2010 24th IEEE International Conference on Advanced Information Networking and Applications

# Towards Trust Establishment for Spectrum Selection in Cognitive Radio Networks

Sazia Parvin, Song Han, Li Gao, Farookh Hussain and Elizabeth Chang
Digital Ecosystems & Business Intelligence Institute
Curtin University of Technology, Australia
Perth, Australia
{sazia.parvin, li.gao1}@postgrad.curtin.edu.au
{Song. Han, Farookh.Hussain, Elizabeth.Chang} @cbs.curtin.edu.au

***Abstract*—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. As cognitive radio network (CRN) is a general wireless heterogeneous network, it is very essential for detecting the misbehaving or false nodes in the network. So in this paper we propose a trust aware model which provides a reliable approach to establish trust for CRN. This approach combines all kinds of trust values together, including the direct trust and indirect trust value for the secondary users. Depending on this trust value, it is decided that whether the secondary user can user the primary user's spectrum band or not. The mathematical results show that our trust model can efficiently take decision for assigning spectrums to the users.**

***Keywords-cognitive radio networks; spectrum; trust; primary user; secondary user***

## I. INTRODUCTION

Among different kinds of wireless technology supporting Internet access and other services, a very effective idea is to merge different wireless networks and to use one of them appropriately depending on the communication environments and the application requirements. Cognitive radio pioneered by J.Mitola iii [1] from software defined radio (SDR) was originally considered to improve spectrum utilization. There is an ever increasing demand of spectrum for emerging wireless applications and there is a shortage of spectrum for the wireless applications. Considering these things Federal Communications Commission (FCC) has considered to make the licensed spectrum available to the unlicensed users. So the unlicensed users can use the fallow spectrum provided they cause no interference to the licensed users. Most of the radio systems today are now aware of the radio spectrum. Cognitive radio is a paradigm for wireless communication in which either a network or a wireless node changes its transmission or reception parameters to communicate efficiently avoiding interference with licensed or unlicensed users. A cognitive radio senses the available spectrum, occupies it and can vacate the spectrum on sensing the return of the primary user. We can call future wireless networks as cognitive radio networks (CRN), which is pretty much consistent of Haykins's definition of cognitive radio [2]:

"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."

As referenced by [3, 4] once cognitive radios can find the opportunities using the " spectrum holes" for communications, cognitive radio networking to transport packets on top of cognitive radio links is a must to successfully facilitate useful applications and services. A mobile terminal with cognitive radio capabilities can sense the communication environments (e.g. spectrum holes, geographic location, available wire/wireless communication system or networks, available services), analyse and learn information from the environments with user's preferences and demands, and reconfigure itself by adjusting system parameters on forming to certain policies and regulations. For example, when a cognitive radio mobile terminal sensed that there WIFI and GSM systems nearby while spectrum holes exist in the frequency band of digital TV, it may decide to download files from a certain WiFi Ap, make a phone call through GSM system and communicate with other cognitive radio users using those spectrum holes. Cognitive radio technology could also facilitate interoperability among different communication systems in which frequency bands and/or formats differ [4].

Cognitive radio, on the other hand, sits above the SDR (Software Defined Radio) and is the "intelligence" that lets an SDR determine which mode of operation and parameters to use. Actually an SDR is simply a radio that puts most of the Radio Frequency (RF) and Intermediate frequency (IF) functionality, including waveform synthesis, into the digital (rather than the analog) domain, allowing great flexibility in the modes of radio operation (called "personalities") [1]. A cognitive radio network is thus not just another network to interconnect cognitive radios. The CNRs are composed of various kinds of communication systems and networks, and can be views as a sort of heterogeneous networks. The

1550-445X/10 $26.00 © 2010 IEEE
DOI 10.1109/AINA.2010.161

heterogeneity exists in wireless access technologies, networks, user terminals, applications and service providers [5]. So free spectrum sensing is a key characteristic used in CRNs. Through this sensing process, unlicensed user can determine whether the radio can be used or not. But if the unlicensed user is not a trust worthy node, then it can break down the normal activities of the CRNs by injecting some malicious attacks. That's why establishing trust for CRN is an open and challenging issue. In this paper, we propose a trust aware model which provides a reliable approach to establish trust for the spectrum selection in CRNs.

