RESEARCH ARTICLE OPEN ACCESS

Joint Relay and Jammer Selection for Secure Two-Way Relay Networks

Prof. Ms. Gulnaz Thakur[1], Prof. Trupti Dhumal[2], Prof. Ms. Ifra Kaladgi[3]
Prof. Ms. Asiya Khan[4]
Department of Computer Science and Engineering[1,3 & 4]
BMIT Solapur, India
Department of Computer Science and Engineering[2]
SSPM Polytechnic
Barshi, India

ABSTRACT

In this paper, we investigate joint relay and jammer selection in two-way cooperative networks, consisting of two sources, one eavesdropper, and a number of intermediate nodes, with secrecy constraints. Specifically, the proposed schemes select two or three intermediate nodes to enhance security against the malicious eavesdropper. The first selected node operates in the conventional relay mode and assists the two sources to exchange data with each other in the amplify-and-forward protocol. The second and third selected nodes are used in different communication phases as jammers in order to create intentional interference upon the eavesdropper. We find that in a scenario where the relay and jamming nodes are randomly and sparsely distributed, the proposed schemes with cooperative jamming outperform the conventional non-jamming schemes within a certain transmitted power range. We also find that, in a scenario where the intermediate nodes gather as a close cluster, the cooperative jamming schemes may be less effective than their non-jamming counterparts. Therefore, we introduce a hybrid scheme to switch between jamming and non-jamming modes. Simulation results validate our theoretical analysis that the hybrid switching scheme further improves the secrecy rate.

Keywords:- Eaves Dropper, Jammer, Joint Relay.

I. INTRODUCTION

Traditionally, security in wireless networks has been mainly focused on higher layers using cryptographic methods. Pioneered by Aaron Wyner's work, which established fundamental results of creating perfectly secure communications without relying on private keys, physical layer based security has drawn increasing attention recently. Later work in studied the secrecy capacity of the Gaussian wiretap channel, and extended Wyner's approach to the transmission of confidential messages over the broadcast and wireless fading channels. In, several cooperative jamming schemes were investigated for different scenarios to increase the secrecy capacity of networks with secrecy constraints. Recently, two-way relay channel has been well studied for its potential application to cellular networks and peer-to-peer networks. In a cooperative network, the efficiency of relay or jammer selection has a great impact on the performance of the whole system. In, a relay selection scheme was proposed for two-way networks with multiple relays, which maximized the worse receive signal-to-noise ratio (SNR) of the two sources. In, several relay selection techniques were proposed in one-way cooperative networks with secrecy constraints. Although cooperative networks have received much attention by far, the physical layer security issues with secrecy constraints in two-way relay networks have not yet been well investigated.

This paper proposes a scheme which can implement information exchange against eavesdroppers in two-way cooperative networks, consisting of two sources, one eavesdropper, and a number of intermediate nodes, with secrecy constraints. Specifically, an intermediate node is selected to operate in the conventional amplify-and-forward (AF) relay mode and assists the sources to deliver data to the corresponding destinations. Meanwhile, another two intermediate nodes that perform as jamming nodes are selected and transmit artificial interference in order to degrade the eavesdropper links in the first and second phase of data transmission, respectively. The principal question here is how to select the relay and the jamming nodes in order to increase information security and protect the source message against eavesdroppers. Several selection algorithms are then proposed, aiming at promoting the assistance to the sources and the interference to the eavesdropper. The analysis and simulation results reveal that the proposed techniques with cooperative jamming can improve the secrecy rate of the system by a large scale within a certain transmitted power range. However, in some special scenarios, the proposed jamming schemes are less efficient than the non-jamming ones.

Then we propose a hybrid scheme with intelligent switch mechanism between the jamming and non-jamming modes, which can overcome this problem.

II. EXISTING SYSTEM

In Existing System, we use one way co-operative network transmission. The nodes to be operate in the conventional relay mode and a number of intermediate nodes to be transmitted the signal, sometimes eavesdropper could be crash the transmission to hack the file.

