A Hybrid Scheme For Secure Two-Way Cooperative Networks

First Author
MS Suresh Reddy
Student, Department of Computer Science and Engineering,
Marri Laxman Reddy Institute of Technology, Dundigal,
Hyderabad, Andhra Pradesh, India.

Second Author
P Dayaker
Assistant Professor, Department of Computer Science and Engineering,
Marri Laxman Reddy Institute of Technology, Dundigal,
Hyderabad, Andhra Pradesh, India.

Abstract - In wireless networks security is a concern as eavesdroppers can access information illegally. Intentional interference to eavesdroppers can degrade the effect of eavesdropper on wireless network. When a node can act as relay node and jammer node, the problem of eavesdropping can be handled effectively. Recently Chen et al. proposed schemes which for securing two-way relay networks. In this scheme some intermediary nodes are chosen to ensure security. This kind of node can perform two duties. They are relaying information for effective communication and also enhancing security of the network by acting as jammer to degrade the impact of the eavesdropper. In this paper we implemented that scheme practically in Microsoft .NET platform. We built a prototype application to demonstrate the proof of concept. The experiments made using our custom simulator reveal that the jamming model outperforms the traditional non-jamming schemes.

Keywords - Jamming, relation section techniques, two-way relay networks

1. INTRODUCTION
Wireless networks are vulnerable to attacks. Traditionally cryptographic methods are used at higher layers to protect networks. The fundamental security issues in wireless networks were focused by Wyner [1] which focused on building secure communications without the need for private keys. Security at physical layer has been given importance in research of late. Later on in [2], [3], [4], [1] the security mechanisms proposed by Wyner were extended in order to send messages over wireless media confidentially. Many cooperative jamming schemes were explored in [5], [6], and [7] in order to enhance security of wireless networks. For peer to peer networks and cellular networks recently two-way relay channels are used [8], [9], and [10]. It is found that the performance of a network can be improved by using jammer and relay selection, especially in cooperative networks. The relay selection scheme was also explored in [11] with multiple relays. The results revealed that it exhibited increase in worse receive signal – to – noise ratio. One way cooperative networks were explored in [12] with many relay selection techniques. Though there were many security mechanisms based on physical layer, there is less research on the two-way cooperative relay networks.

This paper implements a scheme that protects network from eavesdropper in a two-way cooperative networks that contain many intermediate nodes for forwarding data, one eavesdropper and two sources. Some intermediate nodes
act as jamming nodes that generate interference to the links used by eavesdropper so as to protect network from them. In order to ensure security to data many selection algorithms are proposed. We also built a prototype application that simulates the proof of concept. The simulations revealed that the proposed scheme improve the security of the network. The remainder of the paper is organized as follows. Section II presents the problem statement and various selection techniques proposed. Section III presents experimental results while section IV concludes the paper.

2. SYSTEM MODEL AND SELECTION TECHNIQUES

For demonstrating two-way relay networks and joint relay and jammer selection process, we consider very simple network with two source nodes named S1 and S2, a single eavesdropper denoted as E, and multiple intermediary nodes. The intermediate nodes are meant for transmission of data. They strengthen signals and forward packets to destination. Intermediate node can also be used as a jammer. When it is used as jammer, it produces artificial interference to the links used by eavesdropper in order to protect network from him. The sample network and two phases of communication are visualized in figure 1.

As seen in figure 1, the first phase is known as broadcasting phase. In this phase, two source nodes send their data to intermediate nodes. One of the intermediate nodes is selected as jammer. For instance in figure 1, J1 is chosen as jammer which sends interference signals to eavesdropper continuously so as to degrade its effect on the network. However, other nodes do not know the presence of jammer. For this reason the interference also causes the source-relay nodes links to degrade in performance. In phase 2, node R is chosen as relay node while another intermediate node J2 is chosen as jammer node. However, the source nodes are not able to reduce the interference from the jammer. A channel fading environment is assumed in the two phases.

