International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Survey on Trust Management Mechanism in Cognitive Radio Network

S. Kavyashree[1], B.M. Nandini[2]

[1]M. Tech, Dept of ISE, National Institute of Engineering, Mysuru, Karnataka, India
[2]Assistant Professor, Dept of ISE, National Institute of Engineering, Mysuru, Karnataka, India

---

Abstract-*Spectrum sensing being a primary functionality of Cognitive Radio Networks, trust plays a very important role in spectrum allocation decisions. Reliable spectrum sensing results from the secondary users ensure efficient spectrum utilization and improves throughput. Trust management among the secondary users is a matter of concern in Cognitive Radio Networks (CRN). A good Trust management mechanism ensures fair and accurate spectrum access decision and even has the capability to identify and mitigate problems that arise from malicious users in the network. This paper provides an overview on importance of trust in CRN and few trust management mechanisms employed in centralized and distributed CRN. Trust management mechanisms discussed here are focused on attaining various objectives like improving accuracy in spectrum sensing results, identifying malicious secondary user and taking appropriate measures on identified malicious users.*

Key Words: Cognitive Radio Networks (CRN), spectrum sensing, cooperative sensing, cognitive cycle, centralized structure, distributed structure

1. INTRODUCTION

A huge range of applications rely on wireless communication technology. Wireless applications and services have increased demand for spectral resources. Spectrum is limited and is also one of scarce resource. The requirement for more spectral resources on one hand and underutilization of available spectrum by the licensed users on the other hand motivated for the need of a new scheme. Joseph Mitola III first proposed the concept of the cognitive radio (CR) to address the problem of spectrum usage efficiently.

The CR paradigm endeavors to mitigate the scarcity of spectral resources for wireless communication through intelligent sensing and agile resource allocation techniques[1].CR have the capability of detecting available free channels and self-configuring the transmission and reception parameters according to the environmental changes

1.1Architecture of Cognitive cycle

CR is different from the traditional radio because of its cognition capability and re-configurability. CRs continually execute cognition cycle. The cognitive cycle enables the cognitive radio to observe spectral opportunities, create plans to adapt itself, decide, and act to explore the best opportunities [2].Most of the trust management mechanisms are based on the cognition cycle , hence let us have a brief look at the cognition cycle. The functional architecture of cognition cycle is given in the fig has three main components namely Spectrum Sensing, Spectrum Analysis and Spectrum Access Decisions.

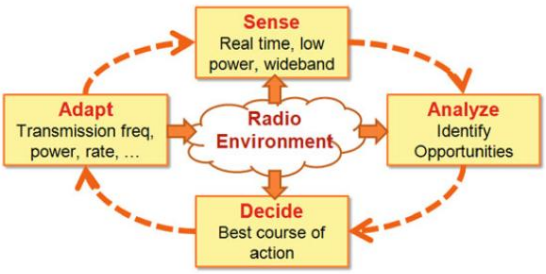

Fig -1: Cognitive cycle

Spectrum Sensing. Spectrum sensing refers to the ability of a cognitive radio to measure the electromagnetic activities due to the ongoing radio transmissions over different spectrum bands [2].
Spectrum Analysis: Spectrum analysis is deducing the current spectral opportunities in the surrounding radio environment based on the sensed radio environment parameters [2]
Spectrum Access Decisions : This is the decision making step in the cognitive cycle. Spectrum information gathered is used in adapting the transceiver parameters for the upcoming transmissions over the identified frequency bands [2].

1.2 Types of Cognitive Radio Networks

Based on the infrastructure requirements CRN are classified as centralized infrastructure based CRN network and distributed ad-hoc CRN.

A. Centralized Cognitive Radio Networks

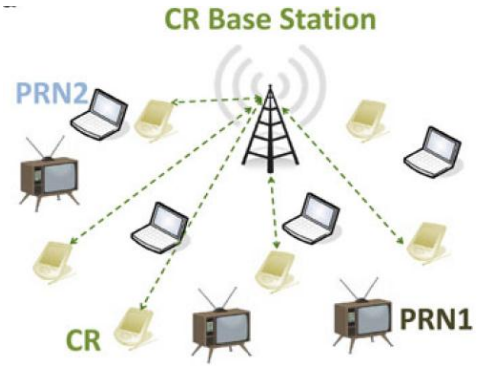

Fig-2: Centralized CRN

The network comprises of second users along with a centralized base station. The base station monitors all the secondary transmissions across licensed and unlicensed band by collecting all the spectrum-related information from the secondary users. Based on the collected information the base station takes final decision on spectrum allocation.

