Trust & Recommendation Based Security in Cognitive Radio Networks

Juber Ahmad and Sri E.V. Narayana

ECE Department, Jawaharlal Nehru Technological University Kakinada
UCEK, JNTUK, Kakinada, India

juber.np@gmail.com

***Abstract*— Cognitive Radio (CR) is a prominent technology in a world of wireless communication that promises to alleviate the spectrum shortage problem and improves the efficiency of spectrum utilization. Cognitive Radio Networks (CRNs) deal with opportunistic spectrum access to utilize the limited radio spectrum in its full scale. Since, CRN is dynamic in nature any node can join or leave the network at any time. These flexible characteristics mean that the issue of secure communication in CRNs becomes more critical than for other conventional wireless networks. The successful deployment of CRN and the realization of their benefits depend on the security measures of the networks. Thus a trust & recommendation based security system for CRNs has been proposed here. This paper introduces a new algorithm for calculating trust and recommended trust value in Cognitive Radio Networks based on the quality of service characteristics expected to be fulfilled by nodes. The communicating nodes trust & recommended trust value is analyzed according to their activities and behaviour. Depending on the trust as well as recommended value, only trusted node will be given chance to participate in the communication process of the network. Trust value is the measurement of honesty of secondary users.**

Keywords — Security, Trust, spectrum, Networks, User.

I. INTRODUCTION

Cognitive Radio (CR) has been considered as a promising concept for improving the utilization of limited radio spectrum resources for future wireless communications and mobile computing. The concept of CR has emerged from the fact that the limited radio spectrum should be used to its maximum level. The primary objective of Cognitive Radio Network (CRN) is to scan the spectral band and identify free channels which will be used for opportunistic transmission. The current researches suggest that several radio frequency bands are not used to their maximum level. These underutilized areas are known as spectrum holes or white spaces [1]. CRs offer a solution which addresses the scarcity of spectrum by reusing the underutilized spectrum. National regulatory bodies like the Federal Communications Commission (FCC) assign spectrum for particular types of services that are licensed to bidders for a fee [2]. CR pioneered by Mitola [3] from software defined radio (SDR) was originally considered to improve spectrum utilization. We can obtain an overview of CR functionalities from Haykins's definition of cognitive radio [4]: "Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understandings-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit power, carries-frequency, and modulation strategy) in real time, with two primary objectives in mind: highly reliable communication whenever and wherever needed, efficient utilization of the radio spectrum". CR has two main properties: Artificial Intelligence (AI) and Dynamic Spectrum Access (DNS) [5]. AI involves reasoning and learning. This gives CR its 'intelligent' characteristics and allows it to learn about its changing environment. DNS is the process of getting a CR to detect and occupy a vacant spectrum. It involves spectrum sensing, spectrum management, spectrum mobility and spectrum sharing [5]. There are two broad classes of users in CR: the primary user (PU) is a licensed user of a particular radio frequency band, and the secondary user (SU) is an unlicensed user who cognitively operates without causing harmful interference to the primary user [6].

The organization of this paper is as follows: In Section 2, related works is reviewed. In Section 3, our proposed architecture is described. In Section 4, we show our trust computation. Simulation result is shown in section 5. Section 6 includes conclusion.

II. RELATED WORK

A Markov chain-based trust model has been proposed for analysing trust value in distributed multicasting mobile ad hoc networks [7]. Also proposed was an approach for selecting the Certificate Authority (CA) and Backup CA (BCA) [7]. The impact of a trust model in CRNs is discussed briefly in [8]. The authors in [9] integrated trust and reputation to mitigate the threat of Spectrum Sensing Data Falsification (SSDF) attack on CRNs. However, they did not propose any trust modelling for CRNs. The authors suggested potential ways for incorporating trust modelling in CRNs including: identity management, the trust building process and possible mechanisms for disseminating the trust information [8]. Furthermore, no experimental results were established for these discussions. A trust-aware model was proposed for spectrum sensing in CRNs in [10] but the authors fail to evaluate the system. A Trust Value Updated Model (TVUM) is proposed in a layered and grouped ad-hoc network for ensuring the authentication [11]. Yan et al. [14] proposed a

system to provide effective security decisions about network activities based on trust evaluations, as traditional cryptographic solutions cannot fully defend against threats from compromised nodes. Ngai and Lyu [15] proposed a public key authentication service based on a trust model to monitor malicious and colluding nodes. Their model allows mobile nodes to monitor and rate each other with an authentication metric. Trust-based community formation in peer-to-peer file sharing networks has been proposed in [13]. In this paper, we propose a community-based trust mechanism for secure communication in CRNs.