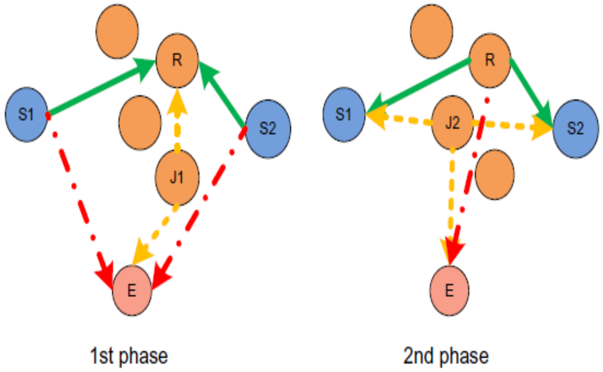
Disadvantages:

1. Low Network Capacity.
2. Malicious Eaves Dropper

III. PROPOSED SYSTEM

In proposed system, we use two-way cooperative network transmission. A number of intermediate nodes with secrecy constraints transfer the files with enhance security against the malicious eavesdropper and to exchange the data with the amplify-and-forward protocol.

In cellular network, and peer-to-peer network efficiency performance of the whole system. In a relay selection scheme was proposed for two-way networks with multiple relays, which maximized the worse receive signal-to-noise ratio (SNR) of the two sources.



IV. MODULES DESCRIPTION

1. Two Ways Co-Operative network
2. Conventional selection without jamming
3. Optimal Switching
4. Optimal Switching with jamming
5. Simulation Results

Two ways Co-Operative Network

In this module, we can implement information exchange against eavesdroppers in two-way cooperative networks, consisting of two sources, one eavesdropper, and a number of intermediate nodes, with secrecy constraints.

Specifically, an intermediate node is selected to operate in the conventional amplify-and-forward (AF) relay mode and assists the sources to deliver data to the corresponding destinations.

Meanwhile, another two intermediate nodes that perform as jamming nodes are selected and transmit artificial interference in order to degrade the eavesdropper links in the first and second phase of data transmission, respectively

Conventional selection without jamming

In this module, in a conventional cooperative network, the relay scheme does not have a jamming process. The conventional selection does not take the eavesdropper channels into account and the relay node is selected according to the instantaneous signal – to- noise ratio (SNR) of the links between *S*ource 1 to *S*ource 2.

Optimal Switching

In this module, the original idea of using jamming nodes is to introduce interference on the eavesdropper links. However, it simultaneously degrades the links between the relay *R* and the destinations. In some specific situation is close to one destination, continuous jamming may decreases secrecy seriously, and acts as a bottleneck for the system. In order to overcome this problem, we introduce the idea of intelligent switching between

Optimal Switching with jamming

In this module, the optimal selection with jamming assumes knowledge set and ensures a maximization of the sum of instantaneous to defined as the overall signal -to-interference-and-noise-ratio (SINR) of the channel The overall secrecy performance of the system is characterized by the ergodic secrecy rate that is the expectation of the sum of the two sources' secrecy rate for different types of channel feedback.

Simulation Results

The intermediate nodes spread randomly within the square space. It is clear that selection with jamming outperform their non-jamming counterparts within a certain transmitted power range. Outside this range the secrecy rate of OSJ converges to a power-independent value. Whereas the ergodic secrecy rate of OS continues to grow with a slope. This validates the analysis the suboptimal scheme SSJ performs almost the same as the optimal scheme OSJ. Furthermore, it can be seen from that OW provides better performance than any other selection techniques with or without continuous jamming. Within this configuration, we also compare the performance of different selection techniques measured by secrecy outage probability.

V. SYSTEM REQUIREMENT

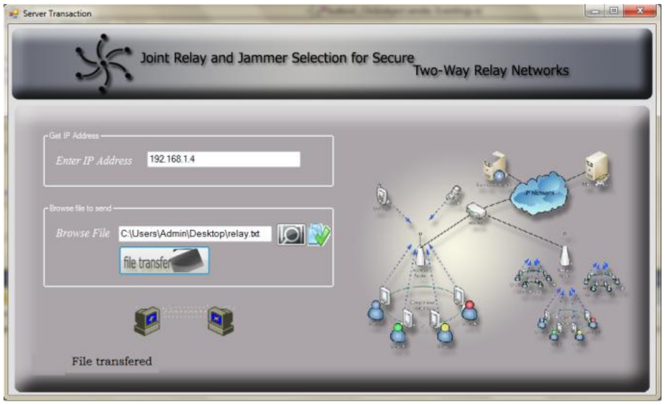
Hardware Requirements:

○	System	:	Pentium IV 2.4 GHz.
○	Hard Disk	:	40 GB.
○	Floppy Drive	:	1.44 Mb.
○	Monitor	:	15 VGA Color
○	Mouse	:	Logitech.
○	Ram	:	512 Mb.

Software Requirements:

○	Operating system	:	Windows 7 Ultimate.
○	Coding Language	:	C#.Net

Screen Shots:



Enter IP Address 192.168.1.4

Browse File C:\Users\Admin\Desktop\relay.txt

File transfered

VI. CONCLUSION

This paper has discussed relay selection issues in two-way cooperative networks with secrecy constraints. The proposed scheme enables an opportunistic selection of one conventional relay node and two jamming nodes to increase security against eavesdroppers based on both instantaneous and average knowledge of the eavesdropper channels. The selected relay node helps to enhance the information transmission between the two sources via an AF strategy, while the jamming nodes are used to create intentional interference at the eavesdropper. We found that jamming is effective solutions within a certain transmitted power range for scenarios with sparsely spreading relay/jamming nodes. The proposed hybrid scheme which switches intelligently between jamming and non-jamming modes is efficient in providing the highest secrecy rate in almost the whole transmitted power regime in two-way cooperative networks.

REFERENCES

[1] User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.

[2] Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.

[3] Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.

[4] Data Communications and Networking, by Behrouz A Forouzan.

[5] Computer Networking: A Top-Down Approach, by James F. Kurose.

[6] Operating System Concepts, by Abraham Silberschatz.

[7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[8] “The apache cassandra project,” http://cassandra.apache.org/.

[9] L. Lamport, “The part-time parliament,” ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.

[10] N. Bonvin, T. G. Papaioannou, and K. Aberer, “Cost-efficientand differentiated data availability guarantees in data clouds,” in Proc. of the ICDE, Long Beach, CA, USA, 2010.

[11] O. Regev and N. Nisan, “The popcorn market. online marketsfor computational resources,” Decision Support Systems, vol. 28, no. 1-2, pp. 177 – 189, 2000.

[12] A. Helsinger and T. Wright, “Cougaar: A robust configurable multi agent platform,” in Proc. of the IEEE Aerospace Conference, 2005.

[13] J. Brunelle, P. Hurst, J. Huth, L. Kang, C. Ng, D. C. Parkes, M. Seltzer, J. Shank, and S. Youssef, “Egg: an extensible and economics-inspired open grid computing platform,” in Proc.of the GECON, Singapore, May 2006.

[14] J. Norris, K. Coleman, A. Fox, and G. Candea, “Oncall: Defeating spikes with a free-market application cluster,” in Proc.of the International Conference on Autonomic Computing, New York, NY, USA, May 2004.

[15] C. Pautasso, T. Heinis, and G. Alonso, “Autonomic resource provisioning for software business processes,” Information and Software Technology, vol. 49, pp. 65–80, 2007.

[16] A. Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler,H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, “Web services on demand: Wsla-driven automated management,”IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004.

[17] M. Wang and T. Suda, “The bio-networking architecture: a biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications,” in Proc.of the IEEE Symposium on Applications and the Internet,2001.

[18] N. Laranjeiro and M. Vieira, “Towards fault tolerance in web services compositions,” in Proc. of the workshop on engineering fault tolerant systems, New York, NY, USA,2007.

[19] C. Engelmann, S. L. Scott, C. Leangsuksun, and X. He,“Transparent symmetric active/active replication for service level high availability,” in Proc. of the CCGrid, 2007.

[20] J. Salas, F. Perez-Sorrosal, n.-M. M. Pati and R. Jim´enez-Peris, “Ws-replication: a framework for highly available webservices,” in Proc. of the WWW, New York, NY, USA, 2006.