International Journal of Grid and Distributed Computing
Vol. 9, No. 11 (2016), pp.247-260
http://dx.doi.org/10.14257/ijgdc.2016.9.11.21

A Novel Anti-Jamming Technique for Cognitive Radio Network

Poonam, Ravi Kant and Chander Kumar Nagpal

Department of Computer Engineering,

YMCA University of Science and Technology, Faridabad, India
poonamgarg1984@gmail.com, kant.ravi196@gmail.com

Abstract

As the use of wireless applications is increasing every day; it results into shortage of limited available spectrum. Licensed spectrum is unutilized and unlicensed spectrum is overcrowded, so to increase the efficiency of allocated spectrum and to fulfill the need of unlicensed spectrum, CRN is proposed. Some routing protocols are designed for wireless communication keeping in mind that all nodes are cooperating. So this approach can solve the problem of spectrum scarcity. However due to the flexibility of such network, it is vulnerable to many security threats. Jamming attack is one of the most popular security threats which cause denial of service in the network. Various solutions are available in the literature to deal with jamming attack but still there are some open challenges in jamming attack. In this paper various anti-jamming techniques and analyze the open issues of jamming which are still there in the cognitive radio network. An anti-jamming technique is proposed in this paper to deal with the open issues. Simulation is done in MATLAB-2013 and results show that proposed method performs well.

Keywords*: Cognitive Radio Network, Security, Jamming Attack, Denial-of-service attack, Anti-Jamming Techniques, Jammer etc.*

1. Introduction

To improve the spectrum usage in the environment of limited spectrum which was not utilized efficiently Cognitive Radio Network (CRN) [1] was proposed as a most promising technology. Cognitive radios can be programmed and configured dynamically; these features of CR make it intelligent. It is a form of dynamic spectrum management. Main constitutes of CRN are primary and secondary users. Primary users are those legitimate users who have bought the spectrum and have legal rights to access the spectrum. On the other hand secondary users are those users who do not have their own spectrum. These users use the spectrum of primary users opportunistically. Secondary users leave the channel free whenever a legitimate user come into existence so that there is no interference in the network between primary and secondary user. For this, users have to sense the channel all the time and the sensing information is shared among the secondary user. This point is the weakest point of cognitive cycle because this information can be used by the jammer to jam the network. All this happens on physical link layer on which jamming attack usually occur.

- Jamming Attack-In Jamming Attack [2-6] a jammer which can be any one among constant, reactive, deceptive or random jammer sends the packet on the channel to hinder the channel, as a result of that legitimate user either could not sense the channel. In this, attackers sends the same frequency signal but relatively of high power which intercepts the signals send by legitimate user and causes denial of service attack. Mainly it occurs at physical layer but it may affect multiple layers (cross layer attack). It is a form of DOS attack [7]. Figure 1 describes the working of jammer.

ISSN: 2005-4262 IJGDC

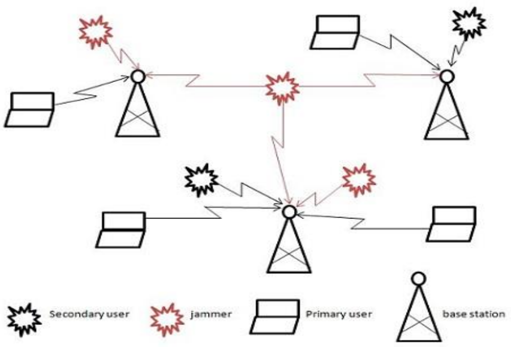


Figure 1. Jamming Attack Model

There are primary and secondary users connected to the base stations in the figure 1. Few jammers are there among secondary users shown by red nodes which utilize the spectrum sensing information shared by other users and continuously send high power signals of same frequency as the normal secondary users so that other cognitive users could not access the channel in near future. There are many type of jammers described below which jam the network in different scenarios.

- Constant Jammer-This type of jammer continuously sends high power signals on the channel without considering other users on the channel. These signals represent the random bits generated by bit generator because it does not follow any protocol of MAC layer.
- Random Jammer-It works in two modes sleeping mode and jamming mode randomly. It is called random jammer because it takes “random” breaks during sending the jamming signals. In sleeping mode it sleeps regardless of traffic. Packet drop ratio increases in this mode and size of the packet decreases. In jamming mode it may behave either as a reactive jammer [8] or constant jammer [2] and also it does not follow any MAC protocol.
- Deceptive Jammer-It sends the packet of same type on the channel continuously which makes the legitimate users to switch into receiving state because legitimate user detect a constant stream of data packets which seems legal data to these users. These jammers are protocol aware and internal to the system. They increase the channel sensing time for the legitimate users.
- Reactive Jammer-It only works when it detects transmission on the channel and alters some part of the signal with noise so that receiver cannot check the packet whether it is correct or not. As a result of this, receiver discards the packets. This jammer raises packet drop ratio in the system.