III. SYSTEM ARCHITECTURE OF PROPOSED MODEL

A Cognitive Radio Networks (CRNs) is composed of Primary Users Network (PUN), Secondary User Network (SUN), Primary Users (PUs), Secondary Users (SUs), Primary User Base Station (PUBS) and Secondary User Base Station (SUBS). As like Wireless Networks, CRNs can be deployed in various kinds of network configurations such as Centralized, Ad-hoc and Mesh Architecture. The system architecture of proposed model is shown below.

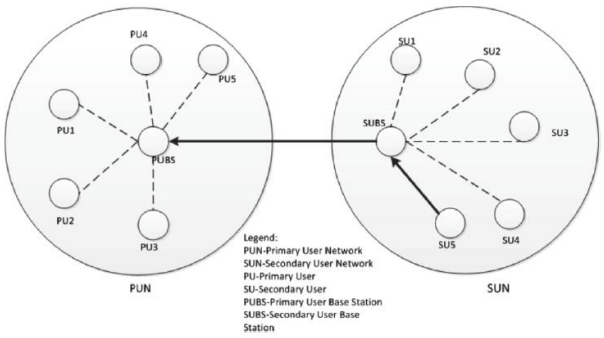

Figure 1. System Architecture of Proposed Model

The architecture of proposed model is somehow similar to [17], but there is a great difference. In my model PUBS is taken as a helper node for primary user network and SUBS is considered as a helper agent for secondary user network. We have evaluated model based on trust and recommended trust value between SUs and SUBS as well as between SUs in SUN. Here, SUs sense the spectrum of PUs and identify spectrum holes and utilize it without causing harmful interference with the transmission of other users. If SUs can detect more than one PU's free spectrum, Cognitive Radio (CR) should decide the best spectrum band over all available spectrum bands. SUs will be given chance to access the white spaces of PU's in a non interference basis if it is trustworthy. It will achieve trust and recommendation trust value from the SUBS. The SU can access the PU's underutilized spectrum as soon as it achieves the trustworthiness.

Trust is a mutual relationship between two entities whereby one party can believe, expect and accept that the other trusted party will act or intend to act accordingly [16]. Based on our CRN research, the concept of trust can be defined as a representation of the degree to which a CR node would be trustworthy, secure or reliable in respect to any interaction with other CR nodes and PUs. There are various ways to measure the trust value and recommended trust value we denote the trust as T and recommended trust value as T_R.

IV. TRUST COMPUTATION

Defined in our trust model, whenever a CR node m_i stays in a network, the residential time of the node represents the extent of its trustworthiness. If the node m_i spends a long time in the network, the node is more trustworthy. Since, a malicious node will be detected and excluded from the network as soon as possible. So the TIME that the node spends in the network, is one factor of the trust metric, measured in a time unit such as ms. Past behaviour of the node could be the other trust metric. In this section, we consider two factors for the trust metric:

Residential Time --- TIME
Recent Activities --- ra

The recent trust rt of one node can reflect the past behaviour of node m_i . So here we will define the trust as a function that depends on how long a member node had been in the network and on the past to which this node belonged in recent. As referred by [12], we define

$$N = 0.51 + rt \quad (1)$$

Let W denote the time factor,

$$W = k^{TIME} \times ra \quad (2)$$

Here k is a discount factor between 0 and 1 and ra is the node's recent activities, which can include a successful packet forwarding and so on. Finally, the trust value is evaluated as follows:

$$T = \lambda \times \frac{1-N^{(1+W)}}{1-N} \quad (3)$$

Where λ is a scaling factor to keep the trust T at a value between 0 and 1. Each member node selects the values of λ and k independently to measure the T.

Actually trust is measured over (- ∞ to ∞) and can be normalized as T (0 to 1) [21]. 1 as the normalized means trust in full (confidence) and 0 means no trust at all. It is also notice that trust is irreversible, that is the trust between SU1 to SU2 may not be same between SU2 to SU1. Each cognitive node will calculate trust value for all its surrounding nodes & SUBS and store these values for later use. These values should be updated in specific time period based on new interactions.

