



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

Simulation on Routing-Toward-Primary-User (RPU) Attack and Belief Dissemination-Based Defense in Cognitive Radio Networks

Pilaka Anusha and Kaki Leela Prasad*

Vignan's Institute of Information Technology, Visakhapatnam, India

[E-mail: leelaprasad3@gmail.com](mailto:leelaprasad3@gmail.com)

Abstract: Wireless communications have become widely popular in recent years. Wireless Data Communications are an essential component of mobile computing. In wireless networks the frequency band which will be assigned to the particular channel is unable to increase. So cognitive radio networks are used to resolve spectrum scarcity problem. Cognitive radio network is an adaptive and self-organizing network, which is capable of responding to the environmental changes such as interference etc. Any network is prone to various kinds of attacks. In cognitive network various attacks have been discovered. Different layer attacks are discovered like primary user emulation (PUE), Denial of service (DOS) attack. A new and powerful network layer attack, routing-toward-primary user (RPU) attack in CR networks. In this attack, huge numbers of packets are routed intentionally by malignant nodes towards primary users (PUs), targeted to data transmission delay increasing gradually and to cause interference to the (PUs) among the secondary users. To prevent this attack and to develop a defense strategy by the belief propagation. Initially a route is detected from the source node to destination node. Every node preserves a table recording from the other nodes feedbacks on the route and exchanges feedback information among the nodes and computed beliefs. Finally, source node can detect the malignant nodes based on the finalized belief values.

Keywords: Adhoc on demand distance vector routing; Base station; Cognitive radio network; Mobile station; Constant Bit rate; Media access control, Personal digital assistant

I. INTRODUCTION

1.1 Cognitive Radio

Wireless communication systems have been developing and evolving with a furious pace. The number of mobile subscribers has been growing tremendously. From handheld PDAs to the communication radio, from cellular communications to the Television, all make use of the Radio Spectrum which is limited. Spectrum is usually allocated by a government agency in every country. Most of the wireless applications use such licensed bands. But with the ever-increasing demand for wireless communications there are not many bands left to license. Radio Spectrum is a scarce resource and now, with the wide-spread usage of wireless devices, people have become aware of this limitation. However, several studies including that conducted by the FCC have shown most of the spectrum is not used for most of the time. This is confirmed by the presence of "spectrum holes in spectrum analysis done in these studies. Spectrum holes (Figure 1) are frequency bands that have been allocated to a particular user but are not being used at a particular time or place [1]. The presence of such unused frequencies has led to the idea of using spectrum that is temporarily unused for the purpose of the unlicensed users of the radio spectrum. However, this utilization can be of two ways: Regulator Dependent Management: This is the case when there is a central regulator which can allocate the unused spectrum to the users that require access to the spectrum. This can be done in various ways like spectrum pooling, spectrum leasing etc. It is the regulator which decides who can use the available spectrum. Regulator independent Management: This is the case when there is no central regulator. The (secondary) users themselves use the spectrum when there are spectrum holes present. The (secondary) users use the spectrum dynamically and opportunistically. This is the case that Cognitive Radio tries to address. Cognitive Radio is a new field of research that has recently gained much prominence and attention in view of the scarcity of the radio spectrum. The term Cognitive Radio was coined by J Mitola. A Cognitive radio is defined as a radio that can change its transmission parameters depending upon on the

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

environment in order to communicate efficiently. A cognitive radio must be usable along with the legacy devices. The cognitive radio must not cause any kind of interference to the already existing legacy user [2-9].

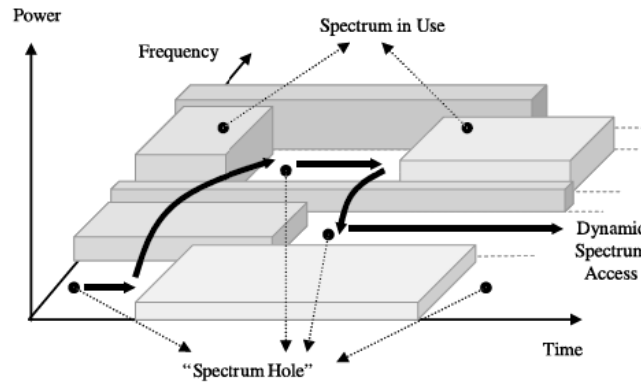


Figure 1: Concept of spectrum holes.

