iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: XII Month of publication: December 2018

DOI:

Study of Primary User Emulation Attack in Cognitive Radio Systems

Daljeet Kaur[1], Mr. Kanchan Sharma[2]
[1, 2]ECE Department, IP University

Abstract: Due to recently developments in wireless communication, have led to many problems like spectrum scarcity with the growing demand of upcoming applications and technologies. After examining a portion of radio spectrum including revenue rich areas, came to know that some frequency bands in the spectrum are largely unoccupied most of the time and others bands are highly used. This leads to underutilization of radio spectrum. Cognitive radio (CR) can deal successfully with these growing demands. It's new way to improve the spectrum efficiency. It is a form of technology in which transceiver can intelligently detect which RF communication channels are in use and which are still ideal, and instantly choose vacant spectrums while avoids the one's which are already occupied and this minimize interference to other users. Therefore, security is an important part to deal with, and attains more attentions recently. There are many layers in protocol stack like physical layer, link layer, network layer, transport layer and application layer, which give rise to many types of attacks at each layer. Therefore, security is an important part to deal with, and attains more attentions recently. In this paper, overview of cognitive radio systems and their security challenges are discussed. Different types of attacks are discussed but more focus on primary user emulation attack (PUEA) as of the main specific attacks on CRN. Performances for primary user emulsion attacks are studied from different point of views. Experimental results demonstrate the statistical characteristics of the probability of false alarm and miss detection and analyse the effectiveness of the proposed approach, both by theoretical analysis and simulations.

Keywords: Cognitive radio system, security, primary user emulation attack, PUEA

I. INTRODUCTION

The huge development in wireless communication has led to the problem of growing spectrum scarcity. Due to increasing spectrum demand day by day for new wireless applications and technologies the available radio frequency spectrum has become scarcer. Radio spectrum is examined and came to know that large amount of spectrum is unused while the other is highly used. This give rise to new technology called cognitive radio system. A cognitive radio (CR) is an intelligent radio system which have the ability to exploit its environment to increase the capacity and spectral efficiency [1]. CR's are regarded as transceivers that automatically detect (sense the existence of) available channels i.e unused spectrum in a wireless spectrum and accordingly, interchange their transmission or reception. Cognitive radio technology gives a promising solution for the spectrum scarcity issues in wireless networks. It allows the efficiently use of spectrum. Here, licensed users are also known as Primary users are defined as users who have right to use the spectrum band whereas unlicensed users which are called as Secondary users are defined as users who can use the spectrum which is temporarily not used by licensed users, without causing interference to them. Therefore, security concerns of cognitive radio plays more vital role in our modern and demanded society as CR networks would pose new challenges to wireless communications. In cognitive radio network, an attack can be defined as an activity that can cause interference to the primary users or licensed users [2]. In this dissertation we also provide a brief explanation of most of the attacks and will focus on PUEA attack as one of the main specific attack on CRN network.

Many methods have been proposed to detect the PUE attacks, which can be generally sorted as location unaware [9],[7] and location aware [6]. Location aware techniques distinguish PUE attacks by detecting the location of the transmitter and perform a comparison with the PU's location. These type of methods mostly need a dedicated wireless sensor network for its localization [6], which leads to high infrastructure overhead and has poor performance when PUE attackers is located around PUs. Deepraj [4] previously proposed analytical modal based on maximum likelihood criterion point of view in which two PU are taken into account and one good secondary user and 10 malicious user. In his paper probability of missed detection is high but symmetrical. And this is possible only when two transmitting antennas have same power. In [8], an analytical model for the probability of PUEA successfully done on the energy detection was proposed, where the received signal power is modelled as a log-normally distributed random variable. In this approach, Markov inequality is used on lower bound for the probability of a successful PUEA. Many other methods have been proposed to detect and defend against PUEA. In [10], a transmitter verification scheme (localization-based defense) was proposed to detect primary user emulation attack. In [10] and [11], the authors proposed a received signal strength (RSS)-based technique to defend against primary user emulation attack.

In this paper, we focus on the scenario that the PUE attackers which are randomly and uniformly distributed near to the good secondary user but excluded the specified region of secondary user. Here, we increased transmitting antennas and increase no of malicious user. And prove that probability of missed detection is decreased near to zero and probability of false detection is also reduced further and obtain optimal system performance.

The rest of paper is organized as follows. In section 2, discuss security issues and security of different layers that is physical layer, link layer, network layer, transport layer, application layer. In section 3, primary user emulation attack is briefly discussed. In section 4, analytical system model is discussed. Simulation results and conclusion are given in section 5 and 6 respectively. In section 7 is of references.

