2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing

Trust-Based Authentication for Secure Communication in Cognitive Radio Networks

Sazia Parvin, Song Han, Biming Tian, Farookh Kadeer Hussain
Digital Ecosystems & Business Intelligence Institute
Curtin University of Technology, Australia
Perth, Australia
{sazia.parvin, biming.tian}@postgrad.curtin.edu.au, Song. Han@cbs.curtin.edu.au, Farookh.Hussain@cbs.curtin.edu.au

Abstract— **Over the past few years, Cognitive Radio (CR) has been considered as a demanding concept for improving the utilization of limited radio spectrum resources for future wireless communications and mobile computing. Since a member of Cognitive Radio Networks may join or leave the network at any time, the issue of supporting secure communication in CRNs becomes more critical than for the other conventional wireless networks. This work thus proposes a secure trust-based authentication approach for CRNs. A CR node's trust value is determined from its previous trust behavior in the network and depending on this trust value, it is decided whether or not this CR node will obtain access to the Primary User's free spectrum. The security analysis is performed to guarantee that the proposed approach achieves security proof.**

Keywords-Trust; primary user; secondary user; authentication; secure; cognitive radio networks; raio.

I. INTRODUCTION

With the rapid development of wireless applications, Cognitive Radio (CR) has offered a promising concept for improving the consumption of limited radio spectrum resources for future wireless communications and mobile computing. The primary objective of Cognitive Radio Networks is to scan the spectral band and identity free channels which will be used for opportunistic transmission. Sometimes, several frequency bands are not used according to their maximum level. These under-utilized areas are known as spectrum holes or white spaces [1]. So, CRs offer a solution for the scarcity of spectrum by reusing the under-utilized spectrum. National regulatory bodies like the Federal Communications Commission (FCC) assign spectrum for particular types of services that are then licensed to bidders for a fee [2]. CR pioneered by Mitola [3] from software defined radio (SDR) was originally considered to improve spectrum utilization. CR, on the other hand, sits above the SDR and is the "intelligence" that lets an SDR determine which mode of operation and parameters to use. 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 processes involved in getting a CR to detect and occupy a vacant spectrum. It involves spectrum sensing, spectrum management, spectrum mobility and spectrum sharing [5]. The Cognitive Radio Networks (CRNs) consist of various kinds of communication systems and networks, and can be viewed as heterogeneous networks. 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]. Since cognitive radios can adapt to their environment and change how they communicate, it is crucial that they select optimal and secure means of communication. Cognitive radio networks operate on wireless media. Compared to wired a network, the nature of a wireless network makes the security vulnerability unavoidable. In a wireless network, the signal has to be transmitted through an open media without real connection. That is to say, the data might be eavesdropped and altered without notice; and the channel might be jammed and overused by an adversary [7]. In addition, the unique characteristics of CRNs make security more challenging. Still, there are some crucial issues which have not yet been investigated in the area of security for cognitive radio networks. When a CR node initially tries to form a CRN or tries to connect a node to join an existing CRN, it is practically impossible to implement conventional security functions as CRNs have resource constraints such as power and memory. A typical public key infrastructure (PKI) scheme which achieves secure routing and other purposes in typical ad-hoc networks is not enough to guarantee the security of CRNs, given their limited communication and computation resources. Therefore, a trusted mechanism is necessary in CRNs, while authentication is a part of trust along with other technical or non-technical factors. To ensure smooth operation of CRN to support ubiquitous computing, trust forms the foundation of

978-0-7695-4322-2/10 $26.00 © 2010 IEEE
DOI 10.1109/EUC.2010.95

security platform of CRNs. However, trust for CRNs is quite different from that of other wireless scenarios and of other areas of computing trust. Trust is critical in CRN operation and is beyond security design since security usually needs communication overhead advance. So in this paper, we propose a trust-based authentication mechanism for secure communication in cognitive radio networks.

This paper is organized as follows: In Section 2, related works is reviewed. In Section 3, our proposed scheme is described. In Section 4, we show the security proofs of our proposed scheme. We conclude the paper in Section 5 including remarks on future directions.