2. Related Work

Anti-Jamming Techniques-

A. AONT system

In 1997, Ronald Rivest proposed a system called “All or Nothing Transform” [9]. No encryption is performed because no secret key is used but its output is encrypted block by block. AONT is applied on the secret key rather than storing it. All kind of cryptographic schemes can be protected if a system is built in which there is a threshold which is small than the value calculated from AONT system. To avoid jamming attack packet hiding method is used. The sender transmits the packets of fix sized blocks then these blocks are transferred to AONT with secret key applied on it. These encrypted packets are received by receiver and the same key is applied by the users on the packets to get the same message.

B. JAM (Jammed Area Mapping) protocol

A. Wood, J. Stankovic, S. Son [10] proposed a detection and moderation method of jamming attack in 2003. This method works on the nodes utility of channel means if utility of any channel fall below a certain point called threshold then the presence of jammer is detected in that area within 1-5 seconds and node detection system flood the jammed or unjammed alert message accordingly to the neighbors. Threshold can be set on the basis of number of failures to get wireless channel i.e. 10. After getting the jammed message, neighboring node of jammed node create a group of group ids and direction vector pointing to the jammed node then it declare a timer to get all jammed messages. As the timer expires, the BUILD message is send by the node to its neighbor nodes which has the group id and membership list .If the direction vectors are compatible, they are joint together. When join time expire the mapping node, send the BUILD message again having the dominant group id and merge member list. Other nodes do the same and after removing the jammed node an unjammed message is send by jammed node. After the mapping phase all messages follow different route in the network.

C. Channel surfing and spatial retreat

W. Xu, T.Wood, W. Trappe, and Y. Zhang [11] in 2004 provides the method in which mobile nodes which feel jamming attack on the specific channel are moved to the safe location. In this the detection can be determined by measuring the noise levels at physical layer or at the MAC layer using CSMA but before switching channel, next channel is computed by using the formula

k(n+1)=(k(n)+1)%m where, m are number of orthogonal channels.

If it is an infrastructure based network then it is to be ensured that all registered users are on the same channel and broadcast the channel change with a private key authentication. After movement of users, network has to be reconfigured.

D. Using PDR with consistency checks

In the traditional method only PDR is used to detect the jamming but jamming is not the only reason of low PDR so, W. Xu, T.Wood, W. Trappe, and Y. Zhang (2005) proposed a method [12] “PDR with consistency check” to detect and confirm the jamming attack. High signal intensity means high PDR ratio but when it comes to low signal intensity it does not mean there is low PDR value so if signal power is high and value of PDR is low than the PDR’s value of neighbor but if anyone of neighbor has high PDR value it means jamming attack is not there but if neighbor nodes have low PDR, jamming is discovered. If there is no neighbor for this type of node, effect of jamming is not considered because PDR value for this node will be low. After detecting the area of the jammer, jamming attack can be easily removed from the network.

E. Ant system

R. Muraleedharan, L.A. Osadciw proposed an algorithm [13] in 2006 to detect jamming attack at physical layer and send an alert message to suitable destination. This system is based on the hypothesis to test whether a DoS attack is real or not. Ant system gathers the information of different routes to a particular destination by traversing a node back and forth in the network. This information is saved in ‘tabu’ list for further use. For detecting the jamming the energy and distance information is used. Four types of jammers are used in this scenario. SNR and PDR based techniques are used to detect jamming attack. The system checks the values frequently to see that whether the jamming is real or not. It measures the probability of connection between two nodes, if the probability is lesser than threshold value then link is traversed otherwise network is jammed. When there is a jamming at a link the link is not taken in the route and other routes are taken into consideration.

F. Game theoretic modeling

In this [14] method there are 2 players, monitors and jammers nodes. Jammers are here to maximize the DoS attack to the registered users while registered users try to improve the throughput of the system. Monitors are used to detect the constant jammers and reactive jammers by sensing the channel and average retransmission rate of packets. It identifies the user whether it is group jammer or non-jammer. Monitors can be of any type continuous or periodic. It is based on carrier sensing failure count, retransmit data and retransmit RTS. Euclidean distance is calculated for each node to check the attribute (jamming and un-jamming) of the nodes.