II. SECURITY ISSUES IN COGNITIVE RADIO

As compared with traditional wireless networks, security challenges of cognitive radio technology are more complicated and more chances open to attackers. Therefore, security of cognitive radio network (CRN) has become a challenging task.[9] Quality of service (QoS) provisioning and security requirement for the entire network is very affected by these type of weaknesses and vulnerable aspects, which was introduced by the nature of cognitive radio [3]. Many general schemes proposed in the past cannot satisfy this type network requirements, since the spectrum is used dynamically in cognitive radio.

Cognitive radio network is more alike to wireless network. But the nature of transmission here (wireless media) is open air, it is more vulnerable to attacks as compared to that of wired network. The data in the wireless media may be eavesdropped or altered without notice and the channel might be jammed or overused by the adversaries. The cognitive radio technology opens more chances to attackers due to its intrinsic nature [3],[4].

A. *Inherent Reliability Issues*

Some of inherent reliability issues of cognitive radio networks are discussed [4] as follows:

1) *High Sensitivity to primary user signal:* The secondary users should recognize the primary transmission in order to prevent interference. One of the stringent requirements for cognitive network is to predict the temperature interference on nearby primary receiver and keep it below a threshold. This type is known as energy based detection. As a result of this the sensitivity towards the primary user signal is usually set to high. In this case high sensitivity increases false detections.
2) *Unknown primary receiver Location*: The secondary user must know the exact location of primary user, so that the interference to primary user is minimized. Unknown location of primary receiver location may lead to hidden node problem. By exploiting the receiver power leakage, the location of primary receiver can be identified.

B. *Security at Different Layers*

The attacks associated with the five layers in the protocol stack i.e., the physical layer, link layer, network layer, transport layer and application layer [3], [8].

1) *Physical layer*: Physical layer is the lowest layer which provides an interface to the transmission medium. Cognitive radio network (CRN) does not operate on a fixed frequency or on a particular frequency[10]. Here, signals can be transmitted and received at various frequencies across wide frequency spectrum band. Thus, this makes the operation of physical layer in cognitive radio more complicated.

a) *Intentional jamming attack:* The malicious secondary user (SU) intentionally transmits signal in a licensed band which results in jamming of primary and other secondary users. This problem would be worse when the malicious user launches attack in one geographical area and then moves to other area before being identified [3].

b) *Primary receiver jamming attack:* The secondary user does not know the location of the primary receiver, the attacker may take advantage of this to launch a primary receiver jamming attack

c) *Primary User Emulation Attack (PUEA)[4] :*In PUEA malicious user can imitate the primary user, while other secondary user in the network thinks that the primary user reappears and they terminate their communication in between and release the frequency band.[5] This prevents the secondary users from accessing that particular empty band.

d) *Overlapping secondary user attack:* In cognitive radio networks, multiple secondary networks may exist at the same time in the same region. The transmissions from malicious users in a network can cause interference to the primary and secondary users of the other network. Since the malicious users or so called attackers may not be under the direct supervision of the secondary base station of the victim network, this type of attack is very difficult to find [3].

2) *Link layer:* Link layer is just above the physical layer in the protocol layer stack. This layer is responsible for transfer of data from one node to other in single hop.

a) *Biased utility attack:* Here, a malicious secondary node or user may try to change the parameters of utility function in order to increase its own bandwidth. As a result, the good secondary user may not be able to use that available bandwidth [8].

b) *False feedback attack:* In cognitive network, secondary user (SU) will sometime makes a wrong decision due to false feedback from one malicious secondary user. This will in turn causes severe interference or distraction to the licensed user [4].

c) *DOS attack:* In DOS attack, the main objective of malicious node or user is to prevent good secondary nodes from accessing the vacant radio frequency band. Again arises a problem.

3) *Network layer:* The main objective of network layer is to provide end-to-end packet deliveries. Some of the functions of the network layer are routing, flow control, ensures quality of service (QoS). Every node here maintains routing information about its neighbouring nodes in the network. Before establishing connection setup, every node identifies which of its neighbors should be present in the next link in the path towards the destination.[3],[6] An attacker in the path can drastically busy in altering routing by either redirecting the packets in the wrong direction or by broadcasting incorrect routing information to its neighbors. Following are some of the possible attacks associated with the network layer.

a) *Hole attack:* In the hole attack the node which pretends is called a hole. There are various types of hole attacks such as Black hole attack, Worm hole attack, gray hole attack.

b) *Ripple effect attack:* In ripple effect attack the malicious node is to provide wrong channel information so that the other nodes change their channel.