II. Related Work

To ensure the smooth operation of CRNs in supporting ubiquitous computing, the establishment of trust for CRNs is an open and challenging issue. Trust has been widely mentioned in the existing literatures in relation to trusted computing and web computing, ad hoc networks and even social science [8]. However, trust in terms of CRNs is completely different from all of these other scenarios. Trust is critical to CRN operation and beyond security design, as security usually needs communication overhead in advance. The authors [9] describe the trust in CRN as an essential part of the following phases:

- A cognitive radio senses a spectrum hole and, to dynamically access the spectrum for transmission, requires "trust" from the originally existing system (i.e. primary system) and regulator, even without creating interference to PS.
- A cognitive radio may want to leverage another existing cognitive radio to route its packets, even though another CR is not the targeted recipient terminal. It requires "trust" from another CR.
- A cognitive radio can even leverage PS to forward its packets to realize the goal of packet switching networks. It needs "trust" from the PS, not only at network level but also in service provider

A Markov chain-based trust model has been proposed for analyzing trust value in distributed multicasting mobile ad hoc networks [10]. They also proposed the approach for selecting the Certificate Authority (CA) and Backup CA (BCA) [10]. The impact of trust model in CRNs is discussed briefly in [11]. The authors in [12] integrated trust and reputation for the threat mitigation of Spectrum Sensing Data Falsification (SSDF) attack on CRNs. However, they did not propose any trust modeling for CRNs. The authors suggested potential ways for incorporating trust modeling to CRNs including identity management, the trust building process and possible mechanisms for disseminating the trust information [11]. Furthermore, no experimental results were established for these discussions. A trust-aware model was proposed for spectrum sensing in CRNs but the authors failed to evaluate the system [13]. A Trust Value Updated Model (TVUM) is proposed in layered and grouped ad hoc networks for ensuring the authentication [14]. In this paper, we propose a trust-based authentication mechanism for secure communication in CRNs. We also propose the trust table update procedure when one new CR node wants to join the network or leave the network. Here we discuss how this joining and leaving event impacts on the trust table in CRNs.

III. Proposed Scheme

Trust and Security in Cognitive Radio Networks are always interlinked. They complement each other and are mutually inclusive as shown in Figure 1.

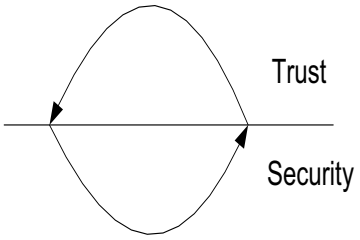


Figure 1. Trust and Security Relation in CRNs.

Whenever a CR node turns on, there will be many available access networks around it. Here, available access networks are those networks which are able to obtain authorization to use their network resources. In order to be authorized to obtain network resources and then services, the CR node should first be trusted [9]. So, trust is the foundation to ensure smooth and secure communication in CRN as shown in Figure 2.

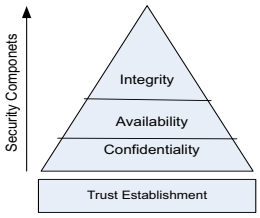


Figure 2. Security Components in CRNs.

Whenever one SU (Secondary User) wants to use a PU's free spectrum, the PU needs to check the authenticity of this Secondary User for security purposes by using trust. So, the aim of this paper is to propose a trust-based authentication scheme for secure communication in CRNs. The system structure of the proposed model is as follows:

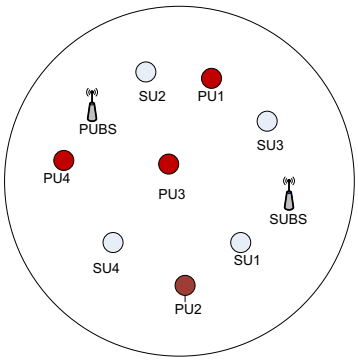


Figure 3. System Architecture of Proposed Scheme

In the system architecture, primary users and secondary users are deployed in one geographical area. PUs are connected to PUBS (Primary User Base Station) and SUs are connected to SUBS (Secondary User Base Station). Both PUBS and SUBS are connected to a CA (Certificate Authority). In network security, the third party, known as the Certificate Authority (CA), always achieves secure authentication [10] . So the SUs and PUs are connected to the CA via SUBS and PUBS respectively. Whenever one SU searches a PU's free available spectrum, the PU is connected to the CA to see the trust value of the requested secondary user. Then the PU calculates the trust value based on the previous interaction of the SU and assigns the free spectrum depending on the trust value.

