Trust-Based Data Conveyance by Collaborative Spectrum Sensing In Cognitive Radio Network

G. Elanagai, C. Jayasri

Abstract— Energy efficacious-cooperative spectrum sensing (EE-CSS) protocol based on Trust and Reputation Management (TRM) unit is proposed. This protocol reduces the number of sensing reports exchanged between secondary users and its base station. Trust and Reputation Management unit was proposed to alleviate the malicious behaviour in Cognitive Radio Network (CRN) and to ensure there is no link disconnection in secondary users in the network. The Experimental result shows that the energy consumption in the proposed protocol can be much lowered than other Traditional spectrum sensing method.

Index Terms —: Cognitive Radio Network, Collaborative Spectrum sensing, Data Fusion, Energy Detection, Energy efficacious, Fusion centre, Trust and Reputation.

1 INTRODUCTION

Cognitive Radio (CR) has been proposed as a solution to destroy Radio Spectrum Scarcity. In CRN communication devices changes its transmission and reception parameters for efficient utilization of spectrum this is called as Dynamic Spectrum Access. In CRN, Secondary users (SU) can sense unused licensed spectrum band. Important activity of CRN is to allocate unused spectrum holes to SU without providing interference to Primary users. Spectrum Sensing is the method used to detect the unused spectrum and sharing it. Cooperative spectrum sensing (CSS) has been proposed in which sensing reports are coming up with few decision making authorities to ensure about reliable decision on the state of spectrum usage. However in the presence of malicious SU's integrity of report need to be checked to avoid interference. Hence Trust and Reputation Management unit is used it is not only used to combat the malicious behaviour, it ensures that there is no link disconnection in the network. Since the network is coming up with few decision authorities there is no secondary users loose the chance to utilize the spectrum when they are within the range of CRN simultaneously malicious nodes are avoided to sense the spectrum. Including decision making authorities in the cognitive radio network reduces the energy consumption. Reduction of total number of sensing report is our main objective this will be achieved by using the proposed protocol. There are some spectrum sensing techniques are there which are just used to allocate the unused spectrum holes hence we including few decision making authorities in the network to produce the efficacious and trusted communication.

2 OVERVIEW OF PREVIOUS WORK

2.1 Sensing Methods

Sensing methods are vital for finding the state of spectrum band. The main methods are [1]: Matched filtering, Cyclostationary detection and Energy detection. Energy detection method is commonly used it doesn't need any knowledge of Primary User signal. Sensing reports are gathered for cooperative spectrum sensing process.

2.2 Data Fusion Technique

In centralized CRN, Fusion Centre receives sensing report from SU's and produce a final decision on state of each band. Data fusion techniques such as AND/OR rule [2] [3], KI rule [4], Majority rule [5]. There are some other techniques which use Neyman-Pearson test [6] based on Bayesian criterion.

2.3 Trust and Reputation Management

It records the accuracy of previous sensing report send by SU's and compute a trust value for each SU which is taken as a trustworthiness for future sensing. This unit is used to alleviate malicious nodes. There are several different methods used to calculate the trust values, important of them are Abnormality Detection [3], multistage filtering and Beta distribution. These methods are proposed to defend against malicious attacks. Normally transmission of sensing reports leads to signaling overhead. Sensing reports needs energy for transmitting and receiving. Traditional CSS methods [8], [9] requires at least of one sensing report from each secondary users which leads to increase in Bandwidth and energy. Few studies are coming up with reducing bandwidth usage. In [10] uses two decision thresholds, SU compare its sensed energy with two thresholds and finds whether channel is idle or busy here sensing reports are reduced but energy used was high. In [11], a brute force approach is used to find the optimum number of reports needed in this approach sensing reports are drastically reduced but there is signaling overhead and high energy usage. To overcome those approach disadvantages EE-CSS protocol is proposed. In our proposed method TRM unit is not only used to combat the attacker it ensures that there is no link outage between secondary users and the cognitive radio network.

3 NETWORK SIMULATOR SOFTWARE

NS is a discrete event simulator targeted at network research. NS provides technical substantial support for simulation of TCP, Routing and multicast protocols over wired and wireless network.

