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)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

Defense against Selfish PUEA in CRN based on Modified HMAC

Pranay Prajapati, T.S.Londhe,

Department of Electronics and Telecommunication Engineering, Sinhgad Academy of Engineering, Pune, India

Professor, Department of Electronics and Telecommunication Engineering, Sinhgad Academy of Engineering, Pune, India

ABSTRACT: Cognitive Radio (CR) technology is developed to overcome the spectrum scarcity due to rapid development in wireless networks. Both licensed and unlicensed users can utilize the spectrum using this technology. Cognitive Radio Networks (CRNs) have been projected as a promising technology to alleviate the spectrum shortage and under-utilization drawback., an outsized quantity of attempt has been placed on CRNs. However, very little attention has been paid to knowledge aggregation drawback, one in all the foremost necessary communication protocols in wireless networks thanks to its potency in each energy conservation and latency reduction. In this paper, we investigate the minimum latency data aggregation scheduling problem in CRNs.The system also carried out the three different algorithms to provide the highest security during the data communication. HMAC protocol has been used to authenticate the secondary user and Genetic algorithm based technique has been used to select the best node as head (RN). The Broadcast Tree Construction (BTC) has used to select the best node to forward data to Primary User (PU station) as request. The experimental analysis shows the how proposed system better than classical defense mechanisms in CRN.

KEYWORDS: Cognitive Radio Network(CRN), Data aggregation, Security, Primary User Emulation Attack(PUEA),Hash Message Authentication Code(HMAC).

I. INTRODUCTION

The entire communication process completely depends on the wireless medium. Due to increase in number of devices and wireless technologies, bandwidth and spectrum shortage problem arises. Cognitive radio network(CRN) is a technology which is developed to solve spectrum shortage problem in wireless networks. CRNs consist of two types of users: primary users, also known as licensed users, and secondary users or cognitive radio (CR) devices, also known as unlicensed users.

Primary Users(PUs) are assigned a fixed spectrum band which they can operate during their licensed period. Secondary Users(SUs) can only operate an unlicensed band or the licensed band of PU when the PU is not utilizing it. If a Primary User(PU) arrives when a SU is using its assigned spectrum band then SU has to leave that spectrum band and switch to another available free spectrum band or wait for PU's activity to finish [1].

The security of cognitive radio network has been attracting growing attentions. Because various unknown wireless devices are allowed to opportunistically access the licensed spectrum in the architecture of cognitive radio, cognitive radio systems are vulnerable to malicious attacks. Besides, CRNs not only face all the security threats in traditional wireless networks, such as eavesdropping, tampering, imitation, forgery, and noncooperation etc., but also new security threats related to unique cognitive characteristics, such as primary user emulation attack, falsifying data, denial of service attack etc [2].

Security is a major concern for every network. For CRNs, security implementation is difficult to achieve due to the dynamic behavior of the network. NC is applied in CRNs to achieve security by detecting multiple types of attacks.

DOI: 10.15680/IJIRCCE.2019. 0706006

One of the common attacks in CRN is PUE attack. In a PUE attack, an attacker tries to mimic the signal characteristics of a PU to achieve the highest priority and to access the available spectrum band.

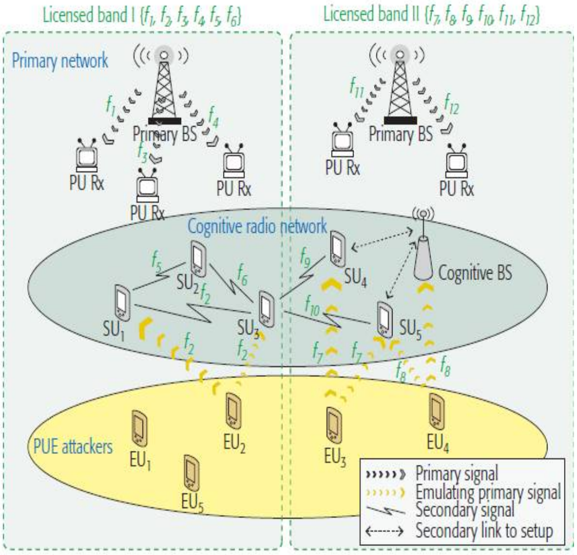


Figure 1: Illustration of PUE attacks in the CR network

The impact of PUE attacks in Cognitive Radio Networks results in Bandwidth waste, QoS degradation, Connection Unreliability and Denial of Service(DoS).