Flowchart of trust & recommendation trust model is shown in figure 2. Initially when a secondary node tries to use one of

PU's free radio spectrum band, at first SU scans the spectral band of PU and identify free channels. If the PU's spectrum band is free then authentication process is followed to ensure the authenticity of SU. It is noted that only wanted node can access the PU's free spectrum. The requesting SU should be authenticated from SUBS. The requesting node should be trusted with other SUs presented in secondary user network too. SUBS check the trust value of the requesting node and if it is trustworthy then the recommended trust value will be checked for the requesting node. If the requesting node is again trustworthy then the requesting node will be authenticated.

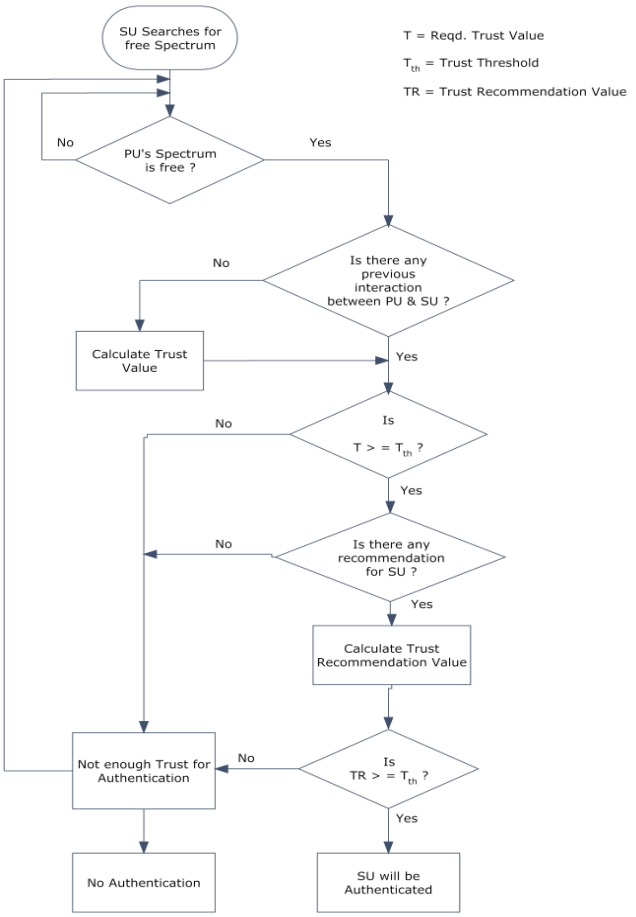

Figure 2. Flowchart of Trust & Recommendation Model

The recommended trust value can be evaluated as

$$T_{Ri} = \min \{T_i, t_{i(N-1)}\} \quad (4)$$

Where,
i = i_{th} requesting SU

T_i = T between SU_i and SUBS

$t_{i(N-1)}$ = The average trust value between the requesting SU_i and the SUs presented in SUN.

N = Number of SUs presented in SUN

The benefit of using trust recommendation along with trust value is to enhance the security in cognitive radio network as it added extra measure to ensure the authenticity of secondary node.

V. SIMULATION RESULT

From Fig.3, it is seen that the trust value increases with the increment of packet transfer for a fixed time period.

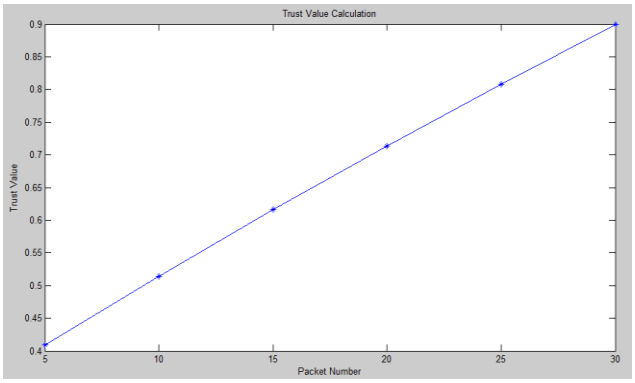

Figure 3. Trust Value Vs Packet Number for a fixed time period

In the simulation result, the initial trust value assigned by SUBS to the requesting node was 0.4 and after forwarding some packets for a fixed time period it incremented to 0.4092 and hence for number of times the increase in the packet forwarding resulted the final trust value of 0.8990. Thus it is concluded that the more number of packets forwarding/ receiving for a fixed time or in a small time period increases the trust value of the requesting node.