G. Channel hopping

In proactive hopping communication channels are changed after time to time whether there is jamming or not in the channel but this is very inefficient in terms of energy. K. Pelechrinis, C. Koufogiannakis, S.V. Krishnamurthy (2009a) [15] shows that only 4 jammers can jam an entire 802.11a spectrum of 12 orthogonal channels because 1 jammer can jam 3 channels with 2 adjacent channels if the jammers are placed at proper positions. The main disadvantage of this technique is limited numbers of orthogonal channels and little band gap between channels, so to improve it Pelechrinis et al (2009a) consider advocate frequency hopping [16] but it is effective when there are large number of orthogonal channels. A threshold value is fixed for waiting time of accessing channels. If waiting time crosses the threshold then only hop the channels by some pre-defined mechanism or by random. Random number generation is the best technique where jammers cannot jam the channel even if it knows the history of the hopping.

H. Trigger nodes identification

Reactive jammers are not easy to find out because they are active only when transmission is in the process. So to identify reactive jamming, a method is proposed called trigger nodes identification [17]. Trigger nodes are those which can make active the reactive nodes. Victim nodes are those who are affected by triggered jammers. Group testing, disk cover and clique based clustering is used to find out the presence of jammers. All victims can be found by using breadth first search. In the second phase testing is done so that all the victims can be find out which are affected by same jammer. In the third phase, the trigger nodes are identified using a group testing mechanism, called non-adaptive combinatorial testing. Once the trigger nodes are known, a different route is selected for routing packets.

I. Fuzzy inference system

S. Misra, R. Singh, S.V.R. Mohan (2010) proposed a method [18] on the basis of signal to noise ratio and packet dropped per terminal. The base station checks the number of nodes received by the receiver in a time span. Thus we know the presence of the jammer. This system finds out the presence of jamming by calculating signal to noise ratio, if SNR value is low the presence of jamming is high and we don't consider PDPT value in this case. But when SNR is medium, jamming depends on PDPT value and when

SNR is high probability of jamming is low then we grouped neighboring nodes into clusters of non-jammed and jammed nodes.

J. T-attacker model

In this model [19] Lu Zhanga, Qingqi Peia, Hongning Lib consider a distributed CRN with n cluster and m jammers in 2012. Secondary users cannot access the channel unless cluster head want it to do so. Cluster head can change the location of control channels dynamically. It gives the unique id to each secondary user. A key is generated based on the unique ID of secondary user. This key is helpful to correctly judge the location of control channel and successfully reception of the message in the presence of the jammer. At each time interval the control information is send over various control channels so a secondary user can access only one channel at a time and cannot jam the network.

K. Jamming attack detection and isolation technique

In 2015 H. Khosla, R. Kaur, proposed a technique [20] to improve efficiency of network. When jamming attack is done on the network it increases the delay and decreases the throughput of the network at steady rate due to malicious node. This technique is done on the AODV routing protocol. Firstly a route is considered on the basis of hop-count and sequence number but when the throughput of the network fall below a certain point then network goes into search mode and find out the jammer. ICMP packets are generated on source side and flood on the network. These packets are used to monitor the network to find out the jammers. As a result of this, source node knows the exact route and the route affected by jammers and then stops packet forwarding on affected route.

Table 1. Comparison Table of Anti-jamming Techniques

Technique	Year	Type	Advantage
AONT	1997	Jam avoiding technique	Provides protection to all kind of cryptographic schemes
JAM	2003	Jam Avoiding protocol	Very fast detection of Jam.
Channel surfing and spatial retreat	2004	Anti-jamming technique	Works on both infrastructure based and infrastructure less network
Using PDR with consistency checks	2005	Jam detection technique	More efficient than PDR method to detect jamming.
ANT	2006	Jam detection and prevention algorithm	System can detect fake DOS attack.
Game theoretic modeling	2007	Jam detection	Able to detect group-ids of jammer
Fuzzy interference system	2009	Jam detection and avoidance technique	Identifies reactive jamming which is very difficult to find out.

Channel hopping	2009	Anti-Jamming technique	Jammer cannot jam the channel even if it knows the history of hopping. Very effective in case of large number of orthogonal channels.
Fuzzy interference system	2010	Jam detection technique	Separate cluster formation for both jammed and unjammed nodes.
T-attacker model	2012	Anti-jamming technique	Works fine in case of presence of jammer.
Jamming attack detection and isolation	2015	Anti-jamming technique	Batter performance in terms of packet loss.

