Enhancing Detection Rate in Selfish Attack Detection Scheme in Cognitive Radio Adhoc Networks

Sneha Thankachan M.E[1], M.Jebakumari M.E,[2]

[1] *Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore*

[2] *Associate professor, Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore.*

Abstract— **Cognitive radio (CR) is a significant communication technology in which the unlicensed users use the maximum available bandwidth. When the spectrum is not used by the licensed primary user, the obtainable channels are allocated for the unlicensed secondary users (SUs). But the problem is that some of the secondary users act selfishly to occupy all the channels. Hence, in order to overcome this problem, a selfish attack detection technique called COOPON (Cooperative neighboring cognitive radio Nodes) is in use where the secondary user frequently broadcasts the multiple channel allocation information to all its neighboring secondary users. If the selfish secondary user sends a larger number of channels than the available channels, this method detects the attacks by the cooperation of other legitimate neighboring secondary users. But the drawback of this method is that it is capable of detecting only one selfish node. To conquer this trouble and to detect selfish users effectively an innovative technique called distributed reaction mechanism is proposed in this paper which detects multiple selfish attacks and improves the detection rate by considering the parameters like traffic flow, signal strength and primary user access time.. Experimental results show that high accuracy and efficient detection performance in cognitive radio networks are achieved compared to the existing system.**

Keywords— **Cognitive radio network, Selfish attack, Distributed mechanism, channel state information**

I. Introduction

Due to the enormous growth in the utilization of wireless communication devices, there is an increasing need for high spectrum bands. In conventional spectrum management, the spectrum is allocated to the licensed users for limited use. A cognitive radio technology is carried in two steps: Firstly, by utilizing the spectrum-sensing technology it finds the obtainable spectrum bands for the secondary users. If the spectrum is not used by the licensed primary users, the secondary user utilizes the available spectrum. Secondly, the obtainable channels are allotted to the secondary users. Suppose, if the primary user is in the cognitive radio network, the secondary user releases the spectrum band immediately.

In the cognitive radio network, some of the secondary users try to use all the available channels. This can be carried out by transmitting the false channel state information. If a secondary user identifies the occurrence of a primary user, the secondary user won’t use the licensed channels. Actually the secondary user knows the currently available channels by broadcasting the sensing channel state information. So, in this case a selfish secondary user sends fake channel state information to all its neighbors in order to occupy all the available channels. If a selfish secondary user uses only two out of five channels, it will broadcast that all five channels are in use and occupy all the channels.

To distinguish the selfish attack in the cognitive radio networks, a selfish attack detection method called Cooperative neighbouring cognitive radio Nodes (COOPON) [11] is used where single selfish attack detection toward multiple channel access is focused. Every secondary user broadcasts the current channel state information to know the status of the channels. So, the secondary user sends fake information to occupy all the obtainable channels. By utilizing the COOPON technique, a selfish secondary user can be detected by the cooperation of other legitimate neighbouring secondary users. But this method is able to detect only one selfish node; it cannot be used to detect multiple selfish nodes in the cognitive radio network. We propose a distributed reaction mechanism in which adaptive and non adaptive schemes are being used based on local information like traffic flow, primary user access time and signal strength to enhance the detection rate and to avoid the selfish misbehaviours of the nodes in the cognitive radio networks.

II. LITERATURE REVIEW

Stephen B. Wicker et.al suggested a game-theoretic model of multi-packet slotted Aloha with perfect information [1]. In this, there a central control containing systems where the system designer decides which nodes in the system must execute based on an algorithm. As the size of the networks and the diversity of node necessities in the network grows, however exerting direct central control on a network becomes computationally inflexible. Additionally, in open network specifications users have an incentive to alter their communication nodes to enhance the network performance, making it impractical to make sure that a particular algorithm will be run by all of the nodes in the network.

Haojin Zhu et.al proposed a method to find the probable security threats towards the collaborative spectrum sensing in cognitive radio networks [2] and to locate several privacy related attacks in collaborative sensing reports and their physical location. To avoid these types of attacks, a new privacy preserving framework is proposed in collaborative spectrum sensing to prevent location privacy leaking. But the drawback of this method is inadequate security.

