Detection Threats and Mitigation Techniques in Cognitive Radio based on Localization of Signal Source and Trustworthiness

Mahmod Ammar[1], Nick Riley[2], Meftah Mehdawi[3], Anwar Fanan[4], and Mahsa Zolfaghari[5]

Abstract— the 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. In the conventional spectrum management paradigm, most of the spectrum is allocated to licensed users for exclusive use. 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. The successful deployment of CR networks and the realization of their benefits will depend on the placement of essential security attributes in sufficiently robust form to resist misuse of the system. Improving trustworthiness among nodes in CR is a particularly important problem that needs to be addressed. The key to addressing this problem is being able to distinguish primary user signals from secondary user signals in a robust way, However, the secondary user ability to sense and exploit the spectrum in the cognitive radio network imposes some threats and provides an opportunity for some malicious users to intrude the network and disrupt the performance of cognitive radio spectrum sensing [1].

Our technique for threat detection is based on the localization of signal Source, the proposed scheme takes advantage of the fact that it is not possible for the malicious user to mimic both the coordinates and the power level of the primary user, so we can verify the transmitter based on the distance measured on basis of coordinates and received signal power level. The algorithm of our work has clarified the problem of verification to identify the level of trust for all three types of users, i.e. primary, secondary, and the malicious user. Simulation result proved that the trustworthiness of the primary user is much higher than the malicious user.

Also we have presented a scheme which is based on trust and penalty for secure spectrum access in cognitive radio networks, the technique estimates the distance of a user in terms of both the location coordinates and received power level, by verifying distance values, trusted values are evaluated and assigned to each SU , the SU executes spectrum sensing by itself and sends the local spectrum sensing information to a FC (Fusion Centre) , then The FC makes the final decision about the presence of the primary user using the majority rule and the trust weights of the nodes.

Keywords---Cognitive Radio; Secondary user; Primary User Emulation Attack (PUEA); Fusion Center.

Mahmod Ammar[1], School of Engineering, University of Hull ,Hull, UK.
Nick Riley[2], School of Engineering, University of Hull , Hull, UK.
Meftah Mehdawi[3], School of Engineering, University of Hull, Hull, UK.
Anwar Fanan[4], School of Engineering, University of Hull, Hull, UK.
Mahsa Zolfaghari[5], School of Engineering, University of Hull, Hull, UK.

I. Introduction

IN the process of wireless communication technology development, the growing business demands are restricted by the limited spectrum resource. The Federal Communications Commission (FCC) suggests that currently spectrum scarcity is largely due to the inefficient and rigid regulations rather than the physical shortage of the spectrum [2]. Recently, cognitive radio network (CRN) has been brought to the forefront due to its potential to solve the conflict between limited spectrum supply and spectrum demand from ever-increasing wireless applications and services, which is defined as a wireless network employing technology to obtain knowledge of its operational and geographical environment, established policies, and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve end-to-end network objectives; and to learn from the results obtained [3].

Because CRNs are an open and random access network environment, where the unlicensed secondary users (SUs) can use the channels that are not currently used by the licensed primary users (PUs) by spectrum-sensing technology. Therefore, they not only face all the security threats in the traditional wireless networks, but also new security threats that have arisen due to their unique cognitive characteristics, such as the following:

Primary user emulation attacks (PUEA): In this type of attacks, attackers may transmit at forbidden time slots and effectively emulate the primary user to make the protocol compliant SUs erroneous conclusion that the primary user is present.

Spectrum sensing data falsification attacks (SSDF): Attackers send false observation information, intentionally or unintentionally, to the fusion centre (FC), and let the FC make the wrong decision. PUEA and SSDF attacks focus on the physical layer of a CRN. Furthermore, these could also make MAC layer threats-vulnerabilities and IEEE 802.22 specific threats, cross-layer attack that adversaries can launch attacks targeting multiple layers.

In practice, several drawbacks make local sensing difficult. Such drawbacks include severe multipath fading, shadowing, or the secondary user inside buildings with penetration loss. As a result, the secondary user may not detect the presence of

the primary user, and so accessing the licensed band and causing interference to the primary user.

This paper works on the ensuring the trustworthiness among nodes in CR networks. It implements a mitigation technique for PUEA that does not rely on examination of pdf; rather on localization of signal source. A security algorithm for transmitter verification scheme based on two parameters (distance and received signal power level) is proposed in order to identify the primary and malicious users.

