International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 2, Issue 9 (May 2013) PP: 24-28

Secure and Efficient Transmission Using Jammer and Relay Networks

Mr. R. Prabu, Miss. S. Nishanthy
Assistant Professor, Department Of Information Technology,Vel Tech Multi Tech Dr Rangarajan, Dr Sakunthala Engineering College, Avadi, Chennai
M.Tech- Information Technology Final Year,Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College,Avadi, Chennai.

Abstract: *Here, we present the Relay and Jammer for Secure and Efficient Transmission. It consists of two sources, number of intermediate node and one eavesdropper. The proposed algorithm selects two or three intermediate nodes to enhance the security against eavesdropper. The first selected node operates as relay mode which is used to deliver the data from source to destination using the amplify and forward algorithm. Second and third nodes are used in two different communication Phases as jammer in order to provide the secrecy. The jamming schemes become less efficient in some cases 1.Intermediate nodes cluster locates near to one of the destination. 2 .Intermediate nodes cluster locates near to the eavesdropper. To overcome these cases a hybrid scheme i.e. intelligent switching mechanism between jamming and non jamming modes is used.*

Keywords: *Relay Node, Jammer Node, Eavesdropper, Hybrid Scheme, Amplify and Forward Strategy.*

I. Introduction

Traditionally security in wireless networks has been mainly focused on higher layers using cryptographic methods. Pioneered by Wyner's work, which introduced the wiretap channel and established fundamental results of creating perfectly secure communications without relying on private keys, physical-layer-based security has drawn increasing attention recently. The basic idea of physical-layer security is to exploit the physical characteristics of the wireless channel to provide secure communications. The security is quantified by the secrecy capacity, which is defined as the maximum rate of reliable information sent from the source to the intended destination in the presence of eavesdroppers. Wyner showed that when the wiretap channel is a degraded version of the main channel, the source and the destination can exchange secure messages at a nonzero rate. The following research work studied the secrecy capacity of the Gaussian wiretap channel, and extended Wyner's approach to the transmission of confidential messages over broadcast channels.Very recently, physical-layer security has been generalized to investigate wireless fading channels, and various multiple access scenarios.

In this paper, I propose a scheme that can implement information exchange in the physical layer against eavesdroppers for two-way cooperative networks, consisting of two sources, a number of intermediate nodes, and one eavesdropper, with the constraints for physical-layer security. Unlike, in which the relay selection is operated in an environment with no security requirement, our work takes into account the secrecy constraints. In contrast to, where many relay selections based on the DF strategy for one-way cooperative wireless networks were proposed and a safe broadcasting phase was assumed, the problem we consider here involves a non security broadcasting phase, and the information is transferred bidirectionally.

The theoretical analysis and simulation results reveal that the proposed jamming schemes can improve the secrecy rate of the system by a large scale, but only within a certain transmitted power range. In some particular scenarios, the proposed schemes become less efficient than the conventional ones. We then propose a hybrid scheme with an intelligent switching mechanism between jamming and non jamming modes to solve this problem.

II. System Model

A. System Model

We assume a network configuration consisting of two sources S1 and S2 , one eavesdropper E , and an intermediate node set Sin= {1,2,….K} with K nodes. As the intermediate nodes cannot transmit and receive simultaneously (half-duplex assumption), the communication process is performed by two phases. During the first phase, S1 and S2 transmit their data to the intermediate nodes. In addition, according to the security protocol, one node J1 is selected from Sin to operate as a "jammer" and transmit intentional interference to degrade the source-eavesdropper links in this phase. Since the jamming signal is unknown at the rest nodes of Sin, the interference will also degrade the performance of the source-relay links. During the second phase, according to the security protocol, an intermediate node, denoted by , is selected to operate as a conventional

relay and forwards the source messages to the corresponding destinations. A second jammer J2 is also selected from Sin , for the same reason as that for J1 . Note that S1 and S2 are not able to mitigate the artificial interference from the jamming nodes.

B. Selection without Jamming

In a conventional cooperative network, the relay scheme does not have the help from jamming nodes.We derive the following solutions under this scenario.

1) Conventional Selection (CS):

The conventional selection does not take the eavesdropper channels into account, and the relay node is selected according to the instantaneous SNR of the channel between node S1 and S2 node only.

2) Optimal Selection (OS):

This solution takes the eavesdropper into account and selects the relay node based on the instantaneous channel knowledge for all the links.

3) Suboptimal Selection (SS):

The suboptimal selection implements the relay selection based on the knowledge set, which gives the average estimate of the eavesdropping links. Therefore, it avoids the difficulty of getting instantaneous estimate of channel feedback.

III. Existing System:

Two-way communication is a common scenario in which two nodes transmit information to each other simultaneously. The existing system consists of two source node S1 and S2, many intermediate nodes and one eavesdropper. Source 1 transmits the information to source 2 via intermediate node. Eavesdropper is the silent listener. In phase 1 the relay mode receives the data from the source nodes, the jammer here blocks the eavesdropper by disconnecting it from the relay mode. In phase 2 the relay mode forwards the data to the destination, the jammer 2 blocks the eavesdropper signal by disconnecting from the sources. We also find that, in the scenario where the intermediate nodes gather as a close cluster, the jamming schemes may be less effective than their non-jamming counterparts.