1.2 Cognitive Radio Cycle

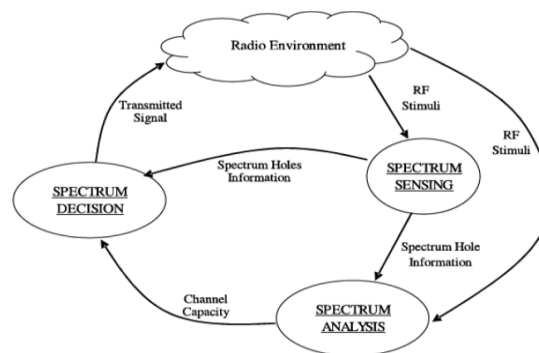


Figure 2: Cognitive cycle.

A basic cognitive cycle comprises of following three basic tasks in Figure 2:

- Spectrum Sensing
- Spectrum Analysis
- Spectrum Decision Making

1.3 Cognitive Radio Architecture

Cognitive Radio networks are deployed in network-centric, AdHoc and distributed and mesh networks serves the needs of both licensed and unlicensed users [7]. It contains three main components:

- Mobile Station (MS)
- Base Station /Access point (BS/AP)
- Back-bone / Core networks

There are three components will combine form 3 kinds of architectures: Infrastructure, adhoc, mesh architectures [6].

1.3.1 Infrastructure architecture:

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

In this architecture, mobile station(MS) and base station(BS) can communicate with each other over the base station(BS) are possible only when the mobile stations are under the same transmission range of base station(BS) and these are routed over the backbone/core networks (Figure 3).

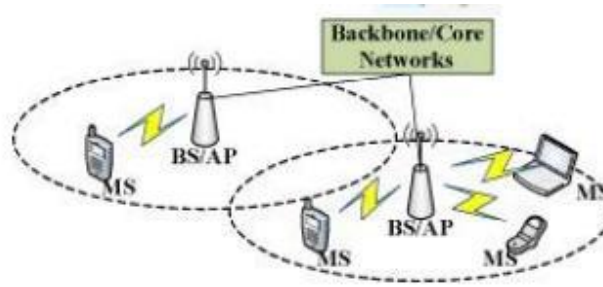


Figure 3: Infrastructure Architecture

1.3.2 Ad hoc architecture:

There is no infrastructure support (or defined) in ad-hoc architecture. (e.g. Wi-Fi, Bluetooth) are discussed in Figure 4.

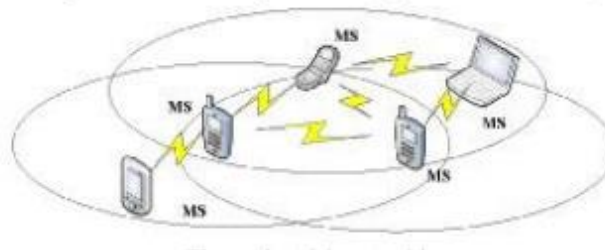


Figure 4: Ad hoc architecture.

1.4 Cognitive Radio's Key Benefits

Cognitive Radio offers optimal diversity (in frequency, power, modulation, coding, space, time, polarization and so on) which leads to:

- **Spectrum Efficiency**

This will allow future demand for spectrum to be met and is the basic purpose of implementing CR.

- **Improved Quality of Service (QoS)**

Suitability, availability and reliability of wireless services will improve from the user's perspective.

- **Benefits to the Service Provider**

More customers in the market and/or increased information transfer rates to existing customers. More players can come in the market [9].

- **Future-proofed product**

A CR is able to change to services, protocols, modulation, spectrum etc. without the need for a user and/or manufacturer to upgrade to a new device.

II. LITERATURE SURVEY

Cognitive Radio (CR) is an adaptive, intelligent radio and network technology that can automatically detect available channels in a wireless spectrum and change transmission parameters based on interaction between the environments where it operates. Cognitive Radio Networks have been emerged as a promising solution for solving the problem of spectrum scarcity and improving spectrum utilization by opportunistic use of spectrum [3]. It can perceive current networking conditions and then plan, decide, acts on those conditions [4,5]. Cognitive Radio (CR) is a revolutionary technique that allows secondary user (SU) wireless devices to use 'spectrum holes' left by idle 'primary users (PU's)'. Many attacks have been discovered for Cognitive Radio networks in various layers [8].



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

- Physical layer →PUE (Primary User Emulation)) attack
- MAC layer →DOS (Denial of Service) attack
- Network layer →RPU (Routing-Toward-Primary-User) attack

2.1 A New Method to Detect Primary User Emulation Attacks in Cognitive Radio Networks

It proposes a new method to detect the PUE attacks in CRNs which not only classified discussion of these two kinds of situations which the primary user is stationary or mobile, but also use the Kalman filter algorithm to process the received mobile source's signal strength (RSS) value. Finally, we use the BP neural network training to complete the detection of PUE attacks [10-13].

