

This paper considers a beamforming approach which induces jamming signals to avoid eavesdropping from a transmitter having an antenna array. Here random masked beamforming is used. A pertinent characteristic of random masked beamforming is that artificial jamming signals can generated without knowing instantaneous channel state information (CSI) of the wiretapper. By knowing the channel distribution information (CDI) and the statistical properties of the eavesdropper channel the ergodic secrecy rate from the transmitter to the original receiver can be obtained. 'Secrecy capacity', is defined as the maximum rate at which the transmitter can correctly communicate a secret message to the prearranged receiver, without the eavesdropper being able to unravel it. But, if the eavesdropper is having a much better channel than the receiver then the secrecy capacity is tends to zero, means that the secrecy cannot be assured. Solution to this problem is elaborated in this work. The transmitter can use some of the accessible power to transmit artificially generated noise. The transmitter can design the artificially generated noise such that only the eavesdropper's channel is vulgarized. Thus, by selectively degrading the medium for the eavesdropper, secret communication can be assured. Turbo codes are capable of achieving an arbitrarily low Bit Error Rate that is less errors. Lower signal power required if turbo channel encoder is used. The main differences from existing approaches are, here instantaneous secrecy rate with signal-to interference- plus-noise ratio (SINR) constraints is considered.

Integration of amplify and forward relay network is carried out and transmission rate based jammer is used to enhance the secrecy rate. Conventional relay selection scheme is used where the relay that has the highest instantaneous SNR to the destination will be selected to become the sender. The SNR of the relays are compared with the predetermined threshold SNR then the relay having maximum SNR is chosen and jamming is done for rest of the relay network. A comparison between beamforming method and transmission based jammer method with beamforming using amplify and relay network is considered.

III. EXPERIMENTAL RESULT

Figure 1 is the plot between symbol error rate (SER) and signal to noise ratio (SNR). The best relay is the relay which is having maximum SNR which is plotted in red colour. The symbol error is reached to zero around 26dB SNR. Figure 2 is the plot between average secrecy capacity and signal to noise ratio. It is seen from the plot that the performance of the amplify and forward relay network with beamforming is greater than that compared with the beamforming method.

Secrecy capacity increases with increase in SNR. When 3 relays are selected at 20 dB SNR it is seen that there is 0.9 nats/symbol increase in secrecy capacity for amplify and forward relay network with beamforming.

