International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

Network Security Based Data Televising by Fraternization Spectrum Sensing in Cognitive Radio Network

G. Elanagai[1]
PG Scholar, Dept. of ECE
AVC College of Engineering
Mannampandal, Mayiladuthurai

C. Jayasri[2]
Assistant Professor, Dept. of ECE
AVC College of Engineering
Mannampandal, Mayiladuthurai

***Abstract*— Nowadays the Challenging task of Cognitive Radio Network is enabling the network security. There was many more Energy efficient Traditional spectrum sensing methods are their but they doesn't bother about the network security. Hence Fraternization Spectrum Sensing (FSS) protocol based on Trust and Reputation Management is proposed, this is nothing but cooperative sensing process. By this proposed protocol we are calculating Trust values for each secondary user's and find out attackers and drop them out from the network. Secondly this proposed method can improve the energy efficiency and reducing delay of existing system**

Keywords*— *Trust and Reputation Management (TRM), Fraternization Spectrum Sensing(FSS), Network Security, Energy Efficiency, Cognitive Radio (CR)

I. INTRODUCTION

Cognitive radio is a Software-defined radio that can able to access unused radio spectrum holes efficiently. The definition adopted by Federal Communications Commission (FCC): "Cognitive radio: A radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets." FSS protocol based on Trust and Reputation Management unit is proposed. The main advantage of this protocol is NETWORK SECURITY whereas none of the traditional methods bother about Network security. By using TRM unit we found the attacker nodes and drop it out from the network and enable the network security. Energy Wastage is the major problem in Traditional CSS method due to more number of sensing reports exchanged .We are using fusion scheme to reduce the total number of sensing reports i.e. sensed energy of each secondary users. The main objective of this paper is find out and drop the attacker nodes from the network, improves the energy efficiency, and reduces the bandwidth consumed by using Hybrid routing algorithm. Beta framework is the method used to find the trust values of each secondary user in the network. From the trust values we can identify the attackers and drop them.

II. DRAWBACKS OF PREVIOUS WORK

CSS techniques can be used in conjunction with TRM to improve the utilization of spectrum holes in CRN's. However, the transmissions of sensing reports from su's can represent a significant overhead. Each sensing report requires energy for transmission, processing, and receiving. Because the number of SU's increases, the energy and bandwidth requirements. The traditional CSS (TCSS) methods in require at least one sensing report from each SU in each time slot. We are interested in strategies which use bandwidth and energy efficiently while satisfying target false alarm (FA) and missed detection (MD) probabilities. A few studies have examined the energy and bandwidth overhead costs associated with CSS methods. The number of reports required from each SU for every spectrum band state evaluation (SBSE) for a method based on weighted sequential probability ratio test (namely WSPRT), DF, and methods based on neyman-pearson test and Bayesian criterion are discussed. In WSPRT the fc receives multiple independent sensing reports from each SU for each SBSE given that the spectrum band under investigation remains unchanged. However, in the other methods the FC only receives one report from each SU for each SBSE. The authors propose an energy detection technique which can reduce the number of reports transmitted by SU's. The technique uses two energy decision thresholds, denoted by $\lambda 1$ and $\lambda 2$, instead of the conventional single energy decision threshold, λ. Sun compares its detected energy, denoted by Un, with $\lambda 1$ and $\lambda 2$ and proceeds as follows:

- If $Un \geq \lambda 2$, the SU decides that channel is busy, i.e. H1
- If $Un \leq \lambda 1$, the SU decides that channel is idle, i.e. H0.
- If $\lambda 1 < Un < \lambda 2$, the SU has low confidence in its decision and does not send are port to the FC.

This method reduces the number of sensing reports sent to the FC. Thus, energy is used more efficiently. A brute force approach is proposed to find the optimum number of reporting su's needed when bandwidth (or energy) efficiency, global false alarm probability (denoted by Q_f), and global detection probability (denoted by Q_d) are considered. An objective function which weights Q_f , Q_d, and bandwidth (or energy) usage is optimized with respect to the number of reporting su's. Although more sensing reports from su's can improve the CSS decision, they also increase signaling overhead, energy consumption, delay before final decision,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

and computational costs. The results show that the number of transmitted reports can potentially be reduced. The number of cooperating su's is optimized given λ, the signal to-noise ratio (SNR) of the PU signal sensed at the SU, and the decision threshold, Dth, at the fc subject to satisfying Qf + Qd < ϱ, where ϱ is defined as the total error rate limit and Qmd = 1 − Qd denotes the global missed detection probability. Unfortunately, the constraint Qf + Qd < ϱ used in does not guarantee that is the target probability, and Qmd is the target md probability.

III. PROPOSED SYSTEM

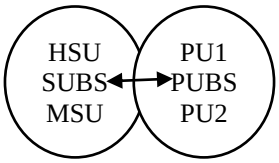


Figure 4.1 CRN Model

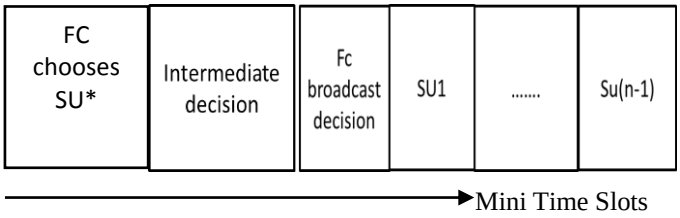
Fraternization Spectrum Sensing (FSS) is our proposed protocol. This protocol is composed of main component is Media access control protocol.