Depending on the position of the primary user PUE attack detection methods can be classified into 2 types:

1. PUE attack detection method when primary user is stationary.
2. PUE attack detection method when primary user is mobile.

2.2 Routing-Toward-Primary-User-Attack and Belief Propagation Based Defense in CRN's

It proposes a new and powerful network layer attack, routing-toward-primary user (RPU) attack in CR networks. In this attack, malicious nodes intentionally route a large amount of packets toward the primary users (PUs), aiming to cause interference to the PUs and to increase delay in the data transmission among the secondary users. To defend against this attack without introducing high complexity, aiming to develop a defense strategy using belief propagation [14]. First, an initial route is found from the source to the destination. Each node keeps a table recording the feedbacks from the other nodes on the route, exchanges feedback information and computes beliefs. Finally, the source node can detect the malicious nodes based on the final belief values [15].

2.3 Anonymous Communications in Mobile Ad Hoc Networks

It proposes a novel anonymous on-demand routing protocol, termed MASK, to enable anonymous communications thereby thwarting possible traffic analysis attacks. Based on a new cryptographic concept called pairing, first proposed an anonymous neighbourhood authentication protocol which allows neighbouring nodes to authenticate each other without revealing their identities [16]. A pairing-based anonymous on-demand routing protocol MASK is which provides strong sender and receiver anonymity, the relationship anonymity between senders and receivers, the unlocatability of mobile nodes, and the untraceability of packet flows under a rather strong adversarial model but the routing information is not authenticated in the current design of MASK.

2.4 Anonymous Routing Protocol for Mobile Ad Hoc Networks

In this papers, author present a novel anonymous on demand routing scheme for MANETs and identify a number of problems of previously proposed works and propose an efficient solution that provides anonymity in a stronger adversary model. ARM is an anonymous on demand routing scheme for MANETs. In this author first identified a number of problems and strengths in previously proposed solutions and proposed a solution that provides stronger anonymity properties while also solving some of the efficiency problems but the computations are more in this protocol [17,18].

III. PROPOSED SYSTEM

This project proposes a new and powerful network layer attack, routing-toward-primary user (RPU) attack in CR networks. In this attack, malicious nodes intentionally route a large amount of packets toward the primary users (PUs), aiming to cause interference to the PUs and to increase delay in the data transmission among the secondary users. To defend against this attack without introducing high complexity, aiming to develop a defense strategy using belief propagation [19]. First, an initial route is found from the source to the destination. Each node keeps a table recording the feedbacks from the other nodes on the route, exchanges feedback information and computes beliefs. Finally, the source node can detect the malicious nodes based on the final belief values.

In Cognitive Radio networks several types of attacks have been discovered i.e., Physical layer, MAC layer, Network layer attacks. In network layer RPU attack has been discovered. In this attack, malicious nodes send fake routing information, claiming that they have optimum route with low costs, which will cause other honest nodes to route data



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

packets through those malicious nodes [20,21]. Shortest path routing algorithm can be used for routing among secondary users in CR wireless networks.

- The shortest path algorithm will be used to find the initial route from the source to the destination, without considering whether there are malicious nodes on the route or not.
- Each node on the initial route keeps a table used for recording feedbacks from other nodes on the route.
- Each node on the route will carry out the measurements and calculates the local Functions.
- Each node will then send some packets to the nodes “after” it, and collect the feedback information from all those nodes.
- The source node will detect the malicious nodes according to final beliefs. If the final belief values of some nodes are below a threshold, those nodes will be seen as malicious nodes.
- The shortest path algorithm will be used to find a new route from the source to the destination, avoiding those malicious nodes.

3.1 Modifications In NS2 To Perform Attacker Model

Numbers of changes were carried out in NS2 to perform attacker model. In a network contains only one primary user and remaining all users act as secondary users. Malicious node is anywhere in the network, it was done in TCL simulation file.

```
[$node_ (3) set ragent_ ] Attack  
[$node_ (7) set ragent_ ] PU  
$node_(0) set X_ 37.608377307314  
$node_(0) set Y_ 195.446991827566
```

In the above example, node 3 acts as an attacker and node 7 act as primary user and remaining all nodes act as secondary users. The X, Y Values for all nodes are declared as some value. The values coming from TCL file were binded in AODV.cc which was declared in constructor function.

```
PrUs =false;  
Node_ =0;  
Attacker = false;  
Dist =1000;
```

