Scientific Research Publishing

Wireless Engineering and Technology, 2016, 7, 105-117
http://www.scirp.org/journal/wet
ISSN Online: 2152-2308
ISSN Print: 2152-2294

Efficient Selfish Attack Detection in Cognitive Radio Network

Shailaja C. Patil[1], Amrita Janardhanan[2]

[1]Department of E&TC, RSCOE, Thathwade, Pune, India
[2]Savitribai Phule Pune University, Pune, India
Email: shailaja.patil11@gmail.com, amrita.janardhanan@gmail.com

How to cite this paper: Patil, S.C. and Janardhanan, A. (2016) Efficient Selfish Attack Detection in Cognitive Radio Network. *Wireless Engineering and Technology*, **7**, 105-117.
http://dx.doi.org/10.4236/wet.2016.74011

Received: July 9, 2016
Accepted: October 18, 2016
Published: October 21, 2016

Abstract

The main intention of developing cognitive radio technology is to solve the spectrum deficiency problem by allocating the spectrum dynamically to the unlicensed clients. An important aim of any wireless network is to secure communication. It is to help the unlicensed clients to utilize the maximum available licensed bandwidth, and the cognitive network is designed for opportunistic communication technology. Selfish attacks cause serious security problem because they significantly deteriorate the performance of a cognitive network. In this paper, the selfish attacks have been identified using cooperative neighboring cognitive radio ad hoc network (COOPON). A novel technique has been proposed as ICOOPON (improvised COOPON), which shows improved performance in selfish attack detection as compared to existing technique. A comparative study has been presented to find the efficiency of proposed technique. The parameters used are throughput, packet delivery ratio and end to end delay.

Keywords

Cognitive Radio Network, ICOOPON, COOPON, Selfish Attack

1. Introduction

The significant growth in wireless networks leads the spectrum to an extreme usage. Cognitive radio is one of the intelligent wireless based communication technologies [1] [2]. To make a better use of the spectrum, Cognitive Radio Networks (CRNs) are used that easily get adapted to the changes in the network. It solves the spectrum shortage problem by allowing unlicensed secondary users to use spectrum band of primary user (PU) without interference [3]. In order to make the maximum utilization of available spectrum bands the secondary user could adopt cognitive radio communication mechanism for effective utilization of available spectrum band.

In Cognitive Radio (CR) most of the spectrum bands are allocated to the licensed users [4] [5], where the CR technology primarily identifies the available spectrum bands which are not used by primary user [6] [7]. Therefore the spectrum bands are dynamically allocated to secondary users based on availability of usable band. However, when the secondary user (SU) senses the presence of primary user and the spectrum is being used by the primary user, then secondary user has to release that spectrum band as primary user has the priority to use it [8]. The reconfiguration of cognitive radio is one of the special characteristics which is used for transmission or reception of data on the basis of automatic detection of available spectrum.

The main challenges faced by cognitive radio are:

1) Topology discovery: The use of non-uniform channels by different cognitive radio users makes the topology discovery difficult [9].

2) Optimization of cooperative sensing: By requesting the sensing information from several cognitive radio users, the user that initiates the cooperative sensing, improves the accuracy but also increases the network traffic. However, this also results in higher latency in collecting this information due to channel contention and packet re-transmissions. These factors must be optimized for correct and efficient sensing in the case of cognitive ad hoc network [9].

2. Literature Review

Minho J. *et al.* [1] proposed a system in which COOPON technique has been used to find the selfish attackers in the cognitive radio ad_hoc network with multichannel resources by cooperative neighboring cognitive radio nodes. Trang V. Mai *et al.* [10], proposed security vulnerabilities in case of cognitive radio networks and discussed various attacks in Physical layer whether it is Primary user emulation (PUE), denial of service attack or jamming attack. Ruiliang C. *et al.* [11], discuss about primary user emulation attack. In this type of attack, the attacker transmits the signal which shows same characteristics as of primary user. These attacks interfere with the spectrum sensing process and reduce the channel resources available to unlicensed users. To overcome this threat, a transmitter verification scheme called localization based defense (LOCDEF) was introduced, which helped to distinguish the primary signals and signals transmitted by attacker on estimating its location and observing the signal characteristics. There is high probability of these attacks in the cognitive radio because of the fact that cognitive radios are highly reconfigurable because of the software based air interface. Husheng Li *et al.* [12] has discussed the approach of combating the primary user emulation attack. In cognitive radio systems, the PUE attacker sends primary-user-like signals during the spectrum sensing period such that honest secondary users leave the corresponding channels, which causes a serious threat to cognitive radio systems. X. Tan *et al.* [13] proposed cross layer altruistic differentiated service protocol (ADSP) for the keen cognitive radio networks to consider the quality of service provisioning in CR Network with selfish node simultaneity [13]. Their purpose is to give minor disruption, problematic throughput, and better quality supply ratios for a cognitive radio network. Position is given to every SU constructed on well-known selfish actions data.