3. Problem Definition

Most of the previous techniques are based on cryptography and internal secondary users to the system. The process of exchanging the keys between users can break down the confidentiality and integrity of the user by some attacks like meet in the middle attack. These techniques are not effective, slow and take too much overhead in the authentication process of the secondary user in hostile network that is why it consumes more energy in the communication process. Since these techniques are not robust in hostile environment so there is a great need of an Anti- Jamming model which is more robust, take lesser energy in communication process and increase spectrum utilization than previous models.

4. Proposed Work

In the proposed model whenever a secondary user made a request to primary user to gain the access of channel, PU provide limited bandwidth to that SU to keep the system safe and IDS (Intrusion Detection System) is used on every primary user to sense the signal sent by secondary user and calculate signal to noise ratio of every secondary user with respect to the signal of network. If SNR ratio is less than 36.5 for any secondary user then that secondary user is a jammer. If a jammer is found then Mac-address of that secondary user is stored in the central database called cognitive engine and when the secondary user move to the next location and send the request to other primary user, after receiving the request from the secondary user primary node checks the central database first if it finds the entry of that particular secondary user in the database then primary user immediately restrict the secondary user to gain the access of the channel because all the primary users are fixed. So all primary users know the location of other primary users that is why there is a need to just check the channel whether it is free or not for the communication.

A. Working environment

Figure 2 shows working environment of a cognitive radio network. Here PU's are fixed and SU's are movable.

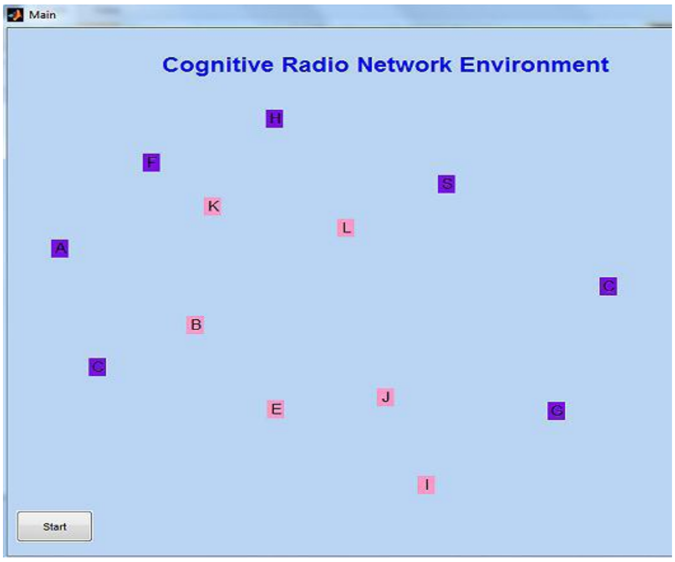


Figure 2. Working Environment of a CRN

B. Procedure

To set up the environment two type of nodes are taken one is fixed and the other is movable. Nodes which are kept fixed called primary user nodes and the nodes which are movable called secondary user nodes. Whenever a SU wants to access the channel and the channel is free, it sends a request to PU and PU provides limited bandwidth to secondary user at first, so that if the SU is a jammer it could not harm the network and the network can easily recovered or prevents the situation of jamming. Every PU monitors the signal sent by SUs for some time and calculates SNR of every secondary user for some time and compares the SNR value. If the value is lesser than 35.6 then the SU is a jammer otherwise it is not a jammer and gives the bandwidth required by SU. If the SU is a jammer then store the entry (MAC address) to a central database so that it can be used in future. If the jammer moves to the new location and requests for the channel to another PU then PU checks the database firstly to find out the SU is a jammer or not. If PU finds out the entry in the table then it will immediately block the SU.

