International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 05, May-2015

A Trustworthy Algorithm for Secure Communication in Cognitive Radio Networks

Chethan H
Dept. of Electronics and Communication Engg.
Bangalore Institute of Technology
Bengaluru, India

K Chandrashekarappa
Dept. of Electronics and Communication Engg.
Bangalore Institute of Technology
Bengaluru, India

***Abstract*–In recent days, major drawback in wireless communication is the improper utilization of spectrum bandwidth. To overcome this, cognitive radio (CR) technique is introduced. CR is a device which has the ability to detect available channels in wireless spectrum and hence changes its transmission and reception parameters as per requirements. In this paper, an authentication algorithm is defined for effective communication in CR networks provided that average energy consumption should be low and bandwidth spectrum utilization is high. Sensing the available spectrum is important here and hence protecting it from vulnerable attacks is considered. Efficiency of spectrum sensing in CR-Networks is increased by the proposed authentication algorithm. This algorithm is implemented using Network simulator tool. Simulation results for CRNs before providing security and after defining authentication algorithm is discussed and compared. Performance analysis of secured CRNs is done based on these simulation results.**

Index Terms – Cognitive Radio Network – CRN, Spectrum Sensing, Efficient Communication, System Security, Primary User-PU, Secondary User-SU.

I. INTRODUCTION

Cognitive Radio is a brilliant wireless technology intended for effective utilization of frequency spectrum in wireless applications. A steep increase in wireless applications day by day, give rise to huge demand for spectrum bandwidth. The allocated spectrum is being utilized inefficiently because of the static allocation of spectrum as it varies at different times and regions. Thus to overcome this problem, accessing the spectrum dynamically and cognitive radio technology is introduced [1]. Main features of CRNs include reconfigurability, frequency agility, and transmission power allocation. Its functions are spectrum sensing, analysis, allocation, management and handoff operation. Components and network architecture of CR were explained in [2]. Co-operative spectrum sensing in CRNs is an important sensing method. Sharing of available spectrum between a licensed user and a group of SUs is discussed. A new detector is proposed to detect spectrum holes reliably and all the decisions are considered by the detector and decisions are made on the presence or absence of Pus in [3]. CR has the ability to immidiately identify available channels in wireless spectrum. An algorithm is proposed for energy efficient and spectrum aware communication requirements in CR network. Spectrum sensing is an important parameter and hence its security aspect is concerned. Using authentication algorithm, it improvises the trustworthiness of spectrum sensing in CRNs [4]. An approach is proposed for detecting primary user emulation attacks in CRs. This approach uses energy detection method to locate the existing users on the frequency band. A novel algorithm for detecting non-intelligent primary user emulation attack is proposed [5]. A new kind of security threat in addition to selfish and malicious primary user emulation attack is defined which is defined as Greedy spectrum occupancy threat (GSOT). It occurs when the number of SUs is more than the channels to be accessed. Wavelet based detection approach is used here where we treat CRN as queuing system and queuing process is represented by state transition diagrams [6].

In this paper, a trustworthy algorithm has been proposed for identifying and removal of black holes and thus ensuring secure communication of data packets between different layers of CR nodes. Next the security threats and aspects of spectrum sensing is discussed to ensure trustworthiness. An efficient communication between CR nodes and effective spectrum utilization is also implemented.

