Improving Detection Performance of Low-Cost Cognitive Radio Networks

تحسين الاداء للشبكات الذكية ذات التكلفة الاقتصادية

Mahmoud Ammar, Faculty of Engineering, Zawia University, m.ammar @zu.edu.ly
Abderaof Elmrabet, Faculty of Engineering, Zawia University, a.elmrabet@zu.edu.ly

1. Abstract

The increasing demand for radio spectrum led to the need to improve the spectrum utilization and spectrum management mechanisms.

Pervasive wireless communications rely enormously on spectrum utilization; the increase in demand for new wireless services and their application has led to spectrum scarcity. Spectrum limitations can be resolved by cognitive radio (CR) which is a technology that allows secondary users (SUs) to use the spectrum when it is not occupied by primary users (PUs). In this paper, the security issues that decrease CR performance are discussed; there are two major threats i.e. primary user emulation attack (PUEA) and spectrum sensing data falsification attack (SSDF).

a transmitter verification scheme (direct scheme) and indirect trust scheme that considers the users' history are presented; Firstly, the direct trust scheme, which obtains user trust values based on the localization of the signal source. This 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 PU, and thus the trustworthiness of the user is obtained by the distances measured using the coordinates and received signal power level. On the other hand, the indirect trust scheme combines the direct trust and the historical trust to obtain the trustworthiness of the users. Simulation results have shown that the trustworthiness of the PU is much higher than that of the malicious user. Moreover, the indirect scheme improves the user's trustworthiness as it considers the historical behaviour of the user.

Also the results proved that if the signal to noise ratio (SNR) is raised, correspondingly the trustworthiness of the PU is considerably increased.

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

2. 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 [1]. 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[2] [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[4].

Spectrum sensing data falsification attacks (SSDF): Attackers send false observation information, intentionally or unintentionally, to the fusion centre (FC)[5], 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 [6]. An optimal linear cooperation scheme base on a likelihood ratio test (LRT) has been proposed in [7]. In [8], 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 [9]. But in our scheme, the mechanisms use a localization technique and user's history to identify malicious users in the system and to create a trustworthy network in order to build a strong relationship amongst nodes in CRNs. This method can improve the sensing performance.

3. Proposed Approach for Users Trust Management

The trustworthiness of users can be exploited to increase the performance of a CRN. Therefore, trust determination models are proposed based on the current and historical trust values of users to identify the PU.

In the proposed scheme, the trustworthiness of the users in the network is calculated. 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. The proposed 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.

3.1 Trust Determination Models

Trust values are classified into two categories, direct trust values and indirect trust values. Indirect trust values are a combination of historical and direct trust values.

Direct Trust Model

This trust is calculated according to current observation only. Malicious users and misbehaving nodes can act as good PUs aiming to disturb the SU's decision about the spectrum occupancy reports and this causes maximum interference and minimum spectrum utilisation. So it is therefore crucial to estimate the trustworthiness of users in order to identify the malicious users.

The direct trust values are achieved based on the transmitter verification scheme. The main idea of this scheme is that because it is not possible for the malicious user to mimic both the coordinates and the power level of the PU, so verifying the transmitter and producing its trust values are based on the distance measured on the basis of coordinates denoted by d_1 and distance measured based on received power level d_2.

The CR user then uses d_1 and d_2 to calculate the direct trustworthiness T_D of a user as follows:

$$T_D = \min\left(\frac{d_1}{d_2}, \frac{d_2}{d_1}\right) \qquad 1$$

where the min function returns the minimum value of the equation's elements.

The distance that is calculated based on the received power d_2 is not accurate; however, the two distances d_1 and d_2 are close in the case of a good PU. Therefore, the T_D of the good PU is always close to 1.

Distance Calculated based on the Location Coordinates d_1:

Let (x, y) be the coordinates of the SU and (x_1, y_1) the coordinates of the PU. The distance between the SU and the PU based on the coordinates can be calculated as follows:

$$d_1 = \sqrt{\left\{(x - x_1)^2 + (y - y_1)^2\right\}} \qquad 2$$

In the simulation assumptions, each user broadcasts its location coordinates, so the distance between the users is calculated.