4). Transport layer: The transport layer have the responsibility of transferring the data between two end hosts. It is responsible for flow control, end-to-end error recovery, congestion control.

a) *Key depletion attack*: Sessions here in cognitive networks last for a short period of time due to frequently after one another occurring retransmissions. Therefore, large numbers of sessions are being initiated. Security protocols such as SSL and TLS establish cryptographic keys at the starting of every transport layer session [8].

5). Application layer: It is the top most layer of the protocol stack and provides application services to the end users. Protocols which run at the application layer rely completely on the services which are provided by the underlying lower layers.[5] As a result of this, any attack on physical, network , link layer or transport layers may have an bad effect on the application layer.

III. PRIMARY USER EMULATION ATTACK

Primary user emulation (PUE) attack is one of the severe threats to cognitive radio systems. It poses severe threat to spectrum sensing. In this attack, a malicious node transmits signals whose characteristics emulate those of incumbent signals [4],[18].

There are two types of primary user emulation attack:

1) *Selfish PUE attacks:* The main objective of this selfish PUE attack is to maximize attacker's bandwidth. For an instance, when malicious node notice about the vacant band, it will prevent other secondary users from using it by transmitting signals that resembles the incumbent signals [4].

2) *Malicious PUE attack*: The main objective of this malicious PUE attack is to obstruct the secondary users (SU) from identifying and using vacant spectrum bands. It's not necessary that malicious user use the vacant band for its own transmission. It is important to note that in PUE attacks, malicious nodes only transmit in vacant bands [3],[4].

A. Primary Exclusive Region (PER)

One of the deployment schemes in recent researches is the primary exclusive region (PER). It's called as a safeguard for primary receivers. The secondary network so called secondary user must be deployed outside PER. This exclusive zone is also called as keep-out region. It gives primary receiver a protection area. It is a way of imposing some distance on cognitive users from the primary user(PU) and hence reduced interference to the primary receiver [17]. Within this region cognitive users are not allowed for transmission. This type of scheme is suitable for a broadcast network. For an instance, network in which there is only one primary transmitter is present for communicating with multiple primary receivers. TV network / downlinks in the cellular network are the good examples of a broadcast network. In these type of networks, primary receivers may represent as passive devices. Such a primary exclusive region (PER) has been proposed for the upcoming spectrum sharing of the TV band [16],[4].