In this paper, we provide a Hash Message Authentication Code to defense PUE attack in Cognitive Radio Network. HMAC is a symmetric key generator for the message authentication. The remaining of the paper,we will explain proposed system and its performance evaluation scheme.

II. RELATED WORK

The CR system is vulnerable to malicious attacks that could disrupt its operation. In PUEA, malicious users mimic the primary signal over the idle frequency band such that the authorized secondary users cannot use the corresponding white space(s). This leads to low spectrum utilization and inefficient cognitive network operation.A well-known malicious attack is the primary user emulation attack [3].According to [4], this system proposed is based on clustering the cooperative sensors which detects a cluster with no malicious sensors and uses sensing result of this cluster. In [5],by considering the cognitive radio sensors in sleeping and censoring modes, the average energy consumed in spectrum sensing process is minimized. In [6], an analytical model for the probability of successful PUEA based on the energy detection was proposed,where the received signal power is modeled as a log-normally distributed random variable. In [7], a transmitter verification scheme (localization-based defense) was proposed to detect PUEA.

It has been shown that using traditional routing protocols based on network topology is not efficient for dynamic ad hoc networks [8]. Therefore, position-based routing protocols have emerged. However, there are many concerns about these methods. Firstly, employing positioning information only does not increase network reliability. For this, enhancements have been proposed, which keep in mind cross-layer information as well as the dynamics of the nodes to increase network performance and quality of service (QOS). However, face-to-face routing is known as the local-maximum problem, especially in low-density networks. Therefore, the design should employ some policy to solve such cases. In addition, in position-based routing, maintaining and distributing position information is a nontrivial and important function. One possible answer to this challenge could be the use of location services aiming at providing solutions to such issues.

The proposed system in [9] is based on probabilities of false alarm and miss detection. With increase in number of malicious users,false alarm probability also increases.

In [10],a proposed model based on Hash Message Authentication Code(HMAC) is used to detect the PUEA in CRN.The HMAC is used to generate a tag at the transmitter, this tag is appended to the message and sent over the channel.At the receiver the secondary user separates the message and tag and regenerates a new tag from the shared key and the received message.By comparing two tags,SU determines if the signal comes from PU or from the attacker.
C. Chen et al made a joint position verification method to enhance the positioning accuracy in [14] . Z. Chen showed how the attacker can emulate the PU signal to confuse the SU and used an advanced strategy called variance detection to mitigate the effect of an attacker using the difference between the communication channel of PUEA and PU in [12].Authentication and encryption will be found in [13]. Proposed model in [14] doesn't need the certificates and the sender can directly encrypt message via using the identity without the progress of public key authentication. Cryptography method and various Network security protocols are described in [15].

III. PROPOSED SYSTEM

We have proposed a Genetically Derived Secure Data Aggregation in CRN as shown in figure 2.In our proposed system,a clustering network is created which will work on dynamic basis. Initially, the CHs are chosen based on the node connectivity, and maximum energy which acts as a data aggregator (DAG).Then, the clustering process is executed using the genetic algorithm. This technique and thereby enhancing the network lifetime and reduces network overhead.After that selection of best nodes takes place using genetic algorithm,Data aggregation algorithm is implemented which will aggregate the data coming from SU.The Hash Message Authentication Code(HMAC) is applied for the authentication.This will verify both the tags from CH and SU to check whether the Sensor node is SU or attacker.If the Sensor node is attacker,then HMAC will take strict action against him and throws it out from the clustering network.Thus ensuring the authenticity and integrity of the sensed data.

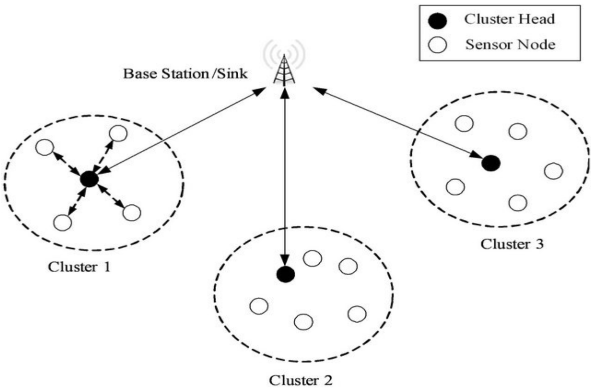


Figure 2: Illustration of our scenario

Modules

a) Cluster Formation :

