Detection of PUE- Attack in Cognitive Radio Networks

Megha Chopra, Mtech Student
Dept. of ECE
JCDM College of Engineering
Sirsa, India
meghachopra.chopra@gmail.com

Sonika Soni, Assistant Professor
Dept. of ECE
JCDM College of Engineering
Sirsa, India
soni_sonika80@rediff.com

Abstract: Cognitive Radios (CR) are the radios that are widely used in the wireless networks. It is a software based air interface network . Due to the air interface, the probability of attacks increases. In cognitive radio network, an attack can be defined as an activity that can cause interference to the primary users or licensed users. Primary User Emulation Attack(PUEA) is a major threat to the spectrum. In this paper to prevent from the PUE Attack firstly Distance Ratio Test(DRT) is used which is a transmitter verification procedure based on location verification is used which calculates the received signal strength(RSS) of the signal. Results are compared by plotting False negative ratio(FNR) with measurement and modeling error. Results shows improved value of FNR. Another method that is used is Time difference of arrival(TDOA) and Frequency difference of arrival(FDOA) which helps on determining the location of target. The parameters that are calculated are: time difference of arrival, frequency deviation and direction cosine of target movement. Simulation results were carried out with the help of Graphic User Interface(GUI) through MATLAB. Simulation results in this paper are better from the previous results and achieves high accuracy on transmitter location verification in CR network, which can improve the ability to resist PUE attack.
.

Keywords: Cognitive Radio , PUEA[5], location verification[1], DRT[1],TDOA,FDOA

*****

I. INTRODUCTION

The need to meet the ever-increasing spectrum demands of emerging wireless applications and the need to better utilize spectrum has led the Federal Communication Commission (FCC) to revisit the problem of spectrum management. The US spectrum is managed either by the FCC for non-governmental applications or by the NTIA for governmental applications [6].The Federal Communication Commission(FCC) defined Cognitive radio (CR) as the radio that can change its transmission parameters based on interaction with the environment in which it operates [7].Recognizing the significance of the spectrum shortage problem, the FCC is considering opening up licensed bands to unlicensed operations on a non-interference basis to primary users. In this new paradigm, unlicensed users (a.k.a. secondary users) "opportunistically" operate in fallow licensed spectrum bands without causing interference to licensed users (a.k.a. primary or incumbent users), thereby increasing the efficiency of spectrum utilization. This method of sharing is often called Opportunistic Spectrum Sharing (OSS)[1] shown in fig1 below as:

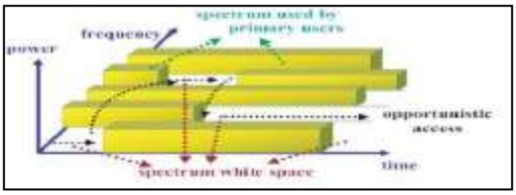


Fig.1. Opportunistic use of spectrum holes

Spectrum Sensing is a key step used in cognitive radio network[4]. Basic requirement of cognitive radio is to scan the radio frequency spectrum and determine fallow bands After identification of the spectrum holes, SUs can utilize these holes in 3 ways: (a) opportunistically, (b) periodically and (c) probabilistically depending upon the properties of the
mechanism used[9]. The most efficient way to identify white space is to detect primary users. Following are the features of cognitive radio[8]:-

- Frequency agility: It is the ability of a radio to change its operating frequency.
- Dynamic frequency selection: It is the ability of a radio to sense signals from nearby transmitters in order to choose best operating conditions.
- Location awareness: Determine its location, permission to transmit, select parameters such as power, frequency allowed etc.
- Adaptive Modulation: Ability to modify transmission characteristics

.

II. RELATED WORK

In [1] , an attack called primary user emulation (PUE) attack that poses a great threat to spectrum sensing. Their investigation shows that a PUE attack can interfere with the spectrum sensing process and reduce the channel resources available to legitimate unlicensed users. To counter this threat , a transmitter verification procedure which employs a location verification scheme to distinguish incumbent signals from unlicensed signals. Two alternative techniques are proposed to realize location verification: DRT and DDT. Simulation results show that factors, such as the location of the attacker's transmitter relative to the LVs, can impact the performance of the two schemes.

In[2] ,author study the denial-of-service (DoS) attack on secondary users in a cognitive radio network by primary user emulation (PUE). Simulation studies and results from test beds have been presented but no analytical model relating the various parameters that could cause a PUE attack has been proposed and studied. They propose an analytical approach based on Fenton's approximation and Markov inequality and obtain a lower bound on the probability of a successful PUEA on a secondary user by a set of co-operating malicious users .