Major work has been done for primary user identification and resource allocation. The security aspect of channel allocation is not addressed thoroughly in the literature. It is also essential to identify the attacker because of which the legitimate user lacks the opportunity of using the channel. In the above papers this issue has not been addressed except [1]. The authors Minho J. *et al.* have presented a technique, namely COOPON [1]. This technique does identify one hop neighboring attackers. However, when selfish nodes are increased, then COOPON technique lacks in efficiency.

To detect selfish attacks in cognitive network, an efficient attack detection technique is proposed, namely Improvised COOPON (ICOOPON) in this paper. The COOPON technique is not efficient to find out selfish nodes that are present far from the network, whereas, the ICOOPON technique can detect such nodes. In the proposed technique Hidden Markov Model (HMM) has been used to improve the efficiency of the attack detection mechanism. The efficiency has been computed using parameters such as Throughput, Packet delivery ratio and End to end delay.

3. Types of Selfish Attacks

Selfish attacks are classified as Type 1, Type 2 and Type 3 described as below:

3.1. Type 1

Selfish attack depends on how it will try to pre-occupy the spectrum resources. The type 1 attack is known as signal fake selfish attack. It prohibits a legitimate secondary user (LSU) from sensing available spectrum bands by sending faked PU signals. The selfish secondary user emulates the characteristics of primary user and this will be overheard by the legitimate secondary user and thinks that the primary user is active. This attack is usually built when there is a transmission between two selfish secondary users, regardless of the number of channels.

3.2. Type 2

Here, the secondary users will be emulating the characteristics of primary users but it is generally carried out in dynamic multiple channel access. In the dynamic signal access process, the secondary users will periodically sense the current operating channel condition in order to know if the primary user is active or not, and if it is so then the secondary user will immediately switch to use other available channels. An attacker can effectively limit the legitimate secondary user performance, by sending fake signal information in a round -robin type [1].

3.3. Type 3

Type 3 attack is also known as channel pre occupation attack. Such attack occurs in the communication environment which is used to broadcast the current available channel information to all other neighboring nodes for transmission. The selfish SU will broadcast fake free channel lists to its neighboring SUs. Thus the usage of available channels is banned to the legitimate secondary user [1]. As depicted in **Figure 1**, even if the selfish secondary user uses only 3 channels it will send fake channel list, regarding the channel list.

4. Detection Mechanism

CR network is having a dynamic characteristic due to which it is difficult to detect the selfish attack in the wireless network. The COOPON technique is used for detection of selfish attack. Here it concentrates on narrow minded assaults of SUs towards different direct access in subjective radio specially appointed systems. It accepts that a single secondary user obliges different channels. Each secondary user will frequently telecast the current station distribution data to the majority of its neighboring secondary users. It includes the quantity of stations in use and the quantity of accessible stations [1] [14].

Among auxiliary ad hoc system CCC (common control channel) has been utilized to show and watch data. Type 3 selfish attack can be found out using the COOPON technique. The secondary users will use the information distributed through CCC to access channel for transmission. In this technique, it considers one node as target node and the other as neighboring node, and it will check the selfish attack of the target node.

From **Figure 2**, among all the nodes, one of the node is target node, *i.e.* T-Node which is a SU but other 1-hop neighboring SUs, e.g. Neighboring-Node 1, Neighboring-Node 2, Neighboring-Node 3, and Neighboring-Node 4, will scan for selfish attack by the nodes. The Neighboring-Node and Target node will be called as N-Node and T-Node respectively hereafter. The target Secondary User and all of its 1-bounce neighboring users will exchange the current channel allocation information list via