Moreover, In order to mitigate the problem of uncertainty in spectrum sensing in a cognitive radio network, cooperative spectrum sensing can be used. Different techniques were proposed for cooperative spectrum sensing. The simplest method is to use an OR or AND operation among the received sensing results [4]. Combing techniques based on maximal ratio combining (MRC) and equal gain combining (EGC) were investigated in [5], an optimal linear cooperation scheme base on a likelihood ratio test (LRT) has been proposed in [6]. In [7], the censor-based cooperative spectrum sensing has been proposed to save energy. And a censor-based cooperative spectrum sensing scheme using Takagi and Sugeno's (T-S) fuzzy logic for cognitive radio sensor networks was proposed in [8]. But in our scheme, a cooperative spectrum sensing scheme based on trust and majority rule for CRSN is proposed, the nodes make local decisions on the presence or absence of the primary user's (PU) signal, and then the FC makes the final decision. This method can improve the sensing performance while saves the node's energy.

We have divided this paper into two phases as follow

PHASE 1:- PROPOSED APPROACH FOR PUEA DETECTION BASED ON LOCALIZATION OF SIGNAL SOURCE

Because it is not possible for the malicious user to mimic both the coordinates and the power level of the primary user, we can verify the transmitter based on the distance measured on basis of coordinates and received signal power level.

In the proposed scheme, we calculate the trustworthiness of the users in the network. Malicious user and misbehaving node can masquerade as the primary user and provide false information to the secondary user regarding occupancy of the spectrum that causes maximum interference and minimum spectrum utilization. Our transmitter verification scheme depend on two parameters-:

Distance Calculated based on the location coordinates

Distance measured based on received power level

Cognitive radio (CR) user has the capability to sense the primary user location, Primary user broadcast the location information to all CR users. A CR user calculates the distance between the secondary user and the primary user based on the two parameters mentioned above. If the distance calculated with both these techniques is match then verify that transmitter is a legitimate user otherwise it's a malicious user. Figure 1 shows the verification process of the primary user and malicious user.

1.1 Security Algorithm

In our technique, the source of the spectrum information is validated , we propose a transmitter verification procedure for spectrum sensing that is appropriate for hostile environments; the transmitter verification procedure is illustrated in Figure 5.1 below. The distinguishing feature of this transmitter verification procedure is that it determines the legitimacy of a given signal source using the signal source's location. If the distance which calculated with two techniques is match then the user is a trustworthy user. In other case, it would be considered malicious user.

