CREDIT RISK VALUE BASED DETECTION OF MULTIPLE SELFISH NODE ATTACKS IN COGNITIVE RADIO NETWORKS

P.V.Niranchana[1], K. Anish Pon Yamni[2]

[1]PG Student, Department of Electronics and communication engineering, Arunachala College of Engineering for Women, Vellichanthai-629203, Tamilnadu

[2]Assistant Professor, Department of Electronics and communication engineering, Arunachala College of Engineering for Women, Vellichanthai-629203, Tamilnadu.

Abstract

The scope of the Cognitive Radio technology is to solve the spectrum scarcity problem by allocating the spectrum dynamically to unlicensed users. In wireless ad-hoc networks, wireless device service degrades the network performance when spectrum is crowded. Licensed spectrum refers to the portions of the spectrum reserved by each country's equivalent of the FCC for specific uses. This portion of the spectrum is further subdivided into frequency bands for military, television signals and commercial services. Designated users utilize the resource exclusively without interference. In Cognitive radio (CR), free spectrum bands that are not being used by the licensed users are used by the unlicensed secondary users. Unlicensed secondary users (SU) which transmits the fake information for its future use Is termed as selfish users. CR networks are vulnerable to selfish attacks, based on spectrum sharing, spectrum sensing and cognitive capability. SU broadcasts fake information to other neighbouring SUs inorder to occupy all (or) a part of the available channel. Selfish nodes highly degrade the network performance. In this paper, we have identified the multiple selfish node attacks using the credit risk information. We propose a method that uses CRV (Credit Risk Value) which helps to detect more than one selfish node. This improves the network performance of the network.

Keywords: *Mobile ad hoc network, Selfish nodes, Cognitive radio, Secondary users, Primary users*

---***---

1. INTRODUCTION

Mobile ad-hoc network (MANET) is a infrastructure less network; hence they are more prone to attacks. Selfish attack is one of them. In CR technology, 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 utilizes 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 [12]. 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 the existing COOPON (Cooperative neighboring cognitive radio Nodes) mechanism, it is not possible to detect selfish nodes if there is more than one selfish secondary user. COOPON uses the autonomous decision capabilities of an ad-hoc network, based on exchanged channel allocation information. In this article, 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 for the future purpose. For single selfish node detection, each SU will regularly broadcast the current multiple channel allocation information to all of its neighboring SUs [12]. In our proposed method, for multiple selfish node attack detection, Credit Risk Value is calculated for each node in the CR network.

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's are dynamic topologies with constrained bandwidth.

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 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, 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. And the solution selfish replica allocation [9] in MANET is shown in the below figure (2.1).

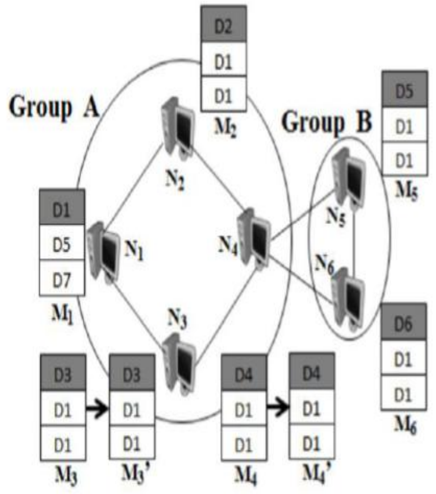
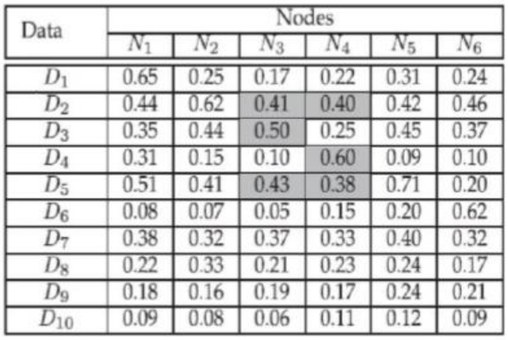


Fig 2.1 Example of selfish replica allocation (Excerpt from [9])

Non cooperative action, such that the node refuses to cooperate fully in sharing its memory space with other nodes. According to the figure [2.1], where nodes N1, N2... N6 maintain their memory space of nodes as M1, M2... M6, respectively, with the specified access frequency information in Table. To achieve high accessibility, duplication of data items is minimized in a group.