IV. Proposed System:

In this system, we propose a scheme that can implement information exchange in the physical layer against eavesdroppers for two-way cooperative networks, consisting of two sources, a number of intermediate nodes, and one eavesdropper, with the constraints for physical-layer security. Specifically, one node is selected from an intermediate node set to operate at a conventional relay mode, and then uses an AF strategy in order to assist the sources to deliver data to the corresponding destinations. Meanwhile, another two intermediate nodes that perform as jammers are selected to transmit artificial interference in order to degrade the eavesdropper links in the first and second phases of signal transmissions, respectively. We assume that both destinations cannot mitigate artificial interference, and thus, the jamming will also degrade the desired information channels. Hybrid switching scheme with an intelligent switching mechanism between jamming and non-jamming modes to solve this problem.

V. Techniques for Jamming:

Selection techniques only concern the secrecy performance in the second phase of transmission. Our work takes into account both the two phases in order to select a set of relay and jammers that can maximize the overall expectation of secrecy rate.

Some of the jamming techniques are:

i) Optimal Selection with Maximum Sum Instantaneous Secrecy Rate.
ii) Optimal Selection with Max-Min Instantaneous Secrecy Rate.
iii) Optimal Switching.
iv) Suboptimal Selection with Maximum Sum Instantaneous Secrecy Rate.
iv) Suboptimal Selection with Max-Min Instantaneous Secrecy Rate.
v) Suboptimal Switching.
vi) Optimal Selection with “Known” Jamming.

i) OS-MSISR:

The optimal selection with maximum sum instantaneous secrecy rate assumes the knowledge set and ensures a maximization of the sum of instantaneous secrecy rate of node S1 and node S2. OS-MSISR scheme here tends to select a set of relay and jammers that maximizes, which means promoting the assistance to the sources.

ii) OS-MMISR:

The Optimal selection with Max-Min Instantaneous secrecy rate scheme maximizes the worse instantaneous secrecy rate of the two sources with the assumption of knowledge set. In addition, in some scenarios, the considered secrecy performance takes into account not only the total secrecy rate of both the sources, but also the individual secrecy rate of each one. If one source has a low secrecy rate, the whole system is regarded as secrecy inefficient. Furthermore, assuring each individual source a high secrecy rate is another perspective of increasing the whole system's secrecy performance.

iii) OSW:

The original idea of using jamming nodes is to introduce interference on the eavesdropping links. However, there are two side-effects of using jamming. Such as the jamming node in the second phase, it also poses undesired interference directly onto the destinations. Given the assumption that the destinations cannot mitigate this artificial interference, continuous jamming in both phases is not always beneficial for the whole system. In some specific situations the continuous jamming may decrease the secrecy rate of both the sources seriously, and act as a bottleneck for the system. In order to overcome this problem, we introduce the idea of intelligent switching between the OS-MSISR and OS schemes in order to reduce the impact of "negative interference."

iv) SS-MSISR:

In some scenario in which the intermediate nodes are sparsely distributed across the considered area, the SS-MSISR scheme can provide similar relay and jammer selection performance with the OS-MSISR scheme.

v) SSW:

Jamming is not always a positive process for the performance of the system; the suboptimal switching scheme refers to the practical application of the intelligent switching between the SS-MSISR and SS schemes. The basic idea is the same as the OSW scheme, but the switching criterion uses the available knowledge set.

vi) OSKJ:

This assumption avoids the initialization period in which the jamming sequence is defined, and thus, it reduces the risk of giving out the artificial interference to the eavesdropper. For comparison reasons, here we propose a "control" scheme, in which the jamming signal can be decoded at destinations and, but not at eavesdropper.

vii) Amplify-and-forward protocol

The amplify-and-forward strategy allows the relay station to amplify the received signal from the source node and to forward it to the destination station.

viii) Hybrid schemes (OSW and SSW)