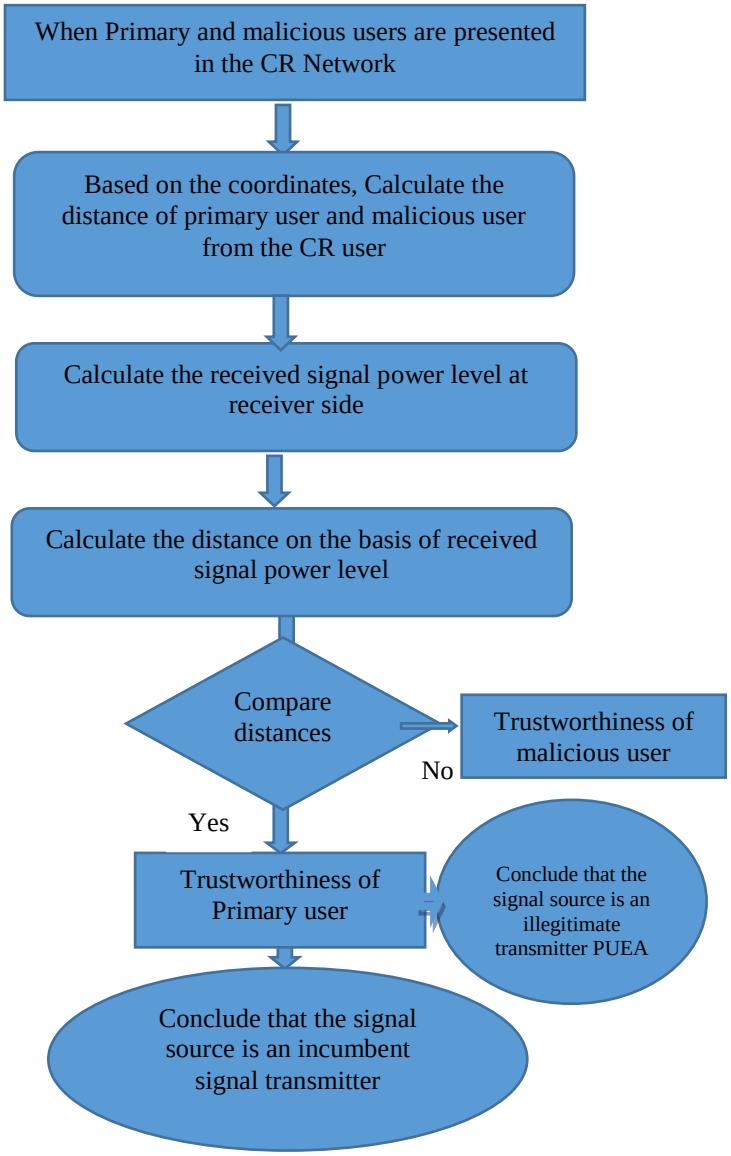

Fig. 1 Proposed PUEA detection algorithm employing the calculation of location based on coordinates as well as received power level

The CR network follow the above steps, One condition applies to the system that if the distance match then it's concluded that the signal source is an incumbent signal otherwise it's an illegitimate transmitter.

1.2 Distance Calculate Based on the Location Coordinates

Distance between the users can be calculated on the basis of the location coordinate. Consider the (x, y) is x and y coordinates of the cognitive user and (x_1, y_1) is x and y coordinates of the primary user. The distance between the cognitive user and the primary user, D, can be calculated by using following equation

$$D = \sqrt{\{(x - x_1)^2 + (y - y_1)^2\}} \quad 1$$

In our simulation assumption, all users broadcast their location coordinates. With this information, distance between any users can be computed.

1.3 Distance measured based on received power level

The whole idea of distance measurement by means of received signal strength (RSS) or received power level is based in ideal case on the assumption that the received power level is a function of the transmitting power and distance on the path between two radio devices. The distance between the secondary and other users can be calculated by measuring the received power level with a known transmitted power level. The received power level P_r with a given transmit power P_t is given by the equation as below

$$P_r = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \quad 2$$

When

P_t	h_t, h_r	G_t, G_r	L	D
Transmit power level	Height of transmitter and receiver.	Transmitter and receiver gain	System loss factor	Distance between transmite and receiver

WE consider h_t, h_r,G_t,G_r and L are constant and equal to one. Therefore, the received power level will depend on the transmit power level and distance:

$$P_r = \frac{P_t}{d^4} \quad 3$$

Distance between the user can be estimated based on the received power level as in the below equation, given the transmit power level is known.

$$D = \sqrt[4]{\frac{P_t}{P_r}} \quad 4$$

The distance calculated using the received power may not be 100% accurate due to the noise level and the impact of channel impediments and some other uncertainties caused by the signal propagation environment. However, many researchers still use the received power level based measurement method because of its simplicity and cost efficiency.

- **Ideal and actual received signals**

The ideal received power P_r is given by

$$P_r(ideal) = \frac{P_t}{d^4} \quad 5$$

The actual received signal power can be calculated as follow

$$P_r(Actual) = \frac{P_t + \text{noise\_power}}{d^4} \quad 6$$

When P_t is the transmitted power, d is the distance between the transmitter and receiver and noise_power is the noise signal power,

1.4 Relative Trustworthiness of the User

As we mentioned in previous sections it is not possible for the malicious user to mimic both the coordinates of primary user and the power level, in our technique, let us consider d_1 is the distance between a cognitive user and other users is calculated based on location coordinates and d_2 is the distance calculated based on received power level. So the relative trustworthiness X of a user is given by

$$X = \min\left(\frac{d_1}{d_2}, \frac{d_2}{d_1}\right) \quad 7$$

Where min function returns the minimum value of the equation elements.

In other words if the distance calculated with both techniques (d_1 and d_2) matches, then the user is a trustworthy user. In other case, it would be considered a malicious user. Based on the noise level, the distance calculated with received power level may not be very accurate. However, statistically, the distance calculated with both of the methods should come close. The trust value is expected to be close to 1 for trustworthy users and low for untrustworthy users.

1.5 Simulation Results and Analysis for phase 1.

In this section, the simulation results for the detection scheme based on localization with the existence of PUEA are explained.

Figure 2 shows the distance measured based on coordinates and the distance measured based on received power level of the primary user from the secondary user. We can see that both distance measurements matches considerably; that is an indication that the secondary user is actually communicating with a trusty user.