Table 2.2 Access frequency table (Excerpt from [9])

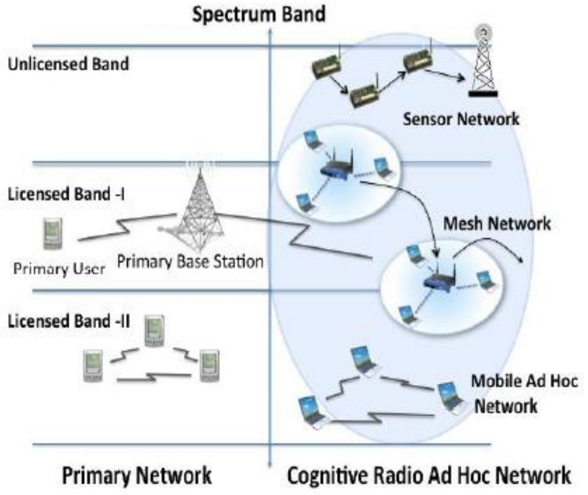


Data	Nodes					
	N_1	N_2	N_3	N_4	N_5	N_6
D_1	0.65	0.25	0.17	0.22	0.31	0.24
D_2	0.44	0.62	0.41	0.40	0.42	0.46
D_3	0.35	0.44	0.50	0.25	0.45	0.37
D_4	0.31	0.15	0.10	0.60	0.09	0.10
D_5	0.51	0.41	0.43	0.38	0.71	0.20
D_6	0.08	0.07	0.05	0.15	0.20	0.62
D_7	0.38	0.32	0.37	0.33	0.40	0.32
D_8	0.22	0.33	0.21	0.23	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. In Centralized Cognitive network, 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. As shown in Fig. 3.1, 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.

In 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 architecture is shown below[5].



.

Fig 3.1 Cognitive Radio Network Architecture

As shown in Figure, the cognitive users can share information with their base station on the licensed as well as the unlicensed spectrum band. Primary network access: CR users can also communicate with the primary base station on the licensed spectrum band with an adaptive medium access control protocol.

3.1 Selfish Node Attacks

Selfish attacks are different depending on what and how they attack inorder to occupy CR spectrum resources. There are many different selfish attack types.

First type of 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 one 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. There must be at least two selfish nodes for this type of attack. Second type of 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. Another type of attack is called a channel pre-occupation selfish attack [12].This type of attacks can occur in the communication environment that is used to broadcast the current available channel information to neighboring nodes for transmission.

In the previous existing methods, there considered 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. The fake information on channel allocation of each nodes in the network. 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. EXISTING METHOD

The existing technique is an intuitive approach 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 as follows;

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

One SU has a maximum of eight data channels and one common control channel. The channel data rate is 11Mb/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 [12] proposed an efficient selfish cognitive radio attack detection technique, called COOPON, (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 the following steps.

- First, it searches for available spectrum bands by a spectrum sensing technology for unlicensed secondary users (SUs).
- Second, allocate the available spectrum dynamically to unlicensed users.

When the licensed primary user (PU) is not using the spectrum bands in the network, they are considered available. Secondary users emulate the characteristics of the primary users by sending the fake information. 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 cannels sent by themselves and other neighboring nodes. In addition, simultaneously all of the neighboring nodes sum the numbers of currently used cannels sent by the target node, TNode. Individual neighboring nodes will compare the summed numbers of the channel used sent by all neighboring nodes to the summed numbers sent by the target node to check if the target SU is a selfish attacker. Here, the broadcasting is carried out through the Common Control Channel In the existing COOPON mechanism, first it checks that all the nodes in the network is validated or not. If not, it checks the nodes one by one using the COOPON method described below. The below figure shows the selfish attack detection algorithm (or) mechanism flow chart of COOPON [12].

