Uncoordinated Cooperative Jamming with Phase Shift Beam Forming for Physical Layer Security

Minu Maria Joseph, Nandan S

Abstract—Wireless networks are widely popular because of its broadcast nature, which makes it easily accessible. This ease of accessibility also makes it vulnerable to eavesdropping, thus raising security concerns. An information-theoretic viewpoint has found conditions for reliable and secure communication and overcomes the disadvantages of traditional cryptographic techniques. One method that ensures such perfect secrecy is by cooperative jamming. The jamming signal is such that it degrades the eavesdropper's channel without affecting the channel of the legitimate receiver, thus ensuring security in communication. An uncoordinated jamming approach such as local nulling does not require any public information and makes use of only the helper-receiver channel information. This paper proposes a scheme which is a hybrid combination of local nulling and phase shuft beamforming such that the secrecy rate achievable with local nulling is maximized.

Index Terms— Beam forming, physical layer security, secrecy rate, uncoordinated cooperative jamming.

I. INTRODUCTION

Security and reliability are two of the most essential requirements for any type of communication. The mobile and accessible nature of wireless networks makes it much popular today. But due to the broadcast nature of the wireless media, data transmissions are often susceptible to eavesdropping. Ensuring security of transmission between authorized transmitters and receivers are quite important, but often difficult. Claude Shannon laid the theoretical foundation for secret communication in a system [2]. The security issues associated with wireless communication were mostly dealt with cryptographic algorithms at application layer, which faces challenges in designing such encryption methods that are reliable. Encryption at the application layer requires key distribution to be perfectly safe, to provide a high level of security, which increases the complexity of the system. The increased importance of security in data transmission has caused the focus to be shifted to implementations of algorithms at lower layers, particularly, at the physical layer. The idea of physical layer security was pioneered by Wyner [3] who proposed a wiretap channel model where the eavesdropper channel was a degraded version of the legitimate channel and introduced the notion of secrecy capacity.

Revised Version Manuscript Received on June 29, 2015.

Minu Maria Joseph, Department of Electronics and Communication Engineering, Mar Baselios College of Engineering and Technology, Thiruvananthapuram, India.

Nandan S, Department of Electronics and Communication Engineering, Mar Baselios College of Engineering and Technology, Thiruvananthapuram, India.

Secrecy capacity is defined as maximum rate at which the legitimate receiver's decoding error probability tends to zero, while the eavesdropper's error probability tends to one [4]. When compared to traditional cryptographic algorithms, physical layer security has a basically different approach where security is achieved by exploiting the physical layer properties of the wireless communication system. It provides information-theoretic security and cannot be broken even when the attacker has immense computing power. The idea of physical layer security was later extended to a Gaussian wiretap channel. But it was seen that if the eavesdropper has a better channel than the receiver the secrecy capacity is zero [5]. An artificial noise injection strategy was later introduced to ensure physical layer security where the noise was transmitted along with the information signal and orthogonal to the intended receiver [5]-[6]. This strategy ensured a positive secrecy rate even when the eavesdropper channel was better than the receiver. The concept of information-theoretic security was later extended to multi-user networks i.e. relays and cooperative networks [7]. Relays may act as both relaying components and jamming partners to enhance secure transmission or they can assume the role of unitary to facilitate the jamming of unintended receivers - called cooperative jamming. The secrecy capacity in cooperative communication can be maximized by utilizing trusted relay components through cooperative jamming. Although schemes using transmit powers of relays and antenna weights were proposed to maximize the secrecy capacity, it was essential that the global channel state information is known, compromising the security of the system [8]. The transmission of jamming noise in a cooperative network can be either coordinated, which requires public information, or uncoordinated, which does not require public information [9]. In coordinated cooperative jamming technique, the helpers coordinate with the legitimate transmitter, Alice and the legitimate receiver, Bob. Hence, for coordinated cooperative jamming the global channel state information is made public. In uncoordinated cooperative jamming scheme the helpers, equipped with multiple antennas, generate jamming noise such that it does not affect the destination. Here, no coordination between helpers is needed. Local nulling is an uncoordinated cooperative jamming scheme in which each helper completely cancels its interference at the destination, using only local information of its channel to the destination [10]. Hence, no global channel state information is required. Secrecy in cooperative communication was further improved by combining relaying and cooperative jamming [11]-[12]. Some of the relays were used to forward the information using distributed beamforming and the others were used for jamming the eavesdropper. Initially decode-and-forward and

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

amplify-and-forward schemes were employed for relay networks which resulted in sub-optimal solutions [12]. In most cases, it requires that the channel state information is perfectly known by the helpers. This makes cooperation more difficult. This paper proposes a scheme which uses a hybrid combination of an uncoordinated cooperative jamming scheme called local nulling and beamforming at the legitimate transmitter, such that the achievable secrecy rate can be maximized. The system includes a set of helpers which transmits interference signals while the source is transmitting to the legitimate receiver. The scheme is considered for a SISO system and a MISO system. The helpers are assumed to know only the information about its own link to the destination. The eavesdropper channel state information is assumed to be unknown. The remainder of the paper is organized as follows. Section II describes the system model. Section III gives the details of the proposed scheme. The experimental results are discussed in Section IV and conclusions are presented in Section V.