Youyun Xu et.al suggested an optimization of cooperative spectrum sensing in which multiple cognitive users assist to accomplish higher detection accuracy with least sensing error probability in multiple cross-over cognitive radio networks. This analysis focuses on two fusion strategies: soft information fusion and hard information fusion [3]. In the soft information fusion, for the energy detector the optimal threshold is derived in both non-cooperative single-user and cooperative multiuser sensing scenarios. For the hard information fusion, based on the rule of minimum sensing error (MSE) the optimal randomized rule and the optimal decision threshold are derived.

Jung-Min Park et.al suggested to identify a threat for spectrum sensing, which is called primary user emulation. In this type of attack, an attacker cognitive radio transmits signals whose uniqueness emulates those of incumbent signals [4]. The extremely flexible, software-based air interface of cognitive radios makes such an attack possible. To detect this attack, a transmitter verification scheme called LocDef (localization based defense), that verifies whether a given signal is that of an incumbent transmitter by calculating its location and examining its signal characteristics. A localization based non-associative scheme is used to evaluate the position of the signal transmitter which was not proved to be effective.

Peng Ning et.al proposed a novel method for validating primary user signals in cognitive radio networks [5]. This method combines cryptographic signatures and wireless link signatures to assure primary user detection (not selfish nodes) in the occurrence of adversaries. An essential concept in this method is a helper node placed physically close to a primary user. The helper node acts as a bridge to ensure a secondary user to validate cryptographic signatures which can be carried by the helper node's signals and then attain the helper node's reliable link signatures to validate the primary user's signals.

Omid Fatemieh et.al suggested a new method called Classification Using Signal Propagation which is based on machine learning that utilizes a trusted initial group of signal propagation data in a region as input to build a classifier by utilizing support vector machines. This classifier is consequently utilized to detect integrity violations [6]. By using classification, it avoids the requirement of random postulations about the propagation of the signals and parameters in favor of direct training data. But the drawback of this method is there is less security and high computation complexity.

Beibei Wang et.al suggested an evolutionary game framework for multi-user decentralized cooperative spectrum sensing [7] to obtain the behavior dynamics and the evolutionarily stable strategy(ESS) of the secondary users and after that prove the dynamics converge to the ESS that renders the opportunity of a decentralized system of the sensing game. Based on the dynamics, it is possible to to extend a distributed learning algorithm so that the secondary users approach the ESS exclusively based on their own payoff annotations.

T-H. Hubert Chan et.al suggested new Private Stream Aggregation (PSA) algorithms that permits users to upload stream of encrypted data of an untrusted aggregator and permit the aggregator to decrypt aggregate statistics for every time interval with an appropriate capability [8]. The aggregation scheme is aggregator insensible as it is not capable of learning any inadvertent information or assuring the distributed differential privacy for each individual contributor. This scheme is highly expensive too.

David C. Parkes et.al suggested the non-cooperative activities of mobile nodes with a game-theoretic method, in which every player intends at increasing its location privacy at a minimum cost [9]. Firstly to estimate the Nash symmetry in n-player entire information games. Since mobile nodes in a privacy-sensitive system do not identify their opponents payoff's and then think imperfect information games,to generate that symmetric Bayesian-Nash symmetry with simple threshold approaches in n-player games is used and it extends the equilibrium strategies.

Insoo Koo et.al suggested a cooperative spectrum sensing scheme for collaborative users in which the sensing reliability of each individual user is used to develop local and global sensing performance, and diminish the number of reports transmitted through the control channel between cognitive radio users and the fusion center (FC) [10]. By using this method, few users satisfying the reliability thresholds will broadcast their local decisions to the FC one by one according to the state order of their credibility.