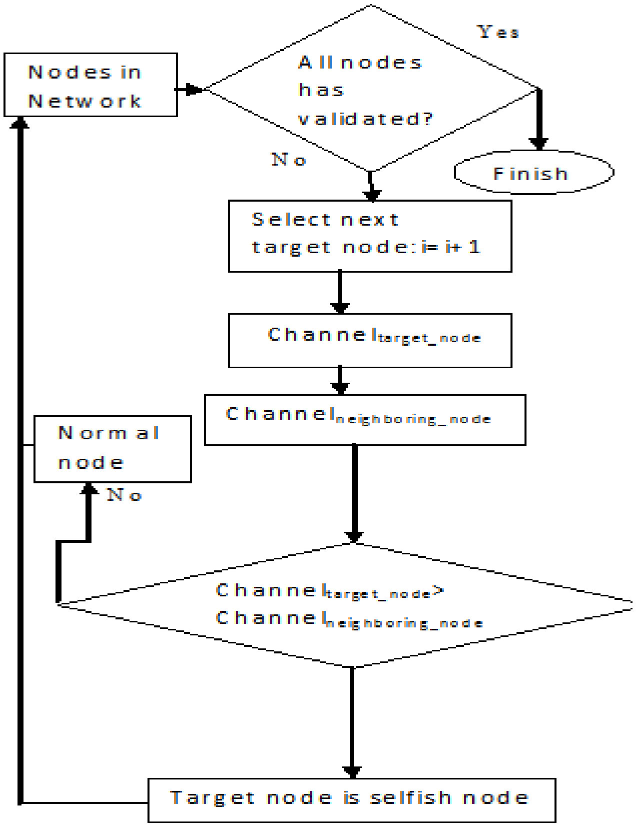

Nodes in Network
All nodes has validated?
Yes
No
Finish
Select next target node: i= i+ 1
Channel$_{\text{target\_node}}$
Channel$_{\text{neighboring\_node}}$
Normal node
No
Channel$_{\text{target\_node}}$> Channel$_{\text{neighboring\_node}}$
Target node is selfish node

Fig.4.1 Selfish attack detection Mechanism

As mentioned above, all currently used channels in the target node and the neighboring nodes are summed up in two steps; the Channeltarget_node and the Channelneigboring_node, based on the channel allocation information. Channel$_{\text{target\_node}}$ is the sum of the number of currently used channels to each neighboring node reported by target node and the Channel$_{\text{neighboring\_node}}$ is the sum of no. of the currently used channels to the target node reported by each neighboring node.Then Channeltarget_node will be compared to Channelneigboring_node. In Figure 4.2the target node, T-Node is also a SU, but other 1-hop neighboring SUs, N-Node 1, N Node2, N-Node 3, and N-Node 4, will scan any selfish attack of the target node. The target SU and all of its 1-hop neighboring users will exchange the current channel allocation information list via broadcasting on the dedicated channel. For this, it uses the common control channel.

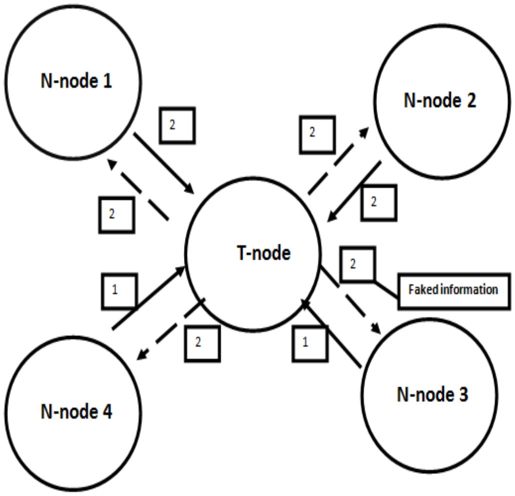


Fig 4.2 COOPON detection mechanism (Excerpt from [12])

The COOPON detection mechanism clearly describes the number of channels used by each node in the network. It is noticed that T-Node 2 reports that there are two channels currently in use, while N-Node 3 reports that there are three currently in use, which creates a discrepancy. N-Node 4 also receives faked channel allocation information from the target node.

On the other hand, all other exchanged information pairs, T-Node/ N-Node 1 and T-Node/N-Node 2, are correct. Thus, all of the 1-hop neighboring SUs will make a decision that the target SU is a selfish attacker. According to the above shown example, the Channeltarget_node is 7 and the Channelneighboring_node is 5. Because 7 > 5, the target secondary node is identified as a selfish attacker. The COOPON mechanism is reliable than the previous detection methods, because the channel allocation information is more deterministic than the stochastic signal characteristics.

5. PROPOSED SYSTEM

The proposed technique is simple to compute. The proposed algorithm is the CRV algorithm. The CRV technique will detect the attacks of selfish SUs in the cognitive radio network by calculating the credit risk value. In economics, credit risk is the measured risk of loss due to a debtor's nonpayment of a loan. A bank examines the credit risk of an applicant prior to approving the loan. The measured credit risk of the applicant indicates if he/she is credit worthy. Similar approach is considered in our system. CRV technology is carried out in the following steps. First it calculates the CRV value before sending any packet, then route the packet, again recalculate the CRV value. The CRV value is a constant value, which denotes the energy consumed for the packet transmission.

$$\mathrm{CRV} = \mathrm{No.\,of\,packets} * \mathrm{Total\,energy} - \mathrm{Remaining\,energy}$$

Where,
Total energy is the initial energy of the node and Remaining energy is the energy after data routing.

