Multiselfish Attacks Detection in Cognitive Radio Ad-Hoc Networks

Gowri Shankar. G[1],
Dept. of Information Technology
KNCET
Trichy, India

Balgani. S[2],
Dept. of Information Technology
KNCET
Trichy, India

Aruna. R[3],
Dept. of Information Technology
KNCET
Trichy, India

Mano. P. S[4],
Dept. of Information Technology
KNCET
Trichy, India

***Abstract* — Cognitive radio network is an awareness communication technology supports unlicensed user to utilize the maximum available number of bandwidth. CR network can identify more available communication of spectrum efficiently. CR Network can support new wireless users in existing busy spectrum. CR Network user uses the free spectrum which is not being used by the unlicensed user without causing any interference to the necessary transmissions. The main aim of the CR Network is used to solve the spectrum scarcity by assigning the spectrum to the unlicensed user dynamically. CR Networks are unsafe to the selfish attacks, because of spectrum allocation in cognitive radio networks capability. SU transmits forged information to the other nearby SUs sequentially to occupy all offered channels. Selfish Nodes are highly reduces the performance of CR Network. In this article we have identified the Multiselfish attacks by using credit risk value. Hence we proposed a method to identify Multiselfish attacks by using credit risk value.**

Index Terms*— *Primary user, Secondary user, Mobile ad-hoc network, cognitive radio (CR), selfish node, Detection Rate (DR).

I. INTRODUCTION

Mobile ad-hoc network (MANET) is an infrastructure less network; hence they recognize several attacks are possible in MANET. Selfish attacks are also one of them. In cognitive Radio technology, primary users are called as licensed user and the secondary users are called as unlicensed users. The Unoccupied frequency band by the primary user called as spectrum holes or white space. The original assignment of cognitive radio networks are used to identify the licensed users. While the licensed users are located nearby the range to identify the available spectrum. Hence, this process is called spectrum sensing.

Cognitive Radio Network (CRN) is a communication technology to make use of the maximum vacant licensed bandwidth for the unlicensed users. It has been established that, the licensed spectrum is not utilized to its full level at all the time. The user faced the too much spectrum demands and to utilizes the vacant spectrum. The main point of cognitive radio is to identify the unoccupied licensed spectrum for secondary usage without interfering with the primary user. Then the licensed primary user (PU) is not using the spectrum bands they consider as available. Next the vacant number of channels will be assign to the unlicensed user by the dynamic signal access behaviors [12].Whenever the primary user (PU) is present from the cognitive radio network, the secondary users (SU) without delay release the licensed bands because the Primary User (PU) has limited privilege to use of them [2&3].

A CRN node struggle to sense available channels [4-7]. But some SUs are selfish, and try to occupy all part of the vacant channels. Usually selfish CRN attacks are carried out by sending the forged signals or forged channels 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 forged PU signals, a selfish SU prohibits other opposing SUs from right to use the channels. In this case sending a fake PU signals a selfish SU prohibits other opposing SUs from accessing the channels. An additional category of selfish attack is carried out when SUs shares the sensed accessible channels.

Usually each SU from time to time informs its neighbouring SUs of recent available channels by broadcasting channel allocation information such as the number of vacant channels and channels in use. In this case, a selfish SU broadcasts forged channel allocation information to other neighbouring SUs in order to occupy all part of the accessible channels. For example, even though a selfish SU uses only two out of five channels. Thus, these selfish attacks decrease the performance of a CRN network significantly.

Because of the dynamic characteristics of CRN networks, it is not possible to use the selfish attack finding techniques used in the traditional wireless communications for the CR networks. In the existing COOPON (Cooperating neighboring cognitive radio networks nodes) mechanisms, if there is more than one selfish secondary user this mechanism is not suitable to detect the selfish nodes. COOPON uses the self-ruling conclusion capability of an ad-hoc network, based on the exchanged channel allocation information. In this article, we focus on the selfish attacks of SUs towards multiple channel right to use in the cognitive radio networks. For single selfish multiple node detection, each SU will frequently transmit the present multiple channel allocation information to all of its neighbouring SUs [12]. In our proposed method, for the multiple selfish node detection Credit Risk Value is calculated for the each node in the cognitive radio network.