III. SELFISH ATTACK DETECTION SCHEME

In the cognitive radio network, to discover the selfish attack a technique called COOPON is used. Each secondary user simultaneously broadcasts the current channel state information to all of its neighboring secondary users to estimate the status of the channel. The selfish secondary user uses this opportunity to send the fake channel state information. This technique will distinguish the selfish attacks by the cooperation of other legitimate neighboring secondary users. The entire neighboring SUs exchange the channel allocation information both received from and sent to the target SU, which will be examined by all of its neighboring SUs. After that each and every individual secondary user will evaluate the total number of channels reported by the target node to the total number of channels reported to be currently used by all of the neighboring SUs. If there is any difference between them, all the legitimate SUs will recognize a selfish attacker.

A. Detection Mechanism

The common control channel is used to broadcast the channel state information for the secondary users. The common control channel is used particularly for managing information. The channel allocation information is broadcasted to all the neighbors. A selfish secondary user sends the false channel allocation information to the neighboring secondary users.

Once the adversaries occupy the available channels, it sends the maximum number of channels than those in actual use. The detection mechanism in COOPON is exclusively designed for adhoc networks. According to the exchanged channel state information the autonomous decision capability of an ad-hoc communication network is identified. Moreover the entire neighboring nodes sum the numbers of currently used channels sent by the target node concurrently. Every individual neighboring node compares the summed numbers sent by all neighboring nodes to the summed numbers sent by the target node to verify whether the target secondary user is a selfish attacker. After that, all the neighboring nodes discover the target secondary user is a selfish node or not. This can be accomplished by the cooperative behavior of neighboring nodes. In the algorithm the sum value is calculated for all currently used channels in the target node and the neighboring nodes in two steps $Channel_{target-node}$ and $Channel_{neighbouring-node}$. After that comparison takes place for these two values. If the number of channels computed in target node is larger than number of channels in channel neighboring node the detection mechanism finds that the target node is a selfish node. The flow chart for selfish attack detection is shown in figure 1.

IV. Distributed Reaction Mechanism

To detect more than one selfish nodes in cognitive radio networks, an innovative technique called Distributed reaction mechanism is introduced. This mechanism provides some alterations in Binary Exponential Back off (BEB) and it can be used in Distributed Coordination Function (DCF) mode and process two reaction methods for detecting the selfish nodes. The first method is non-adaptive and it is used to detect aggressive misbehaviors. The second method is called adaptive and distributed algorithm that permits genuine nodes to regulate their reaction over time in response to the level of misbehavior detected in the network Furthermore, the misbehaving user may modify its behavior, and the number of misbehaving users could change over time. So, there is a need for a uniform, adaptive, and distributed reaction mechanism wherein the genuine users are able to adjust their reaction over time.

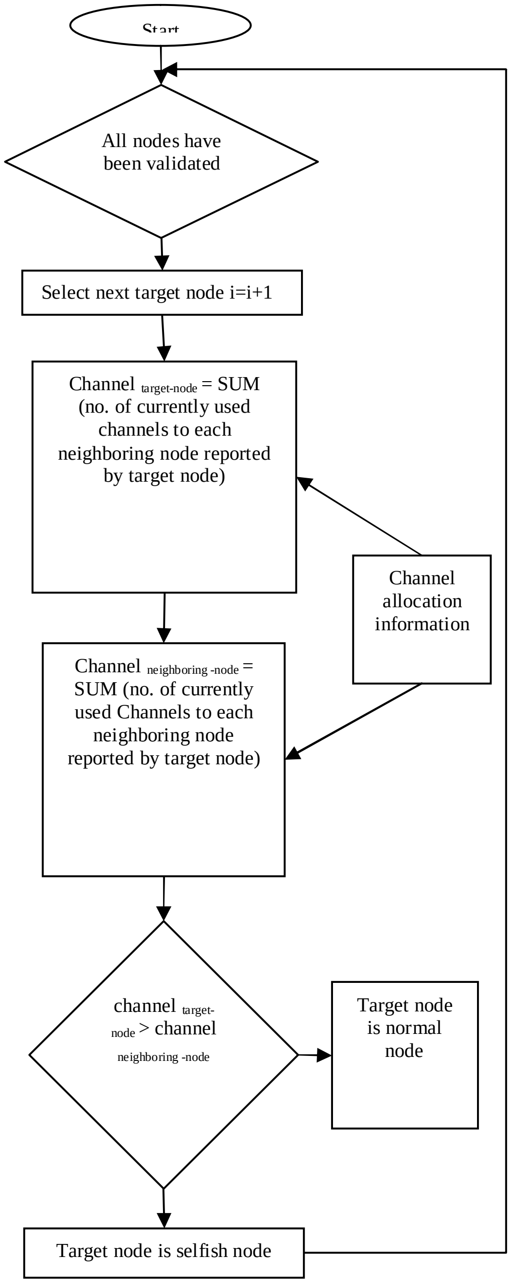
Start
All nodes have been validated
Select next target node i=i+1
Channel target-node = SUM (no. of currently used channels to each neighboring node reported by target node)
Channel allocation information
Channel neighboring -node = SUM (no. of currently used Channels to each neighboring node reported by target node)
channel target-node > channel neighboring -node
Target node is normal node
Target node is selfish node