The organization of this paper is as follows: In section 2, related works is reviewed. In section 3, system architecture of our proposed model is described. In section 4 and 5, we show how trust is calculated and spectrum allocation decision is based on the result. We conclude the paper in section 6 including future remarks.

## II. RELATED WORKS

Now-a-days trust in the human society has become the most important thing for human being's communications, work and lives. However trust can be regarded as criteria for making a judgment under complex social conditions and can be used to guide further actions [6]. Trust and security are very closely interrelated and independent that is difficult to separate each other. But, nowadays, establishing trust for CRN is an open and challenging issue. Trust has been widely mentioned in literatures regarding trusted computing and web computing, ad hoc networks and even social science [7-10].However, trust for CRN is completely different from all of these scenarios. Trust is critical in CRN operation and beyond security design, as security usually needs communication overhead in advance. The authors [11] describes the trust in CRN as follows:

- A cognitive radio senses a spectrum hole and to dynamically access the spectrum for transmission requires "trust" from 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.

Because of all these reasons, the idea of applying trust and reputation model in a CRN has recently attracted research interest. The impact of trust model on CRN is discussed briefly in [12]. In this paper, 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. But no experimental results were established for these discussions. The authors in [13] integrated trust and reputation for the threat mitigation of Spectrum Sensing Data Falsification (SSDF) attack on CRNs. But trust modeling was not the meeting point of their paper. In this paper, we integrated direct trust and indirect trust for using the primary user's spectrum band if the spectrum is available to use.

## III. SYSTEM ARCHITECTURE

Cognitive radio (CR) is a novel approach for improving the utilization for making it possible for a group of secondary (unlicensed) users (SUs) to access the spectrum band which is not being by the primary (licensed) users (PUs) in some geographical location.

### A. A CRN Architecture

As like Wireless Networks, CRNs can be deployed in various kinds of network configurations such as Centralized, Ad-hoc and Mesh Architecture. In our paper we implement an infrastructure-based CRN with centralized network entities. Figure 1 shows a general architecture of CRNs as depicted in [3].

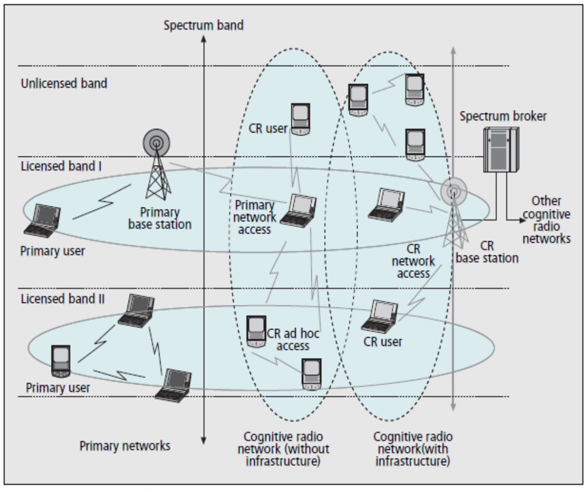

Figure1.A general cognitive radio network architecture [14]

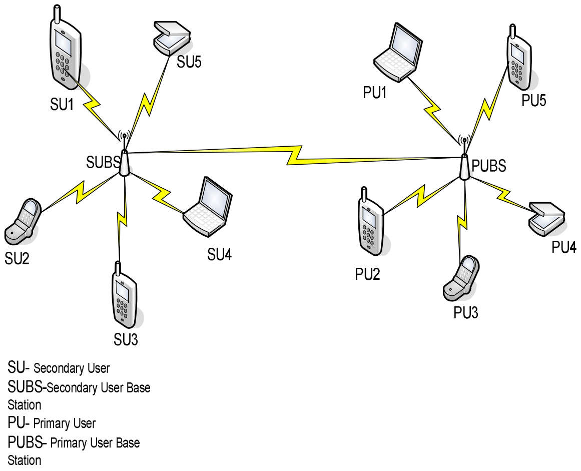

Figure 2. System Architecture of Proposed Model

As referred by [15], we assume that PUs coexist with SUs in some geographical area and PUs are controlled by a fixed PU base station (PUBS). In this CRN, SUs are also distributed in the coverage area of a fixed SU base station (SUBS). SUs can only communicate with each other through the SUBS within the transmission range of the SUBS. The SUs and PUs are not able to communicate between themselves. But the communication between SUBS and PUBS is possible. Figure 2 shows the architecture of our system model.

