RESEARCH ARTICLE OPEN ACCESS

A Review on Multi-Relay Wireless Data Transmission with Delay Aware Load Balancing

Rohitha R. [1], Sheena N. [2]
Department of Computer Science and Engineering
India

ABSTRACT

In recent years, wireless networks have been commonly used in many applications such as environmental monitoring, health care, security, and so forth. We consider cooperative wireless network consist of source destination and multiple relays. These multiple relays are used to transmit data. Eavesdropping attack is more vulnerable attack in wireless networks transmission. An eavesdropper is an attacker having a powerful receiver antenna, which taps the data from the source and destinations. Now a days many researches are conducting on this topic. This paper studies the analysis of multi-relay data transmission techniques to protect the data and to improve overall performance of the wireless network.

***Keywords* :—** Multi-relay, Eavesdropping, Delay aware load balancing.

I. INTRODUCTION

Wireless network have been receiving much attention recently because most of the transactions are done using mobiles and wireless network. Due to the broadcast nature of wireless medium there exist many potential security threats, legitimate transmission may be tapped by unauthorized users. Data transmissions through wireless networks are not secured because of interception and improper manipulation of eavesdropper. Security is an important aspect for data transmission. There are multiple methods available for data protection in networks. In order to achieve confidential data transmission the most common method used to is cryptographic techniques. In cryptographic method security is based on some secret keys. These methods are not perfectly secure because more advanced technologies are developed to trace the secret keys and eaves dropper can attack the data. Eavesdropper is an attacker which grasps the data from the source and destinations. Physical-layer security is emerging as a promising paradigm against eavesdropping attacks, which relies on exploiting the physical characteristics of wireless channels.

In order to improve transmission security against eavesdropping attacks, multi-relay selection scheme is used. The multi relay selection scheme gives the concept of sending data to destination through multiple relay other than single relay. These papers gives the idea about sending data through multi relays and also evaluate the security performance of multi relay data transmission scheme.

II. RELATED WORKS

M. Elkashlan et .al in [1] “On the security of cognitive radio networks” deals with cognitive wiretap channel and deals with the necessary conditions used to secure the confidential message against eavesdropping. Passive eavesdropping is considered, in which the malicious nodes detect the information by listening to the message transmission in the broadcasting wireless medium. Transmission uses multiple antennas to secure the transmission at the physical layer. In this case secondary transmitter sends confidential messages to the secondary receiver in the presence of eavesdropper. The secondary receiver is equipped with multiple antennas to secure data transmission without the need for a secret key or code. The eavesdropper is also equipped with multiple antennas to promote successful eavesdropping. The channel state information of the eavesdropper’s is not available at the secondary transmitter. In this case perfect secrecy cannot be achieved.

Y. Zou et .al in [2] “Improving physical-layer security in wireless communications through diversity techniques” proposed several diversity approaches to improve wireless physical-layer security, including multiple-input multiple-output, multiuser diversity, and cooperative diversity. Traditionally, diversity techniques are exploited to increase transmission reliability, which also have great potential to enhance wireless security. The first section presents multiple-input multiple-output diversity for physical-layer security. In this system consisting of one source and one destination in the presence of an eavesdropping, all the network nodes are equipped with multiple antennas. To avoid attack, the system increases the capacity of the wireless channel. However, the eavesdropper can also exploit the structure to enlarge the capacity of a wiretap channel from the source to the eavesdropper. To avoid this, an adaptive transmit process should be included at the source node to increase the main channel capacity while decreasing the wiretap channel capacity. The next section presents a cooperative diversity system consisting of one source, M relays, and one destination in the presence of an eavesdropper. In this case the best relay selection is another approach to improve wireless transmission security against eavesdropping attacks. In the best relay selection, a relay node with the highest secrecy capacity is chosen to participate in assisting the signal transmission from source to destination. From M number of relay, there is a dedicated relay that will send the exact data. So the eaves dropper will not get real data.

