Security Reliability Trade off Analysis of Multi-Relay Aided Decode- and -Forward Cooperation Systems with Multiple Destinations

Asha .S
Final Year M Tech Student, Dept. of CSE, Cochin Institute of Science and Technology, Kerala, India

Abstract
We considering a wireless network system having a source, and multiple destinations in the presence of eaves dropper .Eaves dropper is an attacker which taps the data from the source and destinations. The System proposes a multi relay–selection with multiple destinations under a cognitive radio network. The multi relay selection scheme gives the concept of sending data to destination through multiple relay other than single relay. The previous system includes single relays and multiple relay with single source and destination. For better output representation we compare proposed system with previous systems. The previous system includes security reliability trade off to avoid attacking from the eaves dropper. The proposed system sends data through multiple relays and the multiple relays depends on the trust values of the nodes. According to the previous system multi relay selection outperforms better than single relay trade off. In proposed system outperforms previous systems.

Key words
Multi relay, single relay, single relay trade off, trust value, eaves dropper.

1. Introduction

Wireless networks and applications have important role in recent days .Most of the transactions are done using mobiles and wireless network. There multiple methods are available for data protection in networks .The most common method is cryptographic techniques. By using new technologies classic cryptographic techniques can be overcome and eaves dropper can attack the data.

Data protection can be achieved by different levels of protection mechanisms. Physical-layer security is emerging as a promising paradigm against eavesdropping attacks, which relies on exploiting the physical characteristics of wireless channels. The cognitive radio networks works with cognitive wiretap channel and propose multiple antennas to secure the transmission at the physical layer, where the eavesdropper overhears the transmission from the secondary transmitter to the secondary receiver.

According to Wireless Information-Theoretic Security two legitimates partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi- static fading channel, the important role of fading is characterized in terms of average secure communication rates and outage probability. Based on the insights from this 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.

From the previous system physical-layer security of a cooperative relay network in the presence of an eavesdropper, with an emphasis on the security-reliability trade-off (SRT) of cooperative relay communications based on the decode-and forward (DF) protocol without considering the amplify-and forward (AF).

The proposed system gives the idea about sending data through multi relays to single or multiple destinations. The proposed system reviews the previous systems such as direct transmission, single relay transmission and Multi relay transmission and it includes trust value based transmission technology which avoids eaves dropper attack.

2. Related work

A. Direct transmission

The first method considered is the direct transmission where data are transmitted directly to the destination from the source. Fig. 1 depicts a wireless system, where a source (S) transmits its scalar signal xs ([xs | 2] = 1) to a destination (D) at a particular time instant, while an eavesdropper (E) attempts to tap the source's

Manuscript received September 5, 2016
Manuscript revised September 20, 2016

transmission. In line with the physical-layer security literature [2]-[9], E is assumed to know the encoding and modulation schemes as well as the encryption algorithm and secret key of the S-D transmission, except for the source signal xs.When S transmits xs at a power of P, we can express the received signal at D as

$$y_d = h_{sd}\sqrt{P}x_s + n_d$$

where *h*sd is the fading coefficient of the S-D channel and nd is the AWGN at D. The transmission of S can be overheard by E and the corresponding received signal is written as

$y_e = h_{se}\sqrt{P}x_s + n_e$

where *h*se is the fading coefficient of the S-E channel and ne represents the AWGN at E.

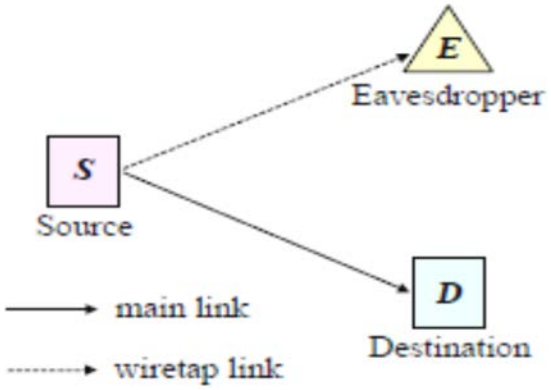

Figure 1: A wireless network comprise of a source(S) and a destination (D) in the presence of an eavesdroppe (E)

In this transmission Rayleigh fading model is considered.

B. Single –relay selection

In this type of transmission the system invokes the decode-and-forward (DF) protocol for the relays in forwarding the transmission of S to D. More specifically, S first broadcasts xs to the N relays, which attempt to decode xs. Given N relays, there are 2N possible relays.