To check whether the node is primary user or an attacker, string comparison functions were developed in AODV.cc

```
if(strcmp(argv[1], "PU") == 0) {  
PrUs =true;  
return TCL_OK;  
}  
if(strcmp(argv[1], "Attack") == 0) {  
Attacker =true;  
return TCL_OK;  
}
```

First function will compare the node is primary user or not, if it is primary user set the node as PrUS is true and second will also compare the node status if it is an attacker set status as Attacker is true [22]. To identify the changes in a neighbouring nodes and placed the values in routing table.

```
if (Node_) {  
rh->PrUs = PrUs;  
Node_->update_position();  
rh->X_ =Node_->X();  
rh->Y_ =Node_->Y();
```



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

```
}
```

To identify the neighboring node is a primary user it first update its positions in a routing table. These values are stored temporarily in a routing table once the operation completes these values are changed according to the neighboring node changes.

Route discovery process begins with the creation of route request packet.

```
rt->rt_req_timeout = 2.0 * (double) ih->ttl_ * PerHopTime(rt);  
if (rt->rt_req_cnt > 0)  
rt->rt_req_timeout *= rt->rt_req_cnt;  
rt->rt_req_timeout += CURRENT_TIME;
```

3.2 AODV Modification

Flow of our AODV protocol. In order to implement this, we had chosen the Simple AODV protocol for wireless networks, already available in NS2, to be modified. This is a reactive protocol used to determine multiple routes between a source and destination. As all the working depends upon the detection of primary user and find out the shortest route between source and destination.

```
structhdr_aodv_reply*rp=HDR_AODV_REPLY(p);  
AODV_Neighbor *nb;  
nb = nb_lookup(rp->rp_dst);  
if(nb == 0)  
{  
nb_insert(rp->rp_dst);  
}  
Else  
{  
nb->nb_expire = CURRENT_TIME +  
(1.5 * ALLOWED_HELLO_LOSS * HELLO_INTERVAL);  
}  
ch->fromprimaryuser= ch->channelindex_;  
}  
nb = nb_lookup(rp->rp_dst);  
nb->Pu = rp->PrUs;  
nb->x = rp->X_;  
nb->y = rp->Y_;  
Packet::free(p);  
}
```

The class information added from mobilenode.cc file to aodv.h file. The neighboring nodes information is stored in lookup table. Once find out the primary user position X, Y axis positions are stored. If the route is not used within the life time it expires. Malicious node collects all the information from the nodes in the network and send fake information to the source.

```
if (Node_) {  
Node_->update_position();  
rq->pcount =0;  
rq->Path[rq->pcount] = index ;  
rq->Px_[rq->pcount] =Node_->X();  
rq->Py_[rq->pcount] = Node_->Y();
```



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

```
rq->pcount++;  
}
```

In the above example, nodes updating their positions and initially count are initialized to 0, path of the selected route is saved and index is displayed i.e., through which node the packets are transferred. The positions of nodes X, Y positions are stored and finally count will be incremented.

```
for(; nb; nb = nb->nb_link.le_next) {  
if(nb->Pu== true)  
{  
for (inti= 0;i<rp->pcount ;i++)  
{  
double ds = sqrt(pow(nb->x-rp->Px_[i],2)+pow(nb->y-rp->Py_[i],2));  
if (dist> ds)  
{  
dist =ds;  
return true;  
}  
}  
}  
}
```

In this case all the nodes in the network are calculated the distance from primary user (PU) to all the nodes by using basic cognitive theory. If the distance is greater than the distance from the selected route the route will be chosen as the preferred route. Malicious node collects the information from all the nodes and sends fake information to the source [23]. Source assumes that the informed route is correct and chooses the route and sends information through that selected route.

IV. PROPOSED SYSTEM DESIGN AND METHODOLOGY

4.1 Algorithm To Implement

The CRN's can be deployed in network-centric, distributed, adhoc and mesh architectures and serve the needs of both licensed and unlicensed applications. There are '2' kinds of wireless communication systems in CRN's.

- Primary System/ Primary user (PU)
- Cognitive Radio System/ Secondary user (SU) [24]

A Primary System operated in the licensed band has the highest priority to use that frequency band (E.g.: 2G/3G cellular, Digital TV broadcast). It can also be operated in the unlicensed band (ISM band) called unlicensed band primary system.

A Cognitive Radio System neither has a fixed operating frequency nor has privilege to access that band [25]. There are '2' components in CR systems. There are Cognitive Radio Base Station (CR-BS) and Cognitive Radio Mobile Station (CR-MS).