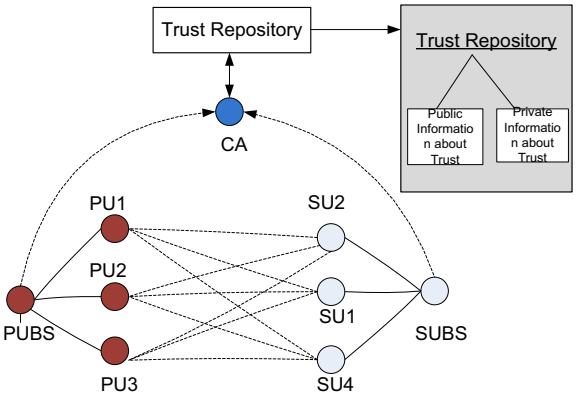


Figure 4. System Model of Proposed Scheme

In our proposed model, whenever the SU wants to use the PU's free spectrum, at first the PU needs to check the SU's trust value for security purpose. Both SUBS and PUBS are connected to the CA which has a trust repository that contains the trust value of every CR node. In the trust repository, there are two values about one node's trust: one is Public value which is visible to every node in the network. Another one is Private value only for the CA to access that value. This value is actually preserved for security purposes. If there is any hacker or attacker in the network and they intentionally alter the trust value, then the CA can check the private value of trust and obtain information about which node has been attacked. Then the CA broadcasts one message to revoke the hacked node from the network. Actually, we have proposed this trust repository concept to check the trust value in order to ensure secure communication.

When one SU tries to access one PU's free spectrum, the PUBS at first checks the SU's trust value from the CA's trust repository. If the value is greater than the predefined threshold, then the PUBS assigns free spectrum to the requested SU. If this is not the case, then the PUBS checks the reference trust value with which the secondary user already has a connection. The PUBS computes the average of the reference values of the trust value and checks the trust value. If it is not an acceptable trust value, then the PUBS declines the request. But if a new node wants to access the Primary user's free spectrum, at first the joining node should meet the agreement with the Base station. The SUBS, PUBS as well as the member nodes assign the trust value to the new joining node by seeing its past reports after the completion of the joining process which is described later in our proposed approach. Then, the PUBS checks its trust value for the spectrum access.

We assume that a node with high trust performances results in a high trust value. The trust value $TV_i(j)$ denotes the trust value of node j evaluated by node i. The average trust value of one CR node is defined as follows:

$$\overline{TV}(j) = \frac{\sum_{n=1}^{N} TV_i^n(j)}{N} \qquad (1)$$

where

$$TV_i^n(j) = \frac{\sum_{i=1}^{|R_R|} TV_i(j)}{|R_R|} \qquad (2)$$

is the trust value of CR node j evaluated by node i of the nth evaluation, N is the number of computations and $|R_R|$ is the number of receivers in network radius. The higher the trust performance that a CR node executes, the higher is the average trust value that the CR node generates[10]. Our proposed model consists of three steps:

1. Creating the trust relationship and Selecting the CA among CR nodes
2. Defining trust level when one new CR node joins to the network and
3. Defining the trust level when one node leaves the network

Step 1: Creating the trust relationship and Selecting the CA among CR nodes

A CR member node's trust value represents its trust manner in the CRN. A CR node with good manners, such as vacating the PU's spectrum band on its arrival, normal joining to the CRN or leaving the CRN, enough residual power and enough bandwidth, will obtain a high trust value. An example of determining CR node's trust values after exchanging individual evaluated trust values among CR nodes is shown in Table 1. The trust table is stored in the CA node. Every node has rights to access the public part of the trust table.

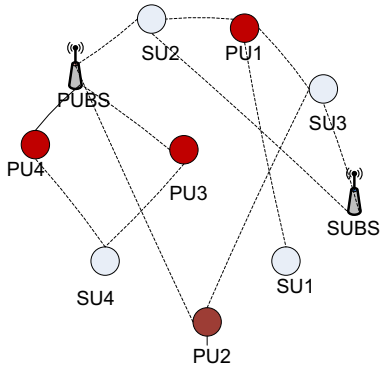


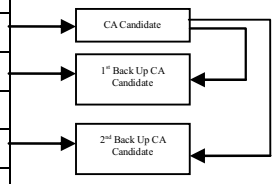
Figure 5. Communication between CR Nodes.