B. System Model For Cognitive Radio Networks (CRN):

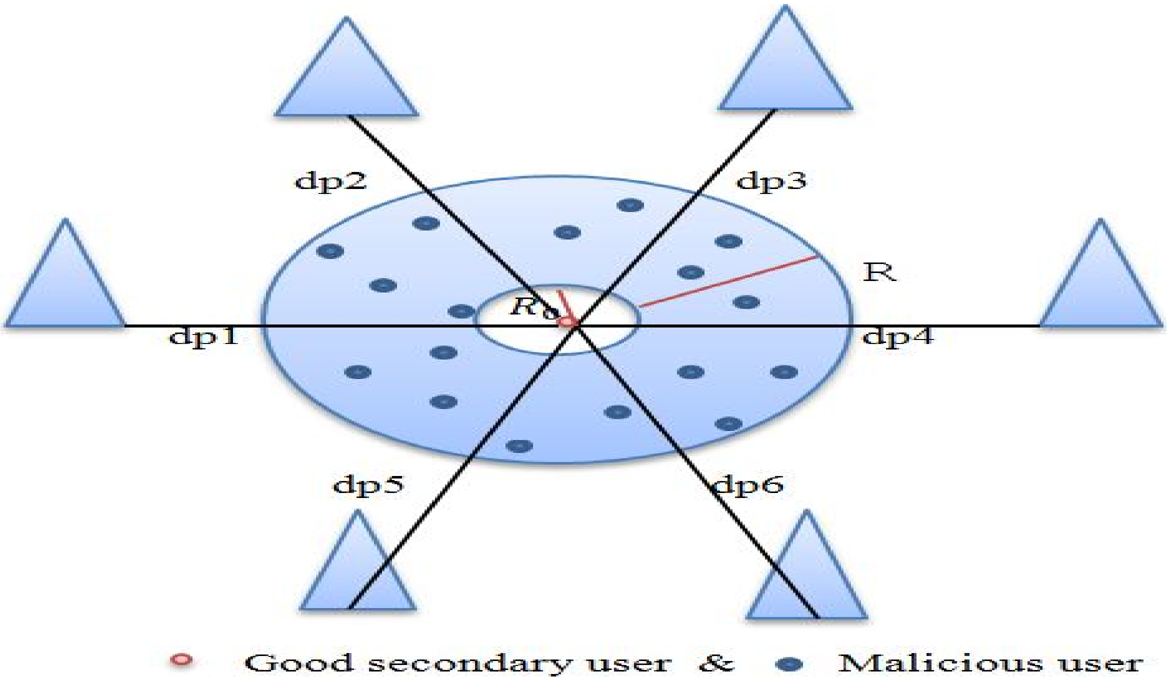

Fig 1: system model for CRN

C. Some Assumptions are Made in this New System Model:

1) There are M malicious users in the network which are randomly and uniformly distributed in circular region of radius R.
2) Here in this new model six primary transmitters Pt1, Pt2, Pt3, Pt4, Pt5,Pt6 are situated in the form of hexagon and their transmissions are independent.
3) The distance between secondary user and Pt1 is Dp1, between secondary user and Pt2 is Dp2, like this between Pt3 is Dp3, between Pt4 is Dp4, between Pt5 is Dp5 and between Pt6 is Dp6 as shown in figure above.
4) No malicious user is present within the specified exclusive region for the secondary user.
5) All the users present in the network may know about the location of primary transmitters.
6) The RF signals present between primary transmitters and malicious users undergo path loss and log normal shadowing.
7) The position of good secondary user (SU) does not change with the primary transmitter position.

IV. ANALYTICAL MODEL

There are M malicious users in the system which transmits at power 'Pm'. The primary transmitter $Pt1$ is at distance '$Dp1$' , primary transmitter $Pt2$ is at distance '$Dp2$', primary transmitter Pt3 is at distance 'Dp3', primary transmitter Pt4 is at distance 'Dp4', primary transmitter Pt5 is at distance 'Dp5', primary transmitter Pt6 is at distance 'Dp6' from all the users and transmits at power 'Pt '. The positions of secondary and malicious users are uniformly distributed in circular region of radius R and are statistically independent of each other. Primary transmitter (Pt) position is known to all the users and is fixed at $(rp,)$[4]. The RF signals from primary transmitter (PT) and malicious users undergo log normal shadowing and path loss. The path loss exponent for transmission from primary transmitter (Pt) is fixed to 2 and that from malicious user is fixed to 4. For any secondary user fixed at coordinates(r,) no malicious users are present within a circle of radius Ro which is known as primary exclusive region (PER) from secondary user. There is no co-operation between the secondary users.

The received power at the secondary user from the primary transmitter1 (pt1) is given by,

$p_r{}^{(p1)} = p_{t1}\, d_{p1}{}^{-2} G_{p1}{}^{2}$ ………………eq(1)

Where, G$p^2 = 10^{\frac{\epsilon p}{10}}$,$^{\epsilon p} \sim N(0, \sigma_p{}^2)$, since p_t and d_p are fixed. The pdf of $p_r{}^{(p)}$ follows a log normal distribution and can be written as,

The received power at the secondary user from the primary transmitter2 (pt2) is given by,

$p_r{}^{(p2)} = p_{t2}\, d_{p2}{}^{-2} G_{p2}{}^{2}$ ……………….eq(2)

From other primary user are given as follows,

$p_r{}^{(p3)} = p_{t3}\, d_{p3}{}^{-2} G_{p3}{}^{2}$ ……………….eq(3)

$p_r{}^{(p4)} = p_{t4}\, d_{p4}{}^{-2} G_{p4}{}^{2}$ ……………..eq(4)

$p_r{}^{(p5)} = p_{t5}\, d_{p5}{}^{-2} G_{p5}{}^{2}$ ……………..eq(5)

$p_r{}^{(p6)} = p_{t6}\, d_{p6}{}^{-2} G_{p6}{}^{2}$ ……………...eq(6)

The total power at receivers is then given by, due to their independence.