Let assume, each node has GPS and node/attacker can know neighbour PU availability. And position is Pos. And we are denoting Route from source to destination as **Ri**,

1) Get_pos(Px,Py) //update own position

2) If *Data ready* in node "S"

- a. If $\exists RS$, //Route already exist
 - i. Send *Data*
 - b. Else



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

- i. Send *Req*
- 3) If *Pktrecv* in node "*n*" //pkt received in some node named as *n*
 - a. *Pkt.type=Req*
 - i. *Upd(Rn,S)* //update route of source to current node *n*
 - ii. If *Pkt.dst=n* //current node is destination
 1. If *Pkt.hop<Old.hop* //new path is shorter route than old
 - a. Send *Rep*
 - b. Set *Old.hop=Pkt.hop* // set current path as short path
 - iii. Else //current node is intermediate node
 1. *Updateinfo→Req*
 2. Rebroadcast *Pkt*
 - b. *Pkt.type=Rep*
//attacker will forward reply packer if one of route member is near to PU
 - i. If node is *Attacker*
 1. For each $m \in Pkt.route.mem$
 - a. If *m.Pos* near *PU.Pos*
 - i. Forward *Rep* to *Src*
 - b. Else
 - i. Ignore *Rep*
 - ii. else *Pkt.hop<Old.hop*
 1. *Upd(Rn,S)* //update route
 2. If $n=Pkt.dst$ //m destination of reply
 - a. Send *Data*
 - b. If $(n,t)not\varified$ //route not verified then has to verify
 - i. Send $FReq \leftarrow Freq.Ttl=Rthop$ // Feedback has to reach till destination (it can be desired by hop count)
 3. Else
 - a. Forward *Rep* //intermediate node has to forward
 - iii. If same *Pkt* not recv already & $Freq.Ttl>0$ //feedback info update process
 1. *Upd(Rs,n)*
 2. Forward $(Freq \leftarrow Freq.Ttl--)$ // forward feedback info to next
 - iv. Elseif not same pkt & $Freq.Ttl=0$
 1. *Updatedinfo→Frep*
 2. Send *Frep*
 - c. *Pkt.type=FReq*
 - iii. If same *Pkt* not recv already & $Freq.Ttl>0$ //feedback info update process
 1. *Upd(Rs,n)*
 2. Forward $(Freq \leftarrow Freq.Ttl--)$ // forward feedback info to next
 - iv. Elseif not same pkt & $Freq.Ttl=0$
 1. *Updatedinfo→Frep*
 2. Send *Frep*
 - c. *Pkt.type=Frep*
 - i. If *Frep.dst=n*
 1. Foreach $m \in Pkt.Nlist$
 2. *UpdateVlist←minfo*
 3. *ConstructVpath(Rn,dst)* // creating the approximate possible path based on location information of nodes
 4. If $Vpath \approx Rs$, // if current route matching with approximate route
 - a. $Rs, \leftarrow \varified$
 5. Else

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

a. $Rtlist \leftarrow Rtlist \setminus R_s$, //if route not match then remove from routing table and mark as malicious route

4.2 Attacker Model

In this attack, huge numbers of packets are routed intentionally by malignant nodes towards primary users (PUs), targeted to data transmission delay increasing gradually and to cause interference to the (PUs) among the secondary users. To prevent this attack and to develop a defense strategy by the belief propagation [26]. Initially a route is detected from the source node to destination node. Every node preserves a table recording from the other nodes feedbacks on the route and exchanges feedback information among the nodes and computed beliefs. Finally, source node can detect the malignant nodes based on the finalized belief values shown in Figures 5 and 6.

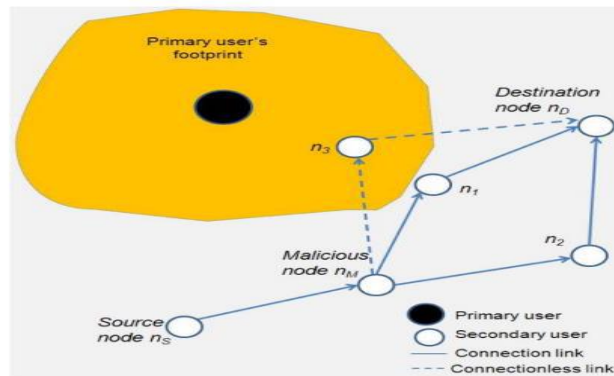


Figure 5: Illustration of routing-toward-primary-user (RPU) attack [14].