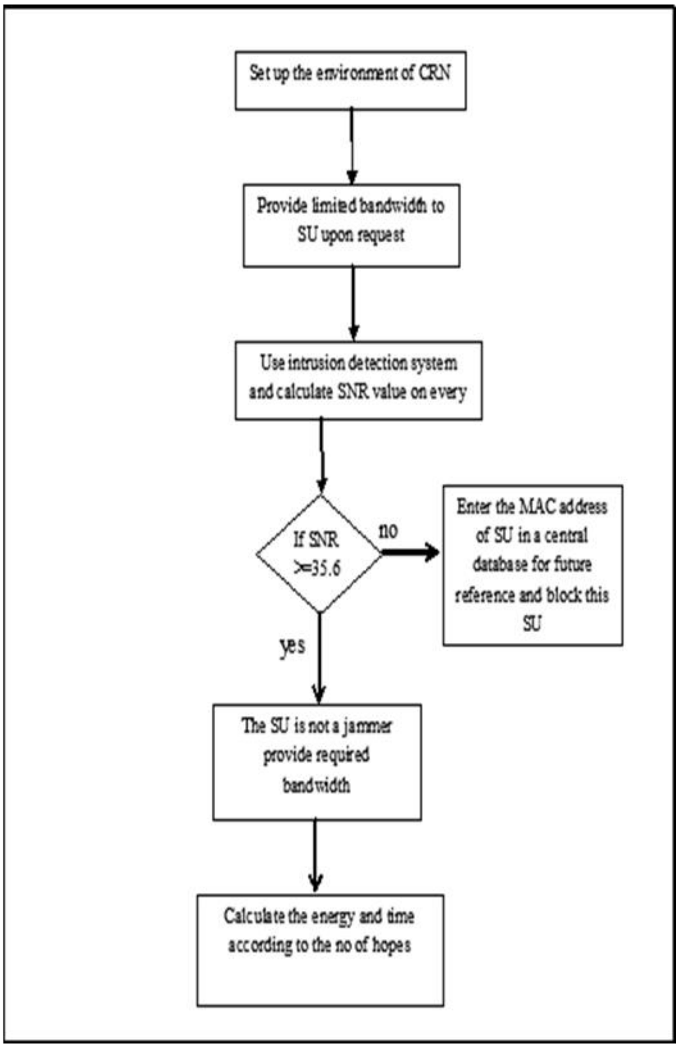

Set up the environment of CRN
Provide limited bandwidth to SU upon request
Use intrusion detection system and calculate SNR value on every
If SNR >=35.6
no
Enter the MAC address of SU in a central database for future reference and block this SU
yes
The SU is not a jammer provide required bandwidth
Calculate the energy and time according to the no of hopes

Figure 3. Flow Chart of the Proposed Method

5. Implementation Results

A simple network terminology is used for simulation. Simulation is conducted with six primary users and 7 secondary users that are located randomly surrounding the primary users. PU's are fixed and SUs are moving with random speeds in random directions. Implementation and simulation of proposed method is done in MATLAB 2013.

Table 2. Comparison Table of Anti-jamming Techniques

Parameter	Parameter value
Total number of nodes, N	13
Number of PU nodes	6
Number of SU nodes	7
Number of channels	1
Maximum velocity with which SU nodes can move	12 kmph
Total area	1000m*1000m

Figure 4 shows the positions of Pus and SUs in the environment at a time before starting the implementation.

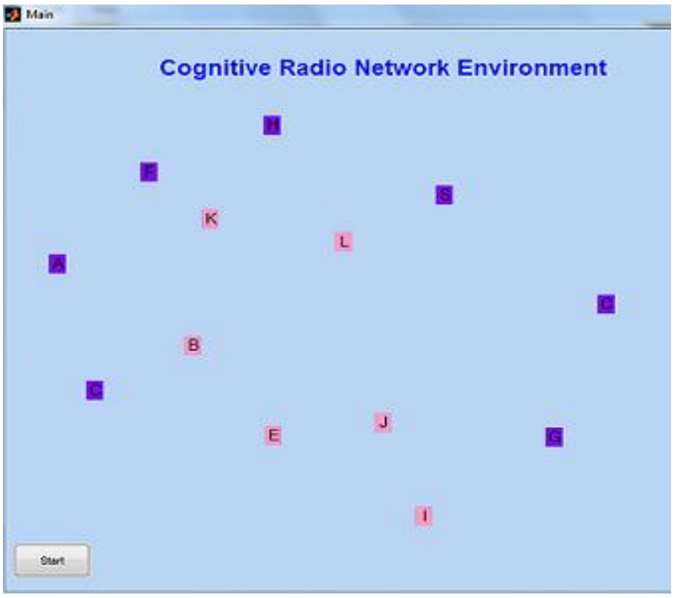


Figure 4. Nodes Positions before Start

Here pink nodes are PU nodes and these nodes are fixed and blue nodes are SU nodes and these nodes are movable. Figure 5 shows the positions of Pus and SUs in the environment after starting the implementation.