From equations, eq(1),eq(2),eq(3),eq(4),eq(5),eq(6)

we get,

$$pr^p = p_r{}^{(p2)} + p_r{}^{(p3)} + p_r{}^{(p4)} + p_r{}^{(p5)} + p_r{}^{(p6)}$$

The total received power at the secondary user from all the malicious users is given by [15],

$$pr^{(m)} = \sum_{j=1}^{M} p_m\, Dj^{-4} Gj^2$$

DF of $pr^{(p)}$ follows a log normal distribution and can be written as[15],

$$p^{(pr)}(\gamma) = \frac{1}{\gamma A\sigma\sqrt{2\pi}}\, \exp\{-\frac{(10log_{10}\gamma - \mu_p)^2}{2\sigma p^2}\}$$

PDF of $pr^{(m)}$ follows a log normal distribution and can be written as,

$$p^m(x) = \frac{1}{xA\sigma_x\sqrt{2\pi}} \exp\{-\frac{(10log_{10}x - \mu_x)^2}{2\sigma_{x^2}}\}$$

V. SIMULATIONS RESULTS

In first scenario, only one transmitting antenna is used pt1 and 15 malicious user. Outer radius is taken to be R= 500 m and inner radius in which only good secondary user is present is taken to be R_0 = 30 m. which is also called primary exclusive region (PER), primary transmitter power Pt=100Kw, Malicious transmitter power Pm=4w, σm=5.5dB, σp= 8dB. Probability of False Alarm is calculated for 500 numbers of simulations. The threshold value chosen for above simulation is set to 2 i.e. λ=2 [8],[9].

In second scenario two transmitting antenna are used pt1 & pt2 and 10 malicious user. If pt1 =100kw and pt2 =100kw. Here R= 200m and inner radius $R_0 = 30m$ Malicious transmitter power Pm =4w, $\sigma m1$ = 8, $\sigma m2$ = 8dB . It is noted that the probability curves show symmetric around 75Km, because we set up two transmitters equally. But probability of missed detection pd2 is not minimized appropriately [4].

In third scenario, lets considered six primary transmitting antennas are used namely pt1,pt2 , pt3 , pt4 ,pt5 , pt6 instead of one primary transmitter. Pt1 and pt2 transmits power pt1=100kw, pt2=100kw. Whereas pt3 transmits =50kw, pt4 =50kw, pt5 =50kw and pt6 =50kw. Distance between pt1 and secondary user is dp1, between pt2 and secondary user is dp2, distance between pt3 and secondary user is dp3, distance between pt4 and secondary user is dp4, distance between pt5 and secondary user is dp5 and distance between pt6 and secondary user is dp6. Outer radius here is increased to 5000 m and inner radius is reduced to 7m. Number of malicious users are increased to 5000. Malicious transmitter power $p_m = 4w, \sigma m = 5.5\ dB,\ \sigma p = 8dB$. The threshold value chosen here is set to 2. In this case performance is better, probability of false alarm is reduced and probability of missed detection pd2 is also reduced to great extent. It can be observed that after using new system model performance is improved to greater extent.