Vishal K. Shah et .al in [3] “A Review on Relay Selection Techniques in Cooperative Communication” discuss different relay selection techniques and cooperative transmission protocols used in the relay station. Relay selection mechanisms can be divided into two, Depending on the relation between the networks entities. They are cooperative Relay Selection and opportunistic Relay Selection. The overall performance of the network can be effectively improved by using proper relay selection. It is in terms of higher data rate/through put, lower power consumption and better bit error rate performance.

C. Xing et .al in [4] “Robust joint design of linear relay precoder and destination equalizer for dual-hop amplify-and-forward MIMO relay systems” proposed a method called amplify-and-forward (AF) multiple-input multiple-output (MIMO) relay system with single relay. The data from the transmitter will be transmitted to the relay and destination simultaneously. First the source transmits data to the relay. The received signal at the relay is data vector. At the relay, the received signal is multiplied by precoder matrix. Then the resulting signal is transmitted to the destination. Then two robust design algorithms were proposed to minimize the average mean-square error. The first one is an iterative algorithm with its the second one is a closed form solution with much lower complexity compared to the iterative algorithm. Both of the proposed algorithms reduce the sensitivity of the amplify-and-forward multiple-input multiple-output relay systems to channel estimation errors, perform better than the existing algorithm.

Mehdi M. Molu et .al in [5] “Low-Complexity Compute-and-Forward Techniques for Multisource Multirelay Networks” a more improved method for low complexity compute-and-forward techniques is proposed. Cooperative network consisting of K source nodes, K relay nodes and one destination node. The entire transmission from sources to the destination is divided into K + 1 time slots, in the first time slot all the source nodes transmit their data to the destination using a shared interference channel. In a second phase consists of K time slots, the relay nodes each compute an equation from the received signal and forward it to the destination node. Propose two new algorithms blind compute-and-forward and partially coordinated compute-and-forward.

M. Bloch et .al in [6] “Wireless information-theoretic security” presents an idea of two legitimates partners communicate over a quasi-static fading channel. An eavesdropper observes their transmissions through a second independent quasi-static fading channel. Fading is characterized in terms of average secure communication rates and outage probability. Based on analysis, a practical secure communication protocol is developed, which uses a four- step procedure to ensure wireless information theoretic security: common randomness via opportunistic transmission, message reconciliation, common key generation via privacy amplification, and message protection with a secret key. A reconciliation procedure based on multilevel coding and optimized low-density parity check (LDPC) codes is introduced, which allows to achieve communication rates close to the fundamental security limits in several relevant instances.

Zhi Chen et .al in [7] “Compute-and-Forward: Optimization Over Multi-Source-Multi-Relay Networks” proposed transmission protocol, namely, compute-and forward (CPF). This system design compute-and forward based multi-source multicast transmission protocol for the topology with an arbitrary number of relays. Which consists of M sources (S1,. . . , SM), K relays (R1,. . . , RK) and L destinations, as shown in Fig. 1. Each source node or relay node is equipped with one antenna and works in half-duplex mode, i.e., cannot transmit and receive data simultaneously. Compute-and forward based transmission protocol consists of M+1 phases. In Phase 1, all source nodes transmit their messages simultaneously to all the relay nodes. At the end of this phase, each relay node decodes one or more linear equations of the combination of individual transmitted messages from all sources with selected integer coefficient vectors. In all phase relay delivers its decoded function message to all destination nodes. At the end of Phase all the destination nodes decode the function message received and store it. Compute-and forward outperform other relaying strategies, such as decode-and-forward (DF) and amplify-and-forward.