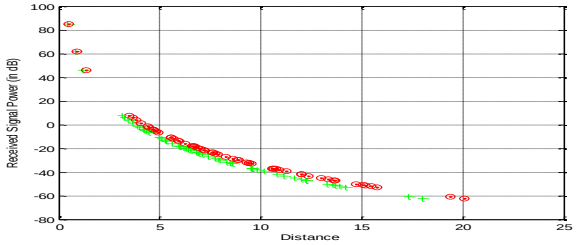

Fig. 2 OOO the distance measured based on coordinates and +++the distance measured based on received power level of the primary user from the secondary user

As we can see from Figure 3 below that shows the trustworthiness of the primary user and malicious user respectively with respect SNR value. When the SNR value increase, correspondingly trustworthiness of the user increases. Trustworthiness of the primary user reach about 100 % value; it means high level of trust and communicates

with primary user. When increase the SNR value trustworthiness constant at about 100 % value, because trustworthiness of the primary user always has higher value.

On another hand, trustworthiness of the malicious user remains constant at around 0.5 % even if the SNR value increases. Malicious user has lower level of trust value as compare to the higher trust value (nearly 100 %) trustworthiness of the primary user.

So it is clearly observed from the plot that the algorithm gives better protection and provide trust management for both types of user (primary and malicious).

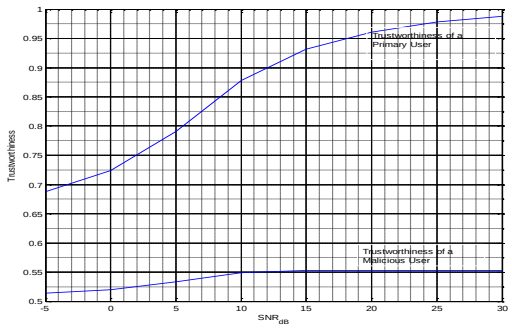

Fig. 3 Trustworthiness of the primary and malicious users

- **Different SNR influence.**

Figures 4, 5 and 6 below show the received power decreases over distances. However, based on different SNR levels, the ideal and actual received power are compared as shown in graphs (ideal and actual received signal power is calculated as mentioned in preview sections. In Figure 4 when SNR=15dB value, there is more noise, the received signal power decreases at the receiver side and signal distortion is very high. When SNR=20dB (increased), the noise level decreased so there is still some different between the actual and ideal received signal as in Figure 5. But when the value of SNR increased to be 25db, it seems like there is no noise level, from this we can conclude that greater the value of SNR, the noise level decreases and ideal and actual received signal power are identical as we can see from Figure 6.