TABLE I. TRUST RELATIONSHIP TABLE

Node, *i*	$N^1(i)$, ***j***	TV_i^j
PU1	SU2	3
	SU3	4
	SU1	3
PU2	PUBS	2
	SU3	3
PU3	SU4	3
	PUBS	4
		2
PU4	PUBS	2
	SU4	3
PUBS	PU4	4
	PU3	5
	SU2	3
	PU2	3
SU1	PU1	3
SU2	PUBS	2
	SUBS	3
	PU1	5
SU3	SUBS	2
	PU1	5
	PU2	4
SU4	PU3	2
	PU4	3
SUBS	SU2	2
	SU3	4

TABLE II. LOCAL RELATIONSHIP TABLE

Node, i	$TV(i)$
PU1	4
PU2	3
PU3	3
PU4	3
PUBS	2
SU1	3
SU2	2
SU3	3
SU4	3



As referred by [10] we calculate the trust value of every member nodes in CRN and select the CA. Each CR node is aware of its *1*-hop neighbor nodes. The *1*-hop neighbor of node *i* is denoted by $N^1(i)$. For instance, CR node *PU1*'s 1-hop neighbors, $N^1(PU1)$, are CR nodes *SU2, SU3* and *SU1*. Node *SU3*'s trust value evaluated by *PU1* is denoted by $TV_{PU1}^{SU3} = 4$. Different nodes evaluate the same node's trust value and may have different results because of its findings and experiences. Each node's trust value including both PU's and SU's trust value is stored in the CA node which is indicated in table 1. From this table, the average trust value of each node is calculated and stored in CA which is indicated in Table 2. The average trust value is formulated by

$$TV(i) = \frac{\sum_{j \in T} TV_j(i)}{|J|} \qquad (3)$$

where T is the whole Network and $|j|$ is the number of nodes that evaluate *i*'s trust value.

Whenever the SU searches the PU's free spectrum, at first the PU accesses the CA's trust table. From the CA's trust table, the PU obtains the average trust value of the requesting SU. Depending on the trust value, the PU makes the decision of whether or not the SU can access the free spectrum. In our proposed approach, we are using the highest trust value for the selection of the CA. The second highest trust value will be selected for the selection of 1st Backup CA. And the third highest trust value for the 2nd Backup of CA as well. In Figure 6, it is depicted that the higher the trust value, the higher chance to be selected as CA. The second highest trusted value node will be selected as back up CA (BCA). But the CA is selected from the Primary CR node. If the CA is detected as malicious or is attacked by any hacker, then the backup CA (BCA) will take the role of CA. In our proposed approach, the highest trust value node of the network will be selected as the CA node to authenticate and authorize the other CR group members. We define the number of times a CR node acted as a CA (NCA) or a Backup CA (NBCA) to justify the trust performance of each node. So if a node has higher trust value, it has higher NCA. The NCA and NBCA are defined as follows [10]:

$$NCA(j) = \sum_{n=1,\text{node j is selected as the CA}}^{N} 1, \qquad (4)$$

$$NBCA(j) = \sum_{n=1,\text{node j is selected as the backup CA}}^{N} 1, \qquad (5)$$

But if there are several members with the same trust value, they will compete for the CA election according to the following rules [10]:

- Priority 1: The member is current CA node.
- Priority 2: The member is current BCA.

The member, who first meets the higher priority rule, will be elected as CA/BCA.

BCA Competition:

If a node wins the BCA competition and not the current BCA or CA, its trust value will be incremented by one. On the contrary, if a BCA or CA node loses the BCA competition; its trust value will be decremented by one.

CA Competition:

If a node successfully wins the competition and not the current CA, its trust value will be incremented by two. Specifically, the CA node is responsible to manage the authority and authentication processes within the Cognitive Radio Network group. The CA should have always the highest trust value. If a CA node fails to win the CA competition, its trust value will be decremented by two.