Fig. shows the cluster creation process and transmission between source and destination node. At the end of each TS network nodes verifies sensed data and broadcast messages to nodes within given Cluster Distance (CD) for cluster creation. Cluster creation uses the Relay Node (RN) and CD to group the sensor in same cluster. Upon accepting the broadcasted message each node verifies the value of RN. If its value is within RN it stores in its memory and compares CD with each node's distance. If the distance between nodes is same or less to CD and sensed value is within given RN then those group of nodes forms a cluster. The nodes NID which are related they will not broadcast message for cluster creation. Nodes which are not participate in cluster creation process based on RN and CD.

b) Cluster Head Selection :

Upon completion of cluster creation task each node has its cluster member NID, Node Location (NL), NTE and Sink Location (SL), battery power information in its memory. The node having maximum energy will calculate minimum distance of each node within range known as Cluster Head (CH) and broadcast CHID to other network nodes. It also measures the node having minimum distance from the sink called Cluster Head Transmission (CHT) and broadcast CHTID to CH. This node (CHT) will be used to transmit data toward sink if remaining CH energy is not sufficient for data transformation after measurement. Once each node knows it's CH it transmits data to CH. Cluster head transmit processed information to the sink, this communication is single hop communication, means it make direct communication with sink.

c) **Boundary Node Formation:**

A dynamic cluster will be built when the target comes close to the boundaries of multiple clusters. A demanding task issue is how the system finds the scenario when the target is approaching the boundaries, especially in a fully distributed way. We use boundary nodes to solve this issue in a fully distributed way.

d) **Multi Hop selection:**

1) The multi-hop planar model:

A CH node transmits data to the BS by forwarding its data to its neighbor nodes, in turn the data is sent to the BS. We have proposed an energy efficient routing algorithm for hierarchically clustered CRNs and it is suitable for the proposed secure data transmission protocols.

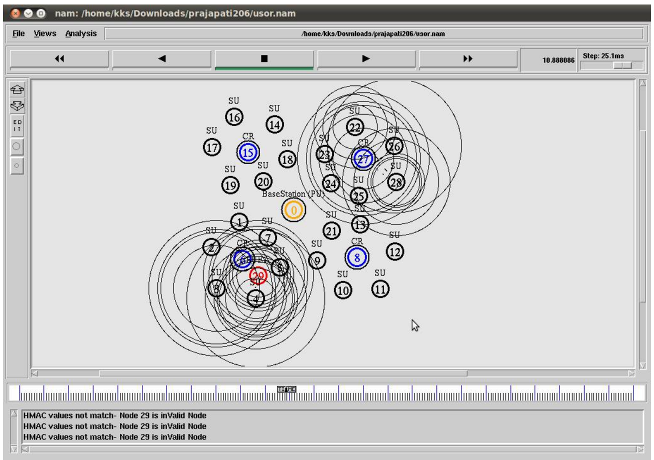
2) The cluster-based hierarchical method:

The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS.

Though the proposed study covers energy efficient reliable routing, it is failed to represent the basic security issues in CRN. The proposed system can be enhanced by using encryption algorithm. When the sensor node sense data from environment can be encrypted and the cipher text can be forwards to base station via cluster head. The base station can decrypt and retrieve the original data.

IV. SIMULATION RESULT AND PROPOSED EVALUTION

In our simulation, each node is set with a single omni-directional antenna, and two-ray ground reflection radio propagation model are applied. Default value used for each parameter in NS-2. The carrier sensing ranges and transmission range dependent on different factors such as the environment, the transmission power and the antenna. While evaluating simulation energy consumption due to radio's energy consumption is focused. System gives the list of the parameters used while evaluation of simulation. To evaluate the performance of proposed system,grid topology scenarios is used. The performance of the scheme deliberates in terms of the Drop Rate,Throughput and Packet Delivery Ratio(PDR).



```
HMAC values not match- Node 29 is inValid Node
HMAC values not match- Node 29 is inValid Node
HMAC values not match- Node 29 is inValid Node
```

Figure 3: Simulation

Algorithm

1. Cluster Head Selection

Input: Cluster set with nodes.

Output: Ch selection with remaining sensor node.

```
Step 1: select all nodes as initial population.
Step 2: Select evaluation set
Step 3: Apply crossover on similar power nodes.
Step 4: Apply mutation on each sensor node.
Step 5: Apply fitness on all nodes power
Step 6: select best node using rout let wheel selection.
Step 7: Check GA evaluations
Step 8: Select final max energy node as CH node.
```

2. Construction of ACO for best node selection

Input: Initial source node *Sn*, Destination node *dn*, Group of neighbour nodes nd *[]*, each node *id*, each node energy *eng*.

