

Selfish Attacks Detection In Cognitive Radio Networks Using CRV Technique

A.Bency¹; S.Manikandan²

PGStudent¹ Assistant Professor of the Department²
Department of Electronics and Communication Engineering,
PSN College of engineering and technology,
Tirunelveli-627152, India

Abstract: Cognitive radio is a promising technology aiming to solve the spectrum scarcity problem by allocating the spectrum dynamically to unlicensed users. It uses the free spectrum bands which are not being used by the licensed users without causing interference to the incumbent transmission. Cognitive Radio networks are vulnerable to selfish attacks, where secondary users increase their accessing probability to enhance their own utilities, resulting in serious performance degradation in CR networks. The proposed work identifies a new selfish attack Channel pre-occupation selfish attack in cognitive radio networks. In selfish attack, a selfish SU broadcasts faked channel allocation information to other neighboring SUs in order to occupy all or a part of the available channels. The proposed work provides selfish cognitive radio attack detection technique, called COOPON, which will detect the attacks of selfish Secondary Users by the cooperation of other legitimate neighboring SUs.

Keywords: Mobile ad hoc network, Selfish nodes, Cognitiveradio, Secondary users, Primary users

1. INTRODUCTION

Spectrum utilization is a critical problem in wireless communication. FCC (Federal communication commission) shows that the spectrum utilization in the 0-6 GHz band varies from 15% to 85%. This given birth to cognitive radio. The IEEE has formed a working group (IEEE 802.22) to develop an air interface for opportunistic secondary access to the TV spectrum via cognitive radio technology. Its key domains are sensing, cognition and adaptation. In CR terminology primary users also called as licensed users and secondary users are called as unlicensed users or cognitive users. The unoccupied frequency band by the primary users called as spectrum holes or white space. The fundamental task of CR network is to detect the licensed users, if they are present then identify the available spectrum. This process is called spectrum sensing

Cognitive radio utilize the maximum available licensed bandwidth for unlicensed users. In traditional spectrum management, most of the spectrum is allocated to licensed users

for exclusive use. CR technology is carried out in two steps. First, it searches for available spectrum bands by a spectrum-sensing technology for unlicensed secondary users (SUs). When the licensed primary user (PU) is not using the spectrum bands, they are considered available. Second, available channels will be allocated to unlicensed SUs by dynamic signal access behavior. Whenever the PU is present in the CR network, the SU will immediately release the licensed bands. CR nodes compete to sense available channels. But some SUs are selfish, and try to occupy all or part of available channels. Usually selfish CR attacks are carried out by sending fake signals or fake channel information. If a SU recognizes the presence of a PU by sensing the signals of the PU, the SU won't use the licensed channels. In this case, by sending faked PU signals, a selfish SU prohibits other competing SUs from accessing the channels.

Because of the dynamic characteristics of CR networks, it is impossible to use the selfish attack detection techniques used in traditional wireless communications for CR networks. In this article, we identify a new selfish attack type and introduce a selfish attack detection technique, COOPON (called Cooperative neighboring cognitive radio Nodes), for the attack type. We focus on selfish attacks of SUs toward multiple channel access in cognitive radio ad-hoc networks. We assume that an individual SU accommodates multiple channels. Each SU will regularly broadcast the current multiple channel allocation information to all of its neighboring SUs, including the number of channels in current use and the number of available channels, respectively. selfish SU will broadcast fake information on available channels in order to pre-occupy them. The selfish SU will send a larger number of channels in current use than real in order to reserve available channels for later use. The COOPON will detect the attacks of selfish SUs by the cooperation of other legitimate neighboring SUs. All neighboring SUs exchange the channel allocation information both received from and sent to the target SU, which will be investigated by all of its neighboring SUs. The target SU and its neighboring SUs are 1-hop neighbors. Then, each individual SU will compare the total number of channels reported to be currently used 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 discrepancy between the two figures, all of the legitimate SUs will recognize a selfish attacker. Our proposed technique is an intuitive approach and simple to

compute, but reliable due to using deterministic channel allocation informations as well as the support of cooperative neighboring nodes. We have proven the reliability of COOPON by simulation.