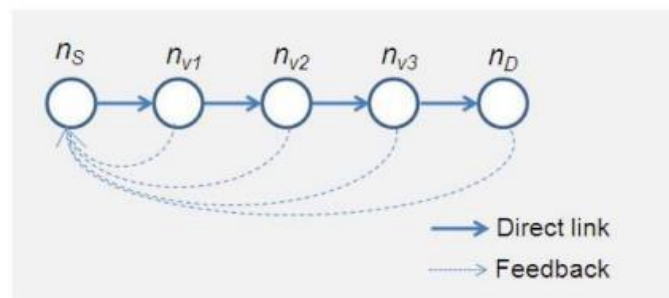


Figure 6: Illustration of defense strategy against RPU attack [14].

4.3 Pseudo Code

```

If(NetworkCreated)
{ N= PU area Node;
Calculate range R = 100;
If(S= Source Node and D= Destination Node)
{ CalculateAllpath(S,D);
ShortestPath = DijkstraShortestPath(Based on min hope count);
While(shortestPath != null)
{ Calculate position of node in path = pos;
If(pos Present in R)
{ Node is sleepMode;
}Else

```



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

```
{ Active Mode;
}
If(all active){
Preferred Path;
}
Else{
Malicious Path
}
}
}
If( R is Varies R= 100+random(100)
{
Calculate position of node in path = pos;
If(pos Present in R) {
Node is sleepMode;
}
}
```

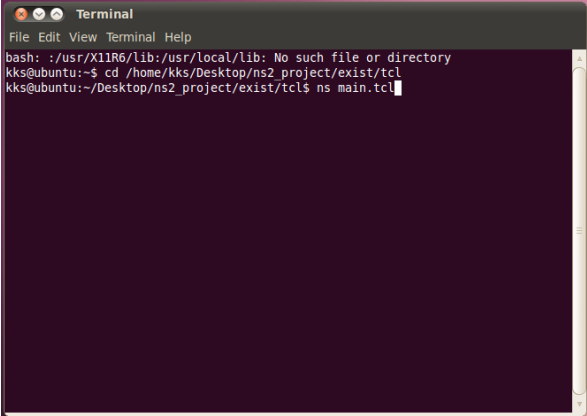
V. RESULTS AND DISCUSSION

Generally CRN is used to search a method where secondary users are allowed for the opportunity to utilize the unused primary bands commonly known as white spaces. It also helps primary users to allow secondary users to access the licensed spectrum opportunistically when PU's are not utilizing [27].

In this project uses Network Simulator for plotting efficient throughput by implementing Routing toward primary user attack in cognitive radio networks in Linux (Ubuntu) by identifying the malicious node in a network by implementing with the help of Tool command language(TCL) and c++ code as front and back end.

5.1 Simulation Starts

Execution of the attacker model output screen shot in Figure 7.



```
Terminal
File Edit View Terminal Help
bash: ./usr/X11R6/lib:/usr/local/lib: No such file or directory
kks@ubuntu:~$ cd /home/kks/Desktop/ns2_project/exist/tcl
kks@ubuntu:~/Desktop/ns2_project/exist/tcl$ ns main.tcl
```

Figure 7: Output files execution of main.tcl

Displaying Broadcasting information in a network Output Screenshot in Figure 8.

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

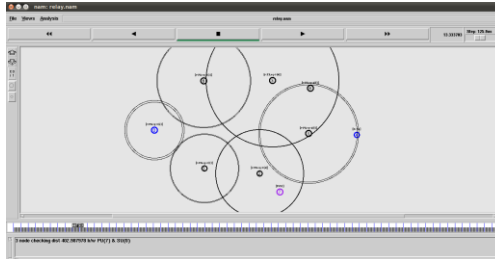


Figure 8: Nodes communicating with each other in order to broadcast packets.

Displaying attacker model output in Figure 9.

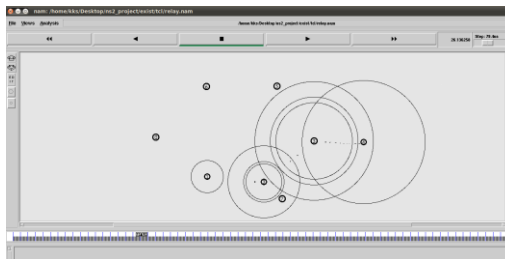


Figure 9: Simulation shows that the packets transferred towards the PU.