Fig 1. Flow chart for selfish attack detection

The misbehaviors do not give away supplementary throughput to the misbehaving node, and does not cause throughput degradation of genuine users. Other parameters, including channel state information ,traffic flow, primary user access time and signal strength are also considered

A. Non-Adaptive Reaction Mechanism

This mechanism considers the N nodes in which all nodes are genuine. These nodes correctly follow Binary Exponential Back off. A lower bound on the channel access probability of a node is derived. Every time, a node selects a back off value uniformly at random from [0,..CW-1], it selects CW-1 with the probability value $\frac{1}{CW}$. Node A selects back off values in this way every time. The access probability of node A indicated τ_A is minimum while the node selects the largest back off value in the permitted interval every time. Using Markov Chain analysis, we characterize the steady state probabilityτ_{min}.

$$\frac{\tau_{min}}{\tau} = \frac{1}{2} + \frac{(1-2p)}{2W_0[(1-p)-p(2p)^m]}.$$

B. Adaptive Reaction Mechanism

An adaptive and distributed reaction method is designed for the genuine nodes to react against mildly selfish misbehaviors. Every genuine node evaluates its throughput degradation with respect to its saturation throughput share T_0 given. The reaction aggressiveness is made proportional to the level of alleged selfishness, and in most cases, the reaction is not as strong so as to lower the overall network throughput terrifically. The saturation throughput scenario with N nodes is to be considered. By using Bianchi's let the individual fair throughput of every node under saturation conditions equal toT_0.

V. Experimental results

Experimental results show the performance of the existing and the proposed systems. In the existing method, a selfish attach detection method called COOPON is used. In the proposed method, distributed reaction mechanisms (DRM) is being tested. The performance is evaluated in terms of detection rate and throughput.

A. Detection Rate

Detection rate is defined as ratio of number of detected selfish secondary users to number of actual selfish secondary users.

Figure 2 . Shows the performance comparison of COOPON with DRM based on detection rate. In order to scrutinize how selfish secondary user density influences detection accuracy, the experiment was conducted with 50, 100, and 150 secondary users, respectively. On the other hand, the detection ratio is found to be very sensitive to selfish secondary user density. If the density of selfish secondary users in the cognitive radio network increases, the accuracy of detection ratio decreases rapidly. The reason is that it is highly possible that more than one selfish secondary user exists in a neighbor with higher selfish node density and in turn they can exchange wrong channel allocation information. If the node density is increased, the detection ratio is increased in the distributed reaction mechanism when compared to the existing selfish attack detection method.