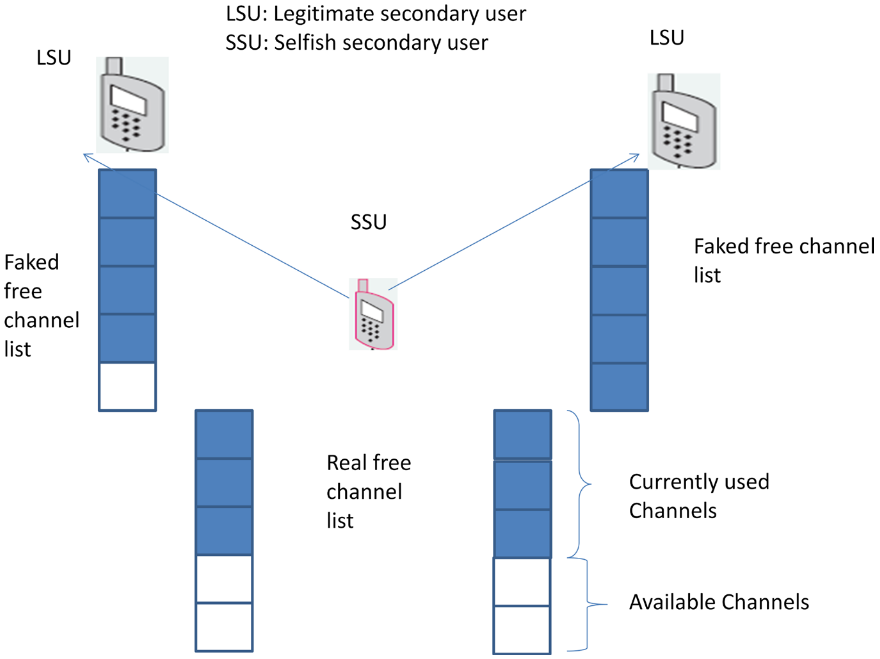


Figure 1. Type 3 attack [1].

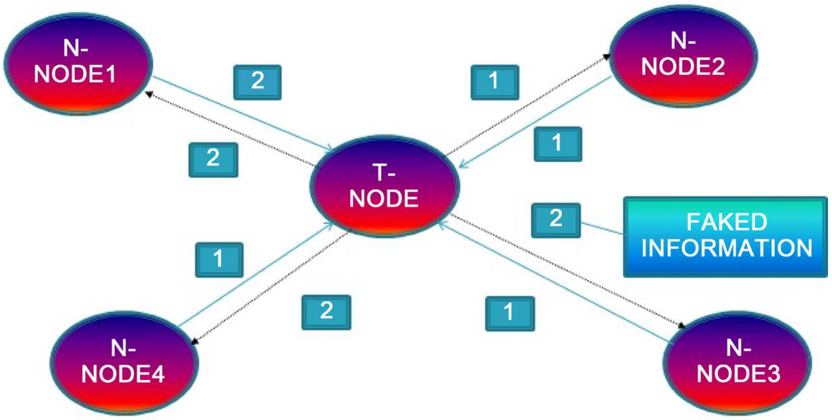


Figure 2. Selfish attack detection [1].

broadcasting on the dedicated channel. When the Target-Node reports that there are two channels currently in use, while Neighboring-Node 3 reports that only one channel is currently in use, creates a mismatch between the target and the neighboring node. N-node 4 also receives the fake channel information. On the other hand T-node and N-node 1, T-node and N-node 4 are correct. Thus all the 1-hop neighboring nodes can easily decide that the target node is the selfish attacker [14].

Detection Algorithm for ICOOPON

The detection algorithm for ICOOPON is as shown in the following section:

- Among the secondary nodes consider one as target node.
- Discover all the neighboring nodes for the current target node.
- Generate the initial probability of all the nodes in the present scenario.
- Store the Probability sequence.
- Find the nodes with states 0 and 1.
- Store Transitions in an array.
- The process repeats for all the nodes present in the network.
- Node/s with high occurrence and probability, identify the selfish attacker.

Figure 3 shows the proposed ICOOPON technique. The HMM is a finite model that describes a probabilistic distribution over an infinite number of possible sequence. This is a double embedded stochastic process with two levels. The upper level is a Markov model and states are unobservable.

In this case, all the nodes initially follow the discovery mode, in which all its neighboring nodes are found. One or more selfish attackers are present in the network. Let one of the nodes is target node and all one hop neighboring nodes are found. Then initial probability of channel occupancy will be generated. Initial probability will be generated for the nodes present in the network. A uniform number generator is used for this process. The nodes with 0 probability will be neglected because it is not using any channel. Then the probability will be set as 0 if the probability is less than 0.6, and if it is greater than 0.6 then it will be set as 1. The node having more probability in number of occurrence will be detected as selfish node or attacker. The base station monitors this

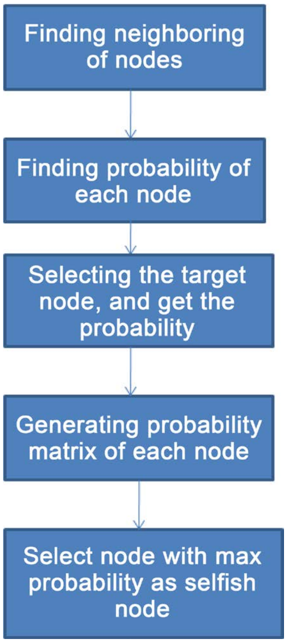

Finding neighboring of nodes
Finding probability of each node
Selecting the target node, and get the probability
Generating probability matrix of each node
Select node with max probability as selfish node

Figure 3. Flowchart of proposed ICOOPON.

channel allocation process. When base station detects, that one or more number of nodes are having more occurrences of high probability of channel occupancy, then those nodes will be declared as selfish nodes.

In HMM, until the end state is reached the sequence of state is generated by moving from state to state according to the state transition probabilities. In the HMM, the state themselves are not directly observed instead we assume that there are some sequence of state in Markov chain that cannot be observed directly, and these states generate observations. Each state may have different distribution. The HMM model falls in a subclass of Bayesian network.