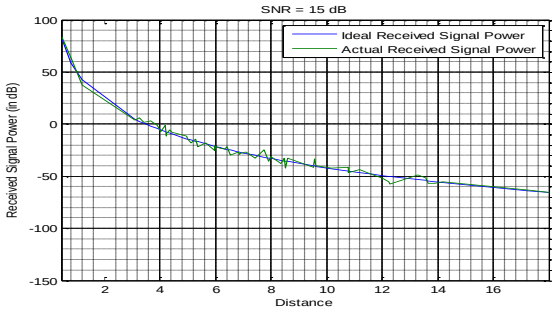

Fig. 4 Received power Vs distances when SNR=15 db

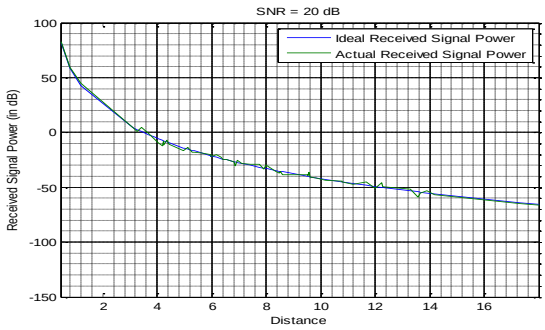

Fig. 5 Received power Vs distances when SNR=20 db

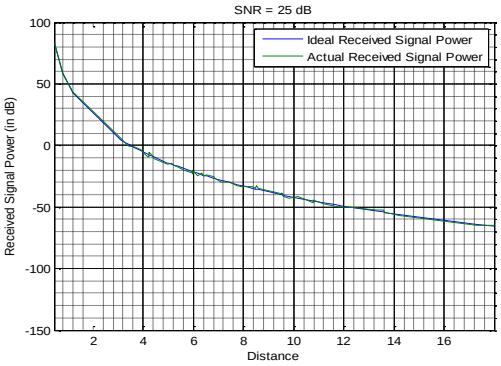

Fig. 6 Received power Vs distances when SNR=25 db

PHASE 2:- TRUST BASED ALGORITHM FOR SECURE SPECTRUM ACCESS IN COGNITIVE RADIO NETWORKS

Different from traditional wireless networks, the reliable spectrum sensing in CR is an important step for any practical deployment. SUs should identify the presence of PUs over wide range of spectrum accurately without significant delay. This process is very difficult as we need to identify various PUs adopting different modulation schemes, data rates and transmission powers in presence of variable propagation losses, interference generated by other secondary users and thermal noise. Traditionally there are three spectrum sensing techniques, which are, energy detection, matched filter detection and cyclostationary feature detection [9]. If SUs are lack of knowledge about the characteristics of PU signal, energy detection is the optimal choice with the least complexity and generally adopted in recent research work. However, the performance of energy detection is always degraded because of signal-to-noise ratio wall or channel fading/shadowing Sus can cooperate to increase the network performance, cooperative spectrum sensing has been shown to greatly increase the probability of detecting the PUs [10-12]. Each SU executes spectrum sensing by itself and sends the local spectrum sensing information to a FC (Fusion Centre) which uses an appropriate data fusion technique to make final spectrum sensing decision.

2.1 The Trust values and penalty scheme

A trust factor is assigned to each user Su_i, A higher trust value indicates a higher probability that Su_i is a normal user. Hence the user that has a high trust factor should contribute more to the final decision. Therefore trust values are used as the weighting factor to calculate the weighted average of the

energy values obtained from the participating SUs. The final decision is made by comparing the weighted sum of the nodes' energy to a detection threshold. In this phase we have used the trust values we obtained in phase 1.

Unlike most existing approaches to cooperative sensing, in our cooperative spectrum sensing that uses a penalty scheme misbehaving users would be punished by FC by declining their trust value; thus, guaranteeing network security via distinguishing attack users . The trust values of users are equal to each other at the beginning. Once the user launches an attack, its trust value will change. The malicious users are severely punished due to their destruction to the network.

The FC can not only store the trust value of each user, but also punish the illegal users in CRNs. In case of collision between PUs and SUs, the PU system would be compensated and a penalty would thus be imposed on the SU system [13]. If all SUs follow the controller's spectrum-access policy and a collision occurs, all of them are responsible and share the ensuing penalty; otherwise, the penalty is imposed on the particular SU who violates the controller's allocation policy.

2.2 System model

In this section, the scenario of cooperative spectrum sensing in CRNs is described and the impact of the majority rule and trust weights is discussed.

2.2.1 Local Spectrum Sensing and Decision

In our simulation model we consider CRN that consists of one PU, n SUs, and one FC as illustrated in Figure 6.3 below. Mathematically, the spectrum sensing is obtained at each individual SU. We suppose each CRSN node using the energy detection. The hypotheses if the primary user is present (H_1) or not (H_0) are as follows:

$$x_i(t) = \begin{cases} n_i(t): & H_0 \\ s(t) + n_i(t): & H_1 \end{cases} \quad (8)$$

Where $x_i(t)$ is the received signal by the i^{th} node, $n_i(t)$ is the additive white Gaussian noise(AWGN) , and s(t) is the transmitted signal from the PU.

The local test static of the i^{-th} node using energy detection is:

$$x_{Ei} = \sum_{k=0}^{N-1} |x_i(k)|^2 \quad , i = 1,2,...,M \quad (9)$$

Where $x_i(k)$ is the k^{-th} sample of received signal at the i^{-th} node, M is the number of nodes, and N is the number of samples, N=2TW , where T and W are detection time and signal bandwidth, respectively[14].

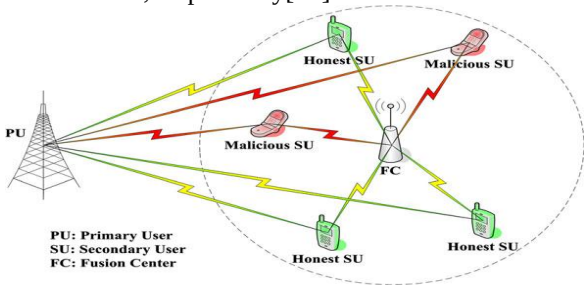

Fig. 7 Scenario model of cooperative spectrum sensing

Then the i^{-th} node detection energy x_{Ei} will be used to make the local decision Ld_i of the i^{-th} node. Ld_i =1 means the PU is present (h_1) and Ld_i =0 means the PU is absent (h_0). x_{Ei} can be approximated as a Gaussian random variable under both hypotheses H_0 and H_1 and denoted as [168]

$$\begin{cases} x_{Ei} \cong N(\mu_{0i}, \sigma_{0i}^2) & H_0 \\ x_{Ei} \cong N(\mu_{1i}, \sigma_{1i}^2) & H_1 \end{cases} \quad (10)$$

Where μ_{0i} , μ_{1i} , σ_{0i}^2 , σ_{1i}^2 are the means and variances under hypotheses H_0 and H_1, respectively.