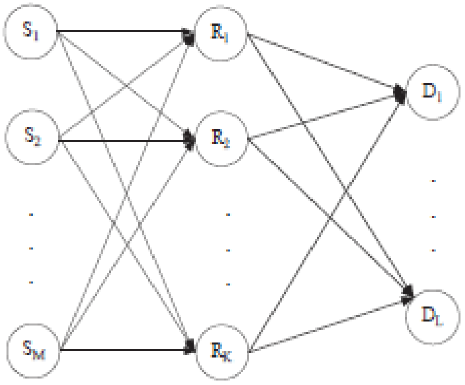

Fig. 1 System model for a multi-source multicast network with the aid of multiple relay nodes

P. K. Gopala et .al in [8] “On the secrecy capacity of fading channels” considers the secure transmission of information over fading channel in the presence of an eavesdropper. They analyze the full Channel State Information (CSI) case, where the transmitter has access to the channel gains of the legitimate receiver and eavesdropper, and the main CSI scenario where only the legitimate receiver channel gain is known at the transmitter. In each scenario, the secrecy capacity is obtained along with the optimal power and rate allocation strategies. This paper deals a non-zero perfectly secure rate is achievable in the fading channel even when the eavesdropper is more capable than the legitimate receiver. It also proposed a low-complexity on/off power allocation strategy that achieves near optimal performance with only the main channel CSI.

III. COMPARISON BETWEEN SINGLE AND MULTIPLE RELAY SELECTION

Cooperative wireless network uses mainly three type of relay selection. They are direct transmission, single relay selection and multi relay selection. It also study the physical-layer security of a cooperative relay network in the presence of an eavesdropper.

A. *Single relay selection*

First consider the direct transmission where data are transmitted directly from the source to the destination. System consist main link for source to destination transmission, wiretap link for source to eavesdropper transmission, as shown in Fig. 2. In this case the data is not secure because only one link is used for transmission. The eavesdropper can easily trace the data.

Single relay selection system consists of one source, destination and multiple relays operating in the presence of eavesdropper. In this type of transmission the system invokes the decode-and-forward (DF) protocol for the relays in forwarding the transmission of source to destination. The system transmit data in the presence of multiple relay, from N number of relay, there is a dedicated relay that will send the exact data. For transmitting data it only use only one relay for the entire transmission Selected relay having the highest capacity between relay and destination.So the eaves dropper will not get real data. Otherwise, if eavesdropper attacks the exact relay which sending actual data then the system will have no effect.

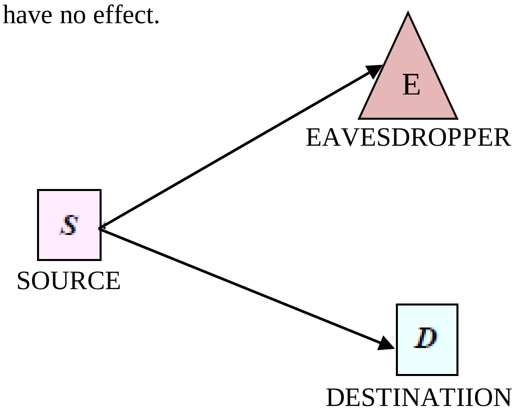

Fig.2 Wireless network comprise of a source(S) and a destination (D) in the presence of an eavesdropper (E)

B. *Multi relay selection*

System consists of one source, destination and multiple relays operating in the presence of eavesdropper, as shown in Fig. 3. Multi-relay selection scheme is used for protecting the data transmission from source to destination against eavesdropping. More specifically, multi-relay selection allows multiple relays to simultaneously forward the source’s transmission to the destination, differing from the conventional single-relay selection where only the best relay is chosen to assist the transmission from the source to destination. Multi relay data transmission uses multiple relay. That is, the actual data is divided into different small data and which is send to destination using multiple relay. The received data is not ordered then it is ordered by using the sequence number in it. By sending data through different relay eaves dropper will not get the complete data from the source. So the outage probability of the system is comparatively higher than previous described systems.