Displaying the noise occurrence in all the nodes (attacker model) output in Figure 10.

```
Terminal
File Edit View Terminal Help
5 dist count 2142
7 dist count 4285
3 dist count 2142
7 dist count 4286
2 dist count 2143
4 dist count 2142
5 dist count 2143
7 dist count 4287
3 dist count 2143
7 dist count 4288
2 dist count 2144
4 dist count 2143
5 dist count 2144
7 dist count 4289
3 dist count 2144
7 dist count 4290
2 dist count 2145
4 dist count 2144
5 dist count 2145
7 dist count 4291
3 dist count 2145
7 dist count 4292
2 dist count 2146
ks@ubuntu:~/Desktop/ns2_project/exist/tcl5
```

Figure 10: Number of RTS packets interfered in 7th node is 4292.

Displaying feedback information transferred output screen shot in Figure 11.

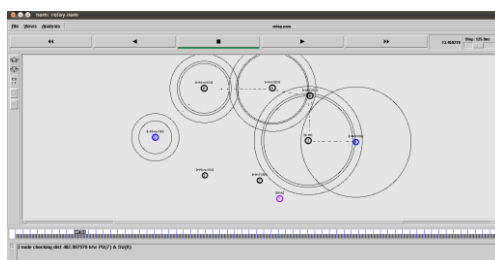


Figure 11: main.tcl nam output simulation.

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

Displaying the noise occurrence in all the nodes output in Figure 12.

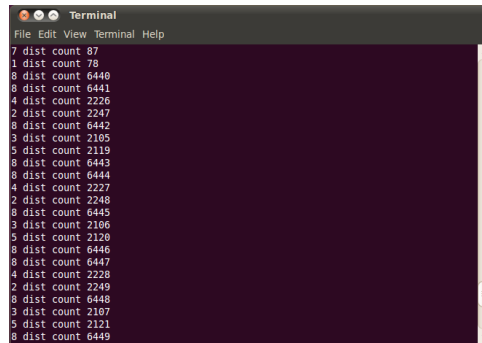


Figure 12: Number of RTS packets interfered in 7th node is reduced to 87.

The simulation results of an attacker model showing that the packets transferred through the primary user (PU) and it will cause disturbance to the PU. The number of request to send (RTS) packets arrived to the primary user will be calculated. The noise occurrence of 7th node i.e., Primary user is 4292. In feedback mechanism initially source will broadcast packets to all the neighbouring nodes, if any node find out as a PU, it will send packets to the other nearest nodes [14]. If any node acts as a malicious node send hello message to the nearest node and it will again send it to their nearest node. By using basic cognitive theory all nodes in the network calculated the distance from PU. Shortest path routing algorithm is used to calculate the distance. This information is collected to the malicious node and it will send fake data to the source. Source claim that the information is correct and transfer the data through the malicious path. So that the data will transfer to the incorrect path. The simulation results shows that in attacker model the noise occurred in PU is 4292 and after using feedback mechanism it will be reduced to 87 in Figure 13.

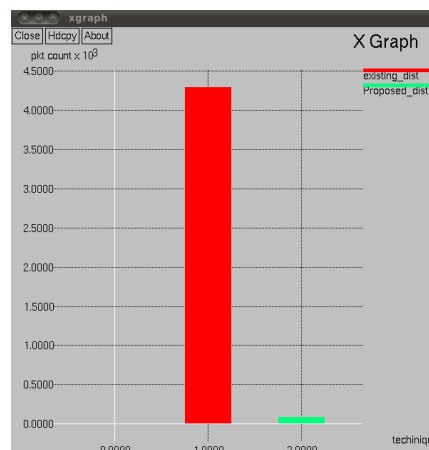


Figure 13: Noise occurrence at primary user reduces from 4.2db to 0.8db.

VI. CONCLUSION

Cognitive Radio networks recently have become an active topic among wireless network researches as it promises to solve the issue of spectrum scarcity. By sharing the unused portion of the licensed band with the unlicensed users, the entire spectrum can be fully utilized. In a network various kinds of attacks have been encountered during spectrum utilization. Finding attacks occurred in various layers so that the spectrum utilized efficiently. Network layer attack i.e. Routing-toward-primary-user (RPU) attacks has been identified and also provided the feedback mechanism to avoid the path which contains malicious users.



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

VII. FUTURE WORK

In Cognitive radios attacks can be occurred because of malicious nodes, detecting the malicious nodes in a network and provided the defense strategy for this attack. In future malicious user detection from this attack can be use detection technique by considering size of network and also consider secondary user channel allocation by considering the Quality of service (QOS).