In the proposed technique, multiple selfish node attacks are detected using the above simple formula.CRV value is the number of packets multiplied by the energy used by the node in the CR network In this method, topology is constructed first and then CRV value is calculated for all the nodes in the network. CRV value is a constant value. Data routing is done after calculating the CRV value for all nodes. Then recalculate the CRV value. The CRV value i.e., the energy for each node packet transmission is inbuild as ten, as the energy required for each and every normal transmission is near to the value ten. If the CRV value is greater than ten CRV, then it detects that node as attacker node and then reroute the packet. Again calculate the CRV value. If the value is less than ten CRV, then again data routing is done. And the process repeated as above. And the process is repeated as above until the routing is finished.

The proposed selfish attack detection CRV algorithm flow chart is given below in figure5.1. Cognitive users in the network can share information with each other in ad-hoc manner on both the licensed and unlicensed spectrum band. Based on the spectrum sensing technology, we define a submission period as certain time duration. Each node needs to generate monitoring messages to report the performance of its neighbours in each submission period.

By using the above formula, we can get the energy consumed for each node's packet transmission. After the topology reconstruction, the CRV value is again calculated for each node by the above formula. Then it checks whether the calculated value is between 4 and 10 CRV (or) not until it checks all the nodes in the network. If the value is in between 4 and 10, then the performance is more efficient. Because, for normal transmission, the credit won't be less than four By using this simple computing procedure, the attacker node in the cognitive radio network can be detected and so the network performance can be improved.

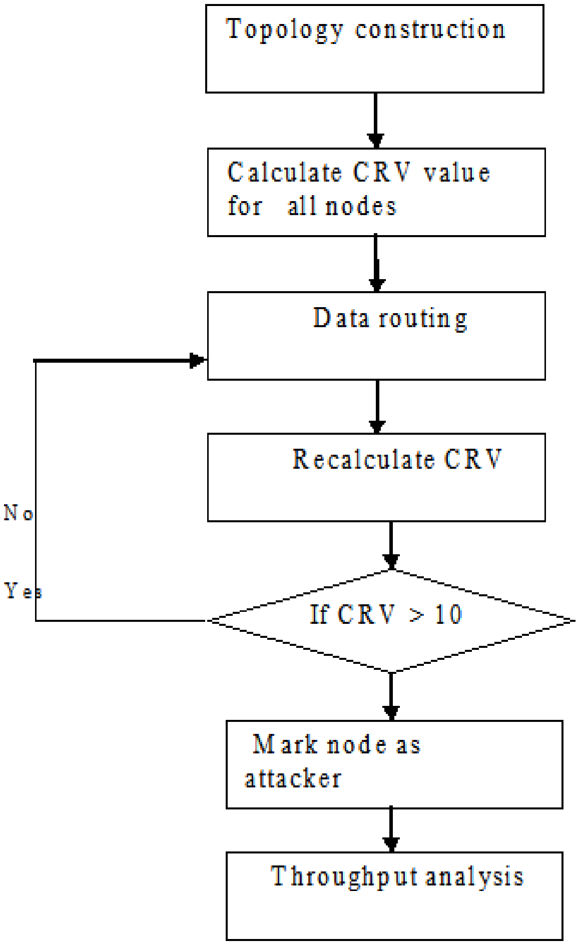


Fig 5.1 CRV algorithm

The CRV value for normal transmission ranges from 4 to 10. By setting this as thresholding value and then calculating the CRV value will be more efficient. After calculating the CRV value, data routing is done again if the CRV value is less than 10.The figure5.2 shows that the CRV value for Node 1 is 8, Node2 is 10 and Node3 is 7.The CRV value for Node4 is 13, which is greater than 10.This means that Node 4 is an attacker node. Thus, more than one selfish node in the cognitive radio network can be detected by using the Credit Risk Value (CRV) technique. This method is simple to compute and more efficient than the existing COOPON method. This method is also a time consuming method, since the formula for calculating the CRV value is simple.CRV detection mechanism is given in the below figure.CRV value is mentioned near in a small circle to each nodes in the network.