5. Simulation Result and Analysis

5.1. Network Scenario

The selfish attacks have been simulated in NS-2. The wireless scenario of 1000 × 1000 square meter area has been considered. Number of nodes has been varied from 10 to 100 at the interval of 20. The simulation results in the presence of selfish nodes and in the absence of selfish nodes has been presented. The parameters that have been analyzed are packet delivery ratio, throughput and end to end delay. In simulation scenario maximum 20 nodes are considered as selfish nodes.

Number of selfish nodes is varied from 2 to 20 and performance of COOPON and ICOOPON is observed. For communication all the nodes use Omni-directional antenna (Table 1).

5.2. Simulation Results

The parameters such as Throughput and Packet delivery ratio has been considered for evaluating the performance of the algorithm.

1) Throughput: It is measured in data packets per second. It shows the rate of information or message delivered over a communication channel.

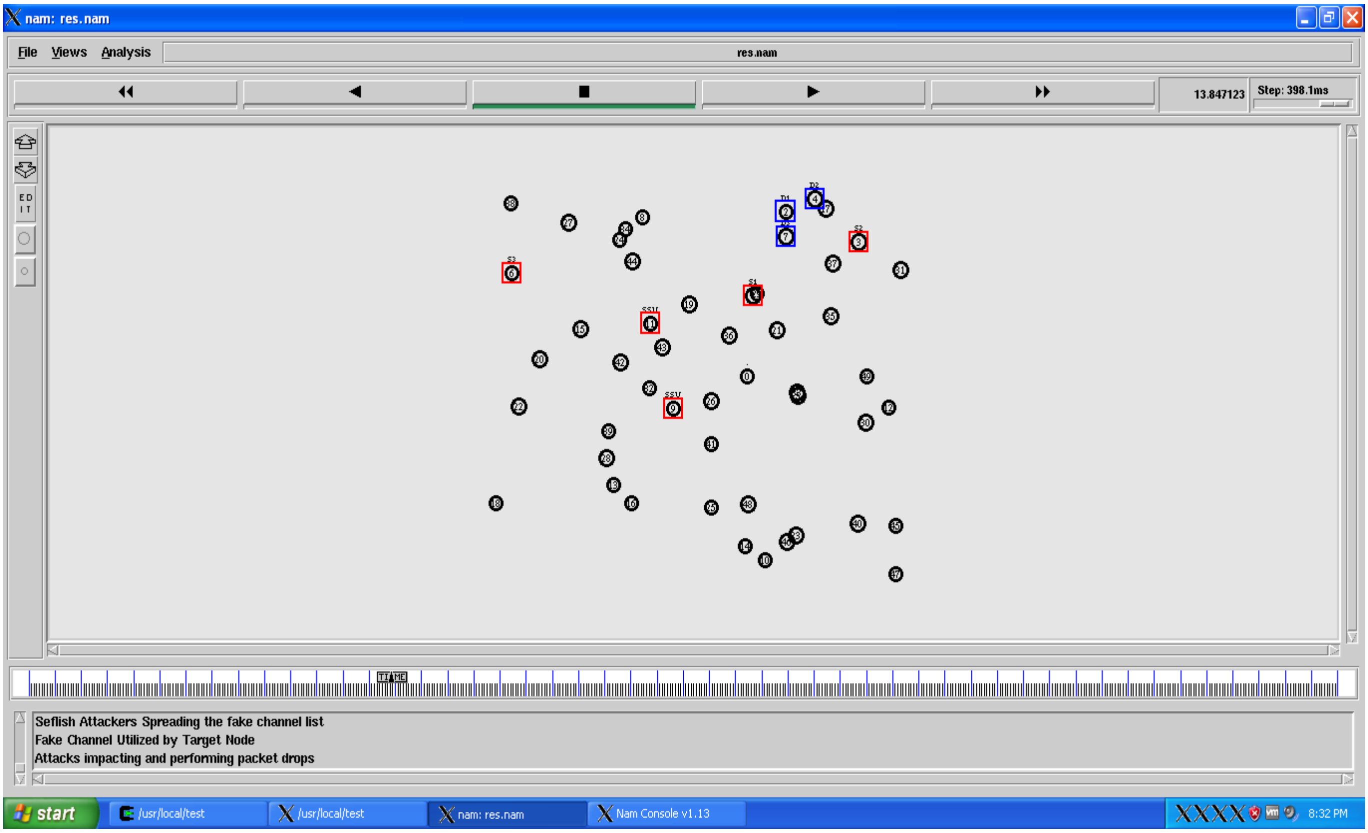
2) Packet Delivery Ratio: It shows the ratio of number of packet transmitted to number of packet that has been received.