The simulation result of figure 3 has been taken from the table 1. The parameter in table 1 is somehow similar taken as in [12].

TABLE 1. Packet Number and Trust value for a fixed time period

Packet Number	Trust Value
5	0.4251
10	0.5145
15	0.6160
20	0.7138
25	0.8081
30	0.8990

In Table 2, we show how the trust value decreases with the increment of forwarding time for a fixed packet transfer. The parameter in table 2 is also somehow similar taken as in [12].

TABLE 2. Time and Trust value for a fixed packet transfer

Time (ms)	Trust Value
5	0.5145
10	0.3172
15	0.3013
20	0.3001
25	0.3000
30	0.3000

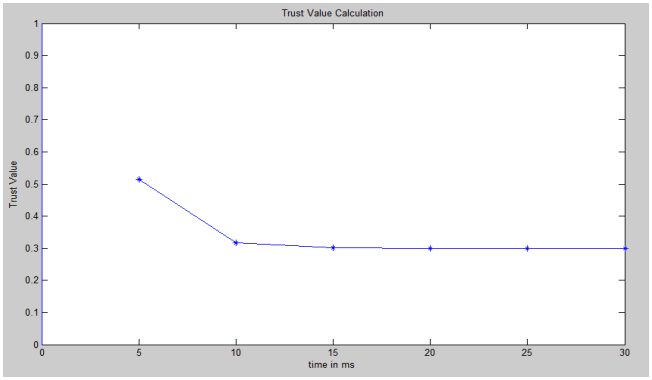

Figure 4. Trust Value Vs Time for a fixed packet transfer

The simulation result has taken again for another node whose initial trust value assigned by SUBS was also 0.4. Though initially it transferred more packets in small amount of time so trust value increased to 0.5145 but later the node had taken much time to transfer the same number of packets resulting in the decrease of trust value and the final value become 0.3000. Hence, it is concluded that trust value decreases as the node takes much time to forward/receive the packets.

The simulation result of figure 4 has been taken from the table number 2.

From figure 5, recommended trust value has been calculated. The trust value between requesting node and SUBS is first calculated and if the trust value of the requesting node is more or equal to trust threshold (T_{th}), 0.4 [17], then the recommended trust value is compared with trust threshold (0.4) for the requesting node. If the requesting node has equal or greater recommended trust value than the trust threshold then the node will be authenticated to use the primary user's spectrum, otherwise the node will not be authenticated and denied to use PU's free spectrum.

We have considered five secondary users in the secondary user network and only 4 secondary nodes have requested to use PU's free spectrum.

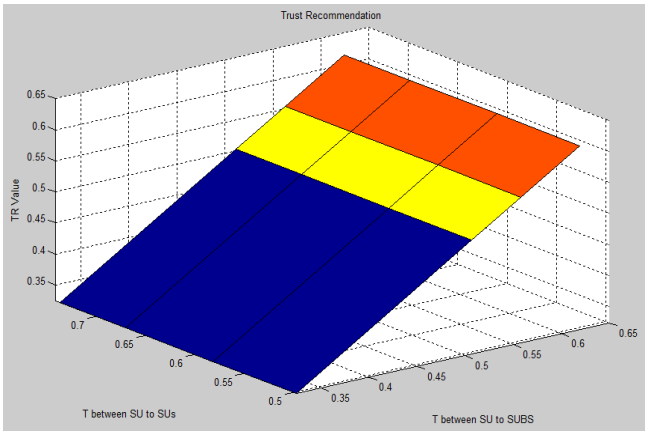

Figure 5. Trust & Recommendation of nodes in CRNs.

The trusts 'T' between requesting nodes and SUBS in secondary user network are (x-axis):

T of SU_i = 0.3240 0.5071 0.5583 0.6197

The trusts 't' between requesting nodes and the presented secondary users in secondary user network are (y-axis):

t of SU_i = 0.4965 0.5809 0.6693 0.7359

And the recommended trust (TR) values of requesting nodes presented in secondary user network are (z-axis):

T_{Ri} of SU_i = 0.3250 0.5071 0.5583 0.6197

Using the recommended trust value along with trust approach, we are able to see from the output that which nodes are authenticated to use PU's free spectrum.