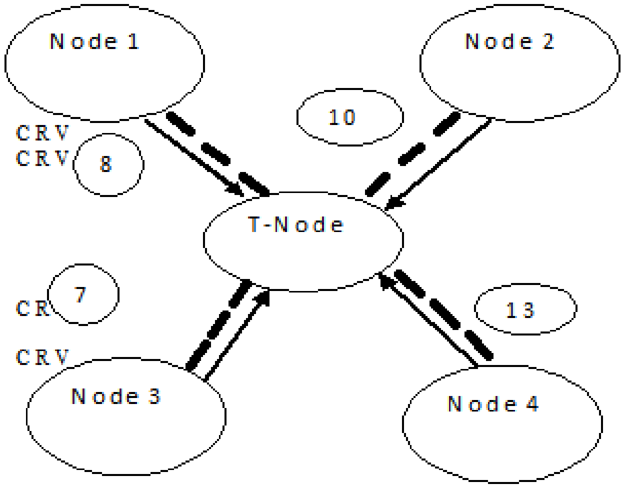


Fig 5.2 CRV detection mechanism

In identifying selfish nodes in the cognitive radio ad-hoc network, the procedure for handling error is as follows:

- After the node creation, CRV is evaluated for each node in the network.
- Compare the CRV score with all other nodes. Then the high CRV value is set as leader.
- Broadcast the leader id to all other nodes. By monitoring all the nodes, it identifies selfish node.

6. PERFORMANCE ANALYSIS

Graph is an essential part of display a result. The graph shows the various result comparisons with packets, throughput, energy efficient, malicious node detection analysis and packet delivery ratio with respect to the simulation time.In particular, selfish nodes are determined to be selfish only when all other nodes in the group agree with the node's Selfishness. We first compare the overall selfishness method with that of COOPON to demonstrate the effectiveness of our detection method (CRV).

We expect that the overall selfishness alarm will be reduced in query processing by detecting selfish nodes effectively with CRV, since many selfish nodes will be removed from the replica allocation phase and many reliable nodes will serve data requests from nodes. It is desirable to observe truly selfish nodes to evaluate the effectiveness of the detection method. A data requester cannot tell an expected node's selfishness from network disconnection, i.e., no reply from the expected node.

The layout of the simulated network of the routing performance of CRV on comparison with the existing COOPON method is shown below.

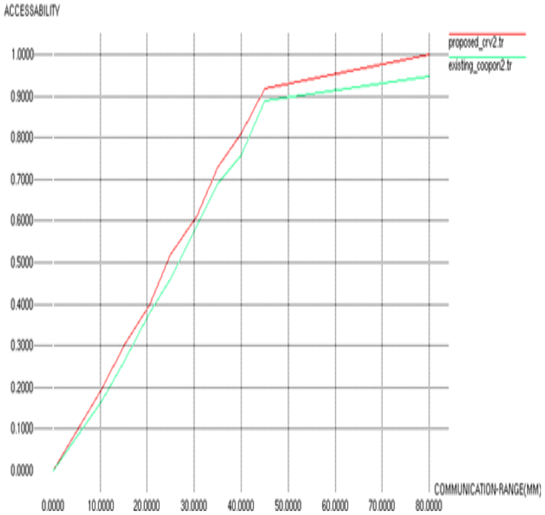


Fig 6.1 Routing performance on average accessibility

The simulation output of the performance level of Intrusion Detection System (IDS) between CRV and the existing method is shown below. In the figure, y-axis represents the number of nodes and the x-axis represents the selfish node detection. The performance level increases with our proposed detection mechanism.

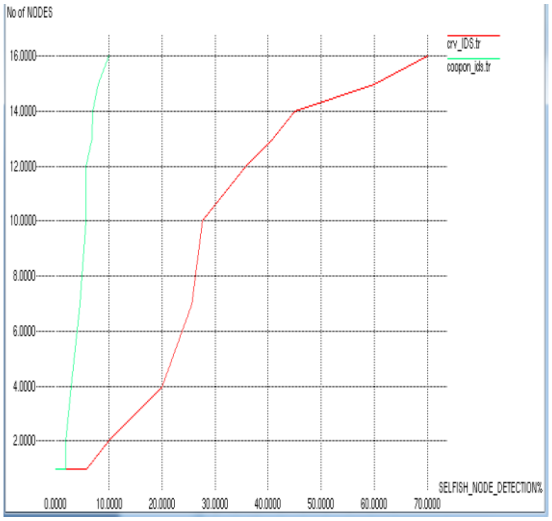


Fig 6.2 Performance level of Intrusion Detection System

Finally, we examine the effect of communication range. The simulation layout of the performance level of selfish node detection time and the communication range is shown below. The selfish node detection time of CRV is less when compared with that of the COOPON method.