II. RELATED WORK

Suitable to the individuality of the performance of CRN, Selfish attack detection technology for a usual wireless network cannot be used for the detecting selfish attacks in Cognitive Radio Networks (CRN). For CRN selfish attacks, first identified a danger to the spectrum sensing, called PU emulation attack. In this attack, a selfish attacker broadcast signals that follows the quality of PU signals. The imitate

signals create valid SUs misinterpret that the PU is active, and so the forged signals hinder SU access to the vacant spectrum band. They identify the faked PUs signals by the teller verification. The teller verification resolve the valid source signal by the signal energy level merged with the starting place of the location. In 2011, Yan applied the game-theoretic approach, Nash equilibrium, to avoid the selfish attacks [12]. Selfish attacks are created by a selfish SU to boost the access probability by shrink the back off window size in a CSMA-based CRN network. In 2012, a cross-layer altruistic differentiated service protocol (ADSP) was proposed for the self-motivated cognitive radio networks to consider the quality of service provisioning in cognitive Radio Network with selfish node coexistence [15]. Their goal is to give lesser interruption, higher throughput, and improved delivery ratios for a cognitive radio network. Status is assigned to each SU based on famous selfish behavior data. A improved status assigned to fewer selfish nodes will added to reduce the chance of a failed rescue Routing is discuss with the status of a SU. Our process to recognized attack type and proposed detection technique, COOPON is various from the earlier ones in the communication situation and conditions. COOPON is proposing for CRN with several channels and is proposed for the case that the channel assign information is transmitting for the transmission.

III. CRN ARCHITECTURE

This section gives an in depth explanation of the cognitive radio network architecture. Along with the architecture, CRN can be classified as centralized or distributed network systems. Moreover, CRN can be classified into two types. They are licensed band operation and unlicensed band operation. CRN can be considered as Network Access, CR Ad-Hoc access, and Primary network access. The base stations communicate directly with each user and manage the medium access and the secondary user from the network. As shown in the above fig.1, the cognitive radio user communicates with each other in an ad-hoc network. Information is shared straightforwardly between the secondary users which drop in the network within communication range otherwise information is shared over multiple hops. In Licensed band operation, this band is devoted for the primary user which is part of the network. This band can be used by the unlicensed user if not occupy by the primary user. Primary Network access is used in CRN the cognitive radio user can access the primary base-station through the licensed band, if the primary network permits. Unlike other access types, cognitive radio users should support the medium access technology of the CR user can also access the primary base station through the licensed band, if

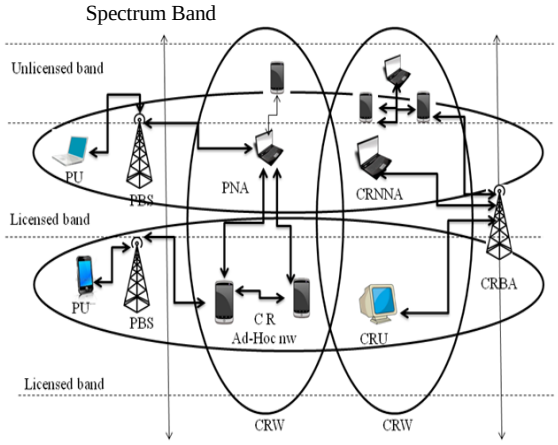

Fig.1. CR Network Architecture

CR Network users should support the medium access technology of primary network.CRN user must vacate the licensed band if the primary user reappear then and move to another vacant spectrum band. Unlicensed band operation: The unlicensed users have the similar correct to make use of the unlicensed band. There is no requiring to vacant the spectrum for the licensed users. CRN architecture is shown above fig.1. The cognitive radio user can split the information with their base station from the licensed

Spectrum band as well as the unlicensed spectrum band. Major network access: CRN user can be communicates with the major base station from the licensed spectrum band with an MAC Protocol.

IV. SELFISH ATTACKS

Selfish attack is types of attacks and then one after the other to occupy cognitive radio spectrum. There are different selfish attacks types.

Type one of the attacks is designed to disallow a legitimate secondary User SU (LSU) from the available spectrum bands by sending the fake primary User signals PU. The selfish SU (SSU) will follow the characteristics of the PU signals. A legitimate SU who overhears the forged signals and makes to takes a decision that the PU is active and then the legitimate secondary SU will give up sensing vacant channels from the spectrum. This type of attack is frequently performed when construction and limited transmission between one selfish SU and another selfish SU not considering of the number of channels. There should be at least two selfish nodes attacks. Type second attacks area selfish SU follow the characteristics of signals of PUs but they are carried out in the accessing of a dynamic multiple channels.

In a regular dynamic signal access process, the SUs will from time to time sense the recent in use band to know if the PU is active or not, and if it is, the SUs will without delay switch to make use of other accessible channels. In these types of attacks, a hinder can efficiently limit legitimate SUs from categorize and using vacant spectrum channels. Another type of attack is called channel pre-occupation selfish attacks [12]. This type of attacks can happen in the communication situation that is used to transmit the recent vacant channel

information to neighboring nodes for communication. In the previous existing methods there will be considered a communication situation the distribution is carried out throughout a common control channel (CCC) which is a channel dedicated only to swap management information. A selfish SU will transmit forged free channel list to its neighboring SUs even though a selfish SUs only make use of three channels, it will send a list of all the five occupied channels. The forged information on channel allotment of each node in the network. Thus, legitimate SUs are proscribed from using the two available channels. Finding of existing selfish technology is possible to be unsure and less reliable, because they are based on expected status or expected characteristics of stochastic signals.