Distance measured according to the received power level d_2:

The received power P_r with a given transmitted power P_t in the two-ray model is generally given by:

$$P_r = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \qquad 3$$

where h_t is the height of the transmitter, h_r is the height of the receiver, G_t is the transmitter's antenna gain, G_r is the receiver's antenna gain, L is the system loss factor, and d is the distance between the transmitter and receiver.

Consider that h_t, h_r, G_t, G_r and L are equal to 1, then the received power is:

$$P_r = \frac{P_t}{d^4} \tag{4}$$

Therefore, the distance d_2 can be calculated by:

$$d_2 = \sqrt[4]{\frac{P_t}{P_r}} \tag{5}$$

The distance calculated using the received power may not be 100% accurate due to the noise level and the impact of the channel impediments and some other uncertainties caused by the signal propagation environment.

The ideal received power P_r is given by:

$$P_r(ideal) = \frac{P_t}{d_2^4} \tag{6}$$

The actual received signal power can be calculated as follows:

$$P_r(Actual) = \frac{P_t + noise\_power}{d_2^4} \tag{7}$$

where P_t is the transmitted power, d_2 is the distance between the transmitter and the receiver, and noise_power is the noise signal power.

Indirect Trust Model

In order to highlight the historical behaviour of a user in the role of trustworthiness evaluation, this model considers a historical trust value denoted by T_H that describes the behaviour of a user in the history of interaction.

This indirect trust value is a combination of direct trust T_D and historical trust T_H. This mechanism adds the function of querying the historical trust values. Therefore, the total value of indirect trust T_T is:

$$T_T = x * T_D + y * T_H \tag{8}$$

where x, y >= 0 and $x + y = 1$. x is the impact weight of direct trust T_D, and y is the impact weight of historical trust T_H.

x, $y \in [0,1]$. x = close to 1 indicates that the direct trust T_D plays a major role in the total trust calculation, and x = close to 0 means that the historical trust T_H plays a major role in the total trust calculation. The proposed approach gives higher weight to the direct trust, rather than the historical trust.

In the simulation of the proposed approach, x is set close to 1 to award the T_D a higher contribution to the T_T. So T_H value has less contribution to the T_T.

4. Simulation System Model

A CRN is considered where there are a PU, SU and malicious users randomly distributed in an area of 15x15 Km^2 as shown in Figure 1 (This area range in general is consistent with various works in literature e.g. [10][11]).

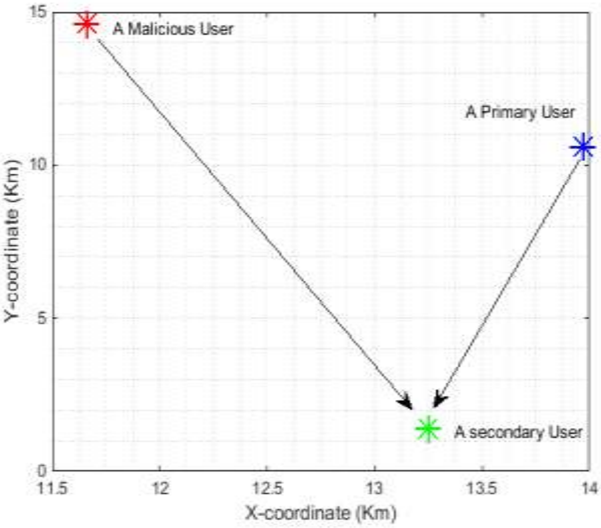

*Figure 1 Random location of primary, secondary and malicious users in an area of 15Km*15Km*

5. Simulation Results and Analysis

To evaluate the performance of the trust-management mechanisms, simulations are carried out via Matlab platform. The simulation results for both models (Direct and Indirect trusts) are discussed in this section. Figure 2 shows the distance measured based on the coordinates and the distance measured based on the received power level of the PU from the SU. It is noted that both distances match considerably, indicating that the SU is actually communicating with a trustworthy user.