Output: Source to destination path when data received success.

```
Step 1: User first select the sn and dn
Step 2: choose the packet or file f for data transmission.
Step 3: if (f! =null)
Step 4: read each byte b form fd when reach null
Step 5: send data, initialize cf1,cf2,pf1,pf2
Step 6: while (nd[i] when reach NULL)
        Cf1=nd[i].eng
        Pf1= nd[i].id
        Cf2=nsd[i+1].eng
        Pf2= nd[i+1].id
Step 7: if (cf1>cf2)
        Cf2=null
        Pf2=null
```

DOI: 10.15680/IJIRCCE.2019. 0706006

```
        Else
        Pf1=pf2
        Cf1=cf2;
        Pf2=null
        Cf2=null
Step 8: end while
Step 9: repeat up to when reach at sink node
```

3. Data Aggregation Protocol

```
Input: existing received data list as TPQ, current received
       packet list IP
Output : 1 if aggregation is possible else 0
Step 1 : for each (data into TPQ) using below formula
```

$$\mathrm{Data}[i] = \sum_{k=0}^{n} p[k]$$

```
Step 2 : validate the similarity between Data[i] to IP[0]
           Result {0,1} ← calcsim(Data[i] , IP[0])
Step 3 : end for
Step 4 : return Result
```

V.RESULT AND DISCUSSION

In this section we present the evaluation of proposed system. After describing our experimental setup, we quantitatively evaluate the analysis with respect to the different parameter used such as Drop Rate(DR),Throughput and Packet Delivery Ratio(PDR). We run our experiments in NS2 simulator version 2.35 that has shown to produce realistic results. NS simulator runs TCL code, but here we use both TCL and C++ code for header input. In our simulation, we use Infrastructure based network environment for communication. For providing access to the wireless network at anytime used for the network selection. WMN simulate in NS2 .TCL file show the simulation of all over architecture which proposed. For run .TCL use EvalVid Framework framework in NS2 simulator it also help to store running connection information message using connection pattern file us1. NS2 trace file .tr can help to analyze results. It supports filtering, processing and displaying vector and scalar data. The results directory in the project folder contains us.tr file which is the files that store the performance results of the simulation. Based on the us.tr file,we have created a database of 5 text files which contains reading of 5 ms each till 25 ms as our simulation time is 25 ms. After that,we read the text file in a program created for the trace in Netbeans IDE 8.2. We got readings of various events in Netbeans from which we have plotted the graph of various parameters such as Drop rate(DR),Throughput and Packet Delivery Ratio(PDR).

1.Drop Rate:

It is defined as the number of packet lost per number of packet sent. The smallest amount value of drop rate states superior performance of the protocol.

$$\text{Drop Rate} = \sum_{i=0}^{n} \left(\frac{\text{packet received } [i \dots n]}{\text{sent packet } [i \dots n]} \right)$$

2. Throughput:

It is defined as the total number of packet delivered over the total simulation time.It is a ratio of total number of packet received in TCP and total number of packet sent. The greater value of throughput states superior performance of the protocol.

$$Throughput = \left(\frac{\sum_{i=0}^{k} received\ packet[TCP]}{\sum_{i=0}^{l} sent\ packet[TCP]}\right) * 100$$

2. Packet Delivery Ratio(PDR):

The packet delivery ratio (PDR) defined as a ratio of numbers of data packets reached to target over the network to number of packets generated. The greater amount value of packet delivery ratios states superior performance of the protocol.

$$PDR = \sum_{i=0}^{n} \left(\frac{packet\ received\ [TCP]}{packet\ sent\ [TCP]}\right) * 100$$

This Parameters are been evaluated and tested for different number of nodes and at different simulation time for knowing the performance of the proposed system.