II. METHODOLOGY & IMPLEMENTATION

A. System Architecture

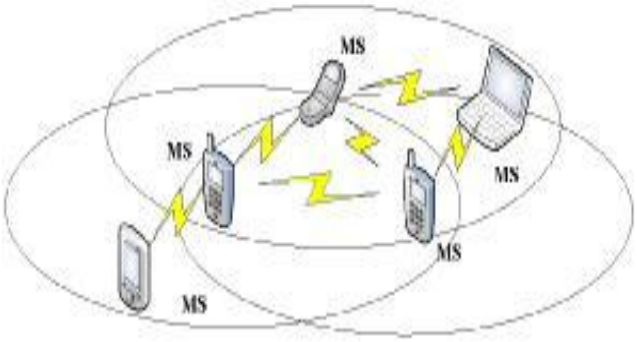

Fig.1 Cognitive Ad Hoc architecture

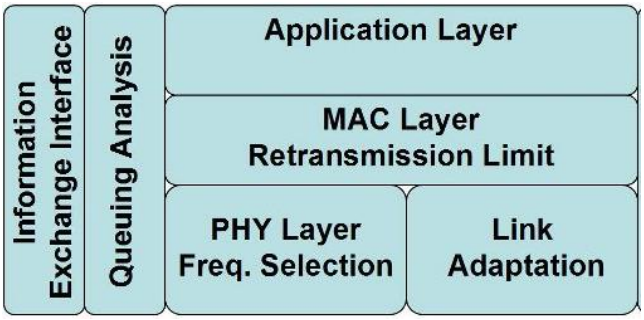

Fig.2 Proposed Cognitive system architecture

In our proposed architecture, Physical layer does unused frequency selection and link adaption layer provides link connectivity.
MAC layer is responsible for providing retransmission of frames and Application Layer sends ftp data from one cognitive node to another. In our proposed method droptail queuing model is used.

B. Proposed work

There are two algorithms and a method flow implemented in the proposed work.
1) An Authentication or Trustworthy algorithm for the detection of Black holes/malicious nodes during transmission of data packets between CR nodes.
2) An algorithm for the removal of malicious nodes from the process of data transmission.
3) Method flow for the identification and removal of malicious nodes process.

Authentication algorithm:

The proposed method is named as PL2 (PreLude, PostLude) method. The proposed solution is an enhancement of the original existing routing protocol to find secure routes and prevent attack on CRN.
Major concept is based on time and neighborhood parameters. This method first checks for malicious activity, then starts to detect malicious nodes.
This algorithm defines a threshold value to the secondary users or CR nodes to overcome the Primary User Emulation attacks. It enables CR nodes to efficiently utilize the available spectrum channels.
Nodes which can find licensed channel opportunities without interfering with the primary system increases.

Malicious removal process:

This algorithm involves the removal of identified malicious nodes. First the ID of the malicious node is extracted and is checked for its existence in Find malicious table. If at all it exists, then vote count is initialized for the malicious node. If vote count is greater than the threshold count, ID of the malicious node is removed from Find malicious table and it is append in Black hole table.