SUs will then send their reports of the local spectrum sensing to FC for further processing. These reports can either be the received energy or a function of it (such as 1-bit hard decision), depending on the fusion rule adopted by the FC as we can see in sections below.

2.2.2 The mechanism flow

In this section, we explain our CSS scheme based on majority theory and trustworthiness degree in CRNs.

As shown in Figure 8, the CSS scheme is carried out in four successive steps, which are combining reports from different Sus, trustworthiness degree , imposing penalty , and then the decision is made based on the trust values of users .

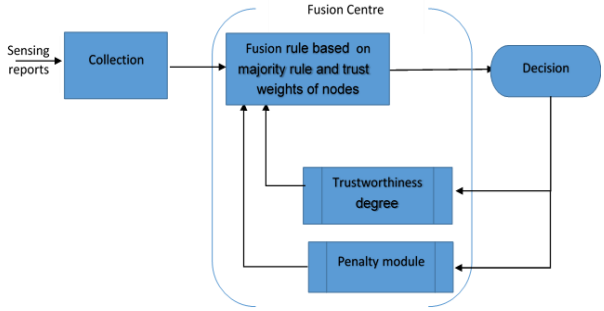

Fig. 8 the flow graph of the scheme

➢ **Distance based trust value evaluation technique**

In this section we will use the trust values obtained in phase 1, as we explained, the trust value of secondary users can be evaluated considering distance between a user and cognitive user. In this technique, distance is measured in terms of two criterions which are distance based on the location Coordinates d_1 and distance based on received power level d_2, thus the trust value of a user (X) is obtained as a relative value of d_1 and d_2 which was given as below:

$$X = MIN\left(\frac{d_1}{d_2}, \frac{d_2}{d_1}\right) \quad (11)$$

Where MIN function returns the minimum value of the equation elements.

➢ **Data Fusion at the FC**

The FC receives Ns local decisions from CRSN nodes. Based on the majority rule [15] and trust weights, the final decision fusion rule is:

$$H = \begin{cases} H_1 : \sum_{j=1}^{Ns} Ld_j T_j^n > 0 \\ H_0 \quad otherwise \end{cases} \qquad 12$$

Where Ld_j is the local decision of the j^{th} node,

T_j is the trust value of the j^{th} node.

And n is the penalty value imposed on the system.

The controller's decision (FC) is characterized by two hypothesis of the absence and presence, denoted as H_0 and H_1, respectively, of the primary user in the considered channel. Indicating that the decision of cooperative spectrum sensing is 0 or 1. In this approach, we adopted the majority sensing rule and trust scheme, which together make a strong and robust cooperative sensing rule characterized by its stringent protection on the primary activities.

2.3 Simulation Results and Analysis for phase 2

To evaluate the performance of the proposed cooperative spectrum sensing algorithm for CRN and to discuss its effectiveness on the detection probability, the Monte-Carlo simulations are carried out with 50,000 samples with various SNR. Also we have used different number of CRN nodes M and different number of malicious nodes in order to verify the scheme. The noise is assumed to be a Gaussian with zero mean and unit variance.

The simulation was run in Matlab and the same system environment is used as in chapter five, to study the impact of the system parameters on our scheme, we run the simulation with different values of penalty factors. We also consider various SNR values (-10, -5, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50). As we can see from figures below. The results show the performance of the scheme with the increase of the number of malicious nodes for different number of trustworthy users. The performance of spectrum sensing can be primarily described by two basic metrics: correct decision and wrong decision about the primary user present. We discuss how the varying of the number of untrustworthy users contributes to the final decision regarding the presence or absence of the PU.

Figure 9 below shows the trust metrics when the penalty factor is equal to 1, we can note that when SNR= -10 dB and the number of trustworthy users is equal to 20, then the number of malicious users must be less than 25 to make a correct decision.

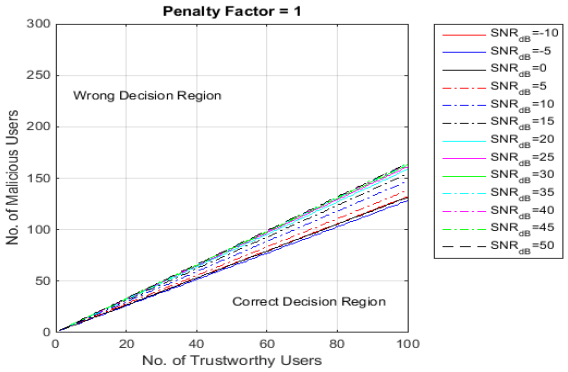

Fig. 9 Trust Metrics for Penalty Factor 1

There is no considerable difference even if we increase the SNR value and this is because the number of malicious users is higher than the number of trustworthy users and the penalty factor is too small.