Table 1:Reading of simulation from 1 to 5 ms

Event Type	**Send**	**Received**	**%**
ACK	1420	1375	PDR = 92.33
AODV	9669	8834	
RTS	1715	1495	
CTS	1385	1385	
TCP (Th)	2033	1966	Th= 96.70
MAC	6708	8494	
RTR	2091	5193	
RTR	1256	1084	
Total Sent	**26277**	**29826**	
Total Drop	**NA**	**1774**	**DR = 6.75**

Table 2: Reading of simulation from 6 to 10 ms

Event Type	**Send**	**Received**	**%**
ACK	3202	3199	PDR=99.90
AODV	1740	1626	
RTS	3811	3384’	
CTS	3222	3215	
TCP	4801	4790	Th=99.70
MAC	13594	9146	
RTR	3348	2417	
RTR	3194	3039	
Total Sent	36912	30816	
Total Drop	NA	695	DR=1.88

Table 3: Reading of simulation from 11 to 15 ms

Event Type	Send	Received	%
ACK	5075	5061	PDR=99.72
AODV	5936	4850	
RTS	6050	5431	
CTS	5130	5114	
TCP	7624	7620	Th=99.94
MAC	21779	18671	
RTR	5449	5052	
RTR	4995	4849	
Total Sent	62,038	56648	
Total Drop	NA	1465	DR=2.59

Table 4: Reading of simulation from 16 to 20 ms

Event Type	Send	Received	%
ACK	4512	4505	PDR=99.84
AODV	2906	2676	
RTS	5228	4716	
CTS	4521	4518	
TCP	6674	6767	Th=99.93
MAC	18995	12880	
RTR	4556	3708	
RTR	4300	4228	
Total Sent	51692	43,998	
Total Drop	NA	875	DR=0.5028

Table 5: Reading of simulation from 21 to 25 ms

Event Type	Send	Received	%
ACK	4236	4231	PDR=99.88
AODV	390	364	
RTS	4607	4312	
CTS	4552	4247	
TCP	6372	6368	Th=99.93
MAC	17369	10878	
RTR	4277	2314	
RTR	4237	4193	
Total Sent	46040	36097	
Total Drop	NA	450	DR=1.023

So after evaluation of parameters,we have calculated the value of Drop Rate,Throughput and PDR using the equations.This values are then plotted in the graph as shown in figure 4,figure 5 and figure 6.

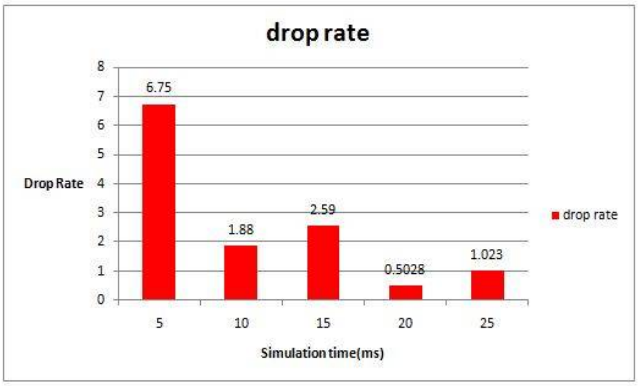


Figure 4: Drop Rate vs Simulation time

The smallest amount value of drop rate states that this system gives better performance superior.As we can see from the figure 4 that drop rate is very less with respect to simulation time.

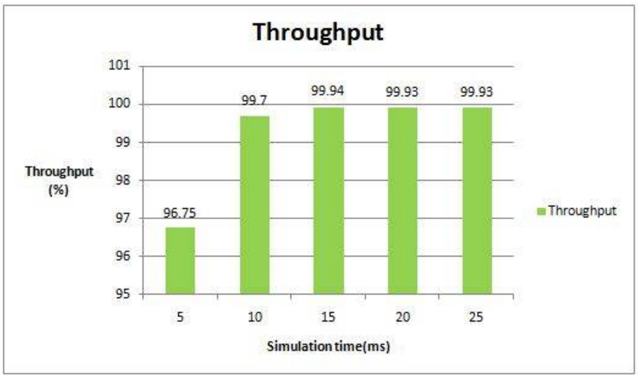


Figure 5: Throughput vs Simulation time

Higher the value of throughput,higher will be the performance of the proposed system.As we can see from the figure 5 that this system gives superior performance than other protocols.

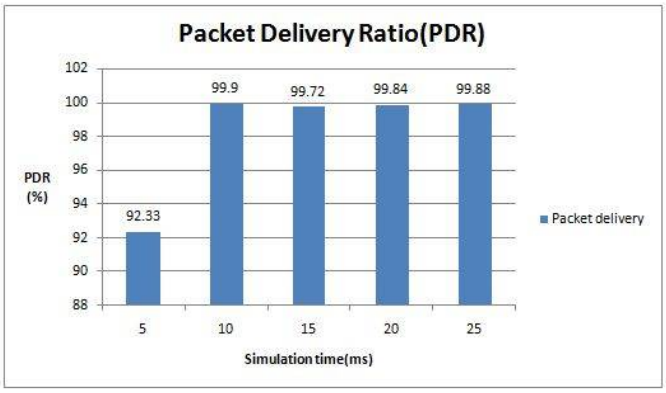


Figure 6: PDR vs Simulation time

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)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

In figure 6,the percentage of packet received by the target is more.