In[3] ,a joint position verification method is proposed to enhance the positioning accuracy. Simulation results show that the method is simple and achieves high accuracy on transmitter location verification in CR network, which can improve the ability to resist the pue attack .

In [4] author firstly discuss the security issues in cognitive radio Then they discuss about the security and its requirement in CR networks. They also discussed the security mechanisms for different protocol layers. Then they have studied the analytical model named Neyman-Pearson Criterion for detecting PUEA in cognitive radio network. Simulations were carried out to determine the performance of the network for PUE attack in terms of probabilities of miss detection and false alarm. In[5] author focus on the primary user emulation attack. They proposed a method for reducing the effect of primary user emulation attack in cognitive radio networks. In this method, benefit of the energy detection based spectrum sensing that is a simplest method of spectrum sensing.

In[6]This site provide the description about the radio frequency spectrum in US.

In[7] author discuss various security issues in cognitive radio networks and then to discuss the PUEA with the existing techniques to mitigate it. In[8] Cognitive radio have been considered since new technologies for wireless communication. Cognitive radio network produce high bandwidth in order to mobile individual via heterogeneous wireless architecture in addition to dynamic spectrum access tactics.

In[9] the objective of this paper is to give a variety of security requirements for cognitive radio networks and then discusses the PUEA with the preventive procedures to mitigate it.

III. PRIMARY USER EMULATION (PUE) ATTACK

In this kind of attacks the attacker emulates the signals that copies the characteristics of the primary user signals and then the secondary user identifies this signal as the primary user signal and prevents to transmit signal on this band. Figure2,below shows the primary user emulation attacks.(5)

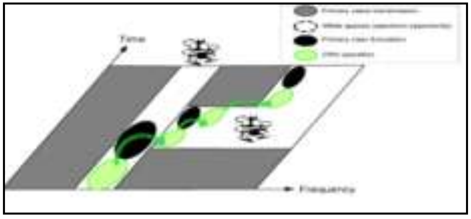


Fig2. Primary User Emulation Attack

A PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack.

- Selfish PUE attacks: In this attack, an attacker's objective is to maximize its own usage of spectrum resources. When selfish PUE attackers detect a fallow spectrum band, they prevent other secondary users from competing for that band by transmitting signals that emulate the signal characteristics of incumbent signals.
- Malicious PUE attack: The objective of this attack is to obstruct the OSS process of legitimate secondary users i.e., prevent legitimate secondary users from detecting and using fallow licensed spectrum bands.

IV. TRANSMITTER VERIFICATION PROCEDURE FOR SPECTRUM SENSING

A. *The transmitter verification procedure[1]*

Some assumptions are taken to do transmitter verification that is primary users are TV transmitters and receivers and secondary users are assumed to be CR devices forming a mobile ad hoc network. An attacker, equipped with a CR, is assumed to be capable of changing the radio's modulation mode and transmission output power as needed. The proposed transmitter verification procedure only considers PUE attacks, which is a security threat unique to CR networks. Based on the above assumptions, we propose a transmitter verification procedure for spectrum sensing that is shown in Fig. 3[1].

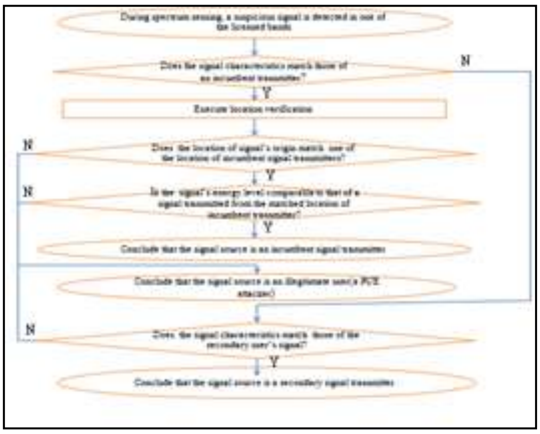

During spectrum sensing, a suspicious signal is detected in one of the licensed bands
Does the signal characteristics match those of an incumbent transmitter?
N
Y
Execute location verification
N
Does the location of signal's origin match one of the location of incumbent signal transmitters?
Y
N
Is the signal's energy level comparable to that of a signal transmitted from the matched location of incumbent transmitter?
Y
Conclude that the signal source is an incumbent signal transmitter
Conclude that the signal source is an illegitimate user(a PUE attacker)
N
Does the signal characteristics match those of the secondary user's signal?
Y
Conclude that the signal source is a secondary signal transmitter

Fig3. A flowchart of transmitter verification procedure for spectrum sensing.[1]