But if we increase the penalty factor (set to 2), as can be seen in Figure 10, the boundary of correct decision region is increased in contrast with the above figure when the penalty factor was set to 1, As the value of SNR increases, the area of a correct decision is increased, for example, with the same penalty factor (2) we increased the SNR to be 50 dB, then a 20 trusty users can make a correct decision even if the number of malicious is 50.

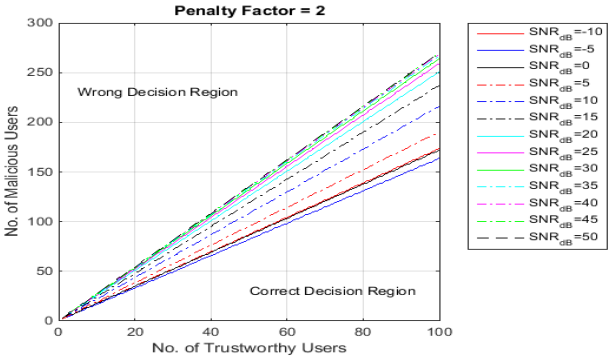

Fig. 10 Trust Metrics for Penalty Factor 2

When the penalty factor set to 3 as in figure 11, for 20 trusty users and 50 malicious users, a correct decision is achievable when SNR=-10 dB, however if we increase the SNR to 50 dB for example, the probability of correct sense is increased to allow 20 trusty users and about 100 malicious users to make the correct decision.

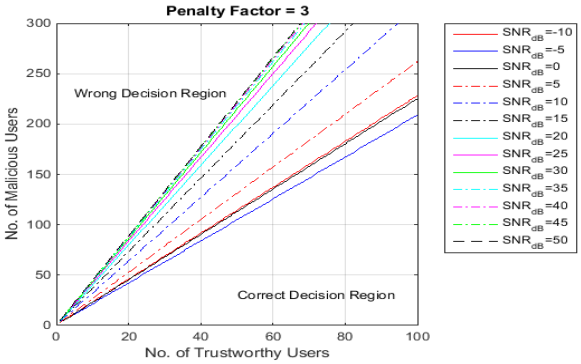

Fig. 11 Trust Metrics for Penalty Factor 3

For all SNR values, if we set the penalty factor a little bit higher (penalty factor=4), the correct decision boundary are dramatically increased as figure 12 shows.

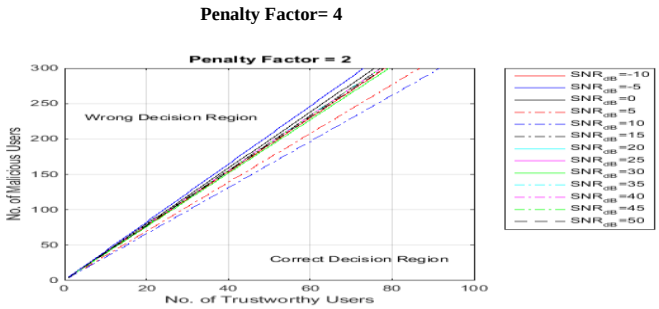

Fig. 12 Trust Metrics for Penalty Factor 4

Overall, higher SNR values yield better algorithm performance in terms of successfully classifying primary signals and PUE signals. Due to the punishment factor and the trust value computation that leads to a more accurate and effective primary user detection even with the existence of a large number of malicious nodes,

Table 1 shows trust metrics at a high SNR value (SNR=50), as the Penalty factor increases, the probability of making a correct decision increases.

TABLE 1
SUMMARY OF TRUST METRICS FOR DIFFERENT PENALTY FACTORS

	For SNR= 50		
Penalty Factor No.	**No. of Trustworthy User**	**No. of Malicious User**	**Decision**
1	20	25	wrong
2	20	40	correct
3	30	70	correct
4	40	100	correct

II. CONCLUSION AND FUTURE WORK

Conclusions: The Cognitive radio is deemed as an efficient solution to the spectrum scarcity problem by sensing the unused spectrum of the licensed users and providing that unused spectrum to the secondary users without causing any interference between primary user and the secondary user. Via cognitive radio it's achievable to increase the efficiency of the spectrum significantly. But the secondary user must make sure that the information regarding the occupancy of the spectrum is provided by a legitimate user. Thus the transmitter verification procedure for spectrum sensing is implemented to ensure the trustworthiness among nodes in CR networks, this mitigation technique for primary user emulation attack PUEA that does not rely on examination of pdf rather on localization of signal source. Our security algorithm for transmitter verification scheme based on two parameters (distance and received signal power level) has been developed in order to identify the primary and malicious users

