ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 4, March 2016*

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

The Scope of Trust Calculation in Single and Multi-relay selection for Reliable Cognitive Radio Networks

Hima Anna Thomas[1], Sajan Xavier[2]

PG Student [AECS], Dept. of ECE, NCERC, Thiruvilwamala, Thrissur, India[1]

Assistant Professor, Dept. of ECE, NCERC, Thiruvilwamala, Thrissur, India[2]

ABSTRACT: In this paper, the effective method for security improvement in cognitive radio networks, the relay selection methods are discussing. Among relay selection the number of relays participating in secondary transmission acts a vital role. The multi-relay relay selection methods can be treated as the most appropriate method that provides maximum security and reliability in CR (cognitive radio) networks. The existing single and multi relay selection is based on the capacity of the channel towards the destination without affecting the eavesdropper channel capacity adversely or favorably. But the usage of trust calculation to identify the relay elements in multi-relay or single relay selection will reduce the chances of packet drop and adding more security and reliability features. In this paper the existing relay selection schemes are simulated with network simulator NS2 and the quality determining parameters are compared with trust based relay selection method's simulation results for proving the scope of trust in these relay selection methods.

KEYWORDS: Cognitive radio, relay selection, secondary transmission, trust

I. INTRODUCTION

Cognitive radio network is vulnerable to most of the security attacks due to its open nature. The prime feature of cognitive radio is the spectrum allocation to the secondary users according to the spectrum occupancy by primary users. The malicious nodes in the network will contaminate this spectrum data and lead to the packet loss and total collapsing of the network security. Trust calculation is a method of finding the reputation or degree of acceptance of a particular node in a wireless ad-hoc network, which is based on the past history or previous deeds of the communicating nodes. Trust based methods have wide acceptance in cognitive radio network. The application of trust value will increase the security in different aspects of a cognitive radio environment

In this paper, discussing about one of the best relay selection method. This existing best relay selection includes single relay selection and multiple relay selection. In single relay selection as the name indicates only one among the N elements of the relay set is utilized for decode and forwarding the signal or data packet to the destination. But in multi-relay selection a set of relay elements are selected for the decoding purpose. The existing method is showing a higher security-reliability trade off as seen in [1]. The scope of trust calculation and the selection of relay elements based on the trust value is the main concern of this paper. The proposed technique is presented with the help of performance comparison of with and without trust using relay selection.

II. EXISTING SYSTEM

Cognitive radio is a new incarnation in wireless communication networks with the efficient utilization of available frequency spectrum. The single and multi-relay selection schemes with good security – reliability trade-off proposed in [1] is considering here as the existing system for this paper. A cognitive radio network is becoming effective with the proper cooperation between primary (licensed) users and secondary (unlicensed users). To maintain this balanced usage of frequency spectrum, the spectrum occupancy details of the network is available to the secondary network elements. This channel occupancy details are misused by the adversary. Various types of security attacks like spectrum sensing data falsification, forged MAC control frames, primary user emulation attacks etc are the results of this open nature of cognitive radio network. This security attacks lead to loss of credibility and leads to more researches on the field of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 4, March 2016*

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

security improvement. The major challenge in security improvement task is to select the most appropriate secondary users at the most suitable time without disturbing the primary user communication as well as ensuring quality secondary transmission. Relaying is one of the best techniques used in CR network to improve both quality and secrecy of the signal transmission.

The system model includes a network contains secondary transmitter (ST), secondary destination (SD) and N number of secondary relays in the presence of an eavesdropper (E)[1]. The relaying technique will divide the path between source and destination into two separate channels. One channel is from ST to SR (secondary relay) and another one is from SR to SD. Also the presence of eavesdropper creates a channel from SR to E. In single relay selection from the available SRs only one SR which is having the highest channel capacity towards SD than towards E is designated as the best relay. This best relay is utilized for transmitting towards SD. In multi-relay selection scheme a set of N relay elements are utilized for transmitting towards the destination where the selection of the best relay set is based on some weight factor. In both the methods the relay selection is utilizing the CSI (channel state information) of the SD without need of eavesdropper CSI. As the number of relay elements increases the security level also increases. Both the methods showing good security and reliability balance[1]. But both the methods are aiming at increasing the capacity of the SR-SD channel capacity without increasing or decreasing the capacity of SR-E channel.

III. SCOPE OF TRUST CALCULATION

The security challenges in cognitive radio networks occur mainly due to the dynamic spectrum access technology which is an inherent nature of it. The occupancy or vacancy of the primary users over the frequency channels is not based on any predefined conditions. By cognitive radio network, primary users are actually giving the opportunity for the secondary users to use their frequency channels when they are not using them. The efficient spectrum usage is the result of this opportunistic spectrum sharing. But this dynamic spectrum allocation makes some undesirable security threats along with its good results. That is the main reason for the security attacks at different layers of communication in cognitive radio networks. Some of the security attacks can be described like below.