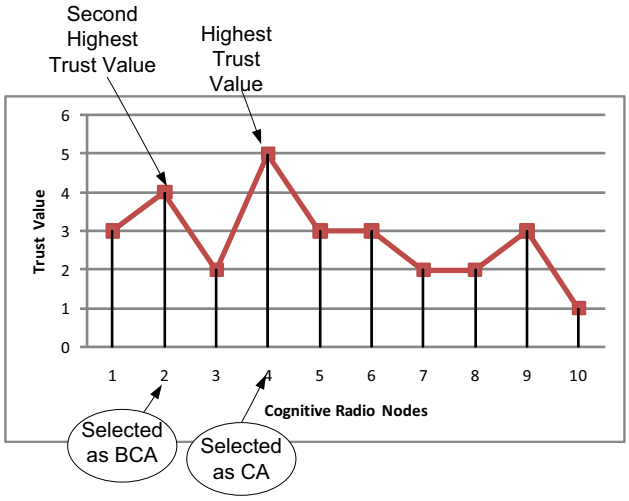


Figure 6. CA and BCA Selection Based on Trust Value

Step 2: Defining trust level when one new CR node joins to the network

If a normal new node wants to join the CRN just by broadcasting a message to the network, this is considered as a normal joining event. For normal joining, the trust value for the new node is incremented by one. If the new node sends many messages in order to join the network, this is an abnormal joining event as the broadcasting of numerous messages will break down the normal network activity. For the abnormal joining event, the trust value is decremented by one. The following Figure 7 shows the flowchart for normal joining to CRN.

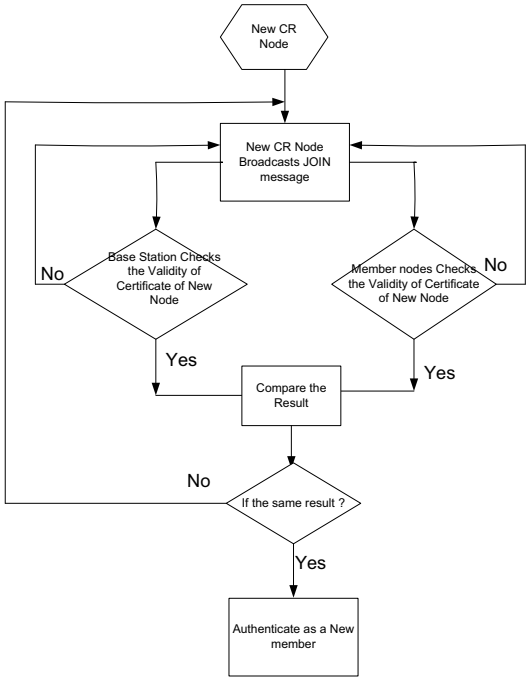


Figure 7. New Node's Joining Process Flowchart.

Whenever the new CR node wants to join the CRN, it should be authenticated by all the trusted nodes. In order to explain the authentication process, we define the following symbols:

New node's Certificate: C_N

Random Number generated by new node: R_N

Base Station's Certificate: C_{BS}

Random Number generated by new node: R_{BS}

Numerical signature of Base Station to message: $S_{BS}(JOIN)$

Numerical signature of New Node to message: $S_N(JOIN)$

For passing the authentication procedure for joining the CRNs, the following steps are followed by the new node:

1. New Node $\xrightarrow{\text{Broadcast}}$ $C_N \parallel R_N$

   The new node broadcasts its Certificate and Random Number to all member nodes in the network as well as to its base station.

2. The base station and the member nodes verify the validity of the new node's certificate. The base station produces random number R_{BS}, calculates the signature to R_N.

$$\text{Base Station} \xrightarrow{\text{Broadcast}} C_{BS} \parallel R_{BS} \parallel S_{BS}(R_N)$$

3. New node verifies the validity of Base Station's certificate C_{BS} and calculates numerical signature $S_{BS}(R_N)$ for R_N and other member nodes also verify the numerical signature to R_N .

$$\text{New Node} \xrightarrow{\text{Broadcast}} S_N(R_{BS})$$

4. Base station and other member nodes verify the numerical signature to R_{BS} and broadcast the result which informs the new node can be passed or not.
5. If the result from the Base station node and the member nodes is the same, the new node passes the authentication process. And the trust value of the node is incremented by one which is shown in the table.

TABLE III. MANNER-BASED EVENT TABLE

Good Manners	Trust	Bad Manners	Trust
Normal Leaving	+1	Abnormal Leaving	-1
Normal Joining	+1	Abnormal Joining	-1

Step 3: Defining the trust level when one node leaves the network

If a member sends a message to the Base station before leaving the network, this is marked as a normal leaving event and the trust value of the leaving member is incremented by one. If the member leaves the network without sending any prior message, this is an abnormal leaving event. If the abnormal leaving event occurs, the member's trust value will be decremented by one as depicted in Table III.