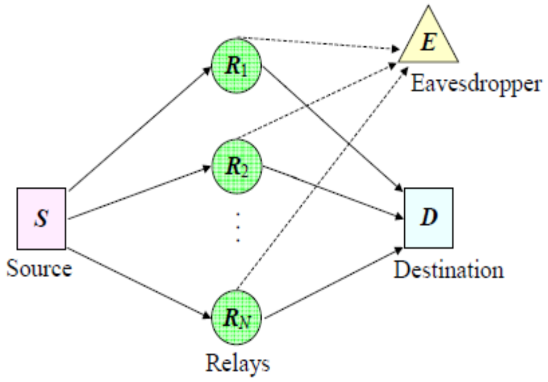

Fig. 3 A cooperative wireless network consisting of one source (S), one destination (E) and NN relays (Rii) in the presence of an eavesdropper (E).

IV. CONCLUSIONS

This paper compares different techniques used in wireless data transmission. This paper studied the relay selection of a cooperative wireless network in the presence of an eavesdropper. Every method has its own advantages and limitations. All methods do not provide complete data security. Since communication through network requires high data security, an efficient and secured method is required. The single-relay and multi-relay selection schemes perform consistently better than all other transmission methods. While using multi relay transmission, packet reordering arises when the packets that arrive at the destination have different order, at destination the received data is ordered using the sequence number in it. To avoid reordering we use delay aware load balancing system. As a future work, combination of multi-relay selection and delay aware load balancing algorithm has to be proposed to improve the security of wireless transmission.

ACKNOWLEDGMENT

I wish to express my sincere gratitude to members of Computer Science and Information Technology department of College of Engineering and Management, Punnapra, for their valuable support and feedbacks. I convey my hearty thanks to my project guide for the moral support, suggestions and encouragement to make this venture a success.

REFERENCES

[1] M. Elkashlan, L. Wang, T. Q. Duong, G. Karagiannidis, and A. Nallanathan, “On the security of cognitive radio networks,” IEEE Trans. Veh. Tech., accepted, Sept. 2014

[2] Y. Zou, J. Zhu, X. Wang, and V. Leung, “Improving physical-layer security in wireless communications through diversity techniques,” IEEE*Network*, vol. 29, no. 1, pp. 42-48, Jan. 2015.

[3] Vishal K. Shah, Anuradha P. Gharge, “A Review on Relay Selection Techniques in Cooperative Communication” IJEIT Volume 2, Issue 5, November 2012.

[4] C. Xing, S. Ma, Y.-C. Wu, “Robust joint design of linear relay precoder and destination equalizer for dual-hop amplify-and-forward MIMO relay systems,” IEEE Trans. Signal Process., vol. 58, no. 4, pp. 2273-2283, Apr. 2010.

[5] Mehdi M. Molu, Kanapathippillai Cumanan, and Alister Burr, “Low-Complexity Compute-and-Forward Techniques for Multisource Multirelay Networks,” IEEE Commun. Lett., Vol. 20, no. 5, May 2016.

[6] M. Bloch, J. O. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[7] Zhi Chen , Pingyi Fan Senior Member, and Khaled Ben Letaief Fellow, “Compute-and-Forward: Optimization Over Multi-Source-Multi-Relay Networks,” arXiv:1406.1081v1 [cs.IT] 4 Jun 2014.

[8] P. K. Gopala, L. Lai, and H. Gamal, “On the secrecy capacity of fading channels ,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698,

[9] Oscar Delgado, IEEE, and Fabrice Labeau, “Delay aware load balancing over multipath wireless networks” IEEE Trans. *Veh. Tech.*, accepted, 2017

[10] Jia Zhu, Yulong Zou, Benoit Champagne,Wei-Ping Zhu, and Lajos Hanzo, “Security-Reliability Trade-off Analysis of Multi-Relay Aided Decode-and-Forward Cooperation Systems”, IEEE Trans. *Veh. Tech.*, accepted,2016.

[11] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, “On secrecy performance of antenna selection aided MIMO systems against eavesdropping,” *IEEE Trans. Veh. Tech.*, accepted, Feb. 2015.

s