The objective of the adversary is to use the licensed frequency bands for their malicious activities. The adversary may cause jamming the cognitive radio transmission by sending wrong and incorrect channel details. The tapping of the transmitted data between the primary users may be also the attacker's aim. Primary user emulation attack (PUE) is one of the important physical layer security attacks. The attacker mimics the primary user activities and this makes secondary users think like that frequency bands are occupied by primary users. So they cannot access the channels even the primary users are actually unoccupied. The PUE attack can be of malicious or selfish type depending upon the nature of attacker. Attackers may also manipulate spectrum sensing data and send it to fusion center, which leads to incorrect channel state perception by the secondary users. This type of attack is spectrum sensing data falsification (SSDF). The malicious users generate incorrect parameters and these are taken as input for objective function by secondary users. The secondary users may end up in an objective function which provides least security level, to make the attacker intervention easier [2][3].

Relay selection methods have high impact on reliability and security of CR networks. Multi-relay selection is having highest performance at the cost of high complexity of synchronization process[1]. The relay selection methods are only focused on increasing the capacity of the channel towards the receiver without increasing or decreasing the eavesdropper channel capacity. But usage of the trust calculation for the relay nodes will enable the relay selection methods perform much better due to the following features of trust calculation as seen in [4].

- Trust calculation have the power of resisting attacks such as forging, united fraud and SSDF.
- It is a continuous process of calculating the trust value.
- Calculation of trust is followed by rewarding the best resources to the trusted one and avoiding the malicious one by giving suitable punishment.

The trust value calculation has various levels of application in cognitive radio networks. It is a method of finding the reputation or degree of acceptance of a particular node in a wireless ad-hoc network. The trust determination is based on the past history or previous deeds of the communicating nodes. Trust calculation can be done by considering the number of packets send and received by the relay nodes. The simulation of the existing relay selection are done using NS2 network simulating tool. The trace file is a record of all events occurred during the simulation time. The recorded details in this trace file are used for the calculation of trust in the proposed method. Based on the trust value the source can identify the best one and have the privilege of providing more resources like transmit power, more data packets etc.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 4, March 2016*

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

Analyzing various methods for security and quality improvement in cognitive radio networks, relay selection methods have found more effective.

The proposed method of relay selection is the application of scope of trust value calculation in single and multi-relay selection schemes. Multi-relay selection is showing better results than single-relay[1], so the multi-relay method is chosen with high priority. Since multiple number of relays are simultaneously transmitting to the destination the synchronization problem can consider as complexity of multi-relay selection scheme[1]. But high ST-SD channel capacity can consider as inevitable and this feature makes multi-relay selection usage is common in cognitive radio communication networks.

IV. RESULTS AND DISCUSSIONS

The scenario of single relay selection and multi-relay selection are simulated using network simulator tool NS2. NS2 Simulator generates a tcl (Tool Command Language) file. On running the tcl file, it results into two different files, first the trace file which contains all the information about the network and second the network animator file (NAM) which is a visual aid showing how packets flow along the network and shows the virtualization of the network according to the trace file. A 40 node sized network is considered for simulation. The following are the comparison of the relay selection methods with and without trust calculation. The comparing graphs are showing the expected performance improvement of trust application.

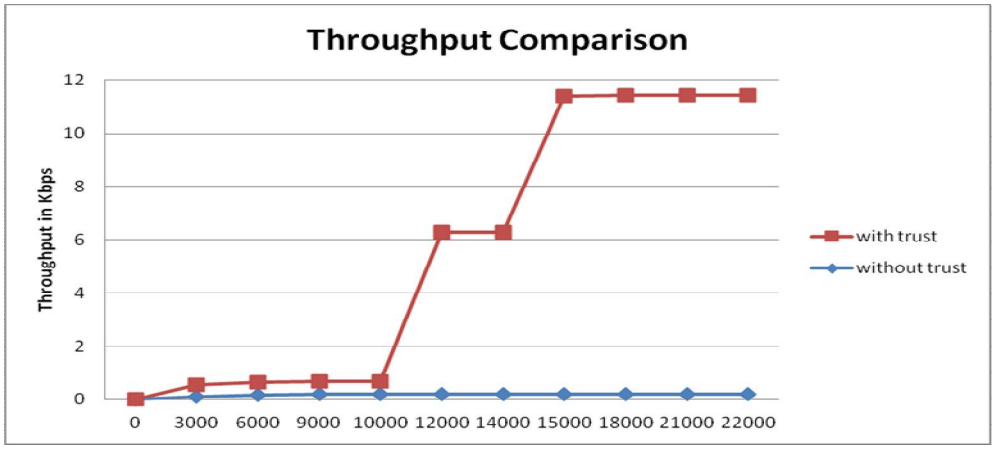

Fig 1. Throughput of receiving packets Vs Simulation time.