2.SELFISH NODE BEHAVIOUR

Several nodes will be participated in the MANET for data forwarding and data packets transmission between source and destination. All the nodes of MANET will perform the routing function as mandatory. They must forward the traffic which other nodes sent to it. Among all the nodes some nodes will behave selfishly, these nodes are called selfish nodes. MANET are Dynamic Topologies Bandwidth constrained, variable capacity links Power constrained operations Limited physical security.

A).Dynamic topologies Nodes are free to move arbitrarily; thus the topology of the network may change randomly and rapidly at unpredictable times in network. Modification of transmission and reception parameters such as power may also impact the topology.

B).Bandwidth constrained: variable capacity links Wireless links will continue to have significantly lower capacity than their hard-wired counter parts. The relatively low to moderate link capacities will leads to the congestion rather than the exception.

C).Power-constrained operations: Some or all the nodes in a MANET rely on batteries for their energy. Thus, for these nodes, the most vital design problem may be that of power conservation. Any node in MANET may act selfishly, which means, using its limited resource only for its own profit, since each node in a network has resource constraints, such as storage and battery limitations. A node would like to enjoy the profits provided by the resources of other nodes in the network, but however it should not make its own resource accessible to help others. Existing exploration on selfish behaviors in a MANET mainly focus on network concerns. For network problems at MANET may be as some selfish nodes may not transmit data to others to conserve their own battery constraints. Even though network disputes at MANET are important, replica allocation is also critical, ever since the vital goal of using a MANET is to provide data services to users. We address the problem of selfishness in the context of replica allocation in a MANET. The problem because of replica allocation refers as if a selfish node may not share its own memory space to store replica for the benefit of other nodes.Selfish replica allocation refers to a node's.

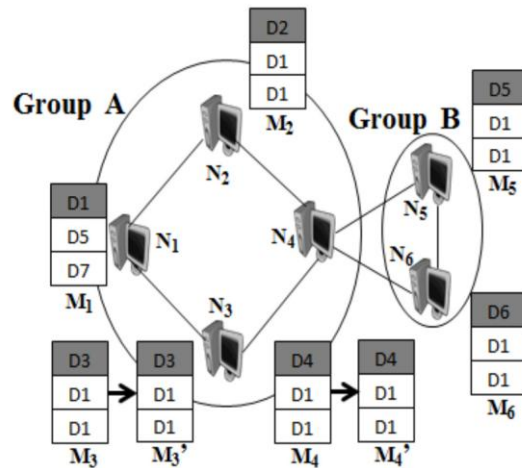


Fig 2.1 Example of selfish replica allocation

Non cooperative action, such that the node refuses to cooperate fully in sharing its memory space with other nodes. According to the figure, where nodes N1, N2... N6 maintain their memory space of nodes as M1, M2... M6, respectively, with the specified access frequency information in Table . Selfish replica allocation refers to a node's Non cooperative action, such that the node refuses to cooperate fully in sharing its memory space with other nodes. According to the figure, where nodesN1, N2... N6 maintain their memory space of nodes as M1, M2... M6, respectively, with the specified access frequency information in Table. As shown in Figure DCG seeks to minimize the duplication of data items in a group to achieve high data accessibility.

