Reducing Attack Effectiveness in Cognitive Radio Networks

Parastoo Razavi[1], Reza Berangi[2]
1- Iran University of Science and Technology, Tehran, Iran.
Email: p_razavi@comp.iust.ac.ir (Corresponding author)
2- Iran University of Science and Technology, Tehran, Iran.
Email: rberangi@iust.ac.ir

Received: February 2012 Revised: June 2012 Accepted: August 2012

ABSTRACT:
Cognitive radio is a revolutionary technology that made significant progress in the effective use of the frequency spectrum. The technology itself can be dynamically adjusted so that the proper utilization of the available radio spectrum can be made. According to various studies conducted, it is observed that the bulk of each frequency band allocated to users leaving unused. The cognitive radio can use these parts of the spectrum that called spectrum holes. Inherent nature of this technology creates the chance for the attacker in these networks. This vulnerability that created due to the inherent nature of cognitive radio technology, Can severely impact on the safety and quality of service in these networks. In this paper, we focus on the primary user emulation attack. In this attack, an adversary transmits signals whose characteristics emulate those of incumbent signals. We proposed the method for reducing the effects of primary user emulation attacks in cognitive radio networks. This method suggests the technique that can merge with spectrum sensing method and can resistant these networks against the primary user emulation attacks. Finally, with run some simulation, we examined the performance of this proposed method in detection of primary user emulation attacks in these networks.

KEYWORDS: cognitive radio networks, primary user emulation attacks, spectrum holes, spectrum sensing, primary user, secondary user.

1. INTRODUCTION

The need to meet the ever-increasing spectrum demands of emerging wireless applications and the need to better utilization of the spectrum have led the Federal Communications Commission (FCC) to revisit the problem of spectrum management. In the conventional spectrum management paradigm, most of the spectrum is allocated to the licensed users for exclusive use. For overcome the ever-increasing need of the spectrum, the FCC is considering opening up licensed bands to unlicensed operations on a non-interference basis to the primary user. In this new paradigm, secondary users "opportunistically" operate in fallow licensed spectrum bands without interfering with primary or incumbent users. The opportunistic use of the spectrum is shown in figure 1.

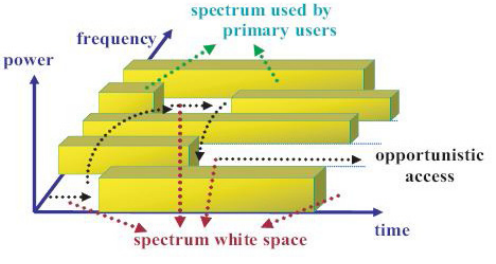

Fig.1. Opportunistic use of spectrum holes [5]

Unlike a conventional radio, a CR can sense and understand its environment and proactively change its mode of operation as needed. Once white spaces are identified, cognitive radios opportunistically utilize these white spaces by operating in them without causing interference to primary users. Ensuring the trustworthiness of the spectrum sensing process 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. Distinguishing the two signals is non-trivial, but it becomes especially difficult when the cognitive radios are operating in hostile environments. In the hostile environment, an attacker can mimic the signal of primary users, thereby it causes secondary users erroneously to identify the attacker as the primary user. To overcome this attack, a scheme that can reliably distinguish between primary user signals and signal that transmit from the attacker is needed.

In this paper, we proposed a scheme for distinguishing between primary user signals and signal that transmit from attackers. In this method, we proposed, each secondary user independently collects the measurement of the received signal strength (RSS) of primary user signal and computes the mean and

variance of the received signal from the primary users. Then each of secondary users base on these estimated values, decides if the signal is transmitted from primary user or this signal is transmitted by the attacker whose run a primary user emulation attack. We then evaluate the performance of this scheme using run some simulation.

The rest of this paper is organized as follows. In section 2, we describe the primary user emulation attack in detail. In section 3, we describe the proposed scheme for distinguish between the signal transmitted by primary users and signals that transmitted by attackers. In section 4, we show the simulation results and in section 5, we conclude the paper and discuss future work.