B. Distributed Cognitive Radio Networks

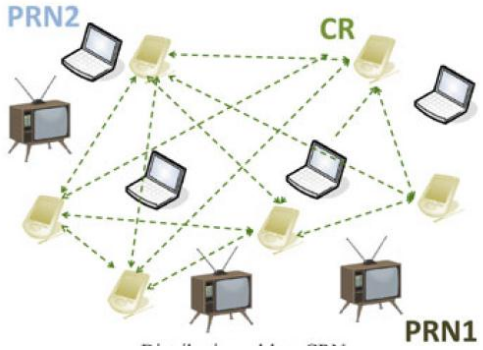

Fig-3: Distributed CRN

Distributed CRN do not possess a base station they communicate with each other via ad-hoc point-to-point connections either over the licensed or the unlicensed bands. In a distributed CRN all the nodes jointly coordinate their spectrum access decisions to share the available spectral opportunities.

2. IMPORTANCE OF TRUST IN COGNITIVE RADIO NETWORKS

CRN accomplishes this objective concept of improving the efficiency of underutilized channels with the help of spectrum sensing by detecting unused spectrum and sharing it, without harmful interference to the licensed users. Spectrum sensing may be either cooperative or non-cooperative.

In cooperative spectrum sensing each secondary user undertakes the task of measuring and analyzing the spectrum utilization within a CRN. A base station on receiving sensed reports from a variety of radios in the network and fine-tunes the overall CRN to suit the requirement whereas in non-cooperative sensing, each radio operates separately within the network to execute its task of measuring and analyzing the spectrum utilization.

Cooperative spectrum sensing is preferred over non cooperative spectrum sensing because of the advantages such as more accuracy in signal detection, reduced false alarms, more resistant to hidden terminal problem and multipath fading problem. The time required for spectrum detection is less when compared to non-cooperative spectrum sensing. In case of Cooperative spectrum sensing there is spectrum sensing at regular time intervals. Every node has to co-operate with every other node for accuracy. But in this aspect trust on every other node in the network plays an important role. Also when a new node wants to join a existing network directly adding the new member into the network without any trust may lead to security breaches. It is not advisable to accept the information given by an untrusted node in the network while taking spectrum allocation decisions. Hence it is always desirable to have a trust management mechanism in the network which enables the new user to pass certain authentication before joining the group, constantly monitor every node's behavior in the network and update the trust value. The trust management mechanism is very much helpful in determining the trust on each node in the network by means of trust value. The trust value is indeed helpful for efficiency in spectrum sensing, better opportunities for a node with higher trust value to satisfy its needs and helpful in identifying the network from selfish and malicious nodes.

3. RESEARCH WORK

A. Trust Management Model in Centralized CRN

This work focuses on building a trust mechanism for centralized CRN in order to resolve the problem posed by dishonest, selfish and malicious network entities in the course of cognitive cycle.

In a centralized CRN the primary users and the secondary users share the same geographical area. The primary base station (PBS) handles the primary users and the cognitive base station (CBS) takes care of the secondary users. The CBS is handed over with the responsibility of monitoring the overall performance of the second users in the network, and make the appropriate incentive or punishment mechanism to ensure the safety and reliability of the cognitive cycle [3].