Table 2.2 Access frequency table

Data	Nodes					
	N ₁	N ₂	N ₃	N ₄	N ₅	N ₆
D ₁	0.65	0.25	0.17	0.22	0.31	0.24
D ₂	0.44	0.62	0.41	0.40	0.42	0.46
D ₃	0.35	0.44	0.50	0.25	0.45	0.37
D ₄	0.31	0.15	0.10	0.60	0.09	0.10
D ₅	0.51	0.41	0.43	0.38	0.71	0.20
D ₆	0.08	0.07	0.05	0.15	0.20	0.62
D ₇	0.38	0.32	0.37	0.33	0.40	0.32
D ₈	0.22	0.33	0.21	0.23	0.24	0.17
D ₉	0.18	0.16	0.19	0.17	0.24	0.21
D ₁₀	0.09	0.08	0.06	0.11	0.12	0.09

3.CR NETWORK ARCHITECTURE

This section provides a detailed description of the Cognitive radio network architecture.According to the architecture, cognitive radio networks can be classified as Centralized or Distributed networks. According to operations point of view, cognitive radio networks can be classified as licensed band operation and unlicensed band

operation. According to Access type, cognitive radio network can be classified as CR network access, CR ad-hoc access, and primary network access

attack in order to pre-occupy CR spectrum resources. There are three different selfish attack types

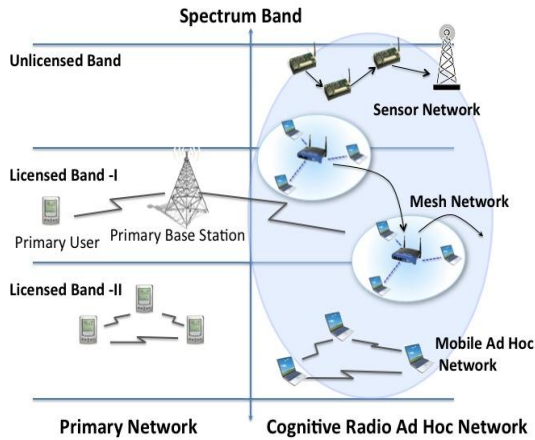


Figure 3.1 Cognitive Radio Network Architecture.

Centralized cognitive network: As shown in Fig. 1.5, the network is infrastructure oriented. A base station is used to manage each CR user in the network. The base station communicates directly with each user and controls the medium access and the secondary users in the network. **Distributed cognitive network:** As shown in Fig. 1.5, the CR users communicate with each other in an ad-hoc manner. Information is shared directly between the secondary users who fall within the communication range otherwise information is shared over multiple hops.

Licensed band operation: This band is dedicated for the primary users in the network. It can be used by the unlicensed user if not occupied by the primary user. CR user must vacate the licensed band if the primary user reappears then and move to another vacant spectrum band. **Unlicensed band operation:** The unlicensed users have the same right to use the unlicensed band. There is no need to vacate the spectrum for the licensed users. **Cognitive radio network access:** As shown in Figure, the cognitive users can share information with their base station on the licensed as well as the unlicensed spectrum band.

Cognitive radio ad-hoc access: As shown in Figure, the cognitive users in the network can share information with each other in ad-hoc manner on both the licensed and unlicensed spectrum band. **Primary network access:** As shown in Figure, the CR users can also communicate with the primary base station on the licensed spectrum band with an adaptive medium access control protocol.

Types of Selfish Attacks:

Selfish attacks are different depending on what and how they

Attack Type 1

A Type 1 attack is designed to prohibit a legitimate SU (LSU) from sensing available spectrum bands by sending faked PU signals. The selfish SU (SSU) will emulate the characteristics of PU signals. A legitimate SU who overhears the faked signals makes a decision that the PU is now active and so the legitimate SU will give up sensing available channels. This attack is usually performed when building an exclusive transmission between oneself selfish SU and another selfish SU regardless of the number of channels. There must be at least two selfish nodes for this type of attack.

Attack Type 2

Type 2 attacks are also a selfish SU emulating the characteristics of signals of a PU, but they are carried out in dynamic multiple channel access. In a normal dynamic signal access process, the SUs will periodically sense the current operating band to know if the PU is active or not, and if it is, the SUs will immediately switch to use other available channels. In this attack type, a continuous fake signal attack on multiple bands in a round-robin fashion, an attacker can effectively limit legitimate SUs from identifying and using available spectrum channels.