3) End to end delay: I t is the total delay that a packet experience as it is travelling through a network.

The following Figure 4 shows a network scenario with 50 secondary users. The nodes shown in square block are selfish secondary users, nodes 9 and 11 are the selfish secondary users that are marked in red and shown as Selfish Secondary User. The source nodes are shown in red circles and destination nodes are marked as blue. The nodes with ID 1, 3, 6 etc. are the source nodes and nodes with ID 2, 4, 7 are the destination

Table 1. Simulation details.

Antenna	Omni directional antenna
Routing protocol	AODV (ad hoc on demand vector protocol)
Network size	1000 m × 1000 m
No. of secondary users	10, 20, 30, 40, 50, 60 up to 100
No. of selfish secondary users	2, 4, 6, 8, 10, 12, 20



Seflish Attackers Spreading the fake channel list
Fake Channel Utilized by Target Node
Attacks impacting and performing packet drops

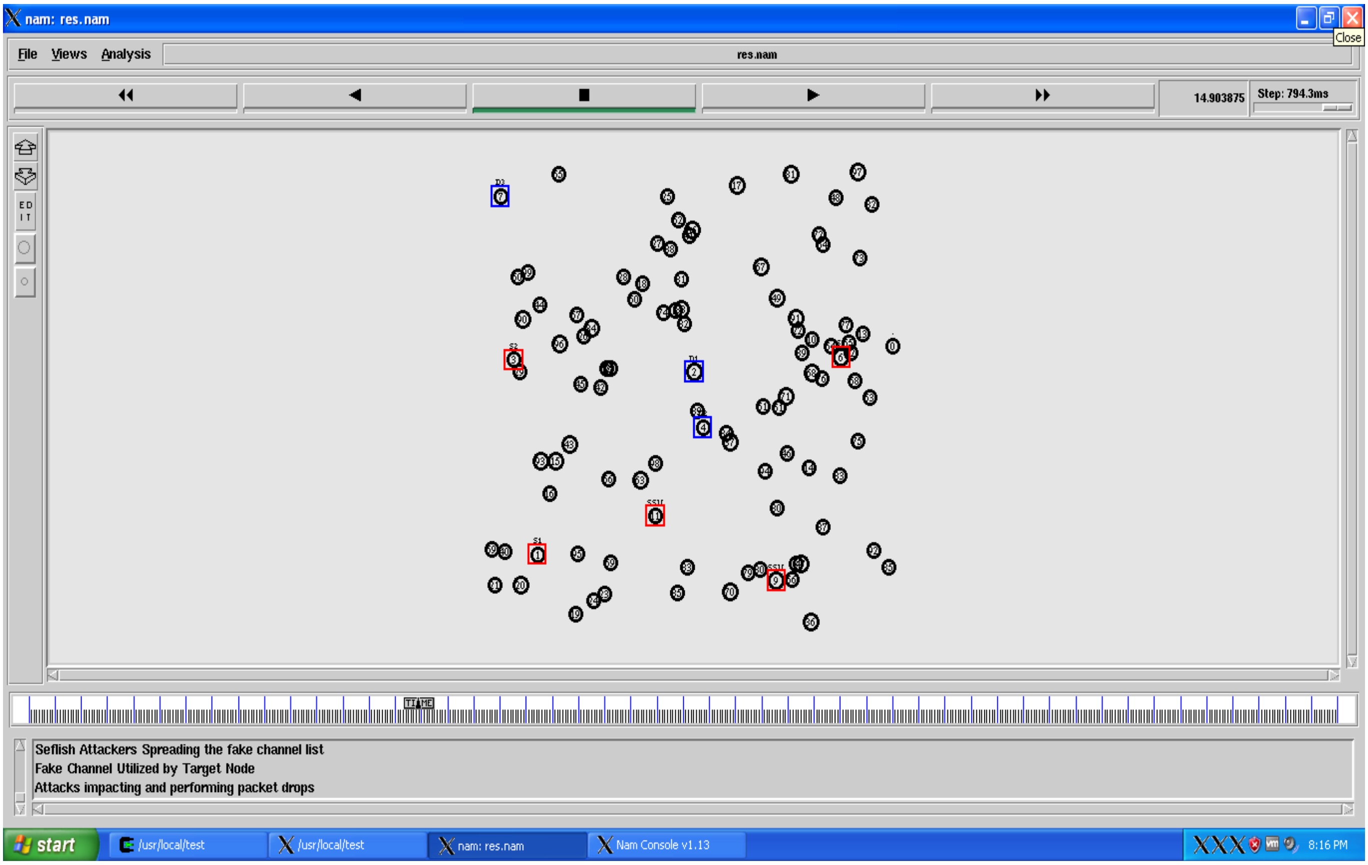
Figure 4. Output of the COOPON with 50 secondary users.

nodes that are marked in blue. The nodes are continuously move and packet transmission takes place among the nodes.