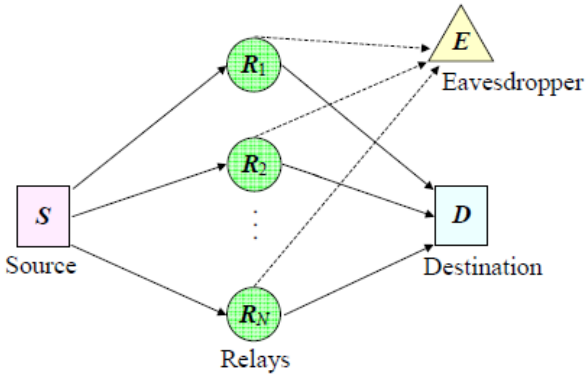

Figure 2: A cooperative wireless network consisting of one source (S), one destination (E) and *N* relays (R*i*) in the presence of an eavesdropper (E).

Considering that S broadcasts *xs* to N relays at a power of P, the received signal at a specific relay Ri is expressed as

$$y_i = h_{si}\sqrt{P}x_s + n_i$$

where hsi is the fading coefficient of the channel spanning from S to Ri and nI is the AWGN at Ri.

Meanwhile, given that the selected relay transmits xs at a power of P, the signal received at E is written as

$$y_e = h_{be}\sqrt{P}x_s + n_e$$

where hbe is the fading coefficient of the channel spanning from the "best" relay to E.

From N number of relay, there is a dedicated relay that will send the exact data. 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.

C. Multi-relay selection

In this transmission all the relays used simultaneously for data transmission from source to destination. That is, the actual data is divided into different small data and which is send to destination and the received data is ordered using the sequence number in it.

The N relays simultaneously transmit xs using a weight vector w, the signal received at D is written as

$$y_d^{multi} = \sqrt{P}w^T h_d x_s + n_d,$$

where $h_d = [h_{1d}, h_{2d}, \cdots, h_{|Dn|d}]^T$.

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. Thes all works are done with cognitive network.

3. Proposed system

A. Multi-relay selection with multiple Destinations

Trust is always defined by reliability, utility, availability, risk, quality of services and other concepts. Here, trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviors. That is, the trust value is used to reflect whether a sensor node is willing and able to act normally in WSNs. In this paper, a trust value ranges from 0 to 1. A value of 1 means completely trustworthy and 0 means the opposite.

Direct trust is a kind of trust calculated based on the direct communication behaviors. It reflects the trust relationship between two neighbor nodes.

Recommendation trust. As mentioned above, since the recommendations from third parties are not always reliable, we need an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust. When a subject node cannot directly observe an object nodes' communication behaviors, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes. we can conclude that there are three main properties of trust: asymmetry, transitivity and composability. Asymmetry implies that if node A trusts node B, it does not necessarily mean that node B trusts node A. Transitivity means the trust value can be passed along a path of trusted nodes. If node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a certain level. The transitivity is a very important property in trust calculation between two non-neighbor nodes. Composability implies that trust values received from multiple available paths can be composed together to obtain an integrated value.

The system proposes cognitive radio network, where the source node sends data to multiple destinations through multi-relays. That is, source sends data to the destinations when the single data is divided into small data packets and sends with different relays. Each relay will carry the different data. Here the network assigns a trust value for each node. When sending the source node evaluates the trust value of each relay node, the data will send through relay with high trust vales. The trust value is the ratio between received packet to send packet from that node.

Trust value=received packet/send packet

At the same source and destination check the distance to each relay. Relay node with lower distance from source and destination will taken for data transmission. This system achieves better packet deliver ratio than the previous system. And final throughput will be high.

4. Performance evaluation

From the implementation it shows the simulation of the proposed system. Using simulation, which shows a co-operative network. Each node in the network got assigned with a trust value and eavesdropper also has a trust value. The multi relay will select node having trust one .So the attacker will not be selected as a relay node because which has trust value less than 1.

The figure-3 shows the multirelay with multiple destinations. where relay includes nodes with trust value one.