If one SU wants to use the PU's spectrum band, then at first the SU needs to sense the spectrum. During the sensing process, each SU senses the PU spectrum bands individually and reports the results to the SUBS. By integrating the sensing results reported by the SUs with its own sensing result, the SUBS determines the activity states of each PU spectrum band and allocates resources to SUs within its range. In this paper, we strongly assume that PUs, PUBS and SUBS are trustworthy entities in the CRN.

### B. *Architecture of Trust Model*

In a CRN, secondary user needs the service provided by primary users. A secondary user can sense the spectrum band of primary user, if it is free then the secondary user will send sensing information to the SUBS. Every user can be denoted by User <User ID, A, V> where

ID denotes the identity of the user,
A denotes the attribute set of user ID,
V denotes the value set of the attributes.

As soon as the cooperation process starts that means the secondary user senses the primary user's spectrum band and sends the sensing result to the SUBS, the trust relationship is set up among the SUs and PUBS. In our trust model, a user is denoted by User <ID, A, V, T>, where T denotes the set of the trust values associated with the attributes as every attribute has its own trust value.

### C. *Trust Model*

Our trust model is a trust a modification of the trust model [16]. Han's model computes trust for wireless sensor network. In our new model, we build trust model for cognitive radio networks considering that the networks consisting of PUs, SUs, SUBS, and PUBS. The architecture of our trust model is shown in the following figure.

As shown in the figure, when the secondary user (Ex. SU1) tries to use one primary user's spectrum band, at first SU needs to sense the PU's spectrum band to check whether it is free or is in using. After sensing the spectrum band, the SU will send the sensing result to the SUBS. Then the SUBS will get the direct trust value for that SU and indirect trust value from other SUs. When the SUBS gets the direct and indirect trust value, the integrated trust module combines both the trust value and the indirect trust value to calculate the integrated trust value.

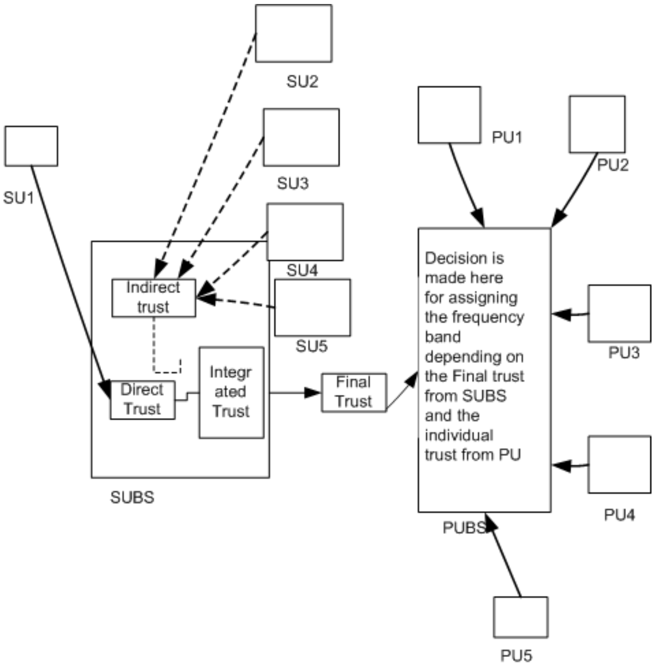
SU2
SU3
SU1
SU4
SU5
Indirect trust
Direct Trust
Integr ated Trust
Final Trust
SUBS
PU1
PU2
Decision is made here for assigning the frequency band depending on the Final trust from SUBS and the individual trust from PU
PU3
PU4
PUBS
PU5

Figure 3. System Model of Proposed Scheme

## IV. CALCULATION OF TRUST

As referred by [2], in our trust model, trust is represented by a real number ranging from 0 (complete distrust) to 1 (complete trust). The trust exists in the user, thus the trust value among the users can also be divided into three categories: direct trust value, indirect trust value and integrated trust value.