Figure 5 depicts a scenario for 100 Secondary Users with 2 selfish nodes. Where nodes 9, 11 are selfish nodes that are marked as red. The nodes are the source nodes 1, 3, 6 and the destination nodes are with ID 2, 4 and 7. The nodes are continuously move and packet transmission takes place among the nodes. Simulations have been performed with 50 and 100 numbers of secondary users with varying selfish node attacks.

Figure 6 shows the average throughput ratio of AODV, COOPON and ICOOPON, which is the rate of successful message delivery over a communication channel. Here, AODV is included in all the plots, just to show how AODV is affected due to selfish attacks. It is measured in bits/second or data packets/second. Here, ICOOPON shows more throughput performance than the COOPON and AODV protocol technique. When the number of selfish node increases the throughput performance of COOPON and AODV technique will undergo degraded performance. Since ICOOPON works with HMM algorithm along with the COOPON technique, the performance of ICOOPON is improved.

Figure 7 shows the performance of packet delivery ratio in AODV, COOPON and ICOOPON protocols respectively. The packet delivery ratio shows the ratio of number of packets transmitted to number of packets received. It should be as high as possible.



Seflish Attackers Spreading the fake channel list
Fake Channel Utilized by Target Node
Attacks impacting and performing packet drops

Figure 5. COOPON with 100 secondary users.

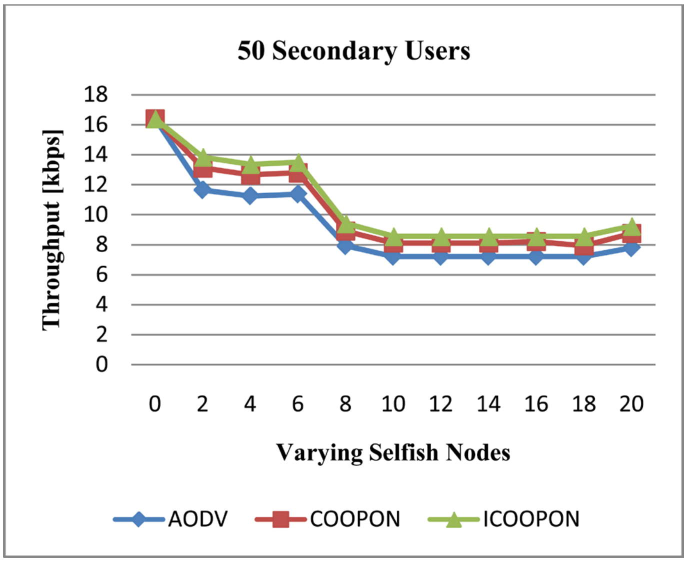


Figure 6. Average throughput.

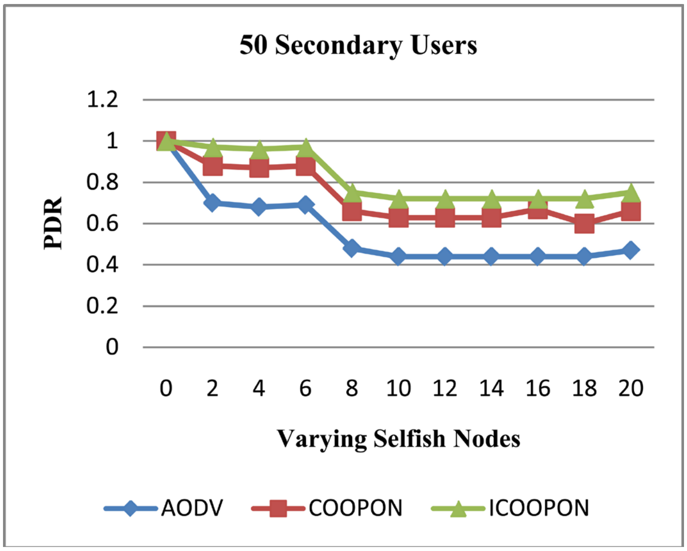


Figure 7. Performance comparison of PDR with 50 secondary users.

From the graph the performance of packet delivery ratio is more for ICOOPON as compared to COOPON and AODV protocol technique. As, ICOOPON technique uses two algorithms, it checks with the probability condition with all the nodes present over there. The main drawback of COOPON technique is that it does not detect selfish attack to search beyond one hop network because of this reason the efficiency is less compared with ICOOPON technique.

Figure 8 shows plot of an end to end delay with varying selfish nodes from 0 to 20. As the number of selfish nodes increases the end to end delay also increases. For example the End to end delay is largest for AODV as compared to COOPON and ICOOPON. The COOPON technique has delay of 0.85 whereas for ICOOPON it is 0.6. Thus even if the number of attackers is increasing, the respective end to end delay is also increasing.

However, there is less effect on ICOOPON as seen in the above figure.