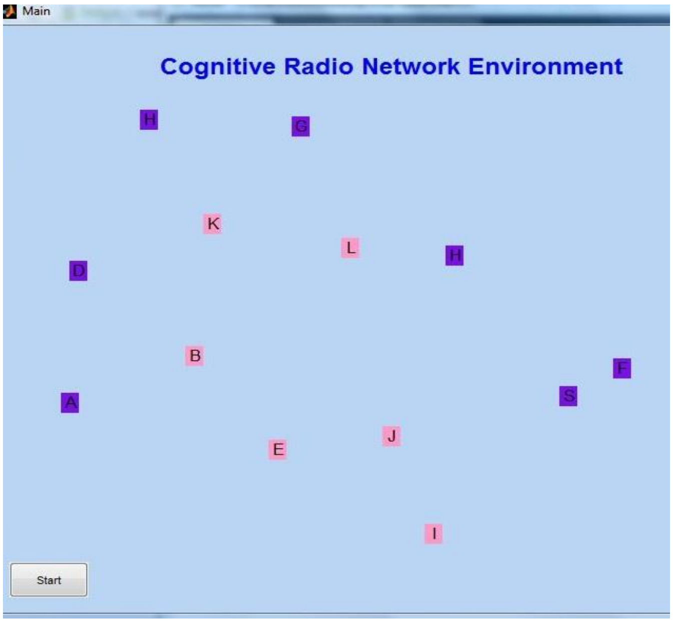
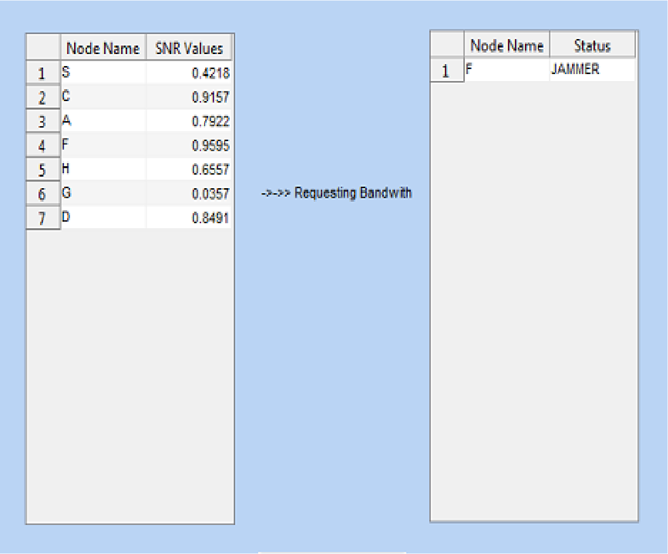


Figure 5. Nodes Positions after Start

Step 1: Give limited bandwidth to every secondary user and calculate the SNR value of SUs on every primary user.

Figure 6 shows corresponding sensing results in sensing table after sensing for 4 seconds. If the SNR value is lesser than 35.6 then the SU is a jammer.



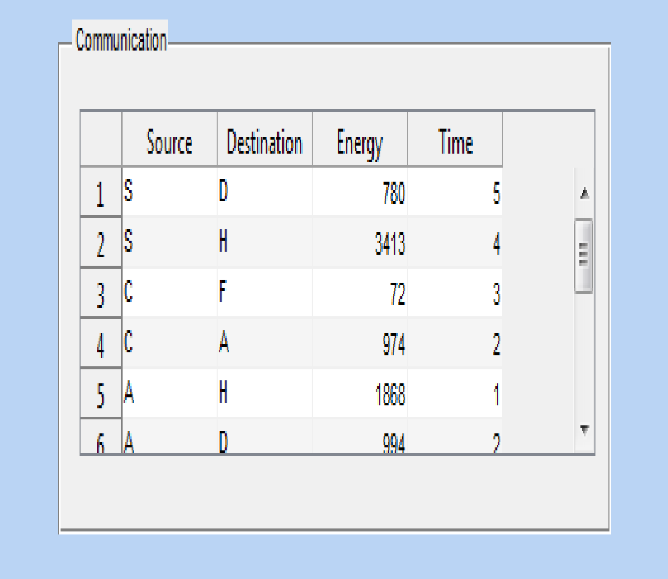
	Node Name	SNR Values
1	S	0.4218
2	C	0.9157
3	A	0.7922
4	F	0.9595
5	H	0.6557
6	G	0.0357
7	D	0.8491

->->> Requesting Bandwith

	Node Name	Status
1	F	JAMMER

Figure 6. Showing SNR of All SU's

Step 2: Figure 7 shows the consumption of energy and time between SU's on the basis of number of hops.



Communication

	Source	Destination	Energy	Time
1	S	D	780	5
2	S	H	3413	4
3	C	F	72	3
4	C	A	974	2
5	A	H	1868	1
6	A	D	994	2

Figure 7. Showing Energy and Time

Step 3: Store the MAC address in the central database for future reference.