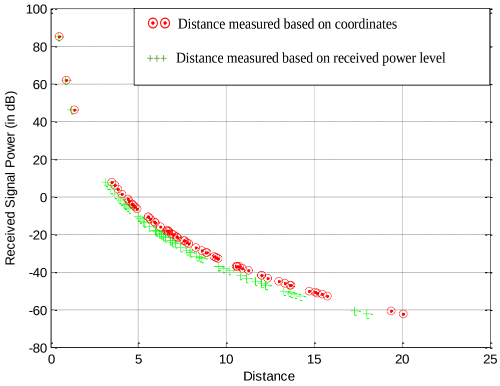

Figure 2 The distance measured based on the coordinates and the distance measured based on the received power level of the PU from the SU

5.1 Trustworthiness of the PU

To verify the performance of the direct trust approach and the indirect trust approach, the trust values are plotted in the same figure. The PU trusts are measured for different values of the historical trust which is denoted by T_H.

Figure 3 shows the trustworthiness of the PU with respect to the SNR values. It is noticeable that if the SNR value is raised, so correspondingly the trustworthiness of the PU increases. It is clear that the trustworthiness of the PU is always high (> 0.65) and reaches nearly 1 because it is a legitimate PU.

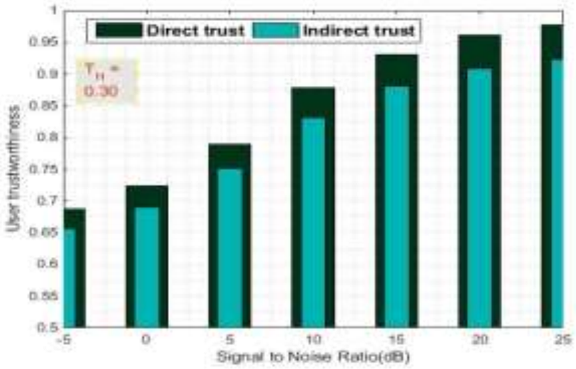

Figure 3 PU trusts vs. SNR when T_H =0.3

To evaluate the impact of the user's history on the total trust value, results are obtained for various T_H.

When $T_H = 0.3$, as can be seen from Figure 3 the direct trust values are higher than the indirect trust values because the direct trust model does not take into account the historical trust behaviour of a user, whilst the indirect trust model considers the history of the user. For example, when SNR =-5 it is noted that the direct trust value is about 0.69, while the indirect trust value is about 0.65. These values of trust are slightly low because the SNR is also low. But if the SNR=15, then the direct trust increases dramatically to reach 0.93, and the indirect trust value is about 0.88, which is affected by the history of the user. However, all trusts are high because it is a good PU.

Figure 4 illustrates the trust values when a user has a higher T_H (T_H =0.5). It is clear that when SNR=-5, the direct trust is still at about 0.69, while the indirect trust value has slightly increased to reach 0.67 (it was 0.65 when T_H was 0.3). All the indirect trust values are still below the direct trusts because the history of the user is still considered as low.

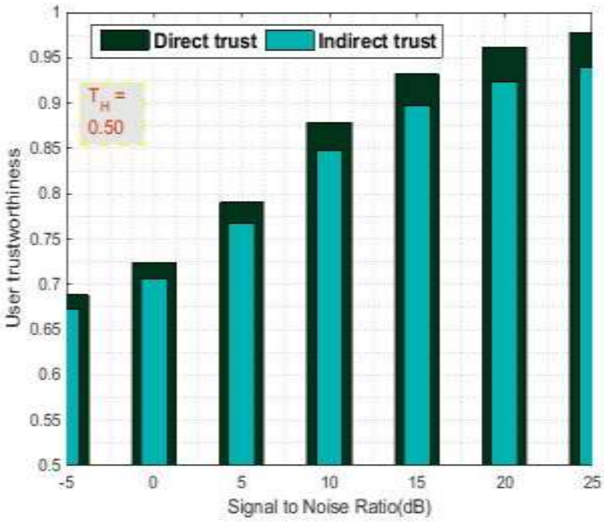

Figure 4 PU trusts vs. SNR when T_H =0.5

When T_H reaches 0.8, as in Figure 5, this will have a positive effect on the trustworthiness; for instance, when SNR =-5, the indirect trust increases from 0.67 to about 0.7. This shows the importance of the good history of a user.