VI.CONCLUSION

Firstly,we have created clustering network with n number of clusters.According to maximum energy ,we have selected cluster head which is known as CR.Data aggregation strategy has been implemented on received data by CH during the communication between SU and CH.The HMAC authentication protocol has been used for drastic authentication of SU with CH.Moreover,system also carried out Broadcast Tree Construction(BTC) technique for internal hop selection when CH communicates with PU. From the calculation of various parameters such as Drop Rate,Throughput and PDR, we can say that this system gives superior performance. Finally,system provided minimum network overhead using data aggregation and trustworthy communication using BTC and HMAC in Cognitive Radio Network environment.

REFERENCES

[1] Li Jianwu, Feng Zebing, Feng Zhiyong, Zhang Ping, "A survey of Security Issues in Cognitive radio Network" China Communications • March 2015.

[2] Meenakshi Sansoy, Kanwaljeet Singh, Avtar Singh Buttar, "Cognitve Radio:Issues and Challenges" Journal of Network Communications and Emerging Technologies (JNCET) Volume 2, Issue 2, June (2015).

[3] R. Chen and J.-M. Park, “Ensuring trustworthy spectrum sensing in
cognitive radio networks,” in Proc. IEEE Workshop Netw. Technol. Softw.*Defined Radio Netw.*, Sep. 2006, pp. 110–119.

[4] Mahsa Ghaznavi and Azizollah Jamshidi,"A Reliable Spectrum Sensing Method in the presence of Malicious Sensors in Distributed Cognitive Radio Network",IEEE SENSORS JOURNAL, VOL. 15, NO. 3, MARCH 2015.

[5] R.K.Sharma and J.W.Wallace,"Correlation-based Sensing for Cognitive radio networks: Bound and experimental assessment",IEEE Sensor J.,vol. 11,no. 3,pp. 657-666,Mar. 2011.
S. Anand, Z. Jin, and K. P. Subbalakshmi, “An analytical model for primary user emulation attacks in cognitive radio networks,” in *Proc.*3rd IEEE Symp. New Frontiers Dyn. Spectrum Access Netw., Oct. 2008,pp. 1–6.
R. Chen, J.-M. Park, and J. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[6] LI F, Wang Y. Routing in vehicular ad hoc networks: A survey. Institute of Electrical and Electronics Engineers (IEEE) Vehicular Technology Magazine. 2007; 2(2):12–22.

[7] Himanshu Sharma and Kuldeep Kumar,"Primary User Emulation Attack Analysis on Cognitive Radio",Indian Journal of Science and Technology,Vol9(14),April2016

[8] Walid Ramadan Ghanem,Mona Shokair, and Moawad I. Dessouky,"Defense Against Selfish PUEA in Cognitive Radio Networks Based on Hash Message Authentication Code", International Journal of Electronics and Information Engineering, Vol.4, No.1, PP.12-21, Mar. 2016.

[9] L. Huang, L. Xie, H. Yu, W. Wang, and Y. Yao,"Anti-pue attack based on joint position veri_cation in cognitiveradio networks", in 2010 International Conference on Communications and Mobile Computing (CMC'10), ,pp. 169{173, Shenzhen, April 2010.

[10] Z. Chen, T. Cooklev, C. Chen, and C. Plmalaza-Raez,"Modeling primary user emulation attacks and defenses in cognitive radio networks", IEEE International Conference on Communications (ICC'09), pp. 208{215,Scottsdale, AZ, Dec 2009.

[11] C. C. Lee, C. H. Liu, and M. S. Hwang,"Guessing attacks on strong-password authentication protocol",International Journal of Network Security, vol. 15, no. 1, pp. 64-67, 2013.

[12] C. Lin, Y. Lv K. Li, and C. C. Chang,"Ciphertext-auditable identity-based encryption", International Journal of Network Security, vol. 17, no. 1, pp. 23-28, 2015.

[13] W. Stallings,"Cryptography and Network Security: Principles and Practice (5ed)",USA: Prentice-Hall, 2010.