We can describe the normal leaving event [14] in the following ways:

1. If the leaving node is either the PUBS or SUBS, the new Base Station will be selected by the election procedure from the member nodes based on trust. Then the new Base Station broadcasts its identity and produces a new shared group key which is distributed to all other members.
2. If the leaving node is a normal member node, then the Base Station sends a message to all members to stop communication with the leaving node. The Base Station produces a new group key and distributes it to all members so that the leaving node cannot obtain any information later. Hence, backward security is guaranteed here in this way.
3. If the CA is a leaving node, then the Backup CA will take the role of CA. Then the new CA produces a new group shared key which is distributed to all Base Stations and other member nodes.

IV. SECURITY PROOFS

The proposed scheme is secure as long as no malicious entity is able to gain access to the CRN. The following services ensure the security proofs of our proposed scheme:

A. Authentication

This service provides the assurance that the requesting entity is the one that it claims to be. We propose authentication by establishing trust value of every CR node which is stored by the CA. Whenever a SU wants to access the PU's free spectrum band, the SU shows its good manners in order to gain spectrum access. Then the PU accesses the trust table from the CA and then the PU makes the decision of whether or not the SU can have access to the free spectrum. So we propose a trust-based authentication scheme for secure communication in CRN.

B. Availability

This service ensures that the desired system or system resources are accessible and usable upon demand by an authorized entity, according to the performance specification for the system [9]. We propose availability here by establishing a first backup of CA and a second backup of CA. The trust table which contains the trust information for every node is stored with the CA. So, in our proposed approach, the CA is executing a major role. If the CA becomes malicious or is attacked by any hacker, then the first CA backup will take on the role of the main CA. In such a case, the backup CA assumes the role of Primary CA. From amongst the available nodes, based on their trust value and reputation, a backup CA is chosen. So in our proposed approach, we are ensuring the service availability in terms of security.

C. Non-repudiation

This service provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication [9]. In our proposed scheme, when one new CR node wants to join and another leaves the network, the shared key is securely transmitted to the new entity and revoked from the leaving entity. The security is ensured here by secure joining of the network or leaving from the network. If the CR node maintains the normal joining or leaving event, the trust value is incremented by one which ensures the security purpose. If the CR node's joining or leaving appears to be an abnormal event, the trust value is decremented by one which indicates that the CR node might be a malicious entity.

D. Access Control

This service prevents the unauthorized use of resources [9]. In our proposed scheme, the authenticity is ensured by checking the trust value in the CA. So, if one CR node has a low value and wants to get access to the network, it is not allowed.

E. *Dara Integrity*

This service provides the assurance that data received are exactly as sent by an authorized entity. In our proposed scheme, we are using the trust table in the CA in two formats. One is Public which could be accessed by any CR member in the network, and the other one is Private. Only the CA has access to the Private part of the trust table. The CA always compares the private trust value with the public trust value. If any anomaly is evident, then the CR node whose trust value is changed, or by whom the trust value is changed, is detected as a malicious node. Later on, the malicious nodes are listed in the blacklist and their own trust value is decremented as well.

V. Numerical Results And Discussion

In this section, as referred by [10], we examine the number of time a CR node acted as a CA (namely NCA) and a BCA (namely NBCA) and the number of rejects (NREJ) by Matlab simulation. From Figure 8, we can see that nodes 1, 3,8,12 who have highest average trust value, they have the higher NCA and less NREJ. On the contrary, the nodes 0, 6, 9, 10, 11, 13, 14, 17 who have the lowest average trust value, they have the lower NCA, NBCA and the higher NREJ.

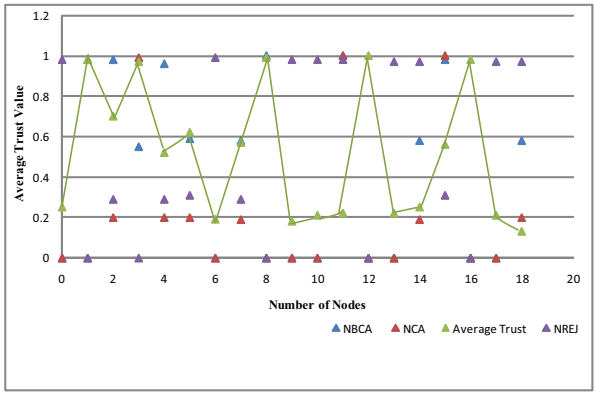


Figure 8. NCA, NBCA, NREJ, and Average Trust Value of Cognitive Radio Nodes.