V. EXISTING SYSTEM

The existing technique is an autonomous approach but due to using deterministic channel allocation information as well as the support of supportive neighboring nodes. The effectiveness is measured by a detection rate as follows:

$$DR = \frac{No.of\ \det ected\quad selfish\quad \sec ondary\quad user}{No.\quad of\quad actual\quad selfish\quad \sec ondary\quad user}$$

One SU has a highest of eight data channel and one Common Control Channel. The data rate of channel is 11Mb/s. One SU can have two to five one-hop nearest SUs. The experimentation was performing below various selfish SU compactness in CRN. The article [12] proposed a resourceful selfish cognitive radio attack detection technique, called **COOPON,** (Cooperative neighboring cognitive radio nodes). In conventional spectrum management, for the most part of the spectrum is allocated to the licensed users for restricted use. From the cognitive Radio Technology is carried out in the following steps.

- First, it investigates the available spectrum bands by a spectrum sensing technology for unlicensed secondary users (SUs).
- Second one is used to assign spectrum dynamically to the unlicensed users.

When the licensed primary user (PU) is not using the spectrum bands in the network, they are considered accessible. Secondary user emulates the characteristics of the primary user by sending the fake signals. Thus, all of the one-hop neighboring SUs will make a conclusion that the target SU is a selfish attacker. All the one-hop neighboring SUs sum of the currently used channels send by themselves and other neighboring nodes. We will describe the number of channels used by each node in the network. Verify if the target SU is a selfish attacker. Here, the spreading is carried out throughout the common Control Channel. The existing COOPON technique, first it verifies all the nodes in the networks are validated or not. If not, it verifies the nodes one by one using COOPON method illustrate below from the fig.3. From the above fig 2 shows the selfish attacks detection algorithm and

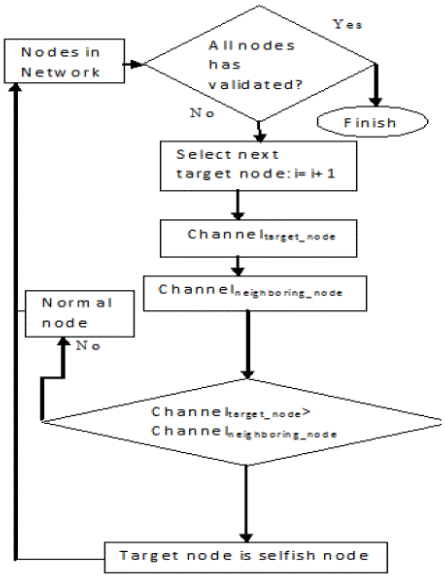

Fig.2. Selfish Attack Detection Algorithm

the mechanisms flow chart of COOPON [12]. As reveal that the flow chart, all the currently used channels in the target node and the neighboring nodes are sum of in steps: The channel target node and the channel neighboring node, based on the channel allotment information. $Channel_{targetnode}$ is the calculation of the number of presently used channels to each neighboring nodes statement by the target node and the $channel_{neighboringnode}$ is the calculation of number of nodes at present used channels to the target node statement by each nearest nodes. Then the channel target node will be match up to the channel neighboring node. In fig.3 the target node, N-Node1, N-Node2, N-Node3 and N-Node4 will check any selfish attack of the target node. The target SU and its entire one-hop neighboring users will swap over the current channel sharing information list via transmit the devoted channels. Using the COOPON detection technique clearly it will describe the number of channels used by each node in the network.

It is pointed that the T-Node 2 reports that have an two channels at this time in use, while N-Node 3 statement that there are two channels at this time in use, while N-Node 3 information that there are three channels currently in use, which creates a disparency N-Node 4 also receives forged channel allotment information from the target node.

On the other hand, all other swap over information pairs, T-Node/N-Node 1 and T-Node/N-Node 2, are accurate. Thus, all of the one-hop neighboring SUs will construct a decision that the target SU is a selfish attacker. According to the above fig.2 shown that the channel target node is 7 and the Channel neighboring node are 5. Because 7 > 5, the target secondary node is notorious as a selfish attacker. The COOPON mechanism is effective than the earlier detection methods, because the channel allotment information is more deterministic than the stochastic signal characteristics.