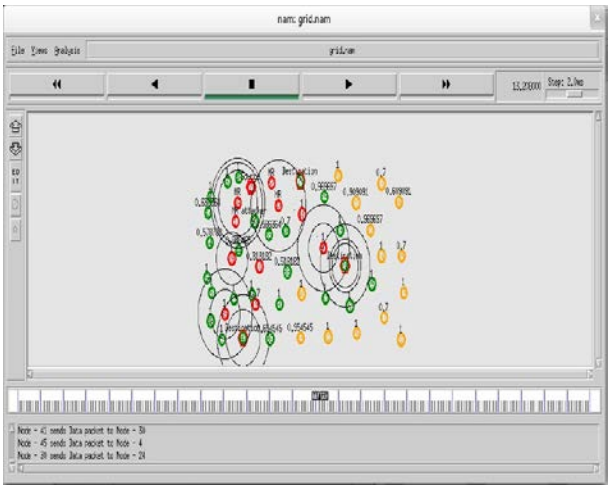

Figure 3:Multi-relay with multiple destinations

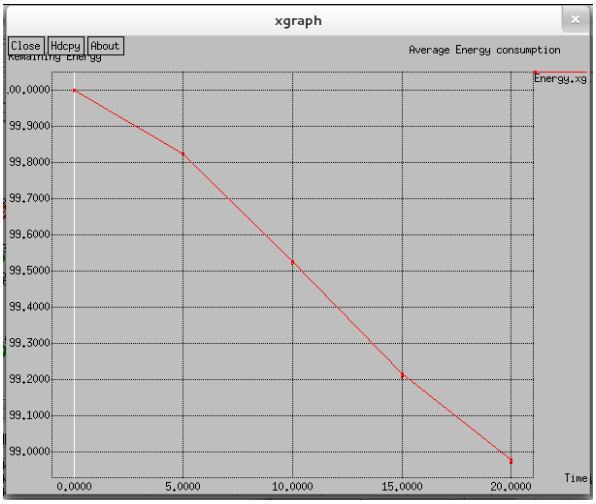

Figure 4: average energy consumption

From Figure-4 it is clear that average energy consumption is low for the proposed system.

Figure-5 shows the drop in the system where drop is zero, which means systems have no drop.

Figure-6 shows the packet delivery ratio in the system where packet delivery ratio is one, which means systems send the complete data.

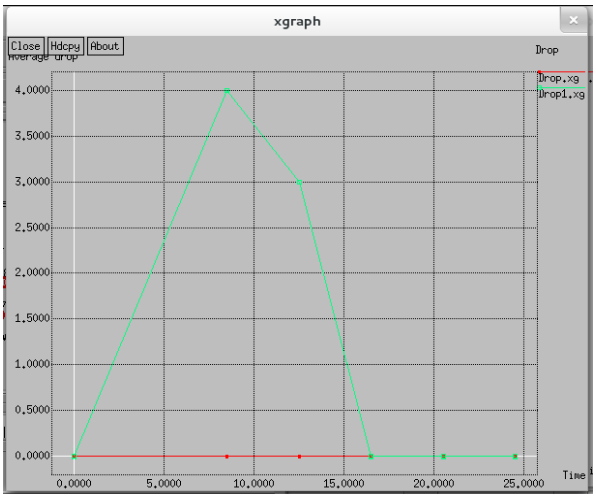

Figure 5: Xgraph of Drop in the system

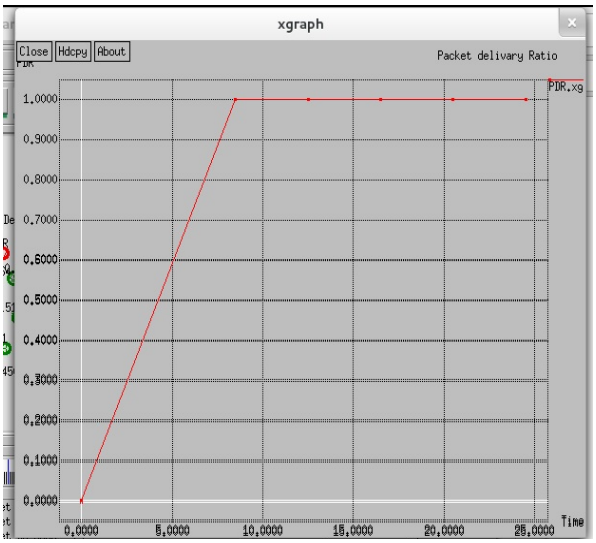

Figure 6: Packet delivery ratio.

5. Result and conclusion

In this paper, we studied the relay selection of a cooperative wireless network in the presence of an eavesdropper and proposed the multi-relay selection scheme with multiole destinations. The system refers the direct transmission, Single relay selection and multi-relay selection. From this study it shows sending data with multiple destinations in the presence of an eavesdropper can be achieved by sending data through multi-relays and trust value.

Finally, the system improves the reliability and throughput with trust value of each node in the relay.

References

[1] Security-Reliability Trade-off Analysis of Multi-Relay Aided Decode-and-Forward Cooperation Systems,Jia Zhu, Yulong Zou, Senior Member, IEEE, Benoit Champagne, Senior Member, IEEE, Wei-Ping Zhu, SeniorMember, IEEE, and Lajos Hanzo, Fellow, IEEE

[2] 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.

[3] G. Ding, J. Wang, Q. Wu, et al., "Robust spectrum sensing with crowd sensors," IEEE Trans. Commun., vol. 62, no. 9, pp. 3129-3143, Sept. 2014.

[4] 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.

[5] J. Ni, K.-K. Wong, Z. Fei, C. Xing, H. Chen, K.-F. Tong, and J. Kuang, "Secrecy-rate balancing for two-user MISO interference channels," IEEE Wirel. Lett., vol. 3, no. 1, pp. 6-9, Feb. 2014.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451-456, Jul. 1978.

[7] 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.

[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, Oct. 2008.

[9] 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.

[10] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," IEEE J. Select. Areas Commun., vol. 32, no. 11, pp. 2222-2236, Nov. 2014.