Node 1 is : Not Authenticated

Node 2 is : Authenticated

Node 3 is : Authenticated

Node 4 is : Authenticated

VI. CONCLUSION

The emergence of the opportunistic spectrum sharing and cognitive radio technology raises new security implications that have not been studied previously. Researchers have only recently started to examine the security issues specific to CR devices and networks. In CRNs, non-compliant CR users may create interference by accessing the primary user's available spectrum band. Such malicious users can seriously break down the whole network performance possibly resulting in the

collapse of the CRN. Hence, the issue of secure communication in CRNs becomes more important than for the other conventional wireless networks. In this paper, we proposed a trust and recommendation based security system as a means of authentication for the CR users in CRN. The trust and recommendation trust value is evaluated and based on the value, the CR users are authenticated. The proposed approach remarkably increases the security measures and allows only wanted CR users to participate in communication process of the network.

REFERENCES

[1] Chaczko, Z., et al. 2010. Security threats in Cognitive Radio applications, in Intelligent Engineering Systems (INES), 2010 14th International Conference on. 2010. p. 209-214.

[2] Leon, O., Serrano, J.H. and Soriano, M. 2010. Securing Cognitive Radio Networks. International Journal of Communication Systems, 2010. 23(5): p. 633-652.

[3] Mitola, J. 2000. Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. PhD thesis,, in Royal Institute of Technology (KTH). 2000.

[4] Haykin, S. 2005. Cognitive radio: brain-empowered wireless communications IEEE Journal on Selected Areas in Communications, 2005. 23(2): p. 201-220.

[5] Zhang, Y., Xu, G. and Geng, X. 2008. Security Threats in Cognitive Radio Networks, in Conference on High Performance Computing and Communications. 2008.

[6] Mathur, C.N. and. Subbalakshmi, K.P. 2007. Digital Signatures for Centralized DSA Networks. in Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE. 2007.

[7] Ben-Jye, C., et al. 2008. Markov Chain-Based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad Hoc Networks. in Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE. 2008.

[8] Clancy, T.C., N.G. 2008. Security in Cognitive Radio Networks: Threats and Mitigation, in Cognitive Radio Oriented Wireless Networks and Communications, 2008. . 2008. p. 1-8.

[9] Chen, R., J.-M.P., Hou, Y. T., Reed, J. H. 2008. Toward secure distributed spectrum sensing in cognitive radio networks, in IEEE Communications Magazine Special Issue on Cognitive Radio Communications. 2008. p. 50-55.

[10] Parvin, S., et al. 2010. Towards Trust Establishment for Spectrum Selection in Cognitive Radio Networks. in Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. 2010

[11] Yang, Y.-t., et al. 2007. A Novel Authentication Scheme Based on Trust-value Updated Model in Adhoc Network. in Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International. 2007.

[12] Parvin, S., Trust-based Security for Community-based Cognitive Radio Networks in Advanced Information Networking and Applications, 2012 IEEE Conference.

[13] Wang, Y. 2004. Trust-Based Community Formation in Peer-to-Peer File Sharing Networks, Proceedings of the 2004 IEEE/WIC/ACM International Conference on Web Intelligence.

[14] Yan, Z., Zhang, P., Virtanen, T. 2003. Trust Evaluation Based Security Solution in Ad hoc Networks, Technical Report, Nokia Research Center, Helsinki, Finland, 2003

[15] Ngai, E.C.H, Lyu, M.R. 2006. An authentication service based on trust and clustering in wireless ad hoc networks: description and security evaluation, in: Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006, pp. 94–103.

[16] McKnight, D.H., Chervany, N.L. 1996. The Meaning of Trust, Technical Report, University of Minnesota, 1996.

[17] Parvin S., F.K. Hussain, O. Hussain, Conjoint Trust Assessment for Secure Communication in Cognitive Radio Networks, 2013 Elsevier journal.

[18] D. Cabric, S.M. Mishra, and R.W. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios", in Proc. 38th Asilomar Conference on Signals, Systems and Computers, pp. 772776, Nov. 2004.

[19] I.F Akyildiz, W Lee, M.C Vuran, S Mohanty, "Next Generation/ Dynamic spectrum access/ cognitive radio wireless networks: A survey" Computer Networks 50 (2006) 2127-2159, May 2006.

[20] Jung-Min "Jerry" Park, kaigui Bian, and Chen R. "Cognitive Radio Network Security" 2010, Elsevier.

[21] Cheng K, Chen, Peng-yu Chen, Prasad N, Liang YC, and Sun Sumei, Trusted Cognitive Radio Networking, Wireless Communication and Mobile Computing (2009).