NS-2: Network simulator version 2. It is a packet level discrete event simulator which provides substantial support to simulate bunch of protocols which is considered as an advantage over NS-3.It is primarily UNIX based and uses TCL as its

scripting language.

Simulation Workflow:

a) Implement protocol model.
b) Setup simulation scenario by defending topology.
c) Run simulation (i.e.TCL file).
d) Analyze simulation result.

4 Proposed System

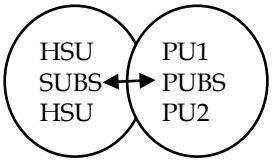

Figure 1.System Model

Fig 1 shows the system model for proposed CRN. Here we are using H -Honest secondary users (HSU) and one Primary user base station (PUBS) and secondary user base station (SUBS) and three primary users (PU).Here SUBS and PUBS base stations are communicated so that PUBS conveys State Band Matrix (SBM) which includes the state of the licensed band. Here Fusion Center (SUBS) requests all SU to sense one band. BSM allows FC to calculate accuracy of its report in addition with the report from SU's.

4.1 Energy Detection Technique

The signal, yn (t), n = 1…N, is the SU's received signal under the idle and busy channel hypotheses, denoted as H0 and H1,

$$H_0: Y_n(t) = W_n(t)$$
$$H_1: Y_n(t) = h_n S(t) + W_n(t)$$

Where s (t), and wn (t) denote the transmitted signal from PUBS. It is assumed that the CSS is performed over one time slot. As derived in [12], the sensed energy Un (K) of the channel at SU is given by

$$U_n(K) = \sum^{2TW-1} yn, k[i]^2$$

In our proposed approach it is calculated using spectrum sensing unit .The local decision at SU for time slot k is

$$Dn(k) = 0 \text{ if } U_n(k) < \text{threshold value}$$
$$Dn(k) = 1 \text{ if } U_n(k) > \text{threshold value}$$

Dn (k) = 0, 1 correspond to hypotheses H0 and H1 respectively.

4.2 EE-CSS

The Proposed EE-CSS has two main components Contention-free Media Access Protocol (MAC) and Data Fusion scheme at FC.

4.2.1 **MAC Protocol**

It uses mini time slots in two phases. It reduces the sensing report based on the observation that HSU agree on the spectrum usage more than disagree.

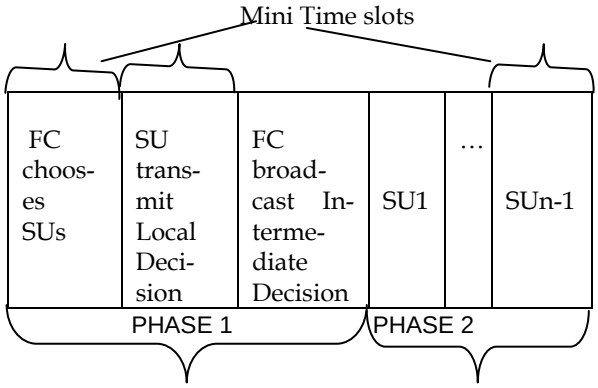

Figure 2 Phases in EE-CSS

PHASE 1:

Based on Trust value of each SU, FC chooses set of Su's to sense the band and transmit the report to FC. FC fuses report from the chosen secondary users with its local decision and broadcast intermediate decision to all SU's.

PHASE 2:

If a SU disagrees with Intermediate decision or doesn't receive the broadcast message reliably it can indicate via transmission. Assume that FC broadcasts special request messages occasionally asking each SU to explicitly transmit sensing reports in their allocated mini time slots. FC ignores the implicit reports from SU's to prevent it from being rewarded or penalized whey they are not in the range of CRN or might be a malicious one.

4.2.2 Data Fusion

Sensing report received from SU's are fused with FC's local decision in fusion process using OR rule to form an Intermediate decision, this is called as Data fusion.

$$Dint(K) = DFC(K) \text{ OR } Dn(K)$$

Where Dint (K) denotes intermediate decision Dn (K) denotes the local decision from SU's to Fusion Centre and DFC (K) denotes FC's local decision.