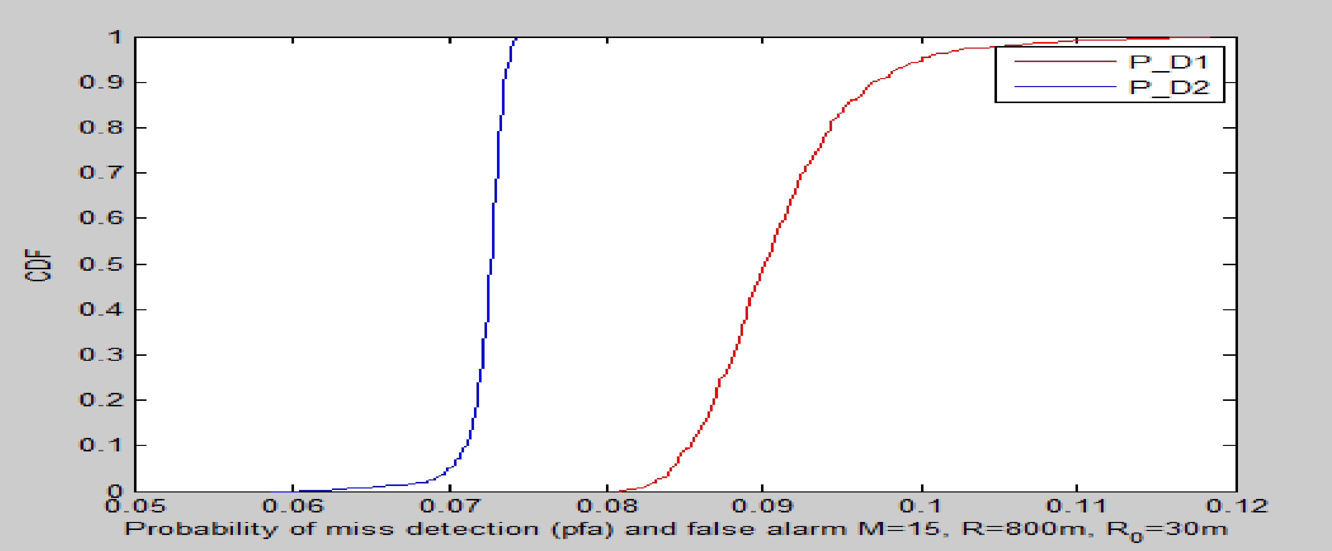

Fig 2: probability of missed detection and false alarm

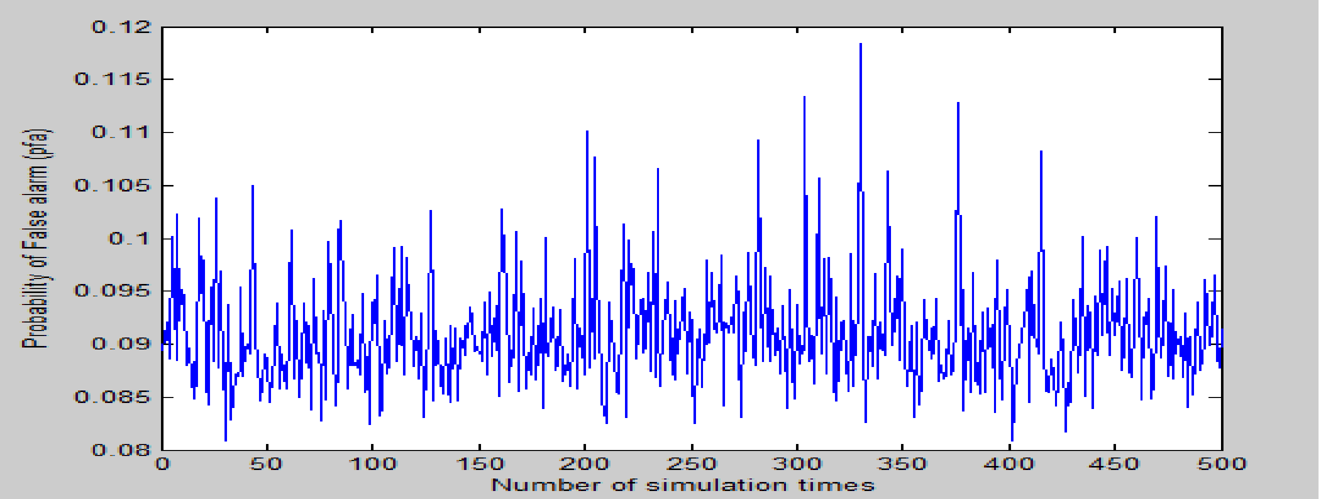

Fig 3: probability of false alarm

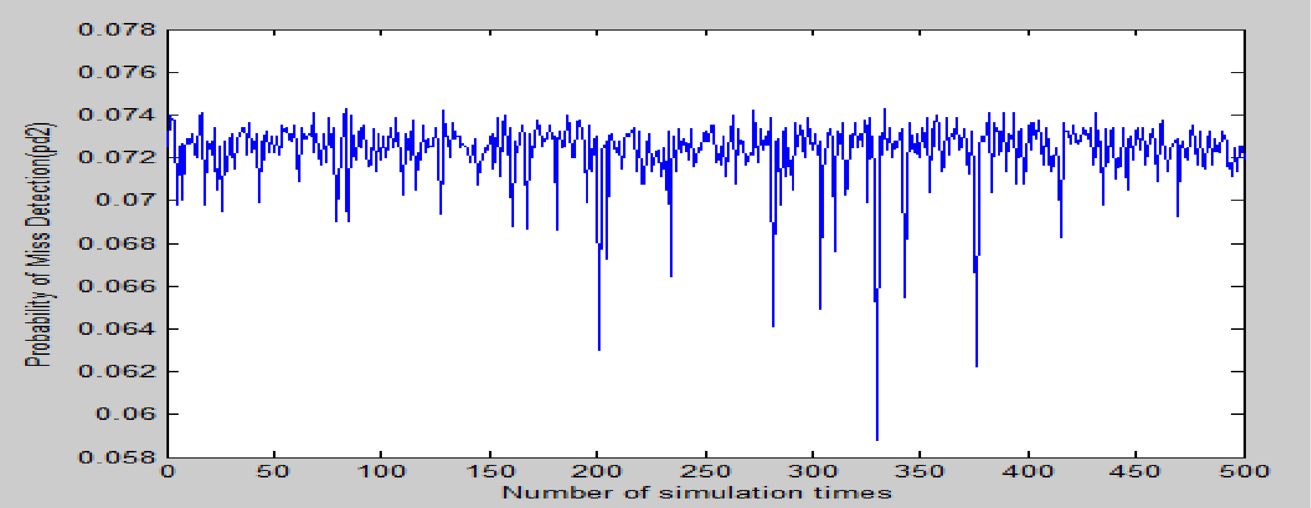

Fig 4: probability of missed detection

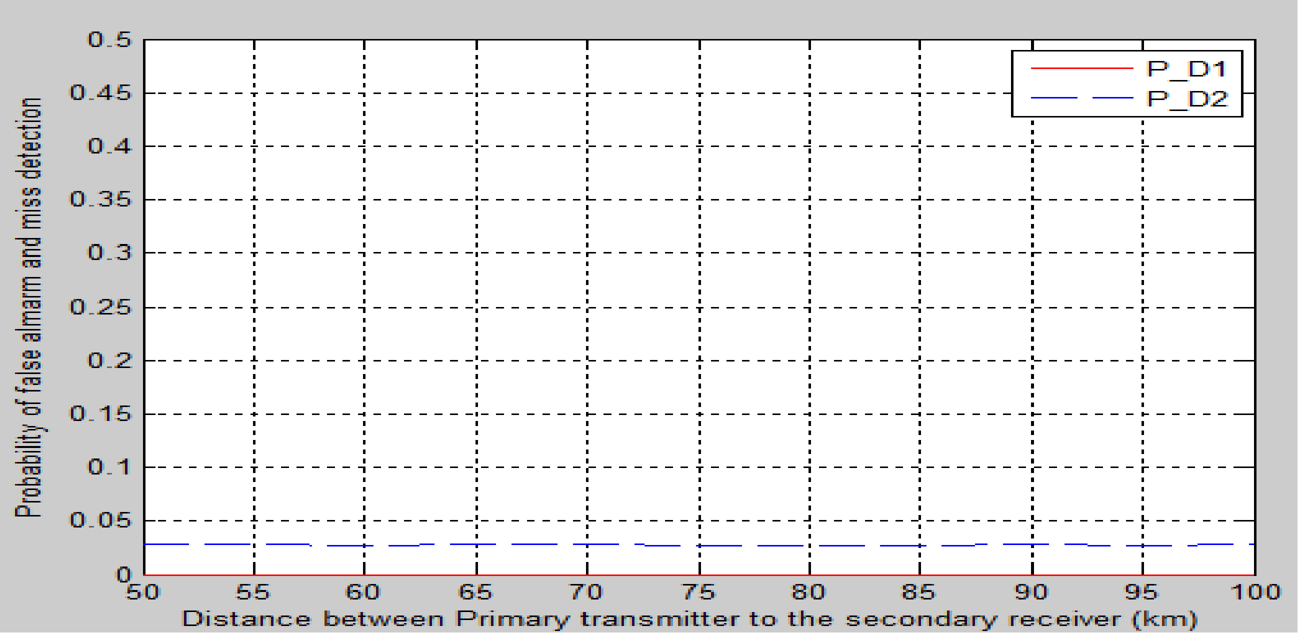

Fig 5: probability of missed detection and false alarm with new system model

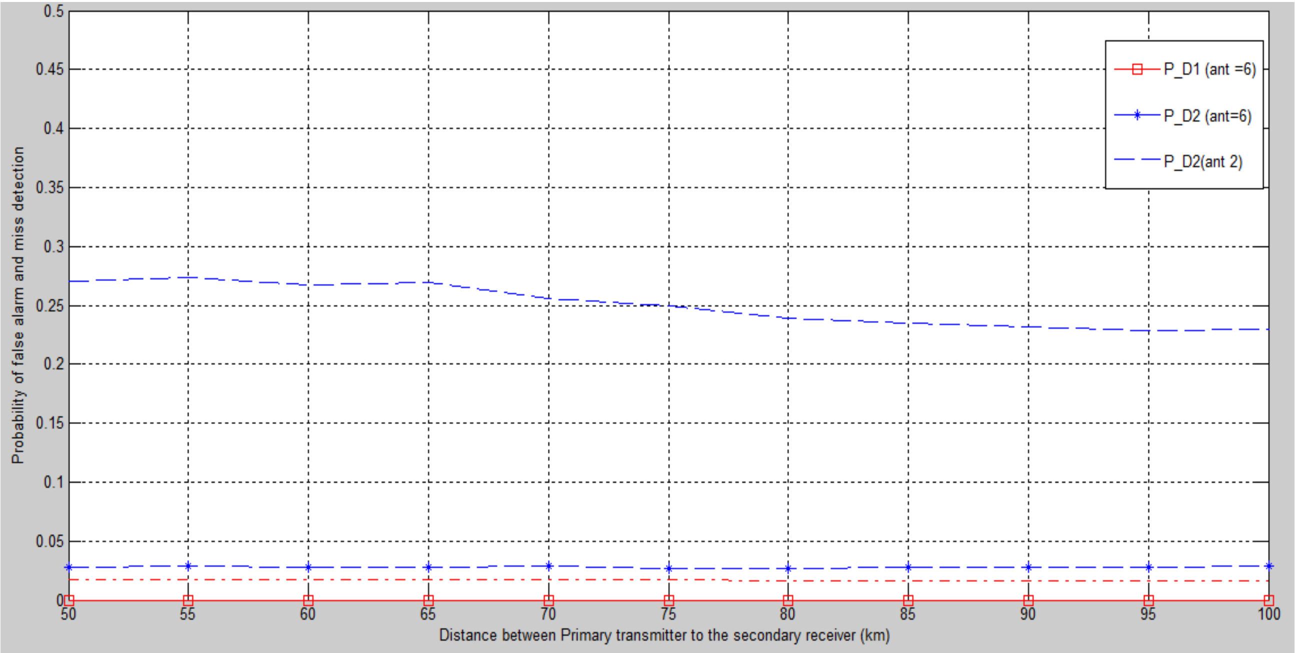

Fig 6: comparison of probability of missed detection and false alarm with antenna 2 and antenna 6.

VI. CONCLUSIONS

Aiming at the primary user emulation attacks, we have proposed a new system model while using six antennas in the form of hexagonal shape, with which we could reach the optimal performance. Simulation results show that how we get better performance with increased area and increased number of malicious user to 5000, and minimum PER of 7m. probability of missed detection is reduced to greater extent and probability of false alarm is also minimized. As per results shown probability of false alarm and missed detection is minimized hence reduced or diminished primary user emulation attack. In the future we will introduce that how many antennas at maximum one can use and its disadvantages and make comprehensive performance comparison with existing research results to obtain better performance.

REFERENCES