Figure 8 and 9 shows the time and energy taken between source and destination with respect to number of hops.

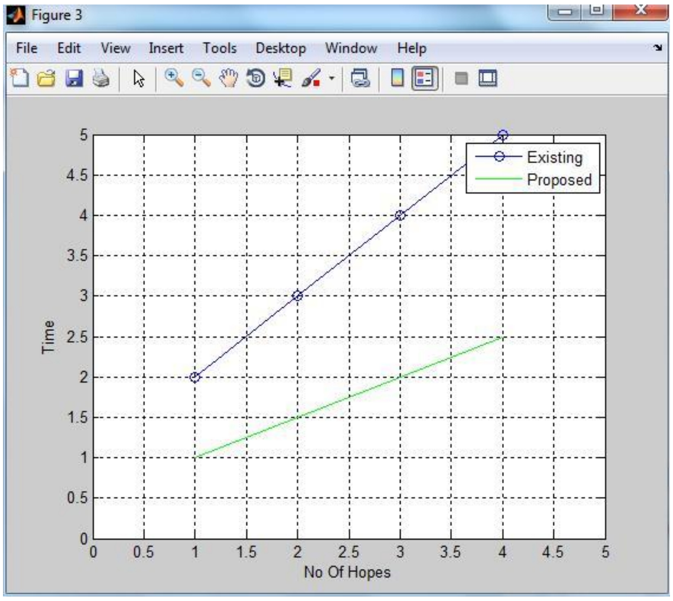


Figure 8. Time Taken from Source to Destination with Respect to Number of Hops

With the increase in number of hops between source and destination, time taken to reach from source to destination is more in existing method in comparison with proposed method. But this increase is gradually more in previous system.

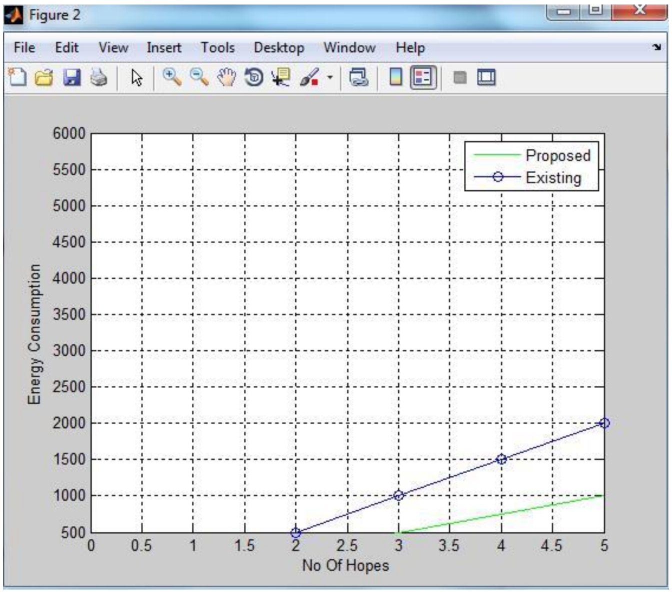


Figure 9. Energy Taken from Source to Destination with Respect to Number of Hops

As the number of hops between source and destination increases, then the energy consumed in sending data packet from source to destination is more in existing method in comparison with proposed method. But this increase is gradually more in previous system.

6. Conclusion and Future Work

Cognitive radio technology helps to efficiently utilize the available spectrum, by providing high bandwidth and best channel for operation. After comparing the results of proposed jamming attack detection and isolation with the existing methods it can be concluded that energy consumption and time taken to send data packet from source to destination increases with the increase of number of hops but it is gradually less in proposed method. Jamming attack is a kind of Denial of Service (DOS) attack, which prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on. Low power jammers are not easy to find while high power jammers are easy to find. Constant jammer consumes all the bandwidth of channels while reactive jammer is active when there is a communication on the channel. After studying all the Anti-jamming techniques it can be concluded that there is at least one technique for every type of jamming attack, it does not matters how much a jammer is intelligent.

In the future work the study may include trust factor of secondary nodes to make the system more robust. Every time a SU connects to the primary user in the network, a table should be maintained according to its behavior and check the impact of this parameter in the proposed work.

References

[1] I.A. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks:A survey,” *Computer Network.*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.

[2] G. Alnifie, S.R MULEPRO: a multi-channel response to jamming attacks in wireless sensor networks. Wireless Communications and Mobile Computing 10(5):704–721, 2010.