The main aspect of the transmitter verification procedure is the estimation or verification of the location of a signal's origin[1]. We focus on technique that is called Distance Ratio Test (DRT), which utilizes the received signal strength (RSS) of a signal source and tells that the test will pass or fail. We assume that location verifiers (LVs) exist for performing DRT. An LV can be a dedicated node, a secondary user with enhanced functions (to carry out DRT), or a fixed/mobile base station[1] We assume that the area spanned by the CR network is populated with two types of LVs: one or more master LVs and slave LVs. A master LV has a database of the coordinates of every TV tower whose signal reaches the area spanned by the CR network. In addition, we assume that all of the LVs are synchronized.[1]

B. *Distance Ratio Test (DRT)[1]*

DRT is based on large scale propagation model which calculates received signal strength as:

$$RSS = P_t G_t G_r \frac{{h_t}^2 {h_r}^2}{d^4 L} \dots\dots\dots\dots\dots (1)$$

where P_t is the transmitted signal power, G_t and G_r are the antenna gains of the transmitter and the receiver, respectively, h_t is the height of the transmitter, h_r is the height of the receiver, d is the propagation distance, and L is other system loss.[1]

We take LV's for performing DRT operation

In a single iteration of DRT, a pair of LVs, represented by LV_1 and LV_2, measure the RSS of a signal in the band obtaining results R_1 and R_2 respectively. The two LVs are assumed to be identical with respect to the parameters of (1) except for their distances to the signal source. Suppose that the positions of LV_1 and $LV_2$are (x_1, y_1) and (x_2, y_2), respectively. The values of R_1, R_2, (x_1,y_1), and (x_2, y_2) are sent to a master LV (note that LV_1 or LV_2 or even another LV may act as a master LV). After receiving the parameters, the master LV goes through the following procedure for each TV tower's coordinate in its database[1].

(1)Suppose that the two dimensional coordinate of the first TV tower is (u_1,v_1). The master LV calculates the reference distance ratio as:

$$\rho = \sqrt{\frac{(x_1-u_1)^2+(y_1-v_1)^2}{(x_2-u_2)^2+(y_2-v_2)^2}} \cdots\cdots\cdots\cdots (2)$$

(2) The master LV calculates the measured distance ratio, given by the following equation, using the RSS measurements:

$$\rho' = \frac{d_1}{d_2} = \sqrt[4]{\frac{R_2}{R_1}} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (3)$$

where d1 and d2 are the respective distances between LV1 and the signal source and LV2 and the signal source.

(3) The master LV checks whether

$$\rho' \in \left[\frac{\rho}{1+\epsilon_1}, (1+\varepsilon_1)\rho\right] \cdots\cdots\cdots\cdots\cdots\cdots (4)$$

where $\varepsilon 1$ (> 0) is the expected maximum error; it includes both measurement error and modeling error.

If (4) does not hold, the location verification for the TV tower fails ; otherwise, it passes the location verification. The above steps are repeated using the coordinates of the next TV tower.(1)

Two instances occurs in DRT that are:

False negative instance: If an attacker is at a location that induces a similar distance ratio as that of an incumbent signal transmitter, the DRT may fail to recognize the signal as an attacker's signal.

False positive instance: If $\varepsilon 1$ is too small, DRT may mistakenly identify an incumbent signal as an attacker's signal, resulting in a false positive instance.

C .*The location theory of Time Difference of Arrival(TDOA) and Frequency Difference of Arrival(FDOA).*

Another localization strategy was suggested by first applying the Time Difference of Arrival (TDOA) method and then the Frequency Difference of Arrival (FDOA).[3]

(a)The localization theory of TDOA

In TDOA the location verification of fixed transmitters are calculated with the help of positioning equations. There are usually three receiving stations. Assuming the location of the target is (*x*, *y*, *z*) and its distances to the central station(x_o,y_o,z_o) and the receiving stations (x_i,y_i,z_i) are r_o and r_i respectively, with the distance difference (known) of Δr_i (i =1,2,3) , the positioning equations are given by 5,6,7.

$$r_o^2 = (x-x_0)^2 + (y-y_o)^2 + (z-z_o)^2 \cdots\cdots\cdots\cdots\cdots (5)$$

$$r_i^2 = (x-x_i)^2 + (y-y_i)^2 + (z-z_i)^2, i = 1,2,3 \cdots\cdots\cdots\cdots\cdots (6)$$

$$\Delta r_i = r_i - r = c \times (t_i - t_o) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (7)$$