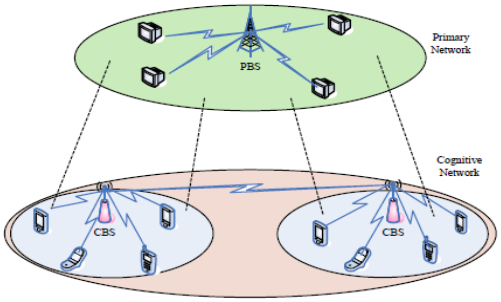

Fig-4: Structure of centralized CRN

The CBS initializes the trust management process by including the newly joined secondary user into the list of second users and assigns a preliminary reputation for it. The secondary users sense the spectrum and send their respective spectrum sensing reports to the base station. The fusion center on receiving the reports from secondary users collectively calculates the final sensing result taking in to account the sensed results and trust states of every secondary user. In addition to this the base station persistently monitors the activities of every secondary user to update their reputation [3]. Based on this decision the CBS allocates the free channels. Along with the spectrum sensing reports the base station considers the trust value of secondary users as a important factor and takes final decision The model for trust management consists of four parts as mentioned below,

1. Trust initialization
2. Updating of reputation
3. Trust assessment
4. Reward mechanism.

1.Trust Initialization

The CBS maintains a trust list where the list contains the entries for every secondary user and their corresponding trust values. Each user is denoted by an integer i and the corresponding reputation value is denoted by R_i. Initially when the secondary user joins the group after completing the authentication it is assigned a vague state which is updated later on[3].

2. Updating of reputation

The reputation of every user is updated by taking into account the past reputation values and the current evidence. The trust is updated in the following way

$$R_{i(updated)} = p_1 R_{i(past)} + p_2 r_i$$

Where $R_{i(updated)}$ is the newly reputation value , $R_{i(past)}$ is the past reputation, p_1, p_2 are fading factors and r_i is the current evidence. The current evidence is influenced by both internal evidence and external evidence[3]. The internal evidence is the value that is observed before the second user is allowed to access the channel. The internal evidence is formed by two evidences e1 and e2. *e1* is the result of the comparison between the reported data by second user and the final sensing result, *e2* is the evidence of whether more than one users make collusion attacks[3].The external evidence is the value after the second user gets access to the channel. The $r_{external}$ is set to $-p$ if the secondary user doesn't take back off or reduce the transmission power. The current trust is calculated as follows

$$r_i = w_1(-1)^{e_1} + w_2(-3)^{e_2} + w_3(-p)$$

where *w1*, *w2* are weighting factors for internal evidence.

3. Trust assessment

There are different trust states where S^1 is to denotes the reliable state, S^* denotes the vague state and S^0 denotes the discarded state[3]. The reputation of the users is updated every time the user involves in spectrum sensing and cognitive cycle. Soon after the trust updation the CBS categorizes every user into one of the three trust categories and updates the same trust values in the trust table.

4. Reward Mechanism

Based on the assessment results the secondary users are either considered eligible for incentives or punishments. Incentives can be in the form of providing priorities to reliable users in decision making or placing the reliable users in the forefront of queue while granting access to channel[3]. Punishments will result in reducing the reputation of malicious, selfish and dishonest users drastically where there is high possibility of removal from the network and low opportunities to gain access to free channel.

B. Using Trust Management to Defend against Routing Disruption Attacks for Cognitive Radio Networks

CRN emerged with the intention of efficiently enabling unlicensed users from utilizing the idle periods of licensed users on the spectrum. The cooperative spectrum sensing strategy in CRN make them vulnerable to various kind of attacks .One such problem is a routing disruption attack where occurs at the network layer. In routing disruption attacks, the malicious nodes attempt to cause packets to be dropped or extra network resources to be consumed[4]. There are different kinds of routing disruption attack like black-hole attack, selective forwarding attack, frame-up attack. Presence of a malicious node on a route may be subjected to Routing Disruption Attack can cause dropping of valuable packets on that route[4]. This work focuses on mitigating Routing Disruption Attacks. The proposed work here uses the trust value to evaluate the shared relationship among two parties. The trust is represented with the link

quality.

The link quality between two SUs is denoted by a value that represents the probability with which packets are delivered successfully [4].Link availability and packet error rate are the factors that influence link quality. If SU_i and SU_j are considered as two second users then the link quality between them governs the probability that SU *i* successfully forwards a packet to SU_j is denoted by p_{ij}. The model has three steps as given below:

1. Observation
2. Trust Update
3. Trust-based Routing Model

1. Observation

At every time t an observation on secondary user SU is made on the basis of forwarding behavior. Evaluation function $\tau(t)$ is used to determine whether the secondary user behavior is honest during the time interval t. Packet forwarding is taken as a binary event. Successful forwarding from user i to user j is represented by x_{ij}. Unsuccessful forwarding is denoted by y_{ij}. The number of successful forwarding is taken as $r_{ij}(t)$.The number of failure forwarding is taken as $s_{ij}(t)$.The probability of binary event distribution is represented using beta distribution[4].