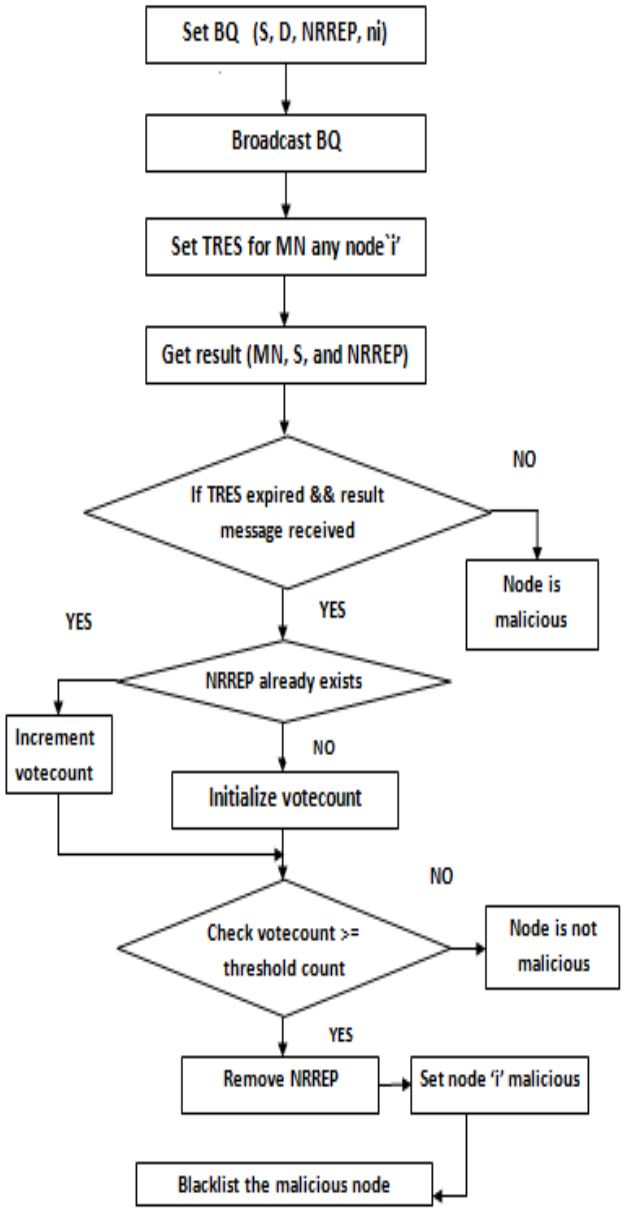

Fig.3 Flow diagram

III. RESULTS AND DISCUSSION

In the proposed work, Linux (ubuntu) platform is used for implementation. Simulations were carried out using NS2 simulation tool which is a discrete event simulator targeted at networking research. NS provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. TCL is chosen as the programming language. Here we calculate the throughput, average energy consumption and noise level for different number of nodes ranging from 20 to 60 and a comparison graph for each parameter is drawn for secure CRN and without secure CRN.

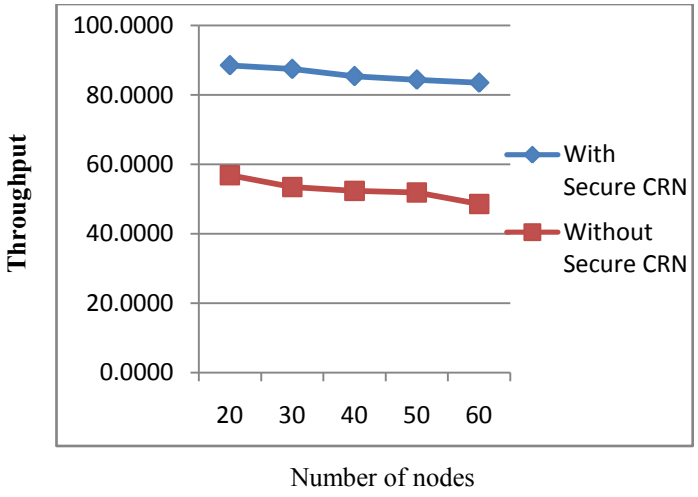

Fig.4 Comparison of throughput

TABLE I
COMPARISON OF THROUGHPUT FOR DIFFERENT NUMBER OF NODES

Nodes	Throughput with secure CRN	Throughput without secure CRN
20	88.5369	56.8967
30	87.4806	53.4589
40	85.4333	52.3472
50	84.4221	51.8943
60	83.5498	48.5746

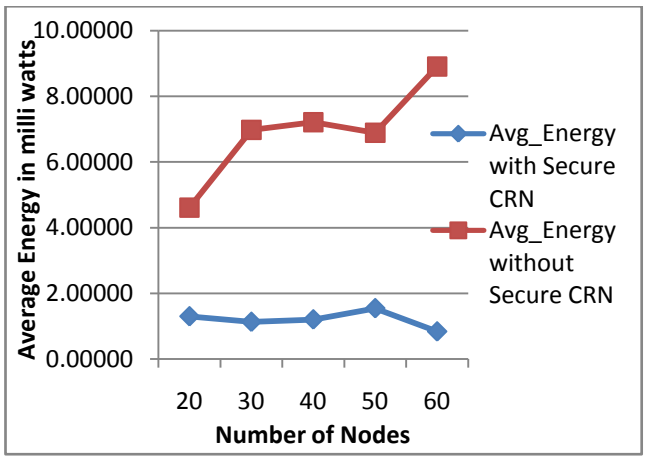

Fig.5 Comparison of Average energy consumption

TABLE II
COMPARISON OF AVERAGE ENERGY CONSUMPTION FOR DIFFERENT NUMBER OF NODES

Nodes	Average energy consumption with secure CRN	Average energy consumption without secure CRN
20	1.29771	4.6126
30	1.12955	6.9834
40	1.20301	7.2195
50	1.54449	6.8934
60	0.83634	8.9136