First of all, regard r_1,r_2,r_3 as known, we can obtain x, y, z expressed by r_i according to the sixth equation, then take x, y, z to the fifth equation to get the relationship between r_o and r_i. Finally, combines the relationship with the seventh equation to get two equations respectively. We can obtain (x_i,y_i,z_i) to achieve positioning.

b) The localization theory of FDOA

In FDOA, target is in motion so frequency changes. That frequency is called as Doppler frequency.[3]

Set the location of the target T to be (*x*, *y*, *z*) , the central station O (0,0,0) and the sounding station S_i (x_i,y_i,z_i) (i = 1,2,3) .So the direction cosine vector OT is given by equations 8,9,10 as:

$$\cos\alpha = \frac{x}{\sqrt{x^2+y^2+z^2}} \cdots\cdots\cdots\cdots\cdots (8)$$

$$\cos\beta = \frac{y}{\sqrt{x^2+y^2+z^2}} \cdots\cdots\cdots\cdots\cdots (9)$$

$$\cos\gamma = \frac{z}{\sqrt{x^2+y^2+z^2}} \cdots\cdots\cdots\cdots\cdots (10)$$

We assume that the target moves along a straight line at a fixed speed of $v = vx\cos\alpha', vy\cos\beta', vz\cos\gamma'$where $\cos\alpha', \cos\beta', \cos\gamma'$is the direction cosine of v .Thus the direction cosine of angle□ θ between vector OT and v□□is $\cos\theta = \cos\alpha.\cos\alpha' + \cos\beta.\cos\beta' + \cos\gamma.\cos\gamma'$

For the sounding station S_1,

OS_1 □□{x $_1$, y $_1$,z $_1$} and S_1T={x-x_1,y-y_1,z-z_1},

So the direction cosine of vector of OT $(\cos\alpha_1, \cos\beta_1, \cos\gamma_1)$ can be given by:

$$\cos\alpha_1 = \frac{x-x_1}{\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2}} \cdots\cdots\cdots\cdots\cdots (11)$$

$$\cos\beta_1 = \frac{y-y_1}{\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2}} \cdots\cdots\cdots\cdots\cdots (12)$$

$$\cos\gamma_1 = \frac{z-z_1}{\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2}} \cdots\cdots\cdots\cdots\cdots (13)$$

And the direction cosine of angle θ_1 □between vector S_1T and v is

$$\cos\theta_1 = \cos\alpha_1.\cos\alpha' + \cos\beta_1.\cos\beta' + \cos\gamma_1.\cos\gamma' \cdots\cdots (14)$$

Assume that the target's emitting signals with frequency f and wavelength λ for the central station O, the received frequency f_0 is given by:

$$f_o = f + f_{do} = f + \frac{v}{\lambda}\cos\theta \cdots\cdots\cdots\cdots\cdots\cdots (15)$$

where f_{do} is the Doppler shift, θ□is the angle between the connection of the transmitter to the receiver and the motion direction of the target. For the sounding station s_1, the received frequency $f_1$is given by,

$$f_1 = f + f_{d1} = f + \frac{v}{\lambda} cos\theta_1 \cdots\cdots\cdots\cdots\cdots\cdots (16)$$

Where f_{d1} is the Doppler shift, θ_1 is the angle between the vector S_1T and v.

Doppler frequency shift between central station O and the sounding station S_1can be expressed as[16],

$$\Delta f_{d01} = f_{d0} - f_{d1} = \frac{v}{\lambda}(cos\theta - cos\theta_1)$$

$$= \frac{v}{\lambda}[(cos\alpha - cos\alpha_1).cos\alpha' + (cos\beta - cos\beta_1).cos\beta' + (cos\gamma - cos\gamma_1).cos\gamma' \cdots (17)$$

And for the sounding stations S_2 ,S_3 Doppler frequency shift between them and the central station O can be expressed respectively as,

$$\Delta f_{d02} = f_{d0} - f_{d2} = \frac{v}{\lambda}(cos\theta - cos\theta_2)$$

$$= \frac{v}{\lambda}[(cos\alpha - cos\alpha_2).cos\alpha' + (cos\beta - cos\beta_2).cos\beta' + (cos\gamma - cos\gamma_2).cos\gamma' \cdots (18)$$

$$\Delta f_{d03} = f_{d0} - f_{d3} = \frac{v}{\lambda}(cos\theta - cos\theta_3)$$

$$= \frac{v}{\lambda}[(cos\alpha - cos\alpha_3).cos\alpha' + (cos\beta - cos\beta_3).cos\beta' + (cos\gamma - cos\gamma_3).cos\gamma' \cdots (19)$$

Combining equations (17), (18) and (19), the location of the transmitter (x, y, z) can be obtained.