Attack Type 3

In Type 3, called a channel pre-occupation selfish attack, attacks can occur in the communication environment that is used to broadcast the current available channel information to neighboring nodes for transmission. We consider a communication environment that broadcasting is carried out through a common control channel (CCC) which is a channel dedicated only to exchanging management information. A selfish SU will broadcast fake free (or available) channel lists to its neighboring SUs. Even though a selfish SU only uses three channels, it will send a list of all five occupied channels. Thus, a legitimate SU is prohibited from using the two available channels. Detection of existing selfish technologies is likely to be uncertain and less reliable, because they are based on estimated reputation or estimated characteristics of stochastic signals.

4. PROPOSED SYSTEM

The proposed technique is an intuitive approach and simple to compute, but reliable due to using deterministic channel allocation information as well as the support of cooperative neighboring nodes. The efficiency is measured by a detection rate, which is the proportion of the number of selfish SUs detected by COOPON to the total number of actual selfish SUs in a CR network:

$$\text{Detection Rate} = \frac{\text{number of detected selfish SUs}}{\text{number of actual selfish SUs}}$$

One SU has a maximum of eight data channels and one common control channel. The channel data rate is 11 Mb/s. In simulation, one SU can have two to five one-hop neighboring SUs. The experiment was performed under various selfish SU densities in a CR network. The article identifies a new selfish attack type in cognitive radio ad-hoc networks and propose an easy and efficient selfish cognitive radio attack detection technique, called COOPON, with multichannel resources by cooperative neighboring cognitive radio nodes. In traditional spectrum management, most of the spectrum is allocated to licensed users for exclusive use. CR technology is carried out in two steps. First, it searches for available spectrum bands by a spectrum-sensing technology for unlicensed secondary users (SUs).

When the licensed primary user (PU) is not using the spectrum bands, they are considered available. Thus, all of the 1-hop neighboring SUs will make a decision that the target SU is a selfish attacker. All 1-hop neighboring SUs sum the numbers of currently used channels sent by themselves and other neighboring nodes. In addition, simultaneously all of the neighboring nodes sum the numbers of currently used channels sent by the target node, TNode. Individual neighboring nodes will compare the summed numbers sent by all neighboring nodes to the summed numbers sent by the target node to check if the target SU is a selfish attacker.

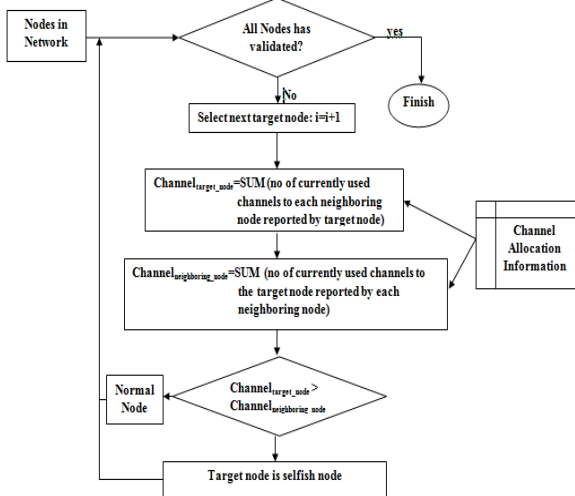


Figure 4.1 Selfish attack detection algorithm

The above figure shows the proposed selfish attack detection algorithm flow chart of COOPON. As we mentioned above, all currently used channels in the target node and neighboring nodes are summed up in two steps Channel target node and Channel neighboring node. Then Channel target node will be compared to Channel neighboring node. According to the example, Channel target node is 7 and Channel neighboring

node is 5 Because $7 > 5$, the target secondary node is identified as a selfish attacker.