From Figure 8, we can realize that a node with higher average trust value has high NCA, NBCA and lower NREJ, and vice versa.

Trust and security is closely related-this theme is depicted in Figure 9 (a) and 9 (b).

From Figure 9 (a), we see that at the beginning the cognitive radio node has less information about other nodes. So the node does not have much trust value at the starting. That's why the security level is very low at the beginning of communication. As time goes on, the node increases its communication with other nodes by using previous experiences and references, so the trust value increases. As trust value increases, the security level also starts to increase.

Figure 9 (b) shows the case where all the cognitive nodes are in a good condition at the beginning. The nodes have high trust values with others. So, the security level is above on the expectation level at the beginning. When the network is running, some nodes are comprised because of various attacks and lack of energy. These situations make the security level goes to low level.

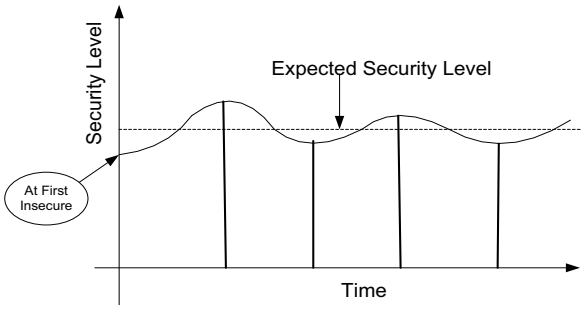


Figure 9 (a). Security Level Started Below Expectation Level

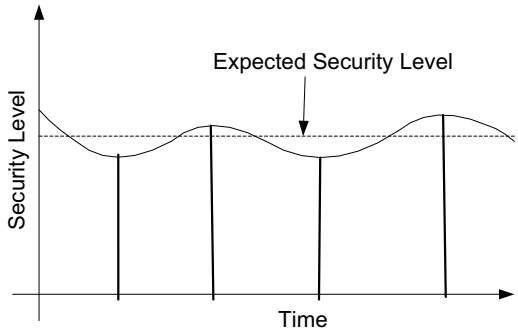


Figure 9 (b). Security Level Started above Expectation Level

VI. Conclusion

In cognitive radio networks, some non-compliant Cognitive Radio users may create interference by accessing the primary user's available spectrum band. Such malicious users can seriously damage the whole network performance possibly resulting in the collapse of the CRN. It is critical to consider that Cognitive Radio Networks operate under resource constraints. As CRNs have dynamic hebaviours, members of Cognitive Radio Networks may join or leave the network at any time. Hence, the issue of secure communication in CRNs becomes more important than for the other conventional wireless networks. Therefore, in this paper we propose a trust-based authentication scheme for secure communication in CRNs. This secure authentication reduces the relative calculating overheads and communication cost. This work thus proposes a secure trust-based authentication approach for CRNs. Moreover, we propose security proof of our proposed scheme. In this paper, we do not deal with the biasing between the CA and other nodes, so the some specific node's trust value will always be higher. In future work, we will focus on the trust of biased nodes in CRNs.

REFERENCES

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

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

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

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

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

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

[7] X. Zhang, C.L., *The security in cognitive radio networks: a survey*, in *International Conference On Communications And Mobile Computing* 2009, ACM: Leipzig, Germany p. 309-313.

[8] Naldurg, P. and R.H. Campbell. *Dynamic Access Control: Preserving Safety and Trust in Network Defense Operations*. in *Proceedings of the Eighth ACM Symposium in Access Control Models and Technologies (ACM SACMAT 2003)*. 2003

[9] K.-C. Chen , Y.-J.P., N. Prasad ,Y.-C. Liang ,S. Sun and *Cognitive radio network architecture: part II -- trusted network layer structure*, in *Conference On Ubiquitous Information Management And Communication* 2008, ACM: Suwon, Korea p. 120-124

[10] Ben-Jye, C., et al. *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.

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

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

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

[14] Yang, Y.-t., et al. *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.