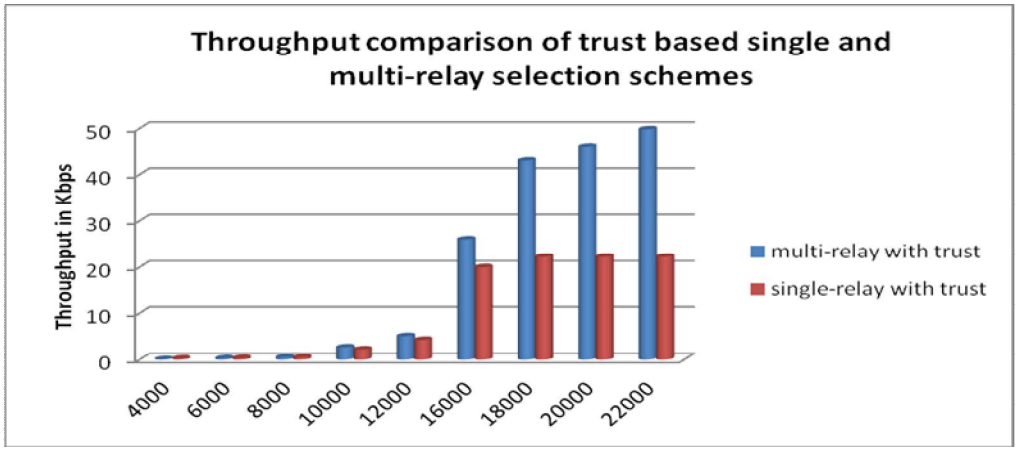

Fig 2. Throughput of receiving packets of single and multi relay selection Vs Simulation time.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 4, March 2016*

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

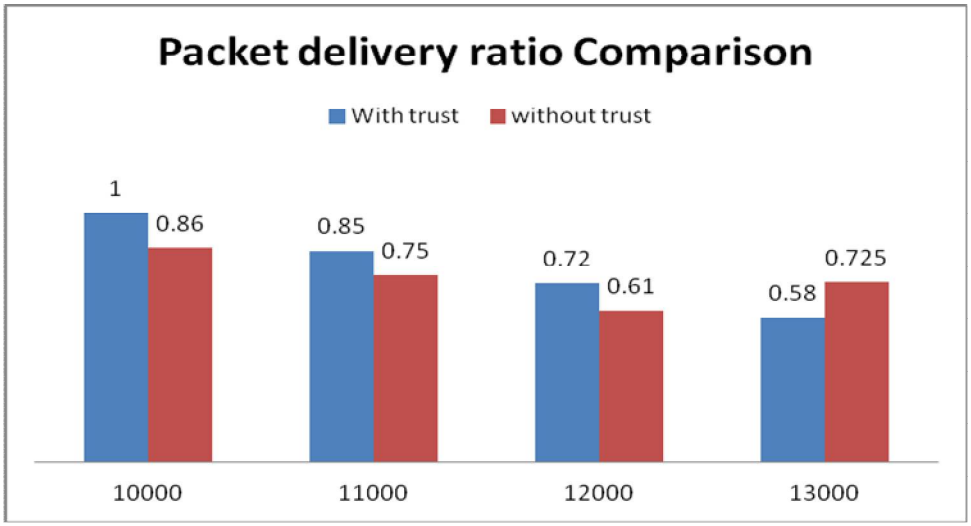

Fig 3. Packet delivery ratio at each instant of simulation time

In the Fig 1, the throughput values of the receiving data packets at the destination are recorded for the relay selection methods with trust calculation and without trust calculation. The throughput values are noted for some particular instances of simulation time. In fig 2, the throughput values of the receiving data packets at the destination are recorded for single and multi-relay selection methods with trust calculation. Multi-relay selection method is always showing a performance improvement when comparing to direct transmission and single relay selection methods. The trust value calculation is done using the information regarding the data packet transmission by nodes. These required details of trust calculation can be obtained from the trace file generated. Fig 3 is the representation of packet delivery ratio improvement by the trust based method in the form of bar diagram. These graphs are showing the performance improvement of the relay selection schemes with the application of trust calculation.

V. CONCLUSION

The scope of application of trust based relay selection in single and multi-relay selection methods in cognitive radio networks are emphasised in this paper with the comparison graphs. The trust based relay node selection will help to avoid the packet loss, black hole attack etc. Application of trust based relay selection has given simulation results showing the scope of trust in a reliable-secure relay selection method. The future work of this paper is to apply this scope of trust in a multi-destination transmission. The research on application of trust calculation on the mentioned future work is under progress by the authors.

REFERENCES

[1] Yulong Zou, Benoit Champagne, Wei-Ping Zhu, and Lajos Hanzo “Relay-selection improves the security-reliability trade-off in cognitive radio systems, IEEE transactions on communications, vol. 63, no. 1, pp. 215-228, Jan 2015.

[2] Wassim El-Hajj, Haidar Safa, Mohsen Guizani,” Survey of security issues in cognitive radio networks”□J IT vol. 12 , no.2, pp.181-198, 2011

[3] Dr. Anubhuti Khare, Manish Saxena , Roshan Singh Thakur , Khyati Chourasia “Attacks & Preventions of Cognitive Radio Network-A Survey”, IJARCET, Vol 2, Issue 3, pp. 1002-1006, Mar 2013

[4] Jianwu Li, Zebing Feng1, Zhiqing Wei, Zhiyong Feng1 and Ping Zhang “Security management based on trust determination in cognitive radio networks” EURASIP Journal on Advances in Signal Processing, 2014, 2014:48