2. PRIMARY USER EMULATION ATTACK

One of the well-known attacks on cognitive radio networks is the primary user emulation attacks. In this kind of attacks, radiation of the radio signals can intentionally disrupt communication in the attacked network. In fact, in primary user emulation attacks, the attacker emulates the signals that mimic the primary user signals and then the legitimate secondary user identifies this signal as the primary user signal and prevents to transmit signal on this band. This kind of attacks substantially decreases the communication performance or even stops communication [8].

In cognitive radio networks, secondary users are allowed to operate in licensed bands on a non-interference basis. Therefore, it is needed to sense the medium continuously in order to detect the presence of primary users. Because of this, one of the keys to the success of cognitive radio networks is the development of effective spectrum sensing mechanisms. If a primary signal is detected in a given frequency, secondary users must switch to one of the vacant bands (a process known as spectrum handoff). On the other hand, if another secondary user is already operating in such band, self-coexistence mechanisms are needed to share the spectrum fairly. This fact poses a security treats in the system, as an attacker could pretend to be an incumbent by transmitting a signal with similar characteristics to a primary signal, thus preventing secondary users from using vacate bands. This attack, coined in [9] as primary user emulation attack, is quite realistic, given the flexibility offered by cognitive radios in terms of transmission parameters. This possibility reinforces the need for sensing mechanisms to recognize primary signals effectively.

The impact of the primary user emulation attack depends on several factors, such as the location of the attacker, and the sensibility of cognitive radios in their measurements.

Selecting an optimal position to perform the attack will cause many secondary users concluding that a given band is occupied and looking for another unoccupied portion of the spectrum. On the other hand, if an energy-based method is used to detect primary users, the threshold value will also play an important role: the lower the threshold is, the easier to perform primary user emulation attack.

According to the target of the attack, we classify primary user emulation attack s into malicious or selfish attacks. The objective of malicious attacks is to prevent secondary users from detecting vacate bands and use them (DoS), whereas selfish attacks aim at maximizing the attacker spectrum usage.

Figure 2, shows the primary user emulation attacks.

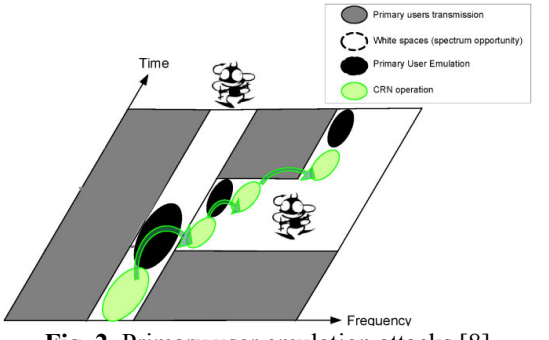

Fig. 2. Primary user emulation attacks [8]

3. PROPOSED SCHEME FOR DISTINGUISHING THE PRIMARY USER SIGNAL FROM ATTACKER SIGNALS

Before describing the transmitter verification scheme for spectrum sensing, we state some of the assumptions that form the foundation of the scheme. The primary user is assumed to be the transmitter that has a fix location and is a TV signal transmitter. A TV signal transmitter output power is normally hundreds of thousands of watts [10], which correspond to a transmission range from several miles to tens of miles. We assumed that each of the secondary users equipped by cognitive radio devices have self-localization capability and have maximum transmission output power within the range from a few hundreds miliwatts to a few watts, this typically corresponds to a transmission range of a few hundred meters. An attacker equipped with a cognitive radio devise and is capable of changing its modulation mode, frequency, and transmission power.

Based on above assumptions, we propose a scheme that can merge with spectrum sensing and can do robust distinguishing between primary user signal and the signals that transmitted from the attacker.

In this scheme, we use the energy detection method for spectrum sensing and with merge this method with our proposed scheme, we can carefully distinguish between signals of primary users and attackers.

In this paper, we consider the two-ray signal

propagation model for mobile radio environments, and moreover, we consider the path loss and the log-normal shadowing for the communication environment. Hence, if the transmitter uses the power of p_t for transmitted signal, then the received signal energy at the receiver is:

$$P_r = P_0 d^{-\alpha} G \quad (1)$$

where α is the path loss exponent, r is the distance between the transmitter and receiver, G is the shadowing random variable and p_r is the received signal power. Here, $G = 10^{\frac{\beta}{10}} = e^{a\beta}$ and based on [12], a=$\frac{\ln 10}{10}$, and β follows a normal distribution, $\beta \sim N(0, \sigma^2)$.