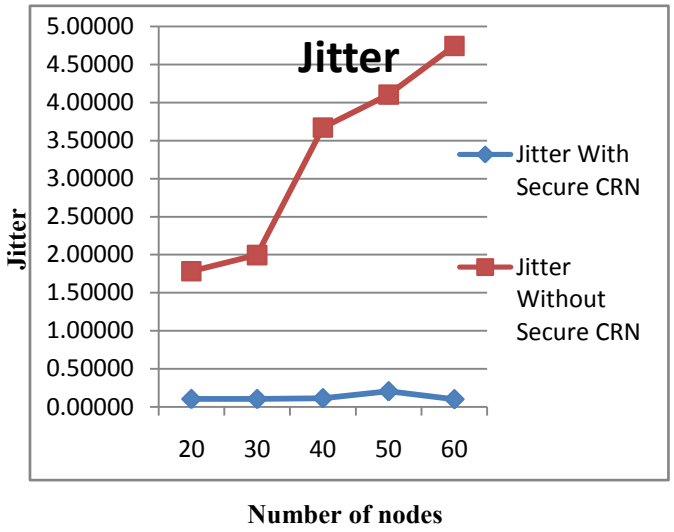

Fig.5 Comparison of Jitter

TABLE III
COMPARISON OF JITTER FOR DIFFERENT NUMBER OF NODES

Nodes	Jitter with secure CRN	Jitter without secure CRN
20	0.10426	1.7856
30	0.10404	1.9978
40	0.11488	3.6718
50	0.20651	4.1038
60	0.10187	4.7429

IV. CONCLUSION

This paper proposes a Trustworthy algorithm for efficient communication and security in CRNs and a flow chart for the same. Separate algorithms are defined for both identifing and removal of malicious nodes during transmission of data packets among different nodes. Performance analysis is done based on parameters such as throughput, average energy consumption and jitter for different number of nodes from 20 to 60 nodes. As seen in the graph, there is a marginal improvement in throughput in the range of 33.25%, decline in average energy consumption by 57.22% and reduction in noise level by 62.68% during transmission of data packets with secure CRN. As the future work, proposed work can be extended for different types of instructions.

REFERENCES

[1] Anita Garhwal and Partha Pratim Bhattacharya, "A Survey on Spectrum Sensing Techniques in Cognitive Radio," International Journal of Computer Science & Communication Networks, Vol.1(2), 196-206.

[2] Sunil Raghuwanshi and Chetan Barde, "A Survey of Cognitive Radio Network Techniques and Architecture," International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, Volume 1,Issue 1,October 2013.

[3] Abbas Taherpour, Masoumeh Nasiri Kenari and Azizollah Jamshidi, "Effective Co-operative Spectrum Sensing in CRNs" The 18th Annual International Symposium on Personal, Indoor and Mobile Radio Communications 2007.

[4] A.Amarnath prabakaran, A.Manikandan, "An efficient communication and security for cognitive radio networks," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol.2, Issue 4, April 2013.

[5] Di Pu, Yuan Shi, Alexander M.Wyglinski and V.Ilyanshenko, "Detecting Primary User Emulation Attack in cognitive radio networks," This paper was peer reviewed at the direction of IEEE Communication Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

[6] Songjun Ma, Yufeng Peng, Tao Wang, Xiaoying Gan, Feng Yang, Xinbing Wang, and Mohsen Guizani, "Detecting the greedy spectrum occupancy threat in Cognitive radio networks" IEEE ICC2014-Wireless Communication Symposium.