3.1 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.

Step 1: Based on the trust value of each SU, FC chooses set of SU's to Sense band and transmit report in mini time slots.

Step2:FC broadcast a message containing the list of chosen SU's and fuses report and broadcast to other su's.



Step3: If an SU disagrees with intermediate decision so it can indicate via explicit transmission in mini time slot remaining SU's are treated as agreement with FC's decision. **Data fusion** is done to form an intermediate decision which was send to all SU's and asks for an explicit report. SU's outside sensing region and attackers gives implicit report hence FC ignores it and also helps Su's for being rewarded or penalted. By this way it avoids the attackers and also users which are outside the spectrum range to operate the spectrum hence the system is Trust worthy and there is no link outage as well as energy consumption was reduced.

3.2 Wireless Routing Protocols

- **Reactive** (AODV,DSR,TORA) on demand
- **Proactive** (DSDV,OLSR,WRP) table driven
- **Hybrid** (ZRP) combination of reactive and proactive.

In this paper we are going to compare three routing protocols to choose the best one that suits our model. Comparison is made between AODV and DSR and with Hybrid and AODV.

3.2.1 AODV

Adhoc-On demand–Distance-**V**ector is the algorithm used here it enables dynamic, multihop routing between the nodes.It allows the nodes to obtain the routes quickly and the operation is loop-free one and it has setup of reverse/forward pointers. The major advantage of this algorithm is it avoids link breakage, AODV causes affected set of nodes to be notified, so we can invalidate the route using lost link.
Route Request (RREQ's), Route Replies (RREP's) and Route Errors (REER's) are the message types defined by AODV algorithm.

Advantages of AODV

Highly suitable for more number of nodes.Use of periodic indication messages to track neighbours the messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network. The connection setup delay is less. RERR (Route error) is defined so we can avoid link breakage.

3.2.2 Dynamic Source Routing

DSR uses source routing concept. When packets are flooded by a source node, the sender node caches complete hop-by-hop route to the receiver node. These route lists are caches in a *route cach*e. The data packets carry the source route in the packet header. DSR uses Route Discovery process to send the data packets from sender to receiver node for which it does not already know the route, it uses a ***route discovery*** process to dynamically determine such a route. In Route discovery DSR works by flooding the data packets in network with ***route request*** **(RREQ)** packets. RREQ packets are received by every neighbor nodes and continue this flooding process by retransmissions of **RREQ** packets, unless it gets destination or its route cache consists a route for destination .Such a node replies to the RREQ with a ***route reply*** **(RREP)** packet that is routed back to real source node .source routing uses RREQ and RREP packets. The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path toward the back. The source caches backward route by RREP packets for upcoming use. If any connection on a source route is wrecked, a *route error* (RERR) packet is notified to the source node.

3.2.3Hybrid Routing Protocol (HRP)

HRP is a hybrid protocol that separates the network into several zones, which makes a hierarchical protocol as the protocol ZHLS (zone-based hierarchical link state). HRP is based on GPS (Global positioning system), which allows each node to identify its physical position before mapping an area with table to identify it to which it belongs. The number of messages exchanged in high ZHLS is what influences the occupation of the bandwidth. Our protocol attempts to reduce the number of messages. Hence the network is zoned in HRP there is no need of periodic updates about the network's source and the bandwidth

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

consumption and the number of reports exchanged is highly reduced.

IV ANALYSIS SNAPSHOT

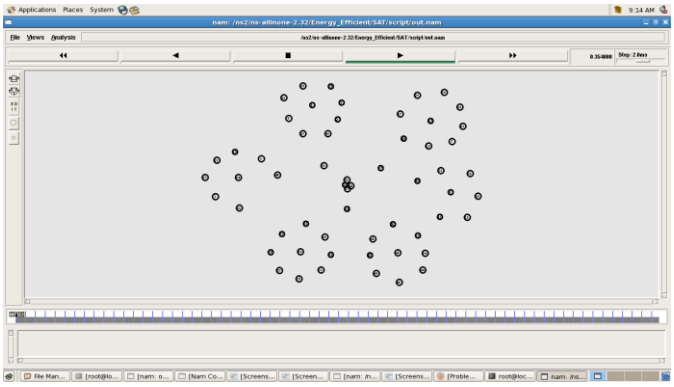


Figure 4.1 Working Snap of NS2

According to Hybrid Routing Protocol Secondary user nodes are clustered up

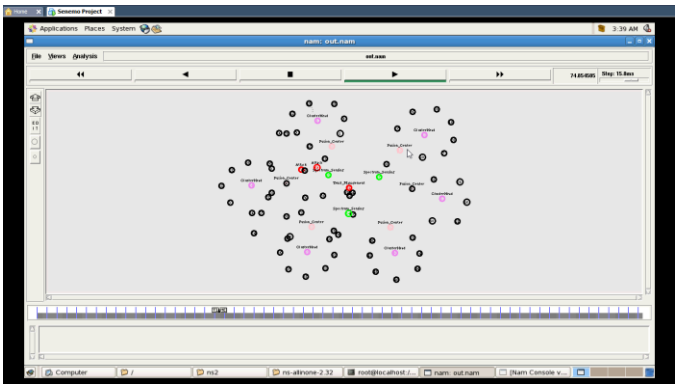


Figure 4.2 Seperation of TRM unit, Spectrum Sensing unit

Nodes in Black colour are Secondary user and nodes in Red colour are attackers they are found and dropped by our proposed method