2. Trust Update

It is always desirable to update trust values often for network efficiency. $T_{ij}(t)$is the trust history of neighboring SU j before time t. evaluation function $\tau(t)$ provides the recent forwarding behaviors of neighboring SU j during the observed time interval . Using $T_{ij}(t)$ and $\tau(t)$, trust value is updated for time t+1 as $T_{ij}(t+1)$. Weighted averaging scheme is used in trust updation [4].

$$T_{ij}(t+1) = (1-w)T_{ij}(t)+w\tau(t)$$

3. Trust-based Routing Model

When the data packet is to be sent from source i to destination j a route is considered in prior. The route selection is a dynamic activity. Initially the trust value of each secondary user is set to value 0.5[4].During the route selection process the trust value of users is taken in to account and users with higher trust values are given more importance than those with lesser values.

C. Network Cloud Simulator for Modeling Trust in CR Applications

This work proposes a network cloud simulator with trust model in it. The currently existing simulators like Cloudsim and Simgrid lack the support for modeling virtual resources and handling requests.NS2 simulator has the complete implementation of TCP/IP but it is applicable for only small data centers. So this work intends to support communication application, elements or tasks like Message Passing Interface (MPI) and workflows. The model also allows the parameters to be configured as desired.

Cooperative spectrum sensing is important in cognitive radio networks because each node determines channel usage based on own measurements and perception. Every node has a local view but not global view. Hence Sharing of information is required because a node can establish the full availability of a channel due to limited emission and reception capabilities [5].Individual nodes send their respective sensing reports to a centralized fusion centre that combines all the reports and takes a final decision

The proposed MPI algorithm for solving trust issue is solves by calculating the trust of a node $1 \le i \le n$ for each node *j* in its vicinity V_i. Node i executes the below given steps at a time instant t.

1. Based on the power received on each of the k channels, the node i *determines* its own description of the spectrum occupancy report[5].

$$Si(t) = \{si,1(t), si,2(t), \ldots, si,k(t)\}$$

2. Node i discovers the other nodes in its vicinity $V_i(t)$ by transmitting a broadcast message to all neighboring nodes, and each neighboring node responds with its NodeId[5].

3.Factors like distance to each node *j in* $V_i(t)$,power calculated by each node on each channel *k*, and using of these parameters to decide the state of each channel[5]

$$S_{i,k,j}{}^{compute} = \begin{cases} 0 \text{ if node j detects the channel k is free} \\ 1 \text{ if node j detects the channel k is busy} \\ X \text{ if node j detects the channel k is busy} \end{cases}$$

4. The information from neighboring nodes $S_{i,k,j}{}^{received}$ is received

5.The information received from the neighbor node *j in the set* Vi is compared with the set calculated by node *i* about node j[5] .

6. The node determines the number of matches by $\propto$, mismatches by $\beta$and the number of cases where no determination can be made as γ[5]

7. The trust level is computed, according to the formula [5]

$$\delta ij(t) = \frac{[1+\gamma(t)]x\alpha ij(t)}{\alpha ij(t)x\beta ij(t)}$$

D. A Jury-Based Trust Management Mechanism in Distributed CRN

Distributed CRN do not possess a control centre like CBS as in centralized CRN. The absence of the fusion centre poses several problems such as selfish users can reject collaborative spectrum sensing, malicious users would modify spectrum sensing results deliberately, and failed users affect spectrum sensing results. Thus, the accuracy of the spectrum sensing results will be decreased substantially. The proposed work tries to address this problem by a jury-based technique[6].

A "jury user" is designed to collaboratively examine the reputation of the cognitive user in the networks and to perform data fusion and spectrum allocation for distributed CRN [6]. The jury system-based trust model uses reputation values for data fusion and spectrum allocation.