II. SYSTEM MODEL

An uncoordinated cooperative jamming scheme called local nulling is considered here. The helpers, equipped with multiple antennas each, generate jamming noise that creates interference to the eavesdropper but does not affect the destination. No coordination between helpers is needed; hence no eavesdropper channel state information is required at the helpers.

The received signal at Bob and Eve is given by [10],

$$y_b = \sqrt{P_0} H_0 x + \sum_{i=1}^{N} h_i^H u_i + n_b \quad (1)$$

$$y_e = \sqrt{P_0} G_0 x + \sum_{i=1}^{N} G_i^H u_i + n_e \quad (2)$$

where, u_i is the noise signal transmitted by the ith helper. n_b and n_e are the AWGN at the receiver. x denotes the message transmitted from Alice. The system model includes a Gaussian wiretap channel with a legitimate transmitter, Alice, an intended receiver, Bob, an eavesdropper, Eve, and a set of helpers, as shown in Fig.1. The legitimate transmitter, Alice, transmits to the legitimate receiver, Bob, through the channel, H_0. The eavesdropper, Eve, intercepts messages through the channel, G_0. The cooperative jamming is done by a set of N helper-relays, each equipped with N_i antennas, where $i = 1...N$. h_i denotes the channel from helper i to Bob and g_i denotes the channel from helper i to Eve. The source transmits a message with source power, P_0 and noise power, N_0. The

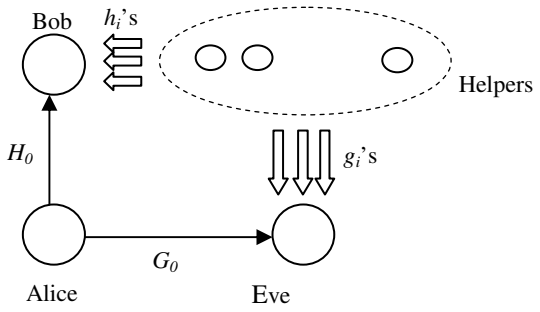

Fig. 1. System model

signal to noise ratio at the transmitter is taken as γ_0 and the signal to noise ratio at the kth helper is taken as γ_i. In the cooperative jamming scenario considered here, while Alice is transmitting the message, the helpers transmit noise such that they remain uncoordinated and does not depend on the message transmitted from the source. The main aim is to maximize the secrecy rate achievable using local nulling by combining it with beamforming. Two cases of beamforming are considered here i.e. simple transmit beamforming for a SISO channel, and phase shift beamforming for a MISO channel. For SISO channel, Alice is assumed to be equipped with two antennas while for MISO channel, Alice is assumed to be equipped with a single antenna.

III. LOCAL NULLING WITH BEAM FORMING

In cooperative jamming via local nulling, since no coordination is required between helpers, global channel state information is not made public. The helpers are assumed to have information about its own link to the destination. Each of the helpers transmits noise which is designed such that it produces a null at the intended destination but degrades the eavesdropper,

$$h_i^H u_i = 0 \,,\; i = 1 \ldots N \quad (3)$$

The noise signal transmitted by each of the helpers is thus cancelled at the legitimate receiver and gets accumulated at the eavesdropper. Hence no degradation occurs at the intended receiver, affecting only the illegitimate receiver ensuring secrecy while transmitting confidential messages. The secrecy rate for the nulling scheme [1] is given by the equation,

$$R = \log_2\left(1+\gamma_0 \left|H_0\right|^2\right) - \log_2\left(1+\frac{\gamma_0 \left|G_0\right|^2}{\sum_{i=1}^{N} \gamma_i (N_i - 1)^{-1} \left\|Q^H{}_i g_i\right\|^2 + 1}\right) \quad (4)$$

where, Q_i denotes the null space of h_i^H, where h_i denotes the channel from helper, i to the intended receiver. To maximize the secrecy rate, the mutual information shared between Alice and Bob must be much larger than the mutual information shared between Alice and Eve. Beamforming improves the channel quality of the signal while cooperative jamming degrades the quality of the eavesdropper channel, thus resulting in a positive secrecy rate. A beamformer is equivalent to a spatial filter that represses the unwanted signal from all directions by destructive interference and bolsters the desired signal by constructive interference. Here, a narrowband phase shift beamformer is considered in the system. A conventional beamformer delays the signal at each antenna, which is equivalent to multiplying the signal by a phase factor. Thus, a beamformer controls the phase and relative amplitude of the signal at the transmitter, such that the information from different sensors is combined to increase the array gain, resulting in beamforming in a particular direction.