In the below figure 4.3 Red strike shows AODV and Green Strike Shows the Hybrid Protocol.This graph proves that our Hybrid routing protocol is more energy efficient than AODV.

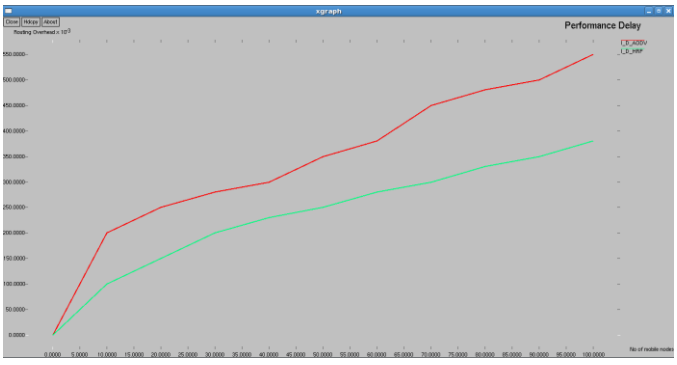


Figure 4.3 Performance Delay comparsion over AODV and Hybrid Protocol.

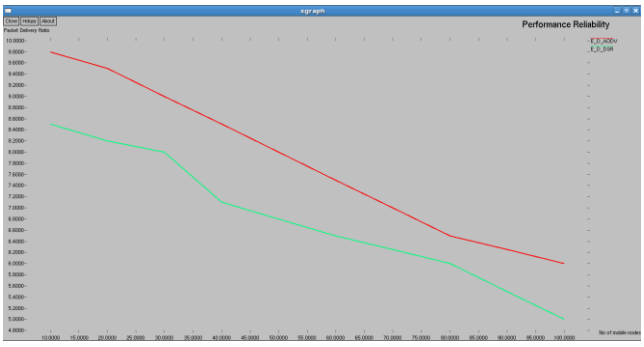


Figure 4.4 X-Graph output showing performance Reliability in AODV and DSR protocols

For enabling the network security we are considering the CRN model containing both Honest and Malicious nodes and our Proposed Protocol is applied and the algorithms such as AODV and Hybrid and DSR are Performed in that model.Performance delay and Performance Reliability are compared between these protocols.Finlly the network performs with hybrid protocol was highly reliable and has less delay.

REFERENCES

[1] A Survey of spectrum sensing algorithms for cognitive radio networks, T.Yucek and H. Arslan, IEEE Commun Surveys, vol 11, 2009.
[2] Optimization Of Collaborative Spectrum Sensing, A. Ghasemi and E.Sousa, J Commun, June 2007.
[3] Catch me if you can: An abnormality detection approach for CSS in Cognitive radio networks, H.Li and Z.Han, IEEE Transaction, Wireless Commun, Nov 2010.
[4] Cooperative Sensing among Cognitive Radios, A.Sahai and S.Mishra, IEEE ICC, 2006.
[5] Optimal linear cooperation for spectrum sensing in cognitive radio networks, Z.Quan and A.Sayed, IEEE J.Sel.Topics, Vol no2, Feb 2008.
[6] On collaborative detection of TV transmission in support of dynamic spectrum sharing, E.Visotsky, S. Kuffner and R.Peterson, IEEE DySPAN, 2005.
[7] Collaborative spectrum sensing with stranger: Trust, or not to trust? , H.Li and Z. Han, IEEE WCNC, 2010.
[8] Attack-proof Collaborative spectrum sensing in Cognitive Radio Network , H.Li ,Y.Sun and Z.Han, IEEE CISS,2009
[9] Cooperative spectrum sensing with double threshold detection based on reputation, L.Duan, L. Zhang, Y. Chu and S. Liu, IEEE WiCOM, 2009.
[10] Optimum number of secondary users in collaborative spectrum sensing considering resource efficiency, Y.Chen, IEEE Commun Letter, Dec 2008.
[11] Yi Zheng, XianzhongXie, Lili Yang, "Cooperative Spectrum Sensing Based on Blind Source Separation for Cognitive Radio",International Conference on Future Information Network(ICFIN),pp. 398-402, Oct 2009.
[12] I. F. Akyildiz, W.-Y. Lee, M.C. Vuran, S. Mohanty, "NeXt Generation / dynamic spectrum access/cognitive radio wireless Networks : a survey", Computer Networks, vol. 50, no. 13, pp. 2127–2159, 2006.