5. GRAPH DESIGNED BASED RESULT

Graph is an essential part of display a result, so plot a graph to show a various result comparison with packets, throughput, energy efficient, malicious node detection analysis and etc. The layout of the simulated network of detection rate versus selfish secondary user density and shows that the number of SUs has a trivial effect on detection rate

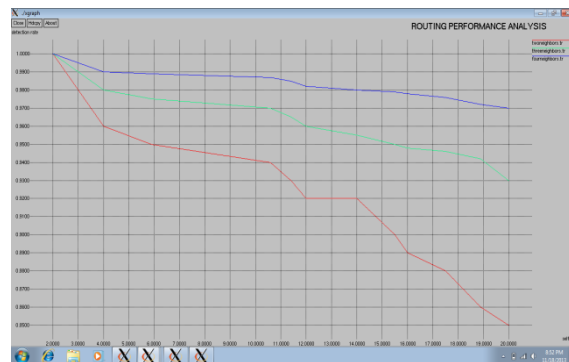


Figure 5.1 Detection rate vs. selfish secondary user density

The below figure shows the simulation results for the throughput and the simulation time. The y-axis represents the throughput and the x-axis represents the simulation time. The throughput increases with respect to the simulation time.



Figure .5.2 Throughput vs. simulation time

6.CONCLUSIONS

The proposed work identifies a new selfish attack, Channel pre-occupation selfish attack in cognitive radio networks and propose a detection approach called COOPON. Because COOPON use the deterministic channel allocation information,

COOPON gives very highly reliable selfish attack detection results by simple computing. The proposed reliable and simple computing technique can be well fitted for practical use in the future. Our approach is designed for cognitive radio ad-hoc networks. The COOPON algorithm make use of ad-hoc network advantages such as autonomous and cooperative characteristics for better detection reliabilities. In future work, the Markov chain model is proposed to do theoretical analysis of more than one selfish SU in a neighbor, which gives less detection accuracy.

7. REFERENCES

- [1] C.-H. Chin, J. G. Kim, and D. Lee.(Mar. 2011), 'Stability of Slotted Aloha with SelfishUsers under Delay Constraint,'KSII Trans. Internet and Info. Systems,vol. 5, no. 3, pp. 542–59.
- [2] G. Xiong, S. Kishore, and A.Yener.(Mar. 2010.), 'Cooperative adaptivespectrum sensing in cognitive radio networks,' in Proc. CISS, pp. 1-6, Princeton, NJ.
- [3] H. Hu et al.(Dec. 2012), 'Optimal Strategies for Cooperative Spectrum Sensing in Multiple Cross-over Cognitive Radio Networks,'KSII Trans. Internet and Info. Systems, vol. 6, no. 12, pp. 3061–80.
- [4] K. Cheng Howa, M. Maa. and Y. Qin(2012), 'An Altruistic Differentiated Service Protocol in Dynamic Cognitive RadioNetworks Against Selfish Behaviors,'Computer Networks, vol. 56, no. 7, pp. 2068–79.
- [5] M. Yan et al. (May.2011),'Intrusion Detection System (Ids) for Combating AttacksAgainst Cognitive Radio Networks,'IEEE/ACIS 10th Int'l. Conf. Computer and Information Science (ICIS), pp. 58–61.
- [6] R. Chen, J.-M. Park, and J. H. Reed.(Jan. 2008), 'Defense against Primary User Emulation Attacks in Cognitive Radio Networks,'IEEE JSAC, vol. 26, no. 1, pp. 25–36.
- [7] S. Li et al.(2012),'Location Privacy Preserving Dynamic Spectrum Auction in Cognitive Radio Network,'IEEE INFOCOM'12, pp. 729–37
- [8] X. Tan and H. Zhang.(Sept. 2012), 'A CORDIC-Jacobi Based Spectrum Sensing Algorithm for Cognitive Radio,' KSII Trans. Internet and Info. Systems, vol. 6, no. 9, pp. 1998–2016.
- [9] Z. Dai, J. Liu, and K. Long.(Oct. 2012), 'Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access,'KSII Trans. Internet and Information Systems, vol. 6, no. 10, pp. 2455–72.
- [10] Z. Gao et al.(2012), 'Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks,'IEEE Wireless Commun., vol.1