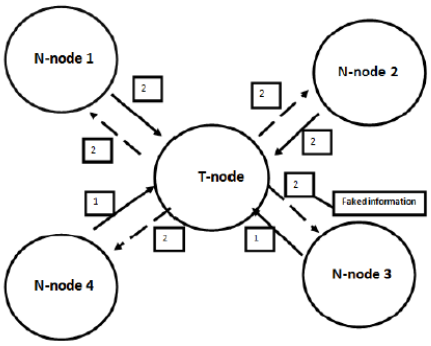

Fig.3. COOPON Detection Mechanism

VI. PROPOSED SYSTEM

The proposed technique is simple to calculate. The Proposed algorithm is the credit risk value algorithm. The credit risk value technique will identify the attacks of selfish SUs in the CRN by calculating the credit risk value. In money matters, credit risk value is calculated risk of loss due to defaulter defaulting of loan. A bank checkup the credit risk of an applicant earlier to approving the loan which is relevant to our research of credit risk value technology is carried out in the following steps. First it calculates the credit risk value earlier than sending any packet, then route the packets, another time recalculates the credit risk value. The credit risk value is steady values, which specify the energy devoted for the packet communication.

CREDIT RISK VALUE=No. of packets* Total energy-Remaining Energy

Where, Total energy is the primary energy of the node and Remaining energy is the energy later than data routing. In the proposed technique, Multiselfish node attacks are identifying using the above simple formula. Credit risk value is the amount of packets multiplied by the energy used by the node in the CR network. In this method, topology is making first and then credit risk value is calculated for all the nodes in the network. Credit risk value is a stable value. Data routing is done after calculating the credit risk value for all the nodes. Then recalculate the credit risk value. The credit risk value is the energy for each node packet broadcast is intrinsic as ten, as the energy necessary for every normal transmission is close to the value ten. If the credit risk value is greater than ten credit risk value, then it detect that node as attacker node and then redirect the packet. Once more calculate the credit risk value. If the value is a lesser amount of than ten credit risk value, then another time data routing is done.

By using the above formula, we are able to get the energy obsessive for each node's packet transmission. After the topology modernization, the credit risk value is once more calculated for every node, then it checks whether the calculated Value is between 4 and 10 credit risk value (or) not until it verify all the in the networks. If the value is in between 4 and 10, and the Performance is more proficient. Because, for regular broadcast,

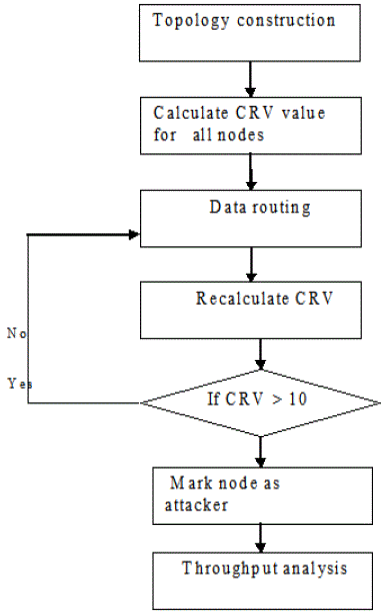

Fig.4. Credit Risk Value Algorithm

between 4 and 10, and the performance is more proficient. Because, for regular broadcast, the value won't be a smaller amount than four by using this simple calculate process, the attacker node in the CRN can be identify and also the network performance can be better.

This method is also the time overwhelming method, since the formula for calculating credit risk value is easy. Credit risk value finding mechanism is given. The credit risk value is point that near in a small circle to every node in the network. The credit risk value for the ordinary broadcast ranges from 4 and 10. By setting this as threshold value and then calculating the credit risk value will be more effective. Later than calculating the credit risk value, data direction-finding is done once more if the credit risk value less than 10. The credit risk value for Node 1 is 8, Node 2 is 10 and Node3 is 7. The credit risk value for Node 4 is 13, which is bigger than 10. This means that Node 4 is a hinder Node. Thus, more than one selfish node in the CRN can be identifying by using the credit risk.

To discover the selfish node in the cognitive Radio ad-hoc network, the process for handling error is as follows:

- After the node creation, credit risk value is calculating for every node in the network.
- Match up to the credit risk value create with all the other nodes. Then the big credit risk value is place as head.
- Transmit the head id to all other nodes. By observe all the nodes, it finds selfish nodes.

VII. CONCLUSION

The existing methodology can predict only one selfish node lies on the entire CR Network. Because, the COOPON uses the deterministic channel share in sequence. In this article, to classify the Multiselfish node attacks using the credit risk information. The proposed CRV algorithms perceive more than one selfish secondary user in the CRN using the credit risk value. Our approach is calculating for the cognitive radio ad-hoc networks. The CRV algorithm construct use of ad-hoc

network advantage such as energy necessary for the packet transmission at every node in the network effectiveness of a better detection. The future work is to implement the detection algorithm to identify the jamming attacks in CRN.

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.