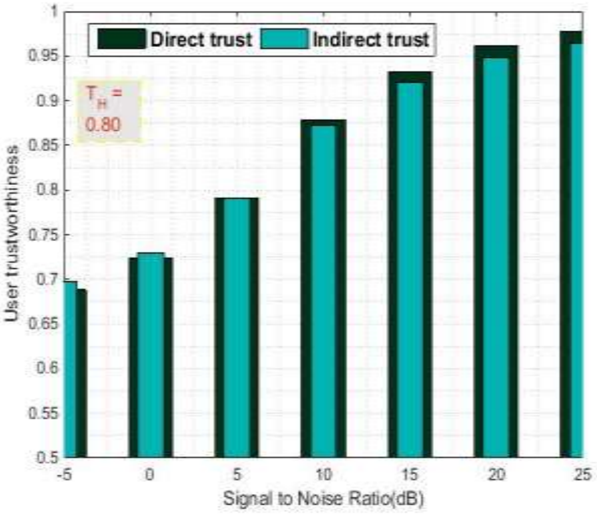

Figure 5 PU trusts vs. SNR when T_H =0.8

In the case where the user has a very good history, i.e. T_H =0.98 as in Figure 6, it is noticeable that the indirect trust reaches 0.72 when SNR=-5 and about 0.93 when SNR=15. In this case, it is clear that all the indirect trusts overcome the direct trusts and this is because the users have a great historical trust value.

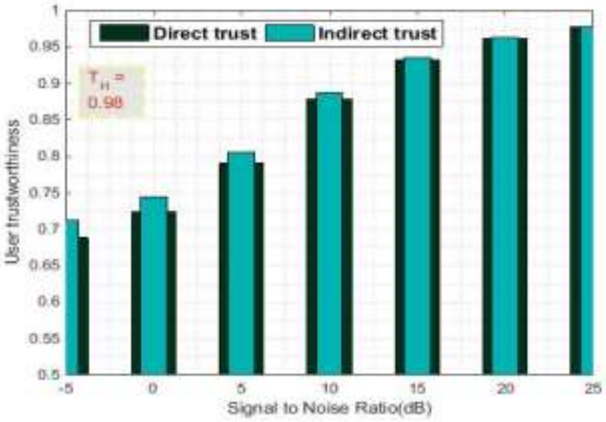

Figure 6 PU Trusts vs. SNR when T_H =0.98

5.2 Trustworthiness of Malicious User

The trustworthiness of the malicious users with respect to the SNR values is plotted in Figure 7; when T_H =0.2 this indicates that the history of the user is very low. It is noticeable that the direct trusts and the indirect trusts for the malicious user are always very low (< 0.64) even though the SNR has increased.

So the malicious user has lower trust values (direct and indirect) compared to the PU trusts, which nearly reach 1 (100%). It is noticeable that because the T_H is very low in this case, the indirect trusts for all SNRs are less than the direct trusts.

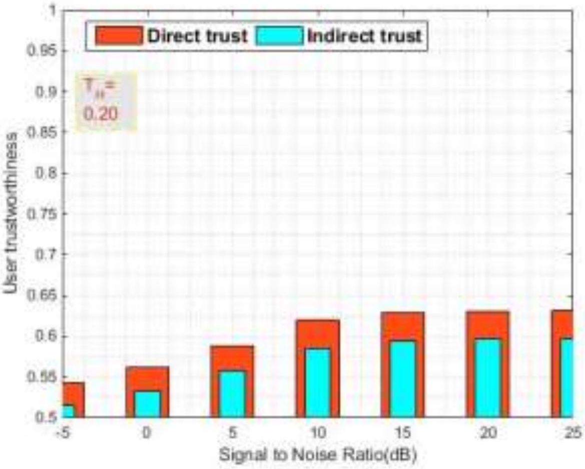

Figure 7 Malicious user trusts vs. SNR when T_H =0.2

Once the T_H is raised, as in Figure 8 when T_H =0.4, the indirect trust values increase but are still below the direct trust as the history value is still low. For example, when SNR = -5, the indirect trust increases from 0.51 (when T_H =0.2) to 0.53, and this is because the user has a higher historical trust value.