Because the location of primary user and attacker is different, the values of σ_p^2 and σ_a^2 are not the same. (Based on [11], $2 \le \alpha \le 8$ and $4 \le \sigma^2 \le 12$).

In this scheme, each secondary user individually collects the values of received signal power transmitted from a primary user. For example, suppose that one secondary user collects the values of receiving signal power $y_1, y_2, ..., y_n$ for receiving signal power from primary user and based on these values, computes the mean of those values base on follow equation:

$$\mu = \frac{1}{n}\sum_{i=1}^{n} y_i \quad (2)$$

Moreover, each secondary user computes the variance of those values base on follow equation:

$$\sigma = \frac{1}{n-1}\sum_{i=1}^{n} (y_i - \mu)^2 \quad (3)$$

Then, each secondary user, using above estimated mean and variance values for deciding whether the received signal is from legitimate primary user or from an attacker how runs the primary user emulation attack. Decision of each secondary user made based on following equation:

If $|p_r - \mu| \le k\sqrt{\sigma}$ signal is from primary user

(4)

If $|p_r - \mu| \succ k\sqrt{\sigma}$ signal is from attacker

Here, k is the constant parameter that can control the threshold of detection in this scheme.

Therefore, based on above descriptions, if an attacker sends a signal that mimic the properties of primary user signals, because the received power of this signal at each secondary user is different base on the equation (1), and at each secondary user mean and variance of power of primary user signal is estimated, by cooperation of more than one secondary user, we can carefully distinguish between primary user signals and signals of the attacker.

In this method, one secondary user only in one way cannot successfully distinguish between signals of primary users and attacker, and it is when the attacker can carefully estimate the received primary signal power at one secondary user, and can transmit his signal in the way that the secondary user erroneously detects this signal as a primary user signal. One attacker as below can adapt his power in the way that secondary user makes a mistake:

$$p_a = p_t (\frac{r_1}{r_2})^{-\alpha} e^{a(\beta_p - \beta_a)} \quad (5)$$

where p_a is power of the attacker, r_1 is distance between primary and secondary users, r_2 is distance between secondary user and attacker.

But, because in the proposed scheme, we benefit of cooperation between more than one secondary users, performance of this method in detection of the attacker, is acceptable. The Probability of attacker detection in this scheme is as follows:

$$P_{detect} = \Pr\left(\left|P_r^a - \mu_r\right| > k\sigma_r\right) \quad (6)$$

we define:

$$c = \sqrt{(e^{a^2\sigma_p^2} - 1)} \quad (7)$$

$$\lambda = \frac{P_a}{P_t} \times (\frac{r_2}{r_1})^{-\alpha} \quad (8)$$

Then

$$P_{detect} = \Pr(P_a r_2^{-\alpha_2} e^{a\beta_a} > P_t r_1^{-\alpha_1} e^{\frac{1}{2}a^2\sigma_p^2}(kc+1)) + \Pr(P_a r_2^{-\alpha_2} e^{a\beta_a} < P_t r_1^{-\alpha_1} e^{\frac{1}{2}a^2\sigma_p^2}(1-kc)) \quad (9)$$

After some computation we obtain:

$$P_{detect} = 1 - \phi(\frac{a\sigma_p^2}{2\sigma_a} + \frac{1}{a\sigma_a}\ln(\lambda(1+kc))) + \phi(\frac{a\sigma_p^2}{2\sigma_a} + \frac{1}{a\sigma_a}\ln(\lambda(1-kc))) \quad (10)$$

The simulation results show the performance of this method in the present of some attacker. The simulation results is shown in next section.

4. SIMULATION RESULTS

For performance estimation of the proposed scheme, we perform some simulation. In these simulations, we propose there is one primary user who transmits signals with fixed power and there are secondary users who distributed in 2000*2000 m^2

region. We run the simulation with a deferent number of attackers and we examined the effect of different number of attackers on probability of correct detection.

Figure 3, show the impact of existence of one attacker on probability of correct detection in the proposed scheme when 20 secondary user are existed. In this figure, we show the impact of one attacker for proposed scheme and for when this method is not existed. Figure 4, show the impact of four attackers on probability of correct detection in the proposed scheme.