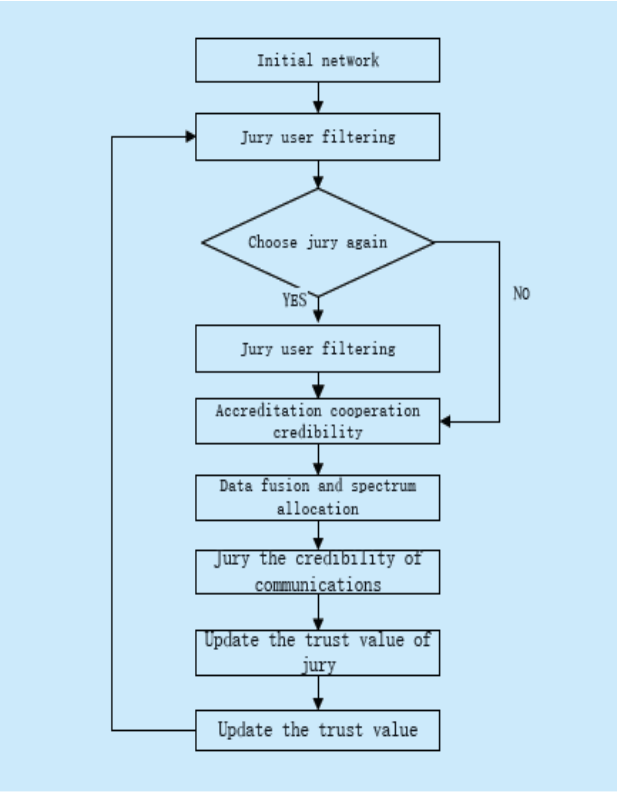

Fig-5: System architecture for jury based model

The jury-based trust management scheme for distributed CRNs as follows:

1. Selection of jury users: At the beginning the cognitive cycle, property value of existing jury users is examined[6].

2. A threshold is fixed for the number of jury users in the network according to the requirements. If the number of jury users is found to be less than the fixed threshold the election is conducted to select the jury user[6].

The requirements to be a jury user, the election process and subsequent steps are as given below.

Election qualification: If a node has to qualify for the service as a jury its reputation, online duration and remaining energy, of the cognitive user is considered[6].

a) The reputation is considered to avoid the effect of malicious users.
b) The online duration is considered because node with high online duration is normally more active
c) The remaining power is considered so that node with high energy can be provided with responsibilities to be accomplished.

Election percentage: For a given election percentage r and N_{SU} cognitive users in the trust domain, if N_j cognitive users need to be elected to serve as the jury members of this trust domain, then,

$$N_j = N_{SU} \cdot r$$

If the election percentage is low, then the network trust scheme will not be robust and resistant to security threats from juries. But a high election percentage means that more jury users will be involved in reputation evaluation, a large amount of data will be exchanged and more power will be consumed [6].

Election Process: The jury provides a parameter called "original application number" for the applicants. The users who desire to join the juries will submit their applications. Taking in to account the election qualification criteria the applicants will be allotted a number. Jury user is elected via modulo computation[6].

$$m = [\, N_A / N_j \,]$$

Where N_A denotes the number of cognitive users who are allocated application numbers. The cognitive users whose application numbers satisfy the following equations are selected to be the jury users [6]:

$$Ai \bmod m = 1$$

(3) Evaluation of collaborative reputation: The jury users evaluate how reliable the collaborative behavior of each cognitive user based on behavior characteristics of the cognitive users during collaborative spectrum sensing, and their score[6].

(4) Spectrum sensing and data fusion: the juries combine spectrum sensing data, allocate the spectrum, and publish the decision-making results .During data fusion reputation value of each cognitive user collected from their historical network behaviors to estimate accuracy and reliability[6]. Sensing reports from users whose trust value is below the threshold is discarded.

(5) Evaluation of communication reputation: The juries monitor and sense spectrum use behavior of each cognitive user during data communication, evaluate how reliable the communication behavior of each cognitive user is, and provide a score[6].

$$G_e^{\theta}(k) = \begin{cases} 1 \text{ involved in perception and accuracy in the info} \\ \delta_f \text{ involved in the perception and error in the info.} \\ \delta_m \text{ not involved in perception} \end{cases}$$

Where i and j denote the ID numbers of the cognitive users, k denotes the serial number of the current cognitive cycle

(6) Updating of reputation values of jury users: update the reputation values of jury users based on evaluation results.