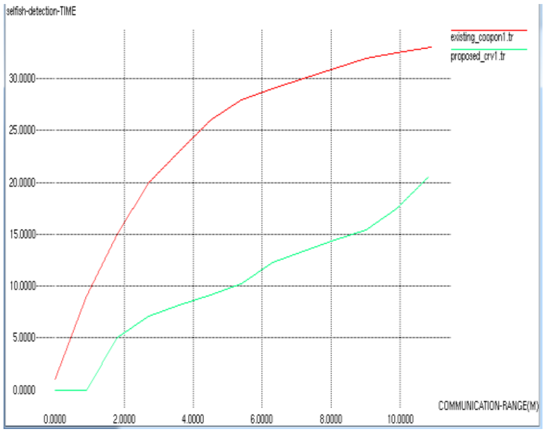


Fig 6.3 Performance level on selfish node detection time

7. CONCLUSIONS

The existing method detects only one selfish node in cognitive radio network. Because, the COOPON uses the deterministic channel allocation information. In this paper, we have identified the multiple selfish node attacks using the credit risk information. The Proposed CRV algorithm detects more than one selfish secondary user in the cognitive radio network using the Credit Risk Value. Our approach is designed for cognitive radio ad-hoc networks. The CRV algorithm makes use of ad-hoc network advantages such as energy required for packet transmission at each node in the network for better detection reliabilities. The proposed reliable and simple computing technique can be well fitted for practical use in the future

8. REFERENCES

[1]. K.Balakrishnan, J.Deng, and P.K.Varshney, ”TWOACK: Preventing selfishness in Mobile Ad Hoc Networks,”proc.IEEE Wireless Comm. And Networking, pp.2137-2142, 2005.

[2]. K. Cheng Howa, M. Maa and Y. Qin(2012), ‘An Altruistic Differentiated Service Protocol in Dynamic Cognitive Radio Networks Against Selfish Behaviors’, Computer Networks, vol. 56, no. 7, pp. 2068–79.

[3]. 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. KSII Trans. Internet and Information Systems, vol. 6, no. 10, pp. 2455–72.

[4]. Z. Dai, J. Liu, and K. Long (Oct. 2012), ‘Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access’.

[5]. Z. Gao et al., (2012), ‘Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks, ’IEEE Wireless Commun., vol. 19, no. 6, pp. 106–12.

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

[7]. 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.

[8]. T.Hara, “Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility”, Proc.IEEE INFOCOM, pp.1568-1576, 2001.

[9]. Jae-Ho Choi, Kyu-Sun Shim, Sangkeun Lee, and Kun-Lung Wu (2012),‘Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network’ IEEE Transactions on mobile computing,vol.11 no.2.

[10]. ”A Survey of Techniques Used Detect Selfish Nodes in MANET”, Karthik.M, Jyothish K John, International Journal for scientific Research & Development /Vol.1, Issue 4,2013.

[11]. S.Li et al., (2012),”Location Privacy Preserving Dynamic Spectrum Auction in Cognitive Radio Network”, IEEE INFOCOM’ 12, pp. 729–37.

[12]. Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter (May 2013), ‘Selfish Attacks and Detection in Cognitive Radio Networks’, Korea University.vol 27, Issue: 3, IEEE Network.

[13]. M. Yan et al. (May.2011),’Intrusion Detection System (Ids) for Combating attacks against Cognitive Radio Networks’, IEEE/ACIS 10th Int’l. Conf. Computer and Information Science (ICIS), pp.58–61

[14]. Nasser N, Chen Y. (2007) “Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network”, in Proceeding IEEE (ICC’07), pp 1154-9.

[15]. 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.

BIOGRAPHIES

P.V. Niranchana gained bachelor’s degree in Periyar Maniammai University, Tanjavur. Joined in the department of Electronics and Communication engineering at Arunachala College of engineering for women, Kanyakumari as a PG student in 2012

K. Anish Pon Yamini gained Master’s degree in Communication System from SRM Institute of Science and Technology. She joined in the department of Electronics and Communication at Arunachala College of Engineering for Women, Kanyakumari as a Assistant professor in 2012.Ms.Anish Pon Yamini has more than 05 research papers to her credit in various International/National Journals, Conferences. She is actively involved in research activities in the ad-hoc wireless networks.