Figure 9 shows the performance of End to End Delay for 50 secondary users with varying selfish nodes from 0 to 20. As the number of secondary users increases, performance decreases with increase in number of selfish nodes.

The following table summarizes the performance study of AODV, COOPON, and ICOOPON.

Table 2 gives the details of Packet Delivery Ratio for 50 and 100 numbers of secondary users. The performance of AODV, COOPON and ICOOPON been analyzed in the presence of 5 selfish attackers. In the case of 50 secondary users AODV is having the least packet delivery ratio of 0.69. The proposed ICOOPON technique has the highest packet delivery ratio of 0.92 for 50 secondary users. In the case of 100 secondary users AODV is having the least Packet delivery ratio *i.e.* 0.59. The ICOOPON approach is having the highest Packet delivery ratio of 0.82.

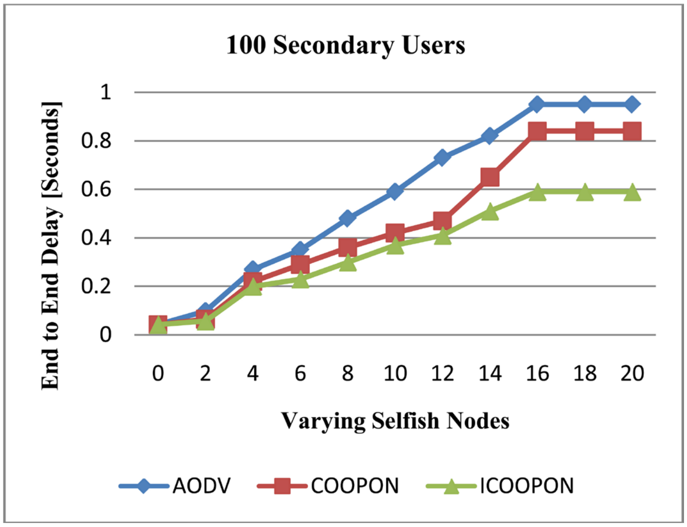


Figure 8. End to end delay of 100 secondary users with AODV, COOPON and ICOOPON.

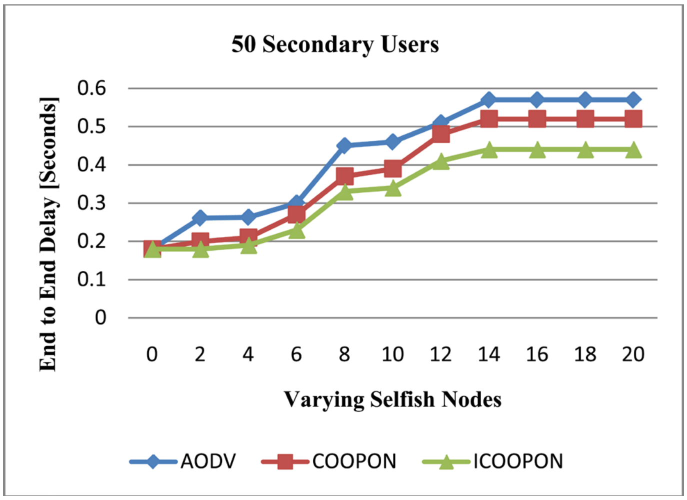


Figure 9. End to end delay of 50 secondary users, with AODV, COOPON and ICOOPON.

Table 3 gives the details of average throughput ratio for 50 and 100 number of secondary users. The performance of AODV, COOPON and ICOOPON has been analyzed in the presence of 5 selfish attackers. In the case of 50 secondary users AODV is having the least average throughput ratio of 11.37 kbps. The proposed ICOOPON technique has the highest packet delivery ratio of 13.5 kbps for 50 secondary users. When the number of secondary users are 100, AODV is having the least value *i.e.* 9.58 kbps. The ICOOPON approach is having the highest value *i.e.* 11.38 kbps.

Table 4 gives the details of end to end delay for 50 and 100 numbers of secondary users. The performance of AODV, COOPON and ICOOPON has been analyzed in the presence of 4 selfish attackers. In the case of 50 secondary users the proposed ICOOPON technique has the least delay of 0.1884 sec and AODV has the highest end to end delay of 0.2637 sec. In the case of 100 secondary users ICOOPON approach has the least delay of 0.2 sec, and AODV is has the highest delay of 0.27 sec.

Table 2. Comparative study of AODV, COOPON and ICOOPON w.r.t. packet delivery ratio.

S. No	No. of nodes	Packet delivery ratio (kbps) (5 selfish nodes)
AODV [1]	50	0.69
	100	0.59
COOPON [14]	50	0.88
	100	0.77
ICOOPON (proposed technique)	50	0.92
	100	0.82

Table 3. Comparative study of AODV, COOPON and ICOOPON w.r.t throughput.