IV. PROPOSED ALGORITHM

The proposed algorithm is implement in GUI in MATLAB

- Deploy N1 number of transmitter nodes and N2 number of receiver nodes in an area.
- Deploy M number of LVs (location verifiers). LVs will have all the information about the authentic users, so it can differentiate between a good node or bad node.
- Deploy O number of attackers in the area.
- Now total number of transmitters=N1+O
- Select a transmitter at random from this set of transmitters without knowing about the possibility of it being a healthy or faulty one.
- This transmitter will transfer information to a receiver of our choice
- In the way, it has to meet some LVs, where the verification process will be done.

V. SIMULATION SETTINGS AND RESULTS

A. *FOR DRT:*

The whole scenario is taken for the TV bands in which we are taking two frequencies: VHF(Very high frequency) having channels from 2-13 ,Bandwidth of 6MHZ and frequency range from 54-216 MHZ AND UHF(Ultra high frequency) having channels from 14-83,Bandwidth of 6MHZ and frequency range from 470-890MHZ. DRT is performed by taking the visualization scenario in which we are taking placements in which primary user, secondary user, receivers and attackers are in actual placement and senders ,receivers and location verifiers(slave and master location verifiers)in practical placement which is shown as:

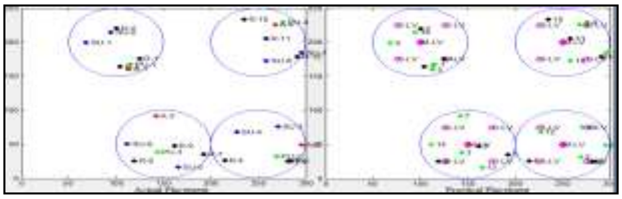
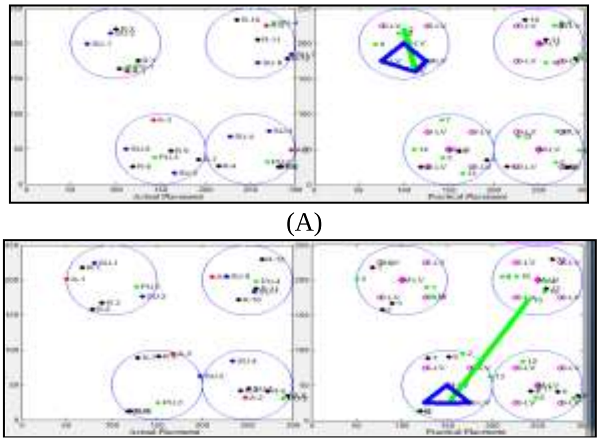


Fig.4 Actual and Practical Placement

Explanation of placements: In this scenario we are taking 4 circles as 4 areas or zones. In actual placement each zone consist of 1 primary user,2 secondary users, 3 receivers and 1 attacker. In practical placement each zone consist of 16 senders(shown by green dots) ,12 receivers(shown by black dots) ,4 slave location verifiers(LV's) and 1 master location verifiers(LV's).

Sending information through DRT: Consider the case of sending information in VHF for channel no.2.



(A)

(B)

Fig.5 : (A) Sending information in same zone, (B) Sending information in different zone

Case 1: Information send in the same zone as shown in the fig.5(A) we consider the case in which sender is node 5 and receiver is node 2.Value of Rho and Rhodash for the case of node 5 to node 2 data transfer comes out from the equation 2 and 3 is Rho=0.46782 and Rhodash=0.46782.

Case 2 : Information send in different zone as shown in the fig.5(B) we consider the case in which sender is node 3 and receiver is node 10.Value of Rho and Rhodash for the case of node 3 to node 10 data transfer comes out from the equation 2 and 3 is Rho=0.87276 and Rhodash=0.87276.

Graph between False negative ratio and measurement and modeling error:

Fig.6 show the simulation result for DRT. The false negative ratio is plotted as a function of the error value. As expected, the increase in the number of LVs caused a decrease in the false negative ratio. The results indicate that the location of the attacker's transmitter relative to the primary signal transmitter has a noticeable impact on the false negative ratio.

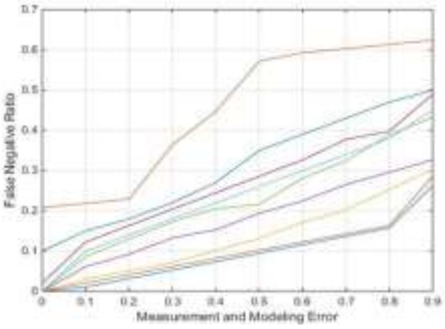


Fig.6 Graph between false negative ratio and measurement and modeling error.