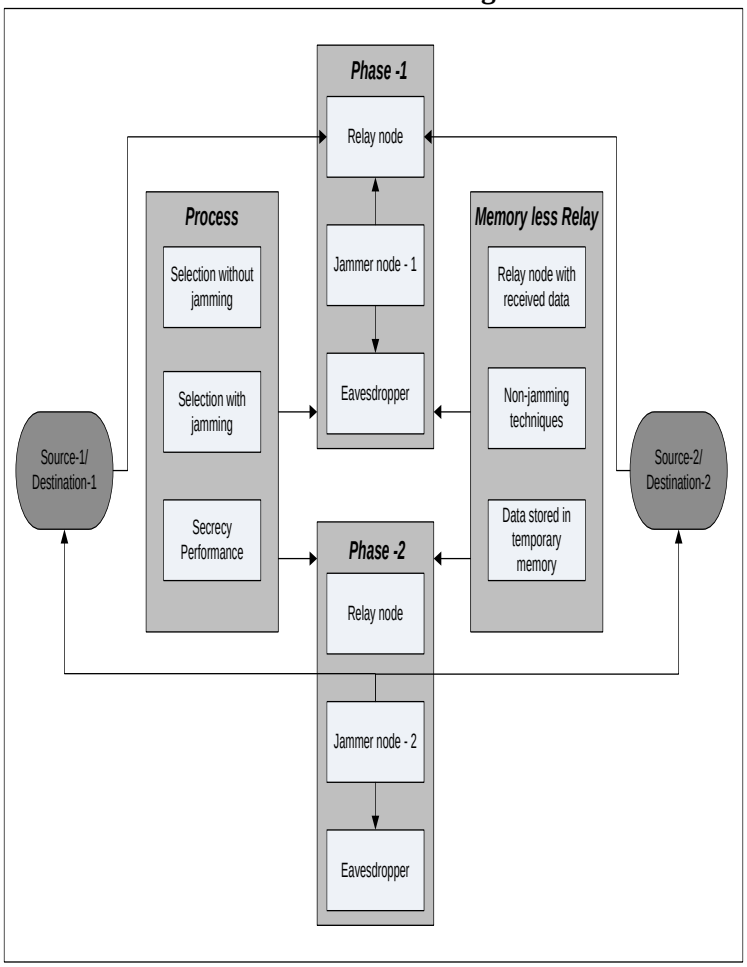
Given the assumption that the destinations cannot mitigate this artificial interference, continuous jamming in all phases is not always beneficial for the whole system. In some specific situations (e.g., jammer node is close to one destination), the continuous jamming may decrease the secrecy rate of both the sources seriously, and act as a bottleneck for the system. In order to overcome this problem, we introduce the idea of intelligent switching between the Optimal Selection with Maximum Sum Instantaneous Secrecy Rate (OS-MSISR) and Optimal Selection (OS) schemes in order to reduce the impact of "negative interference" This is known as **Optimal Switching (OSW)**.

Given the fact that jamming is not always a positive process for the performance of the system, the suboptimal switching scheme refers to the practical application of the intelligent switching between the SS-MSISR and SS schemes. The basic idea is the same as the OSW scheme, but the switching criterion uses the available knowledge set. This process is known as **Suboptimal Switching (SSW)**.

We further enhance our work to choose **non-jamming techniques**. Because jamming will not always result in a positive result. When eavesdropper is very close to either source or destination we will use

non-jamming technique to avoid communication failure. And also we use **memory less relay** node strategy to avoid the data leakage in case of non-jamming technique.

VI. Architecture Diagram



VII. Conclusion

This system has studied secure and efficient transmission using jammer and relay in two-way cooperative networks. The proposed schemes achieve an opportunistic selection of one conventional relay node and one (or two) jamming nodes to enhance security against eavesdroppers based on both instantaneous and average knowledge of the eavesdropper channels.

The selected relay node helps the information transmission between the two sources in an AF strategy, while the jamming nodes are used to produce intentional interference at the eavesdropper in different transmission phases. We found that the proposed jamming schemes (i.e., OS-MSISR, OS-MMISR, SS-MSISR, and SS-MMISR) are effective within a certain transmitted power range for scenarios with the intermediate nodes sparsely distributed. Meanwhile, the non-jamming schemes (i.e., CS, OS, and SS) are preferred in configurations where the intermediate nodes are confined close to each other.

The OSW scheme which switches intelligently between jamming and non-jamming modes is very efficient in providing the highest secrecy rate in almost the whole transmitted power regime in two-way cooperative networks, but it requires instantaneous eavesdropper channel knowledge. On the other hand, the SSW scheme, which is based on the average knowledge of the eavesdropper channel and thus much more practical, provides a comparable secrecy performance with the OSW scheme.

References

[1]. I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Trans. Wireless Commun., vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[2]. Michael R. Souryal, and Branimir R.Vojcic,"Performance of amplify-and-forward and decode-and-forward relaying in Rayleigh fading with turbo codes" IEEE 2006.

[3]. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in Proc. 46th Ann. Allerton Conf.Communication, Control, and Computing, UIUC, Illinois, Sep. 2008.

[4]. T. Cui, T. Ho, and J. Kliewer, "Memoryless relay strategies for two-way relay channels," IEEE Trans. Commun., vol. 57, no. 10, pp.3132–3143, Oct. 2009.

[5]. Mostafa Dehghan, Dennis L. Goeckel, Majid Ghaderiy, and Zhiguo Ding, "Energy Efficiency of Cooperative Jamming Strategies in Secure Wireless Networks," IEEE Trans.Commun, vol.54, no. 10, jan. 2010.

[6]. J. Barros and M. R. D. Rodrigues "Secrecy capacity of wireless channels," in Proc. IEEE Int. Symp. Information Theory, Seattle, WA, Jul. 2006.

[7]. Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp.2470–2492, Jun. 2008.

[8]. P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[9]. Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in Proc. IEEE Int. Symp. Information Theory,Seattle, WA, Jul. 2006.

[10]. Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 976–1002, Mar.2008.