[1] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," IEEE Communications Surveys and Tutorials, vol. 11, no. 1, pp. 116– 130, 200

[2] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[3] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in the Asilomar Conference on Signals, Systems and Computers, Nov. 2004, pp. 772–776.

[4] Deepraj S. Vernekar, "an investigation of security challenges in cognitive radio challenges" IEEE Journal on Selected Areas in computer electronics, vol. 26, no. 1, pp. 25–37, Dec. 2012.

[5] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," IEEE Journal on Selected Areas in Communications, vol. 25, no. 3, pp. 517–528, Apr. 2007.

[6] I. F. Akyildiz,W. Lee, M. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," IEEE Communications Magazine, vol. 46, no. 4, pp. 40– 48, Apr. 2008.

[7] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 26,no. 1, pp. 25–37, 2008.

[8] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in Proceedings of the 28th IEEE International Performance Computing and Communications Conference (IPCCC), 2009, pp. 208–215.

[9] J. Burbank, "Security in cognitive radio networks: the required evolution in approaches to wireless network security," in IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), May. 2008, pp. 1–7. [19] K. Bian and J. Park, "Security vulnerabilities in ieee 802.2," in International Wireless Internet Conference, 2008, pp. 1–9.

[10] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), May. 2008, pp. 1–8.

[11] M. Thanu, "Detection of primary user emulation attacks in cognitive radio networks," in Proc. Int. Conf. CTS, May 2012, pp. 605–608.

[12] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in IEEE International Conference on Communications (ICC), May. 2008, pp. 3406–3410.

[13] B.Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in IEEE Symposium on New Frontiers Dynamic Spectrum Access Networks, Nov. 2005, pp. 124–130.

[14] T. Brown, "An analysis of unlicensed device operation in licensed broadcast service bands," in IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Nov. 2005, pp. 11–29.

[15] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in IEEE International Dynamic Spectrum Access Networks (DySPAN), Oct. 2008, pp. 1–6.

[16] Z. Jin, S. Anand, and K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in IEEE International Conference on Communications (ICC), Jun. 2009, pp. 1–5.

[17] Z. Chen, T. Cooklevand, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks & defences in cognitive radio networks," in IEEE International Performance Computing and Communications Conference (IPCCC), Dec. 2009, pp. 208–215.

[18] H. Li and H. Zhu, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," in IEEE Global Telecommunications Conference (GLOBECOM), Dec. 2009, pp. 1–6.