4.2.3 Final Decision

Finally FC has N sensing reports for the spectrum band including the local FC decision. The FC uses the following Trusted-Weighted sum function to determine the final decision, D (K), at the time slot K. Here we implement the majority rule at the FC by setting threshold as Zero.

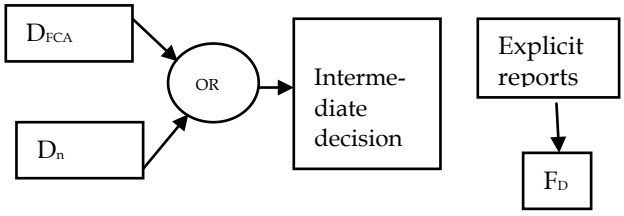

Figure3. Sensing Decision Process at FC

Here DFC is the local decision generated at the Fusion

Centre and Dn is the local decision generated at the SU's and both decisions are OR together and intermediate decision is generated and then SU's are requested to send Explicit reports ,some Malicious user or secondary users not in the range sends implicit reports too. Based on that Final decision is generated and the spectrum is allocated to each secondary user's and band state matrix is also updated.

4.3 Trust Model

The information contained in the base state matrix is used to report the trust value based on the previous sensing reports. In beta frame work probability value of correct decisions over total number of decision is calculated

$$Tn\ (K) = \sum^{k}_{i=1} Pn\ (i) \,/\, \sum^{k}_{i=1} (Pn\ (i) + Nn\ (i))$$

Where Pn (i) is reward and Nn (i) is penalty of its respective decisions.

5. Analysis Snapshot

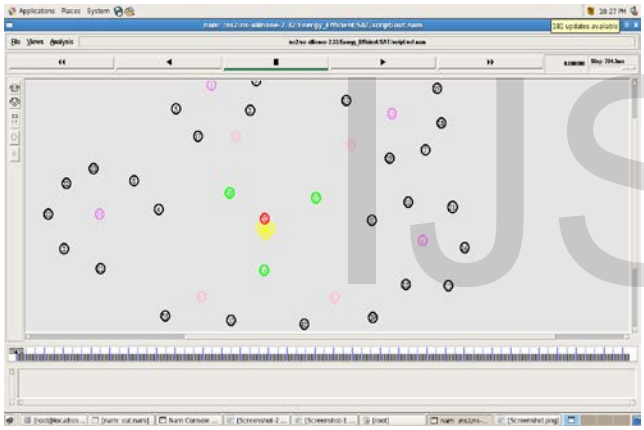

Figure 4 Secondary users shown as cluster nodes and heads, including TRM unit (NS2 working snap).

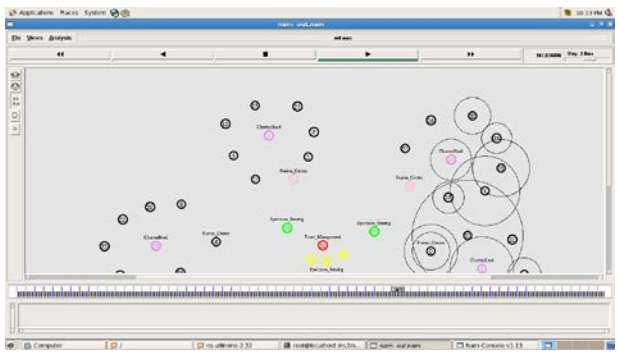

Figure 5 Communication takes place in NS2 software based on our proposed Protocol.

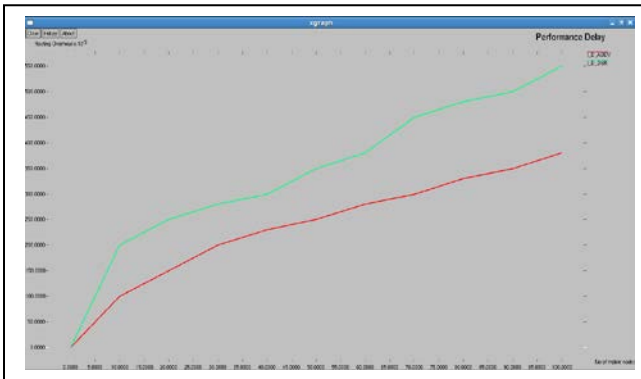

Figure 6 X-Graph output showing performance delay in EE-CSS and T-CSS protocols.