VIII. REFERENCES

1. R Maheshwari, J Gao, et al. Detecting Wormhole Attacks in Wireless Networks using Connectivity Information. IEEE International Conference on Computer Communications 2007; 2: 1231-1234.
2. Lutfu A, N Balasubramaniam, A Two-Stage Power and Rate Allocation Strategy for Secondary Users in Cognitive Radio Networks. Journal of communications 2009; 4: 781-789.
3. L Joseph Mitola, An Integrated Agent Architecture For Software Defined Radio. IEEE 2000.
4. H Ekram, N Dusit, et al. Dynamic Spectrum Access in Cognitive Radio Networks. Journal of communications 2009; 60: 1526-1538.
5. Z Jin, S Anand, et al. Detecting Primary user emulation attacks in dynamic spectrum access networks. IEEE International Conference on Communication 2009; 9: 1772-1791.
6. Y Yuan, B Paramvir, et al. Allocating dynamic time-spectrum blocks in cognitive radio networks. IEEE Mobile ad hoc networking and computing 2007: 130-139.
7. PC Ricardo, SD Richard, et al. Using Cognitive radio for improving the capacity of wireless mesh networks. IEEE Vehicular Technology Conference 2008; 4: 467-471.
8. L Akter, Chandra Interference Minimization Routing and Scheduling in Cognitive Radio Wireless Mesh Networks. IEEE 2010: 139-143.
9. CR Kaushik, AF Ian, Cognitive wireless mesh networks with dynamic spectrum access. IEEE 2008; 26: 168-181.
10. T Roshan Singh, T Bhupendra Singh, Increases Security in Cognitive Radio Networks. National Conference on Recent Advances in Technology and Management for Integrated Growth 2013: 2131-2139.
11. A Manisha, S Vishnavi, A Secure AODV Protocol to Detect Black Hole and Warm hole Attacks in MANET. International Journal of Computer Science and Mobile Computing 2014; 3: 157-167.
12. K Peng, F Zeng, et al. A new method to detect primary user emulation attacks in cognitive radio networks. International Conference on Computer Science and Service System 2014: 674-677.
13. Y Zhou, H Zhu, et al. Routing-toward-primary-user-attack and belief propagation based defense in Cognitive Radio Networks. IEEE 2013; 12: 1750-1762.
14. Z Yanchao, L Wei, et al. Anonymous Communications in Mobile Ad Hoc Networks. IEEE 2013; 22: 1298-1304.
15. SH Chowdhury, G Brendan, et al. Adaptive Reputation based clustering against spectrum sensing data falsification attacks. Transactions on Mobile Computing IEEE 2014; 13: 1707-1782.
16. S Stefaan, P Bart, Anonymous Routing Protocol for Mobile Ad Hoc Networks. IEEE 2013; 13: 1234-1238.
17. SY Jonathan, FT William, et al. Understanding Belief Propagation and Its Generalizations. Mitsubishi Electric Research Laboratories 2003; 13: 2282-2293.
18. Z Sheng, Y Haifan, Towards cheat-proof cooperative relay for cognitive radio networks. IEEE 2014; 25: 2441-2450.
19. AT Ihler, JW Fisher, et al. Non-Parametric Belief Propagation for Self Localization of Sensor Networks. IEEE 2005; 23: 809-819.
20. S Kurosawal, H Nakayamal, et al., Detecting Black Hole Attack On AODV-Based Mobile Adhoc Networks by Dynamic Learning Method," IEEE. 2007; 5: 338-346.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 2, February 2018

21. E Raul, P Abhay, et al. Spectrum Sharing for Unlicensed bands. IEEE Journal on Selected Areas in Communications 2005; 25: 251-258.
22. X Xiongwei, W Weichao, Detecting primary-user-emulation attacks in cognitive radio networks via physical layer networking coding. Computer Science 2013; 21: 430-435.
23. T Di Rocco, Y Hiroyuki, et al. Cognitive Mesh Network under Interference from Primary User. IEEE Wireless Personal Communications 2008; 45: 385-401.
24. R Alberto, QSQ Tony, et al. Cognitive Network Interference. IEEE Journal on Selected Areas in Communications 2011; 29: 480-499.
25. G Jakimoski, KP SubbaLakshmi, Denial-Of-Service Attacks on Dynamic Spectrum Access. IEEE Communication workshops 2008.
26. W Wenkai, L Hushengi, et al. Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Systems. IEEE Information Sciences and Systems 2009.
27. L Sisi, L Loukas, et al. Thwarting control-channel jamming attacks from inside jammers. IEEE Transactions on Mobile Computing 2012; 11: 1545-1567.