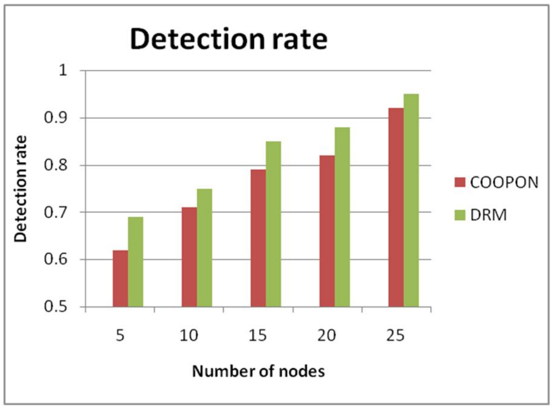

Fig 2 Detection rate

A. Throughput

Throughput is defined as the rate of victorious message received at the receiver over a communication channel. This data may be distributed over a physical link, or pass via a particular network node. The throughput is typically evaluated in bits per second (bps) and sometimes in data packets per second or data packets per time slot.

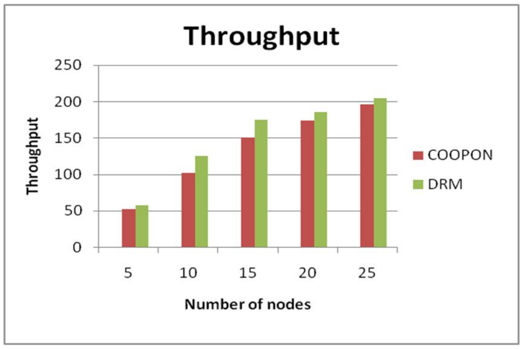

Fig 3 Throughput

Figure 3 Shows performance comparison of COOPON with DRM based on throughput. If the density of the node increases the throughput value increases in the distributed reaction method when compared to the existing selfish attack detection method.

VI. Conclusion and future work

Cognitive radio network is used to achieve efficient utilization of the spectrum. In this paper, we proposed an innovative detection approach called Distributive Reaction Mechanism to detect selfish nodes in Cognitive radio network. It overcomes the disadvantages of existing techniques such as reduced detection rate in the presence of more than one selfish node and degradation in performance By using this method it has been made possible to detect multiple selfish nodes efficiently.

REFERENCES

[1] C.-H. Chin, J. G. Kim, and D. Lee, “Stability of Slotted Aloha with Selfish Users under Delay Constraint,” *KSII Trans. Internet and Info. Systems*, vol. 5, no. 3, Mar. 2011, pp. 542–59.

[2] Z. Gao *et al*., “Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks,” *IEEE Wireless Commun.*, vol. 19, no. 6, 2012, pp. 106–12.

[3] H. Hu *et al.*, “Optimal Strategies for Cooperative Spectrum Sensing in Multiple Cross-over Cognitive Radio Networks,” *KSII Trans. Internet and Info. Systems*, vol. 6, no. 12, Dec. 2012, pp. 3061–80.

[4] R. Chen, J.-M. Park, and J. H. Reed, “Defense against Primary User Emulation Attacks in Cognitive Radio Networks,” *IEEE JSAC*, vol. 26, no. 1, Jan. 2008, pp. 25–36.

[5] Yao Liu, Peng Ning, Huaiyu Dai,” Authenticating Primary Users’ Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures,” The first cognitive radio Wireless regional area network standard. *Communications Magazine, IEEE*, 47, January 2009.

[6] Omid Fatemieh, Ali Farhadi, Ranveer Chandra,” Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks,” In the Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS ’11), San Diego, CA, Feb 2011.

[7] Beibei Wang, K. J. Ray Liu, T. Charles Clancy,” Evolutionary Cooperative Spectrum Sensing Game: How to Collaborate?,” *IEEE Global Communications Conference (Globecom’08)* [23].

[8] Elaine Shi, T-H. Hubert Chan, Eleanor Rieffel, “Privacy-Preserving Aggregation of Time-Series Data,” In SPIMACS’09, pages 21–30, 2009.

[9] Julien Freudiger, Mohammad Hossein Manshaei,” On Non-Cooperative Location Privacy: A Game-Theoretic Analysis,” CCS’09, November 9–13, 2009.

[10] Hiep Vu-Van and Insoo Koo,” Cooperative Spectrum Sensing with Collaborative Users using Individual Sensing Credibility for Cognitive Radio Network, **“**IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011.

[11] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, Korea University, “Selfish attacks and Detection in Cognitive Radio Ad-hoc Networks”.