B For TDOA and FDOA:

The positioning result of the target by using FDOA has higher accuracy than that of TDOA. Thus a lot of Position Location Systems prefer to use FDOA. Furthermore, we consider combining FDOA with TDOA to locate the target in this paper. FDOA is based on the velocity and moving direction of target and TDOA estimates speed of the target by estimating the location of highlight in target movement. Therefore, we can estimate the direction of target movement by TDOA, and then modify the result of TDOA by FDOA.

Time difference of arrival(TDOA):

Location Model for TDOA:

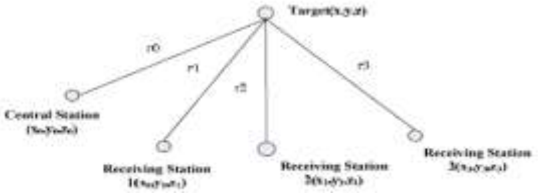

Target(x,y,z)
r0
r1
r2
r3
Central Station (x0,y0,z0)
Receiving Station 1(x1,y1,z1)
Receiving Station 2(x2,y2,z2)
Receiving Station 3(x3,y3,z3)

Fig.7 Model of TDOA

TDOA is used to find location of the target which is at fixed location and also to find the user which may be primary user, secondary user or attacker which is the primary user emulation(PUE) attack.

TDOA is performed by taking the visualization scenario in which we are taking placements in which primary user, secondary user, receivers and attackers are in actual placement and senders ,receivers and central station in practical placement which is shown as:

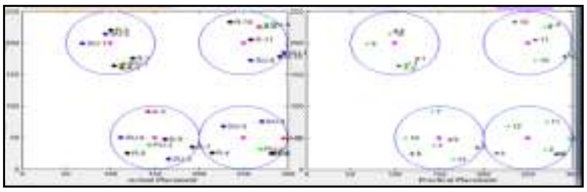
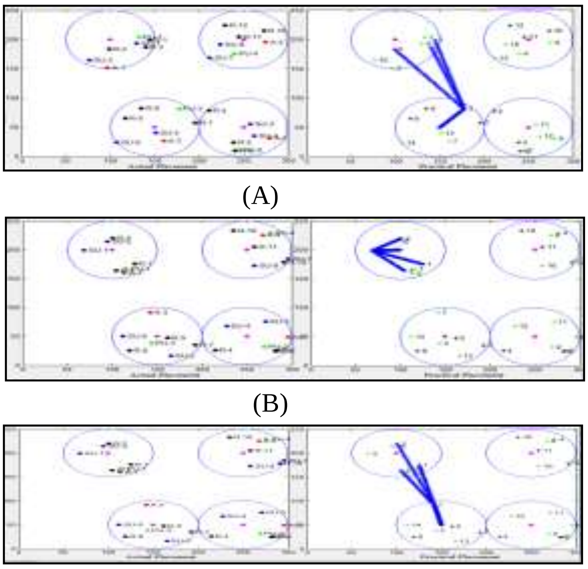


Fig.8 Actual and Practical placement

Explanation of placements**:** In this scenario we are taking 4 circles as 4 areas or zones. In actual placement each zone consist of 1 primary user,2 secondary users, 3 receivers and 1 attacker. In practical placement each zone consist of 16 senders (shown by green dots) ,12 receivers(shown by black dots) and 4 central stations(pink dots).

Sending information through TDOA:

Consider the case of sending information in VHF for channel no.2.In TDOA 3 cases are shown to find the location of target and to find the user.



(A)

(B)

(C)

Fig.9 : (A) Detection of primary user , (B) Detection of secondary user , (C) Detection of Attacker

Case 1: Information send in the zones to find location of target and detect that it is a primary user as shown in the fig.9(A) we consider the case in which the target is 3 and receiving stations are 1,2,3. Location of the target is (1.7749,0.8173).

Case 2: Information sends in the zones to find location of target and detect that it is a secondary user as shown in the fig.9(B) we consider the case in which the target is 9 and receiving stations are 1,2,3. Location of the target is (0.68687,1.9898).

Case 3: Information sends in the zones to find location of target and detect that it is attacker as shown in the fig.9(C)we consider the case in which the target is 7 and receiving stations are 1,2,3. Location of the target is (1.4218,0.91574).

Calculating the time difference of arrival for 16 targets for the same receiving stations 1,2,3.