3. SELECTION TECHNIQUES WITHOUT JAMMING

Relay selection techniques without jamming are also explored in the experiments. The techniques include Conventional Selection (CS), and Optimal Selection (OS). Eavesdropper channels are not considered in conventional selection technique. The conventional selection is done as follows.

\[ R^* = \arg \max_{R \in S_{in}} \{ C_{S_1}(R) + C_{S_2}(R) \} \]
\[ \approx \arg \max_{R \in S_{in}} \{ \Gamma_{CS}^1 \cdot \Gamma_{CS}^2 \} \]
\[ = \arg \max_{R \in S_{in}} \left\{ \frac{\gamma_{S_1,S_2}}{\gamma_{R,S_2} + 1} \cdot \frac{\gamma_{S_2,S_1}}{\gamma_{R,S_1} + 1} \right\} \]
\[ \approx \arg \max_{R \in S_{in}} \left\{ \frac{\gamma_{S_1,S_2}}{\gamma_{R,S_2}} \cdot \frac{\gamma_{S_2,S_1}}{\gamma_{R,S_1}} \right\} \]

The optimal selection, on the other hand, considers relay-eavesdropper links in the relay mechanism with specific knowledge. Optimal selection is done as follows.
4. SELECTION TECHNIQUES WITH JAMMING

Many relay selection techniques are discussed in this section. They are optimal selection with jamming (OSJ), optimal switching (OW), and suboptimal selection with jamming (SSJ). The first technique ensures the maximization of secrecy rate nodes S1 and S2.

$$R^* \approx \arg \max_{R \in S_{in}} \left\{ \frac{\Gamma^{OS}_1}{\Gamma^{OS}_2} \cdot \frac{\Gamma^{OS}_{E_2}}{\Gamma^{OS}_{E_1}} \right\}$$

where

$$\Gamma^{OS}_i \approx \frac{\gamma S_i S_i}{\gamma R_i S_i}, \Gamma^{OS}_{E_i} \approx \frac{\gamma S_i E_i + \gamma}{\gamma S_i R_i}$$

Optimal Switching technique is used to improve the performance of network in terms of security. The jamming idea is to introduce internal interferences to eavesdropper so as to reduce their effect. However, the source and relay nodes also have the impact of the interference. To overcome this problem the switching between two models known as OS and OSJ are used. The jammer threshold is computed as follows.

Suboptimal Selection with Jamming technique is developed keeping optimal selection metrics in mind.

When the knowledge about the links is not available, SINRs are computed as follows.

$$\Gamma^{E_i}_E = \frac{E[\gamma S_i E]}{E[\gamma S_i E] + E[\gamma J_i E] + 1}$$

5. EXPERIMENTAL RESULTS

Experiments are made with relay selection techniques with and without jamming. The techniques used for experiments include OS (Optimal Selection), CS (Conventional Selection), SSJ (Suboptimal Selection with Jamming), OSJ (Optimal Selection with Jamming), and OW (Optimal Switching).

As can be seen in figure 1, the horizontal axis represents transmitted power (Ps) while the vertical axis represents ergodic secrecy rate. The results reveal that SSJ and OSJ provide almost same performance while the best performance is given by OW technique. More details about the techniques can be found in [13].
Fig. 2 - Secrecy outage probability vs. transmitted power

As can be seen in figure 2, the horizontal axis represents transmitted power (Ps) while the veridical axis represents secrecy outage probability. The results reveal that the selection schemes with jamming outperform the selection schemes without jamming.

Fig. 4 – Ergodic secrecy rate vs. transmitted power (relays are close to S1)

As can be seen in figure 4, the horizontal axis represents transmitted power (Ps) while the veridical axis represents ergodic secrecy rate. The results reveal that the OSJ and SSJ are inefficient while the OW outperforms other techniques.

CONCLUSIONS

In this paper we studied two way cooperative networks and the relay selection issues with security constraints. The network supports opportunistic selection of a relay node for data transmission and two jamming nodes that can protect network from eavesdroppers. The relay node enhances communication between two nodes in the network. The jamming nodes on the other hand are responsible to jam traffic coming from eavesdroppers. The eavesdroppers thus could not successfully perform their malicious activities as the intentional interference from jamming nodes does not allow them to do so. We built a prototype application to demonstrate the proof of concept and found that the jamming is an effective solution to protect networks from eavesdroppers. The prototype works in two modes such as jamming mode and non-jamming mode thus making use of advantages of both modes. The experiments revealed that highest secrecy rate is possible with the proposed system.

REFERENCES


About the authors

1. MS Suresh Reddy

Student, Department of Computer Science and Engineering, Marri Laxman Reddy Institute of Technology, Dundigal, Hyderabad, Andhra Pradesh, India

2. P Dayaker received his M.Tech (Software Engineering) in 2010 from JNTU, Hyderabad, India. Now he is working as Assistant Professor in Dept.of CSE in MLR Institute of Technology, Hyderabad, A.P., India. He has more than 4 years experience in academics. He published a paper in International Journal on Network Protocols