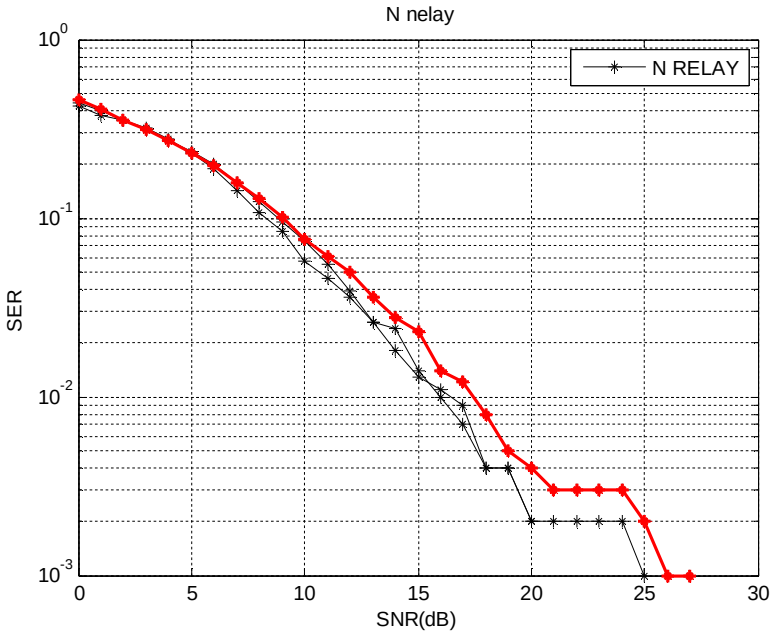

Fig. 1: Selection of the Best relay

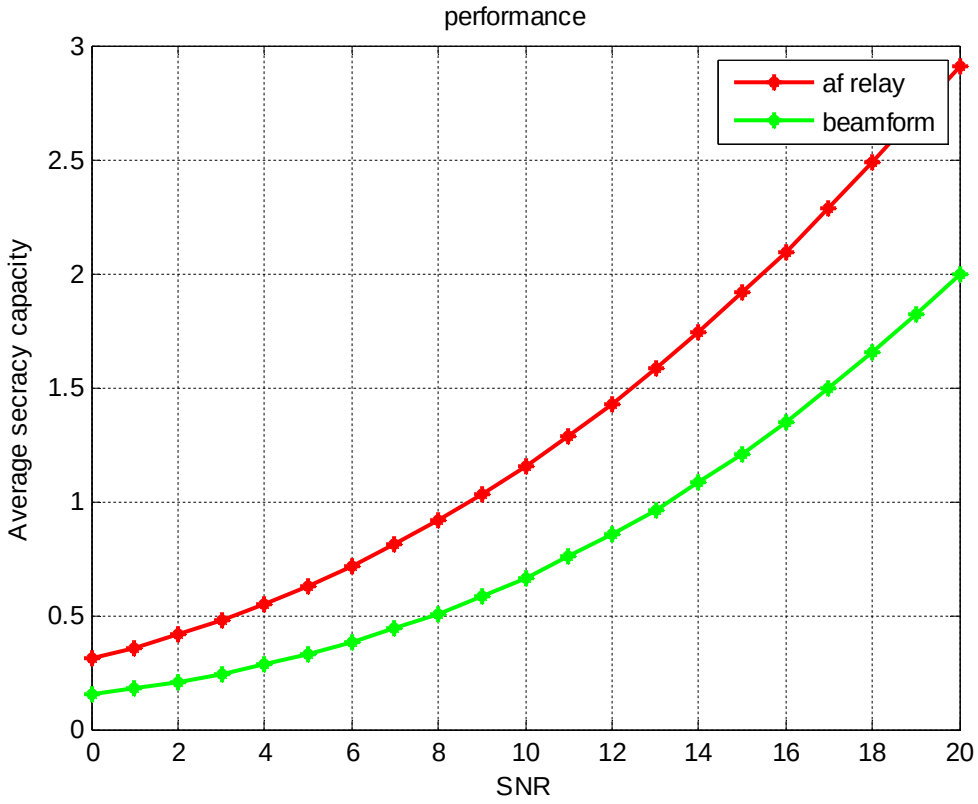

Fig. 2: Comparison of Secrecy capacity

Figure 3 is the plot between symbol error rate and SNR for beamforming and amplify and forward relay network with beamforming. It is seen from the plot that the amplify and forward relay network with beamforming outperforms the beamforming method.

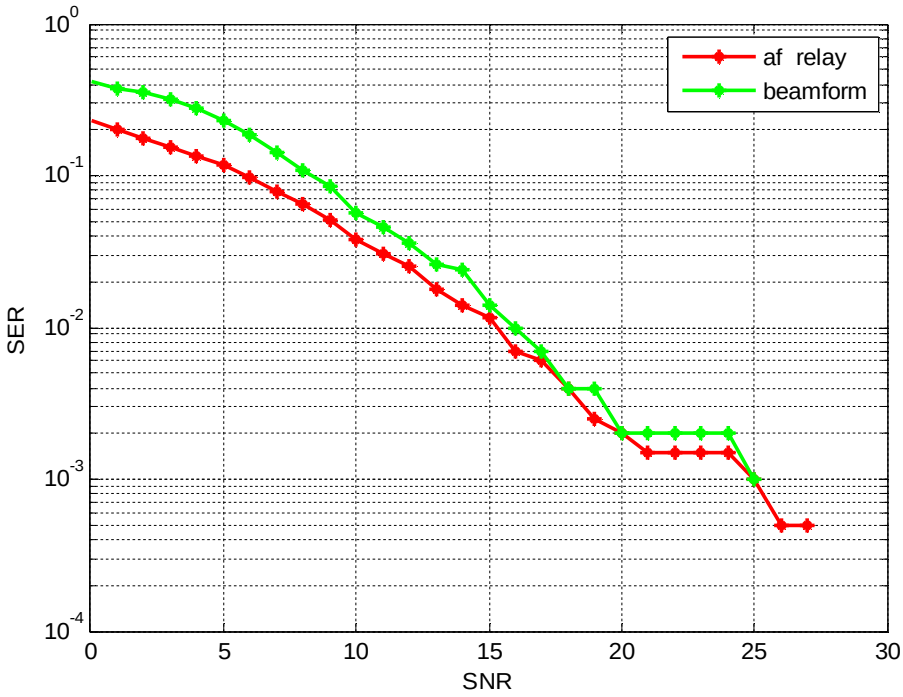

Fig.3: comparison of symbol error rate versus SNR

V.CONCLUSION

This paper considered the problem of secret communication in the wireless environment, in the presence of a passive eavesdropper. A random masked beamforming method to guarantee an instantaneous secrecy rate is used. The key difference from existing approaches is that instantaneous secrecy rate is considered. In the multiple antenna scenario, the transmitter can use the multiple antennas to generate the artificial noise intelligently such that it degrades only the eavesdropper's channel. Turbo channel encoder is introduced to detect and correct the channel errors. Integrating amplify and forward relay network and based on transmission rate we can select the best relay and do jamming for the rest of relays so that we can increase the secrecy rate. When beamforming is introduced to this amplify and forward relay network it outperforms the beamforming method, better secrecy capacity and symbol error rate versus SNR performance are obtained.

REFERENCES

[1] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," in IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 2180-2189, June 2008.
[2] R. Bassily and S. Ulukus, "A new achievable ergodic secrecy rate region for the fading multiple access wiretap channel," 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, 2009, pp. 819-826.
[3] J. Choi, "A Robust Beamforming Approach to Guarantee Instantaneous Secrecy Rate," in IEEE Transactions on Wireless Communications, vol. 15, no. 2, pp. 1076-1085, Feb. 2016.
[4] A. Mukherjee and A. L. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI," in IEEE Transactions on Signal Processing, vol. 59, no. 1, pp. 351-361, Jan. 2011.
[5] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," in IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 2180-2189, June 2008.
[6] W. C. Liao, T. H. Chang, W. K. Ma and C. Y. Chi, "QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach," in IEEE Transactions on Signal Processing, vol. 59, no. 3, pp. 1202-1216, March 2011.
[7] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," in IEEE Transactions on Signal Processing, vol. 58, no. 3, pp. 1875-1888, March 2010.