	Target 1	Target 2	Target 3	Target 4
T0	4.7892	7.9043	5.9914	6.6727
T1	1.6371	1.7072	1.3649	1.1309
T2	6.9462	2.1382	2.0594	6.1855
T3	2.7893	1.621	1.3774	9.8725
	Target5	Target6	Target7	Target8
T0	1.8351	1.161	5.1225	6.5468

T1	6.8327	2.0939	1.5484	1.1112
T2	2.7026	2.2269	2.0612	6.115
T3	6.7077	1.9557	1.4838	9.6675
	Target9	Target10	Target11	Target12
T0	4.8904	1.1061	3.2924	7.388
T1	5.6734	4.6324	1.8338	1.4934
T2	6.7658	3.2925	2.0978	1.8713
T3	6.5857	4.378	1.7132	1.3916
	Target13	Target14	Target15	Target16
T0	5.0707	1.6424	1.657	6.0409
T1	1.3579	1.0357	1.3521	1.232
T2	2.0266	1.594	1.1158	7.4311
T3	1.3553	9.7935	1.1878	1.0831

Table1 :Time Difference of Arrival of TDOA.

Frequency difference of arrival(FDOA):

Location Model for FDOA:

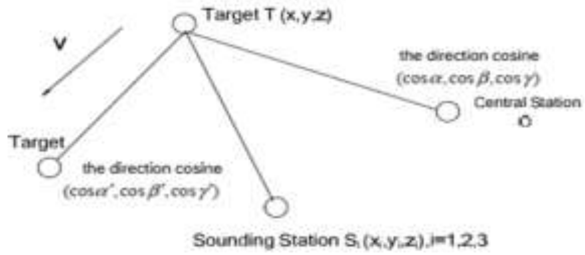


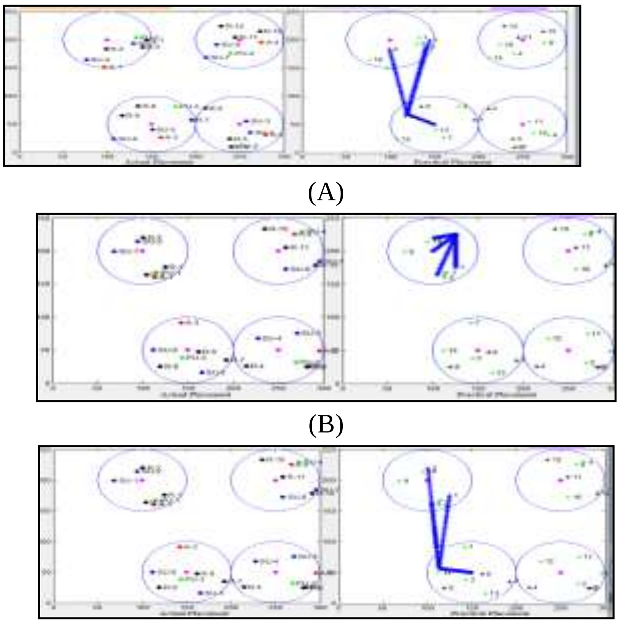
Fig.10 Model of FDOA

FDOA is used to find location of the target which is in motion and also to find the user which may be primary user, secondary user or attacker which is the primary user emulation(PUE) attack.

The placement scenario is same as TDOA.

Sending information through FDOA:

Consider the case of sending information in VHF for channel no.2.In FDOA 3 cases are shown to find the location of target and to find the user.



(A)

(B)

(C)

Fig.11: (A) Detection of primary user , (B) Detection of secondary user, (C) Detection of Attacker

Case 1: Information send in the zones to find location of target and detect that it is a primary user as shown in the fig.11 (A) we consider the case in which the target is 3 and receiving stations are 1,2,3. Location of the target is (1.189,0.68678).

Case 2: Information sends in the zones to find location of target and detect that it is a secondary user as shown in the fig.11 (B) we consider the case in which the target is 9 and receiving stations are 1,2,3. Location of the target is (1.2572,2.2537).

Case 3: Information sends in the zones to find location of target and detect that it is attacker as shown in the fig.11(C) we consider the case in which the target is 7 and receiving stations are 1,2,3. Location of the target is (1.1299,0.56882).

Calculating the frequency deviation for 16 targets for the same receiving stations 1,2,3.