[3] J.T. Chiang, Y.C. Hu, Cross-layer jamming detection and mitigation in wireless broadcast networks. IEEE/ACM Transactions on Networking 19(1):286- 298, 2011.

[4] H. Huang, N. Ahmed, S. Pulluru, On limited-range strategic/random jamming attacks in wireless ad hoc networks. In: IEEE 34th Conference on Local Computer Networks, pp 1–8, 2010.

[5] D. Thuente, M. Acharya, Intelligent jamming in wireless networks with applications to 802.11b and other networks. In Proceedings of the IEEE MILCOM, 2006.

[6] M. Li, I. Koutsopoulos, R. Poovendran, Optimal jamming attacks and network defense policies in wireless sensor networks. In: IEEE 26th IEEE International Conference on Computer Communications, pp 1307–1315, 2007.

[7] J. Bellardo, S. Savage, 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: Proceedings of the 12th Conference on USENIX Security Symposium, pp 15–28, 2003.

[8] M. Strasser, B. Danev, S. Capkun, Detection of reactive jamming in sensor networks. ACM Transactions on Sensor Networks 7(2):16:1–16:29, 2010.

[9] R. Rivest, “All- or- nothing encryption and the package transform”, 4th international workshop on fast software encryption, pages 210- 218, 1997.

[10] A. Wood, J. Stankovic, S. Son, JAM: a jammed-area mapping service for sensor networks. In: 24th IEEE Real-Time Systems Symposium, pp 286–297, 2003.

[11] W. Xu, T.Wood, W. Trappe, and Y. Zhang, Channel surfing and spatial retreats: defenses against wireless denial of service. In Proceedings ofthe 3rd ACM workshop on Wireless security, pages 80–89, 2004.

[12] W. Xu, T.Wood, W. Trappe, and Y. Zhang, The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM International Symposium on Mobile Ad HocNetworking and Computing, pp 46–57, 2005.

[13] R. Muraleedharan, rL.A. Osadciw, Jamming attack detection and countermeasures in wireless sensor network using ant system. In: SPIE the International Society for Optical Engineering, vol 6248, p 62480G, 2006.

[14] G. Thamilarasu, R. Sridhar, Game theoretic modeling of jamming attacks in ad hoc networks.

[15] In: Proceedings of 18th Internatonal Conference on Computer Communications and Networks, pp 1–6, 2009.

[16] K. Pelechrinis, C. Koufogiannakis, S.V. Krishnamurthy, Gaming the jammer: is frequency hopping

[17] effective? In: Proceedings of the 7th International Conference on Modeling and Optimization in Mobile,

[18] Ad Hoc, and Wireless Networks, pp 187–196, 2009a.

[19] K. Pelechrinis, C. Koufogiannakis, S.V. Krishnamurthy, Gaming the jammer: is frequency hopping effective? In: Proceedings of the 7th International Conference on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, pp 187–196, 2009a.

[20] I. Shin, Y. Shen, Y. Xuan, M.T. Thai, T. Znati, Reactive jamming attacks in multi-radio wireless sensor networks: an efficient mitigating measure by identifying trigger nodes. In: Proceedings of the 2nd ACM International Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and

[21] Computing, pp 87–96, 2009.

[22] S. Misra, R. Singh, S.V.R. Mohan, Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. Sensors 10:3444–3479, 2010.

[23] L. Zhang, Q. Pei, H. Li, Eighth International Conference on Computational Intelligence and Security, 2012.

[24] H.khosla, R. Kaur, International Research Journal of Engineering and Technology, Volume: 02 Issue: 04, July-2015.

[25] S.K. Jain, K. Garg, A hybrid model of defense techniques against base station jamming attack in wireless sensor networks. In: Proceedings of the 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, pp 102–107, 2009.

[26] S. Gollakota, D. Katabi, iJam: Jamming oneself for secure wireless communication. Tech. rep., Massachusetts Institute of Technology, 2010.

Author

Poonam received her B.Tech. and M.Tech. from YMCA University of Science and Technology, Faridabad, India. She is currently working as an Assistant Professor in Computer Engineering Department in the same university. She is currently pursuing Ph.D. Her interests include networking and algorithm design

Ravi Kumar, pursuing M.Tech. from YMCA University of Science and Technology, Faridabad, India. His area of interest is Security in MANET.

C.K. Nagpal, Professor, head of department and Ph. D. supervisor in Computer Engineering Department in YMCA University of Science and Technology, Faridabad, India. His interests include networking and fuzzy expert system. He has published more than 40 papers in various national and international publications.