Technique	No. of nodes	Throughput (5 selfish nodes)
AODV [1]	50	11.37
	100	9.58
COOPON [14]	50	12.79
	100	10.18
ICOOPON (proposed technique)	50	13.5
	100	11.38

Table 4. Comparative study of end to end delay for AODV, COOPON, and ICOOPON.

Technique	No. of nodes	End to end delay
AODV [1]	50	0.263
	100	0.27
COOPON [14]	50	0.208
	100	0.22
ICOOPON (proposed technique)	50	0.1884
	100	0.2

From the above tables it can be summarized that when number of nodes increases the efficiency decreases for both the case of packet delivery Ratio, Throughput and end to end delay. However, the ICOOPON is least affected with increase in selfish node attacks as compared to COOPON and ICOOPON.

6. Conclusion

The cognitive radio is currently attracting numerous research efforts, where the major problem is of security. The novel technique, namely ICOOPON is proposed in this paper which has improved performance as compared to COOPON and AODV. For simulation 50 and 100 numbers of nodes have been used with four and five numbers of selfish nodes. The ICOOPON technique provides the improved performance due to HMM. The proposed technique is proved to be more efficient by 32% than the COOPON technique in various parameter performances such as packet delivery ratio, end to end delay and throughput. For future work cryptographic model and game theory can be applied to check the selfish attack detection analysis. The existing parameters can be taken into account for performance analysis and can be analyzed using jitter.

References

[1] Jo, M., Han, L., Kim, D. and In, H.P. (2013) Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks. *Proceeding of IEEE Network*, **27**, 46-50. http://dx.doi.org/10.1109/MNET.2013.6523808

[2] Ding, L., *et al.* (2010) Cross-Layer Routing and Dynamic Spectrum Allocation in Cognitive Radio Ad Hoc Networks. *IEEE Transactions on Vehicular Technology*, **59**, 1969-1979. http://dx.doi.org/10.1109/TVT.2010.2045403

[3] Wang, W.F. (2009) Spectrum Sensing for Cognitive Radio. 2009 *Third International Symposium on Intelligent Information Technology Application Workshops*, 21-22 November 2009. http://dx.doi.org/10.1109/iitaw.2009.49

[4] Akyildiz, I.F., *et al.* (2008) A Survey on Spectrum Management in Cognitive Radio Networks. *IEEE Communications Magazine*, **46**, 40-48. http://dx.doi.org/10.1109/MCOM.2008.4481339

[5] Kim, H. and Shin, K.G. (2008) Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks. *IEEE Transactions on Mobile Computing*, **7**, 533-545. http://dx.doi.org/10.1109/TMC.2007.70751

[6] Akyildiz, I.F., Lee, W.-Y., Vuran, M.C. and Mohanty, S. (2008) A Survey of Spectrum Management in Cognitive Radio Networks. Georgia Institute of Technology, IEEE Communications Magazine. http://dx.doi.org/10.1109/MCOM.2008.4481339

[7] Cheng, G., *et al.* (2007) Joint On-Demand Routing and Spectrum Assignment in Cognitive Radio Networks. 2007 *IEEE International Conference on Communications IEEE*, 24-28 June 2007. http://dx.doi.org/10.1109/icc.2007.1075

[8] Guang, L. and Assi, C. (2006) Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks. 2006 *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications IEEE*, 19-21 June 2006. http://dx.doi.org/10.1109/wimob.2006.1696387

[9] Akyildiz, I.F., *et al.* (2006) NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey. *Computer Networks*, **50**, 2127-2159.

http://dx.doi.org/10.1016/j.comnet.2006.05.001

[10] Mai, T.V., Molnar, J.A. and Rudd, K. (2011) Security Vulnerabilities in Physical Layer of Cognitive Radio. 2011 *IEEE* 54*th International Midwest Symposium on Circuits and Systems* (*MWSCAS*).

[11] Chen, R.L., Park, J.-M. and Reed, J.H. (2008) Defense against Primary User Emulation Attacks in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications*, **26**, 25-37. http://dx.doi.org/10.1109/JSAC.2008.080104

[12] Wang, W.K., *et al.* (2009) Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks. 43*rd Annual Conference on Information Sciences and Systems*, 18-20 March 2009.
http://dx.doi.org/10.1109/CISS.2009.5054704

[13] Tan, X.B. and Zhang, H. (2012) A CORDIC-Jacobi Based Spectrum Sensing Algorithm for Cognitive Radio. *KSII Transactions on Internet & Information Systems*, **6**, 1998-2016.
http://dx.doi.org/10.3837/tiis.2012.09.001

[14] Wagh, S., More, A. and Khavnekar, A. (2015) Identification of Selfish Attack in Cognitive Radio Ad-Hoc Networks. 2015 *IEEE International Conference on Computational Intelligence and Computing Research* (*ICCIC*). http://dx.doi.org/10.1109/ICCIC.2015.7435805