	Target1	Target2	Target3	Target4
Δf_{d01}	1.9588	0.24456	1.131	0.15585
Δf_{d02}	1.8425	0.33936	1.3748	0.1598
Δf_{d03}	1.5886	0.29634	1.0141	0.286
	Target5	Target6	Target7	Target8
$\Delta\square_{\square 01}$	1.9844	0.59487	0.75683	0.23829
$\Delta\square_{\square 02}$	1.7932	0.74733	1.0672	0.30956
$\Delta\square_{\square 03}$	1.5974	0.60194	0.70333	0.43067
	Target8	Target10	Target11	Target12
$\Delta\square_{\square 01}$	1.9535	-0.0027	0.40178	0.55411
$\Delta\square_{\square 02}$	1.8184	0.89389	0.53239	0.70991
$\Delta\square_{\square 03}$	1.5888	1.0443	0.42292	0.57554
	Target13	Target14	Target15	Target16
$\Delta\square_{\square 01}$	1.0701	0.99256	0.19683	0.13139
$\Delta\square_{\square 02}$	1.315	1.2339	0.20067	0.13119
$\Delta\square_{\square 03}$	0.90056	0.83456	0.39498	0.24816

Table 2:Frequency Deviation of FDOA in Hz

Calculating direction cosine of target movement for 16 targets for the same receiving stations 1,2,3

	Target 1	Target 2	Target 3	Target 4
Cosα'	0.46424	0.97989	0.91623	0.81522
Cosβ'	0.88571	0.19952	0.19952	0.57916
	Target 5	Target 6	Target 7	Target 8
Cosα'	0.54215	0.92865	0.95959	0.8191
Cosβ'	0.84028	0.37095	0.28142	0.57365
	Target 9	Target10	Target11	Target12
Cosα'	0.62145	0.39851	0.9814	2.3111
Cosβ'	0.78346	0.91716	0.19195	0.92338
	Target13	Targe14	Target15	Target16
Cosα'	0.99175	0.99703	0.76371	0.82727
Cosβ'	0.12816	0.076997	0.64556	0.5618

Table3:Direction cosine of Target movement

VI. CONCLUSION AND FUTURE WORK

PUE attack is a major threat to the wireless technology. In this paper,firstly transmitter verification procedure based on location verification is done through Distance Ratio Test in which we take two placement scenarios(actual and practical).Simulation results includes the parameter False Negative Ratio(FNR).Next we proposed a joint position verification method against PUE attack in CR networks which includes TDOA and FDOA .We consider the scenario in which we can easily detect the user whether it is primary user, secondary user or an attacker. Various parameters are calculated that are time difference of arrival, frequency deviation and direction cosine for the target movement, Simulation results show that our method can improve the localization accuracy, which strengthens the ability to resist PUE attack. Immediate extensions to our approach consist of the following aspects. First, we will implement the proposed approach in software defined radio and test it in real network environments. Second, we will extend our approach to the environments in which more reference senders could be malicious. Finally, we will investigate using physical layer network coding to detect other attacks on wireless networks. Extension of our approach to determine the lower bounds for the probability of successful PUEA in systems deploying other spectrum sensing mechanisms described in [2] is a topic for further investigation.

VII. ACKNOWLEDGMENT

Thanks to my guide and family members who always supported me helped and guided me during my dissertation. I would like to thank the MATLAB authors for providing the Graphic User Interface for the research work.

REFERENCES

[1] Ruiliang Chen and Jung-Min Park “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks”IEEE Department of Electrical and Computer Engineering, august2006.

[2] S. Anand, Z. Jin and K. P. Subbalakshmi “An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks” Department of Electrical and Computer Engineering Stevens Institute of Technology,2008

[3] Lianfen Huang, Liang Xie, Han Yu, Wumei Wang, Yan Yao “Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks”IEEE International Conference on Communications and Mobile Computing,2010.

[4] Deepraj S. Vernekar “An Investigation Of Security Challenges In Cognitive Radio Networks” Dissertations & Student Research in Computer Electronics & Engineering,december2012.

[5] Parastoo Razavi, Reza Berangi “Reducing Attack Effectiveness in Cognitive Radio Networks” Majlesi Journal of Electrical Engineering,vol.6,No.4, December2012.

[6] http://en.wikipedia.org/wiki/Spectrum_management.

[7] Deepa Das, Susmita Das “Primary User Emulation Attack in Cognitive Radio Networks: A Survey” International Journal of Computer Networks and Wireless Communications , vol.3,No.3, June 2013.

[8] Priti H. Jadhao “ Cognitive Radio Network : A Review” International Journal for Engineering applications and Technology,October2013.

[9] Shikha Jain,Anshu Dhawan andC.K Jha “Emulation Attack In Cognitive Radio Network :A Survey” International Journal of Computer Networks and Wireless Communications.vol.4.No.2,april2014.