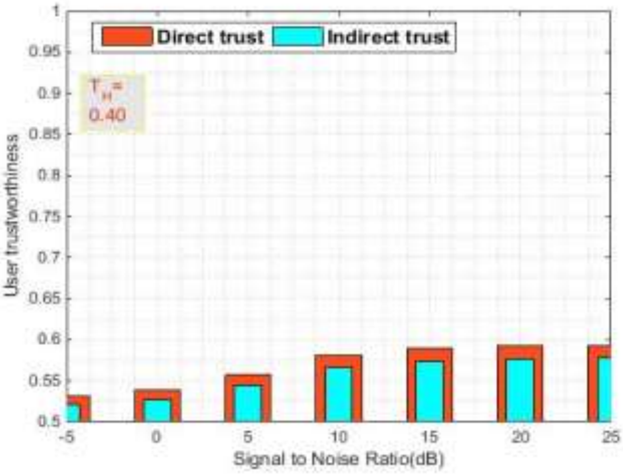

Figure 8 Malicious user trusts vs. SNR when T_H=0.4

On the other hand, when the user has a high historical trust value T_H =0.8, as illustrated in Figure 9, the indirect trusts increase considering the good history of the user to overcome the direct trusts. For example, when SNR =5, the indirect trusts rise from 0.56 when T_H =0.4 to 0.59 when T_H =0.8. However, all the trust values of the malicious user (direct and indirect) are maintained at a low level even though the T_H of the user is high because the direct trust value plays the main role in the total trust calculation.

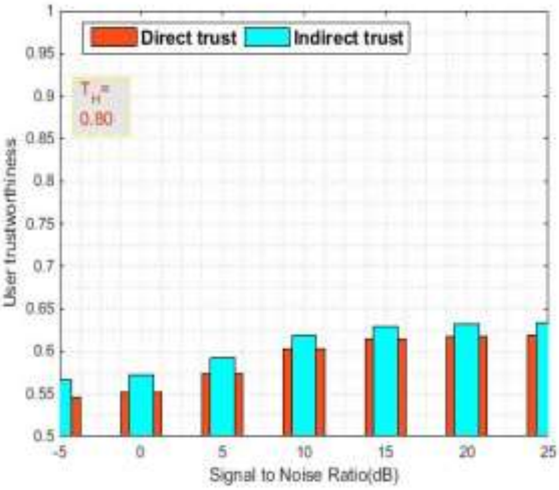

Figure 9 Malicious user trusts vs. SNR when T_H =0.8

6. Conclusion

In this paper, a trust management mechanism has been studied because the user‟s trustworthiness is a crucial factor in a CR detection system. CRN has unique security problems, which are not faced by conventional wireless networks. The main objective of any preventive security mechanism is to eliminate or reduce the impact of malicious operations performed by an adversary. Two trust-management schemes are presented in this paper. Firstly, there is the direct trust scheme, which obtains user trust values based on the localization of the signal source. This 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 PU, and thus the trustworthiness of the user is obtained by the distances measured using the coordinates and received signal power level. On the other hand, the indirect trust scheme combines the direct trust and the historical trust to obtain the trustworthiness of the users. Simulation results have shown that the trustworthiness of the PU is much higher than that of the malicious user. Moreover, the indirect scheme improves the user’s trustworthiness as it considers the historical behaviour of the user.

Bibliography

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.

2 K. Ben Letaief, W. Zhang, Cooperative communications for cognitive radio networks, Proceedings of the IEEE 97 (5) (2009) 878–893.

3 W. Zhang and K. B. Letaief, “Cooperative communications for cognitive radio networks,” Proceedings of the IEEE, vol. 97, pp. 878–893, May 2009.

4 J. Unnikrishnan and V. Veeravalli, “Cooperative spectrum sensing and detection for cognitive radio, ” in IEEE Global Telecommunications Conference, GLOBECOM, Nov. 2007, pp. 2972 –2976.

5 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.

6 H. Ekram and B. V. K, Cognitive Wireless CommunicationsNetworks. Springer Publication, 2007.

7 M. K. Simon and M.-S. Alouini, Digital communication over fading channels. John Wiley & Sons, Inc., 2 ed., Dec. 2004.

8 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

9 A. Ghasemi and E. Sousa, “Opportunistic spectrum access in fading channels through collaborative sensing,” Journal of Communications, vol. 2, no. 2, p. 71,2007

10 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.

11 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.