Direct trust value is the type of trust value can be established between $SU_1$ and SUBS. And this is denoted by $T_{Directtrust}$.

Indirect trust is established when $SU_2$…….$SU_n$ provide its trust value of $SU_1$ to SUBS.

Integrated trust value can be calculated by the SUBS based on the direct trust value of $SU_1$ and the indirect trust value of SU1 from other SUs, denoted by $T_{Integtrust}$.

### A. *Direct Trust Calculation*

The direct trust value of secondary user can be determined by its multi-attribute trust value.

The conditions of a User are always changing, thus the SUBS always need to evaluate trust value of the SU based on its multi-attribute trust value. The information about the past cooperation is assembled in a table of cooperation record among the Users, as shown in the table. As referred by [2] , each attribute has three relevant values : the number of the successes ($S_i$ , i = 1,2, ….n), the number of failures ($F_i$, i = 1,2…n) and the number of the cooperation ($C_i$, i =1,2,…n).

In order to simply our analysis, we assume that the cooperation/non-cooperation behavior is of equal value during the communication process between the Users.

TABLE I. COOPERATION RECORD TABLE

| Attributes | Success | Failure | Cooperation Sum |
|---|---|---|---|
| A1 | S1 | F1 | C1 |
| A2 | S2 | F2 | C2 |
| .... | .... | .... | .... |
| An | Sn | Fn | Cn |

In table 1, $C_i = S_i + F_i$, i = 1,2,….n. The trust value for attribute $A_i$ can be computed based on the table 1 as follows:

$$T_{A_i} = \frac{S_i}{C_i}$$

Thus, the overall trust value for the SU with n attributes $A_i, i = 1, 2, \ldots.n$ (denoted by $T_{node}$) can be computed using $T_{A_i}$ as follows:

$$T_{User} = \frac{\prod_{i=1}^{n} T_{A_i}}{\prod_{i=1}^{n} T_{A_i} + \prod_{i=1}^{n} (1 - T_{A_i})}$$

Since all $T_{A_i}$, i = 1,2,…., n can be calculated using data in table 1, the trust value of Secondary User who wants to sense and use Primary User's spectrum band, can be easily calculated by the SUBS.

### B. Indirect Trust Calculation

When the SUBS sends the cooperation request to other secondary users, three kinds of trust values from reliable nodes, the strange nodes (the node never cooperate with the SUBS before) and the unreliable nodes, are returned to SUBS. The trust value of reliable nodes ($T_{reliable}$) and strange nodes ($T_{Strange}$) can be kept, and the trust value of the unreliable nodes must be discarded. The SUBS assign some weight value to reliable nodes, strange nodes.

Thus the indirect trust can be calculated as follows:

$$R_p = T_{integtrust} \Gamma_{SUBS} + (1 - T_{integtrust}) \frac{\sum_{i=1}^{M} \tau_{ip} \Gamma_{ip}}{\sum_{i=1}^{M} \tau_{ip}}$$

Where

$$W_{realiable} + W_{strange} = 1 \text{ and } W_{realiable}, W_{strange} \in [0,1]$$

### C. Integrated Trust

There are different kinds of cooperation among secondary users and SUBS. So the SUBS can automatically assigns the different weights value based on the requirements of a certain task in our trust model. The weight of the direct trust is denoted by $W_{directtrust}$, the weight of the indirect trust is denoted by $W_{indirecttrust}$.