For a SISO channel, the received signal at Bob after beamforming is given by,

$$y_b = hx + n_b \quad (5)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

where $h = |h_o| e^{j\theta}$. Multiplying the signal by the phase factor results in constructive interference, thus strengthening the transmitted message signal. Considering a MISO channel with one receive antenna and two transmit antennas, the signal received at Bob is given by,

$$y_b = \begin{bmatrix} h_1 & h_2 \end{bmatrix} \begin{bmatrix} e^{j\theta_1} \\ e^{j\theta_2} \end{bmatrix} x + n_b \quad (6)$$

where $h_1 = |h_1| e^{-j\theta_1}$ and $h_2 = |h_2| e^{-j\theta_2}$. The equivalent received signal after beamforming is given by,

$$y_b = \left(|h_1| + |h_2| \right) x + n_b \quad (7)$$

Thus, the equivalent channel after beamforming, $|h_1| + |h_2|$, strengthens the legitimate channel between Alice and Bob and the cooperative jamming degrades the eavesdropper channel, ensuring a positive secrecy rate.

IV. EXPERIMENTAL RESULTS

The simulation results for the proposed scheme are presented in this section. The performance parameter considered here is the secrecy rate. The simulation platform used is MATLAB. All the channel coefficients are randomly generated in each simulation run. h_i, the channel from the ith helper to the receiver and g_i, the channel from the ith helper to the eavesdropper, are taken to be complex Gaussian random vectors with zero mean. Each of the helper is considered to have $N_i = 2$ antennas. The SNR at each of the helper is taken to be 2 dB, considering an individual power constraint at the helpers, which is more practical. Fig.2 shows the output of the phase shift beamformer for a SISO channel. Here, a uniform linear array consisting of 10 elements is considered with element spacing half of the signal wavelength, acting as a single antenna. The signal to noise ratio of source, $\gamma_0 = P_0 / N_0$, is calculated from the beamformed signal. It can be seen that the transmitted signal is much stronger than the interference signal. The improved strength of the transmitted signal in the direction of the intended receiver ensures that the information that is leaked to the eavesdropper is negligible providing a higher secrecy in communication. Thus, beamforming when used in conjunction with local nulling gives a higher value of secrecy capacity. Fig.3 compares the secrecy rate of a network which uses local nulling for cooperative jamming, with and without phase shift beamforming in a SISO channel. The system, which uses a hybrid combination of local nulling and beamforming shows an improved performance in terms of secrecy rate. As the directivity of the transmitted signal increases, the mutual information shared between the transmitter and the eavesdropper is considerably reduced. This maximizes the achievable secrecy rate, resulting in higher performance than a system which uses only local nulling. Fig.4 shows the improved performance of the cooperative jamming system using phase shift beamforming in a MISO channel. The transmitter is assumed to be equipped with two antennas in case of the MISO channel. For transmit beamforming, the message from each of the transmit antenna is multiplied with a complex value equivalent to the inverse of the phase of the channel, ensuring that the signal constructively interfere at the receiver, resulting in beamforming in the desired direction, consequently resulting in a higher secrecy rate. From the figures, it can be seen that even though the power of the signal is fixed, as the number of helpers increase, the secrecy rate also increases. This is because of the power gain contributed by the helper nodes. The rate of increase of the secrecy rate decreases as the number of helpers increase, since having reached a high power, the significance of power gain degrades.

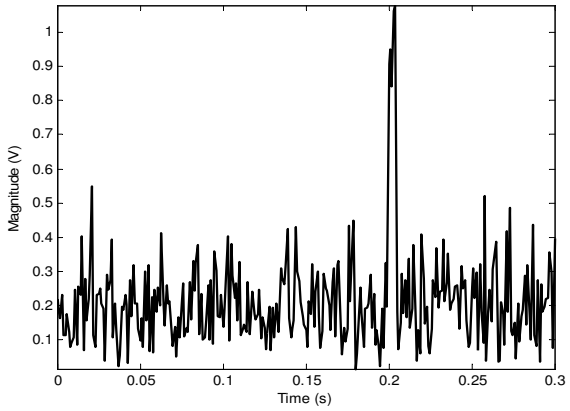

Fig.2. Output of the phase shift beamformer showing the transmitted signal with a higher magnitude than the interference.