(7) Updating reputation values: juries perform cross fusion of their evaluation of each cognitive user. Meanwhile, the evaluation behaviors of juries are supervised to update reputation values of other juries. Finally, total reputation values are updated [6]

$$T_c^i = \sum_{k \in Win^1} G_c^i(k).f(k)$$
$$T_p^i = \sum_{k \in Win^1} G_p^i(k).f(k)$$

$$T^i = \begin{cases} \max(T_c^i x\, \alpha + T_p^i x\, \beta + T_j^i 1) T_c^i x\, \alpha + T_p^i x\, \beta + T_j^i > 1 \\ \max(T_c^i x\, \alpha + T_p^i x\, \beta + T_j^i 1) T_c^i x\, \alpha + T_p^i x\, \beta + T_j^i < 0 \end{cases}$$

Where T_c^i denotes the collaboration reputation value of *SUi*, denotes the communication reputation value of the cognitive user, *Ti* denotes the total reputation value of the cognitive user *SUi*, and β are the weights. The reputation value is a number ranging from 0 to 1[6].

4. SUMMARY

From the above discussed various trust management mechanism we summarize their intended purpose, working, goal and applicability to type of CRN in the table-1.

Paper	A	B	C	D
Type of CRN	Centralized	Distributed	Centralized	Distributed
Purpose	To protect network from security attacks and collusion attacks	To prevent Routing Disruption attack	To avoid Byzantine attack	To examine reputation of users and to perform data fusion and spectrum allocation
Works by considering	Internal and external evidences to calculate current trust value	Link quality and forwarding behaviour	Computing the number of matches and mismatches in the calculation	Evaluation of sensing results by the elected jury members
Goal	Improve fairness and robustness Distinguish malicious users	Improve network throughput and end-to-end delay	To simulate the cognitive radio networks with higher precision	Accurate and fair trust evaluation and flexibility in spectrum allocation

Table-1: Summary table

5. CONCLUSION

Spectrum is a valuable resource in the network which every user is in need of to accomplish their own requirements. CRN which tries to use efficient utilization of idle spectrum of licensed users achieves this objective through spectrum sensing. A major requirement in spectrum sensing is the trust on the user who provides the sensing results. Trust is a major challenging factor that affects the spectrum allocation decisions. In this consideration trusting information provided by the secondary users is of keen importance. In this paper we have tried providing a overview on significance of trust management in spectrum sensing, advantages of trust management and possibility of identifying malicious users and taking appropriate actions against the identified malicious users. Several trust management mechanisms discussed in this paper have shown considerable improvements in network throughput, protection against various kinds of attacks on CRN through their simulation results. Trust management mechanism is a domain where new trust requirements arise along with new threats and attacks. With our paper we hope that the overview of some of the trust mechanisms helps in new trust management mechanism that are more efficient and secure against different kinds of attack

REFERENCES

[1] J. Mitola, III,G. Q. Maguire, Jr., "Cognitive radio: making software radios more personal", Personal Communications, IEEE, vol. 6, pp. 13, 1999.

[2] Khattab A, Perkins D and Bayomi.M. "Cognitive Radio Networks from theory to practice". Springer

[3] Qingqi Pei, Rui Liang, Hongning Li:A Trust Management Model in Centralized Cognitive Radio Networks. CYBERC 11 Proceedings of International Conference on Cyber-Enabled distributed Computing and Knowledge Discovery, Pages : 491-496

[4] Ling Hou, Angus K. Y. Wong, Alan K. H. Yeung and Steven S. O. Choy. "Using Trust Management to Defend against Routing Disruption Attacks for Cognitive Radio Networks". 2016 IEEE International Conference on Consumer Electronics-China (ICCE-China)

[5] Su Wengui1, Liao Yang2." A Jury-Based Trust Management Mechanism in Distributed Cognitive Radio Networks" China Communications July 2015:120-126

[6] George Suciu, Carmen Voicu and Gyorgy Todoran, Alexandru Martian, Simona Halunga and Cristina Butca "Network Cloud Simulator for Modeling Trust in Cognitive Radio Applications". 21st Telecommunications forumTELFOR, 2013