Also we have presented a scheme which is based on trust and penalty for secure spectrum access in cognitive radio networks, the technique estimates the distance of a user in terms of both the location coordinates and received power level, by verifying distance values, trusted values are evaluated and assigned to each SU , the SU executes spectrum sensing by itself and sends the local spectrum sensing information to a FC (Fusion Centre) , then The FC makes the final decision about the presence of the primary user using the majority rule and the trust weights of the nodes. We have verified that this method can improve the sensing performance under the impact of different number of trustworthy and untrustworthy users in the CR network. Our simulation results show that the correct sense rate is safeguarded effectively and can improve the detection probability effectively even with the existence of a large number of malicious nodes.

Future Research Directions

The work in this theses can be extended to include:-

- Performance Evaluation of RSSI-Based Transmitter Identification using USRP: - In order to defence PUE attack experimentally, a hardware experiment using software defined radio is suggested, we propose a transmitter identified method based on RSSI of vary frequency to identify transmitters located in different positions. Using Universal Software Radio Peripheral (USRP) as the transmitter and receiver to verify the method in an indoor environment.

REFERENCES

[1] Chen, R. Park, J. Ensuring trustworthy spectrum sensing in cognitive radio networks. In Ist EEE workshop on networking technologies for software defined radio networks. 2006. P110-9. http://dx.doi.org/10.1109/sdr.2006.4286333

[2] K. Ben Letaief, W. Zhang, Cooperative communications for cognitive radio networks, Proceedings of the IEEE 97 (5) (2009) 878–893. http://dx.doi.org/10.1109/JPROC.2009.2015716

[3] W. Zhang and K. B. Letaief, "Cooperative communications for cognitive radio networks," Proceedings of the IEEE, vol. 97, pp. 878–893, May 2009. http://dx.doi.org/10.1109/JPROC.2009.2015716

[4] H. Ekram and B. V. K, Cognitive Wireless CommunicationsNetworks. Springer Publication, 2007.

[5] M. K. Simon and M.-S. Alouini, Digital communication over fading channels. John Wiley & Sons, Inc., 2 ed., Dec. 2004 http://dx.doi.org/10.1002/0471715220.

[6] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unkown signals over fading channels," in Proceedings of IEEE International Conference on Communications (ICC 2003), pp. 3575–3579, May 2003

[7] A. Ghasemi and E. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," Journal of Communications, vol. 2, no. 2, p. 71,2007 http://dx.doi.org/10.4304/jcm.2.2.71-82

[8] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, \Cooperative spectrum sensing in cognitive radio networks: A survey," Physical Communication, vol. 4, no. 1, pp. 40{62, Mar. 2011.

[9] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty, ―NeXt generation/dynamic spectrum access/cognitive radio wireless networks : A survey,‖ Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 50, Issue 13, September 2006, pp. 2127-2159.

[10] J. Unnikrishnan and V. Veeravalli, "Cooperative spectrum sensing and detection for cognitive radio, " in IEEE Global Telecommunications Conference, GLOBECOM, Nov. 2007, pp. 2972 –2976. http://dx.doi.org/10.1109/glocom.2007.563

[11] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments,"in Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN'05), Baltimore, USA, Nov. 2005, pp. 131–136. http://dx.doi.org/10.1109/dyspan.2005.1542627

[12] S. M. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in Proc. IEEE Int. Conf. Commun., Turkey, June 2006, vol. 4, pp. 1658–1663. http://dx.doi.org/10.1109/icc.2006.254957

[13] G. Ganesan and Y. G. Li, " Cooperative spectrum sensing in cognitive radio–part I: two user networks," IEEE Trans. Wireless Commun., vol. 6, pp. 2204–2213, June 2007. http://dx.doi.org/10.1109/TWC.2007.05775

[14] J Li , Z Feng , Z Wei, Z Feng and P Zhang, "Security management based on trust determination in cognitive radio networks", EURASIP Journal on Advances in Signal Processing ,PP. 01-16 ,2014,Vol. 2014:48.

[15] T.K.XUAN,I.KOO , "A Censor-Based Cooperative Spectrum Sensing Scheme Using Fuzzy Logic for Cognitive Radio Sensor Networks", IEICE Transctions on communications, Vol. E93-B, No.12, 2010, pp.3497-3500