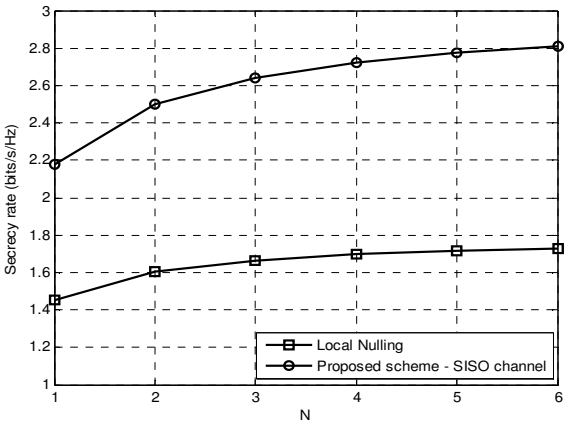

Fig.3. Plotting the secrecy rate of the system vs. the number of helpers, for a SISO channel.

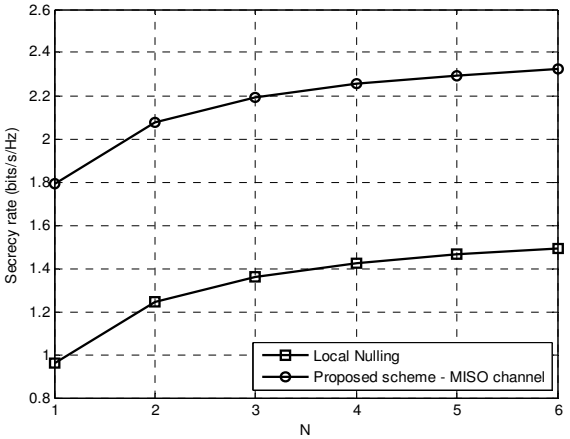

Fig.4. Plotting the secrecy rate of the system vs. the number of helpers, for a MISO channel.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

V. CONCLUSION

Cooperative jamming is one of the main techniques that provide information-theoretic security. The jamming signal is transmitted by the 'helper' nodes, along with the information-bearing signal such that it degrades only the eavesdropper channel. It maximizes the transmission rate in the main channel and the information leaked to the wire-tapper made negligible; thus increasing the secrecy capacity. In an uncoordinated cooperative jamming approach, no coordination between the legitimate transmitter, the helpers and the legitimate receiver is required. In this work, an uncoordinated jamming scheme called nulling scheme has been combined with phase shift beamforming to improve the achievable secrecy rate. Numerical results shows the improved performance of the proposed scheme when compared to a scheme which uses only local nulling and no beamforming.

REFERENCES

[1] S. Luo, J. Li and A. P. Petropulu, "Uncoordinated Cooperative Jamming for Secret Communications", *IEEE Transactions on Information Forensics and Security,* Vol. 8, No. 7, pp. 1081-1090, July 2013.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", *IEEE Communications Surveys & Tutorials,* Issue. 99, pp. 1-24, February 2014.

[3] A. D. Wyner, "The Wiretap Channel", *The Bell System Technical Journal,* Vol. 54, No.8, pp. 1355-1387, October 1975.

[4] L. Wang, C. Cao, M. Song and Y. Cheng, "Joint Cooperative Relaying and Jamming for Maximum Secrecy Capacity in Wireless Networks", *IEEE International Conference on Communication (ICC)*, pp. 4448-4453, June 2014.

[5] R. Negi and S. Goel, "Secret Communication using Artificial Noise", *IEEE 62nd Vehicular Technology Conference*, pp. 1906-1910, September 2005.

[6] S. Goel, and R. Negi, "Guaranteeing Secrecy using Artificial Noise", *IEEE Transactions on Wireless Communications*, Vol. 7, No. 6, pp. 2180-2189, June 2008.

[7] J. Huang and A. L. Swindlehurst, "Secure Communications via Cooperative Jamming in Two-hop Relay Systems", *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1-5, December 2010.

[8] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Cooperative Jamming for Wireless Physical Layer Security", *IEEE/SP 15th Workshop on Statistical Signal Processing*, pp. 417-420, September 2009.

[9] J. Wang, and A. L. Swindlehurst, "Cooperative Jamming in MIMO ad-hoc networks", *2009 Conference Record of the 43rd Asilomar Conference on Signals, Systems and Computers*, Nov 2008, pp. 1719-1723.

[10] S. Luo, J. Li and A. P. Petropulu , "Physical Layer Security with Uncoordinated Helpers Implementing Cooperative Jamming", *IEEE 7th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, pp. 97-100, June 2012.

[11] H. Wang, M. Luo, X. Xia and Q. Yin, "Joint Cooperative Beamforming and Jamming to Secure AF Relay Systems With Individual Power Constraint and No Eavesdropper's CSI", *IEEE Signal Processing Letters*, Vol. 20, No. 1, pp. 39-42, January 2013.

[12] Wang, M. Luo, Q. Yin, and X. Xia, "Hybrid Cooperative Beamforming and Jamming for Physical-Layer Security of Two-Way Relay Networks", *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 12, pp. 2007-2020, December 2013.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.