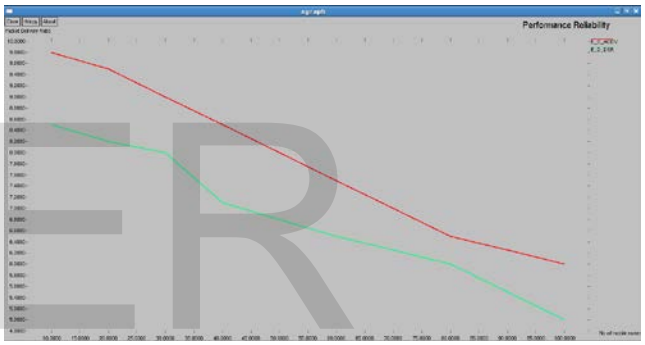

Figure 7 X-Graph output showing performance Reliability in EE-CSS and T-CSS protocols.

6. ROUTING PROTOCOLS

Normal routing protocol used by the Traditional Collaborative Spectrum sensing process was Dynamic Source Routing (DSR) but the overall efficiency reached was below 80 percentage only.Hence we are using Adhoc-On Demand-Distance Vector Routing (AODV) protocol which is more reliable than that protocol.AODV is chosen for another reason also that is in our proposed work we are including forward and backward processes.

7. CONCLUSION

Empirical Analysis without Malicious node is performed and the result is generated which shows that the Energy consumption in EE-CSS protocol is reduced based on Performance delay which shows that the number of sensing reports exchanged between secondary users and its base station was reduced.Performance Reliability graph is generated

which shows that our proposed protocol is more reliable than other traditional CSS protocol. Hence without including malicious node we had reduced total number of sensing reports exchanged than traditional one, which shows this proposed method is more energy efficient.
This work proves there is no link outage in the network hence requested secondary user's spectrum utilization was going correct which will be user-friendly part of our work.

7 Future Work

Including malicious nodes in the cognitive radio network and proceeding with the same protocol is our Future work which will ensure this protocol makes the CRN more authenticated whereas none of the existing systems considered malicious user.This is the future work proposed to considering the security issues in Cognitive radio network.

References

[1] T.Yucek and H. Arslan "A Survey of spectrum sensing algorithms for cognitive radio networks", IEEE Commun Surveys, vol 11, 2009.
[2] A. Ghasemi and E.Sousa, "Optimization of Collaborative Spectrum Sensing", J Commun, June 2007.
[3] H.Li and Z.Han "Catch me if you can: An abnormality detection approach for CSS in Cognitive radio networks", IEEE Transaction, Wireless Commun, Nov 2010.
[4] A.Sahai and S.Mishra"Cooperative Sensing among Cognitive Radios", IEEE ICC, 2006.
[5] Z.Quan and A.Sayed "Optimal linear cooperation for spectrum sensing in cognitive radio networks", IEEE J.Sel.Topics, Vol no2, Feb 2008.
[6] E.Visotsky, S. Kuffner and R.Peterson "On collaborative detection of TV transmission in support of dynamic spectrum sharing", IEEE DySPAN, 2005.
[7] H.Li and Z. Han "Collaborative spectrum sensing with stranger: Trust, or not to trust? ", IEEE WCNC, 2010.
[8] H.Li, Y.Sun and Z.Han "Attack-proof Collaborative spectrum sensing in Cognitive Radio Network", IEEE CISS, 2009.
[9] T.Clansy and N. Goergen "Security in Cognitive Radio Networks: Threats and Mitigation", in Proc.EAI Int.Conf. Crowncom, 2008, pp 1-8.
[10] L.Duan, L. Zhang, Y. Chu and S. Liu "Cooperative spectrum sensing with double threshold detection based on reputation", IEEE WiCOM, 2009.
[11] Y.Chen "Optimum number of secondary users in collaborative spectrum sensing considering resource efficiency", IEEE Commun Letter, Dec 2008.