The integrated trust value can be calculated by the following equation:

$$T_{integtrust} = W_{directtrust} \times T_{directtrust} + W_{indirecttrust} \times T_{indirecttrust},$$

Where

$$W_{directtrust} + W_{indirecttrust} = 1 \text{ and}$$
$$W_{directtrust}, W_{indirecttrust} \in [0,1]$$

## V. DECISION CALCULATION FOR ASSIGNING SPECTRUM

When the SUBS calculates the integrated trust value, then it will send this trust value to PUBS. Then the PUBS will take decision whether SU is able to use Primary user's spectrum or not depending on the following equation:

$$R_p = T_{integtrust} \Gamma_{SUBS} + (1 - T_{integtrust}) \frac{\sum_{i=1}^{M} \tau_{ip} \Gamma_{ip}}{\sum_{i=1}^{M} \tau_{ip}}$$

Where

$R_p$ is the overall sensing result from PUBS for PU spectrum band p;

$T_{integtrust}$ is the trust value for the SU from the SUBS;

$\Gamma_{SUBS}$ is the sensing result provided by the SUBS;

$\tau_{ip}$ is the trustworthiness of $SU_i$ in the context of PU spectrum band p;

$\Gamma_{ip}$ is the sensing result for PU spectrum band provided by $SU_i$ ;

M is the number of SUs whose trustworthiness with respect to PU spectrum band p is above a predefined threshold $\eta$ .

In the case when the variance in trustworthiness of each SU is the context of a primary spectrum band p is not considered,  is set to 0 and all $\tau_{ip}$ are set to 1. Then the second term in this equation reduces to a simple average of all the sensing results obtained from the SUs. It is effectively a weighted sum of the SUBS sensing result and a majority voting from all the SUs who choose to participate in the distributed sensing operation. The final decision $D_p$ is made based on the sign of $R_p$,

$$D_p = \begin{cases} -1, R_p < 0 \\ 0, R_p = 0 \\ 1, R_p > 0 \end{cases}$$

Whenever $D_p$=1, that time the SU will be able to use the primary user's frequency spectrum band p.

## VI. CONCLUSION AND FUTURE WORKS

In this paper, we propose a trust aware hybrid spectrum sensing scheme for CRN. In the CRN, some misbehaviouring SUs may want to access the PU's available spectrum band. Such malicious SUs can seriously impact on the whole network performance. So in this paper, we propose the combination of all kinds of trust values together, including the direct trust and indirect trust value for the secondary users. Depending on this trust value, it is decided that whether the secondary user can user the primary user's spectrum band or not. In the future work, we want to perform the simulation depending on the mathematical terms.

## REFERENCES

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

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

[3] K.Chen,Y.Peng,N.Prasad,Y.Kiang,S.Sun, "Cognitive radio network architecture: part I -- general structure", in Proceedings of the 2nd international conference on Ubiquitous information management and communication 2008. Suwon, Korea ACM.

[4] FCC, E T Docket No 03-222 Notice of Proposed rule making and order. December, 2003.

[5] X.Gao, G.Wu, and T.Miki, "End-to-end quality of service provisioning over heterogeneous networks". IEEE Wireless Communication, 2004. 11(3): p. 24-34.

[6] G.Han, D. Choi, and W. Lim. "A Reliable Approach of Establishing Trust for Wireless Sensor Networks". in IFIP International Conference, Network and Parallel Computing Workshops, 2007. NPC Workshops. 2007.

[7] T. Ghosh, N. Pissinou, and K. Makki, "Towards designing a trusted routing solution in mobile ad hoc networks. Mobile Networks and Applications", 2005. 10(6): p. 985 - 995.

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

[9] G. Theodorakopoulos and J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks", IEEE Journal on Selected Areas in Communications, 2006. 24(2): p. 318-328

[10] A.A. Pirzada, C. McDonald, "Establishing trust in pure ad-hoc networks,. in Proceedings of the 27th Australasian conference on Computer science. 2004

[11] K.Chen,Y.Peng,N.Prasad,Y.Kiang,S.Sun,"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

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

[13] R. Chen, et al., "Toward secure distributed spectrum sensing in cognitive radio networks", in IEEE Communications Magazine Special Issue on Cognitive Radio Communications. 2008. p. 50-55

[14] I.F. kyildiz, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks : A surve",. Computer Networks, 2006. 50: p. 2127-2159

[15] T. Qin,, et al., "Towards a trust aware cognitive radio architecture.", ACM SIGMOBILE Mobile Computing and Communications Review 2009 13(2): p. 86-95

[16] G. Han,, et al. "A Reliable Approach of Establishing Trust for Wireless Sensor Networks", in International Conference on Network and Parallel Computing Workshops 2007: IEEE Computer Society.