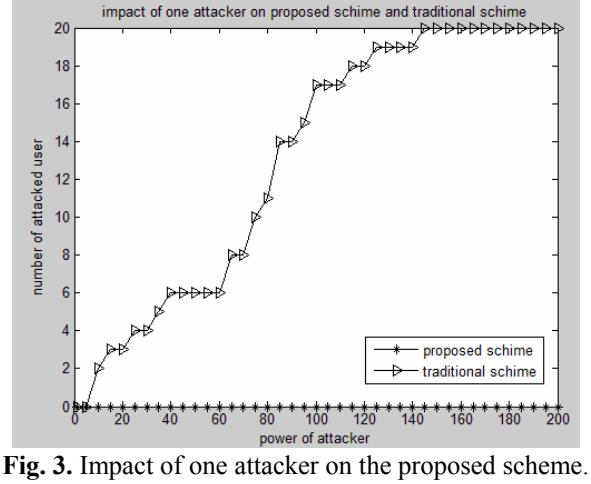

Fig. 3. Impact of one attacker on the proposed scheme.

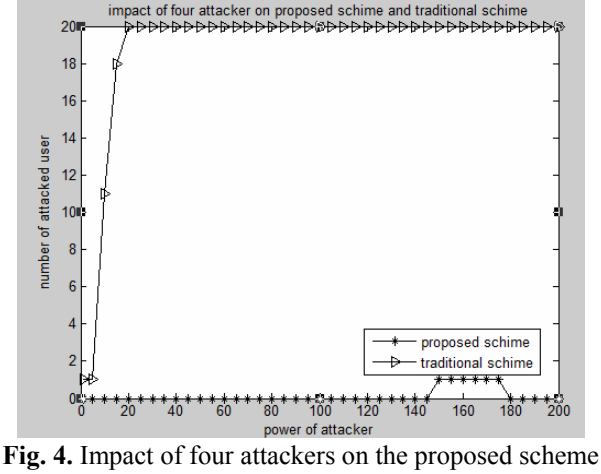

Fig. 4. Impact of four attackers on the proposed scheme

In figure 5, we show the impact of eight attackers on scheme and in figure 6, the impact of existence of sixteen attackers was shown.

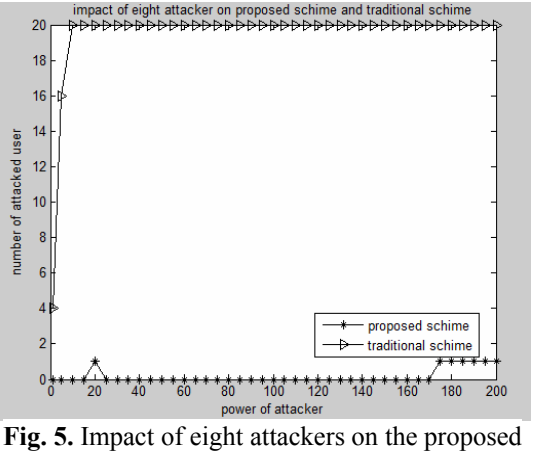

Fig. 5. Impact of eight attackers on the proposed scheme

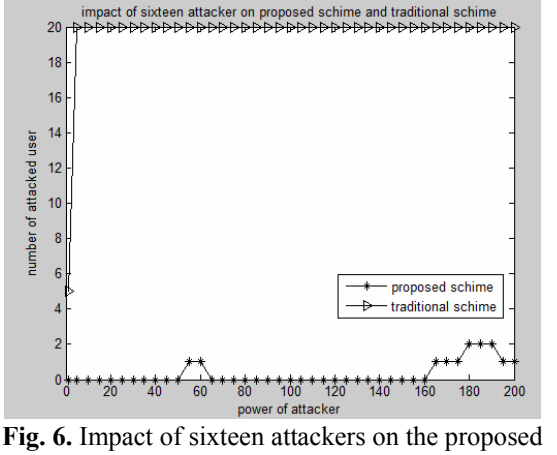

Fig. 6. Impact of sixteen attackers on the proposed scheme

In these figures, we can see that the increase in the number of attackers cannot affect more on correct detection of this method.

Figure 7, shows the impact of deferent value of k parameter on probability of the attacker detection in the proposed scheme.

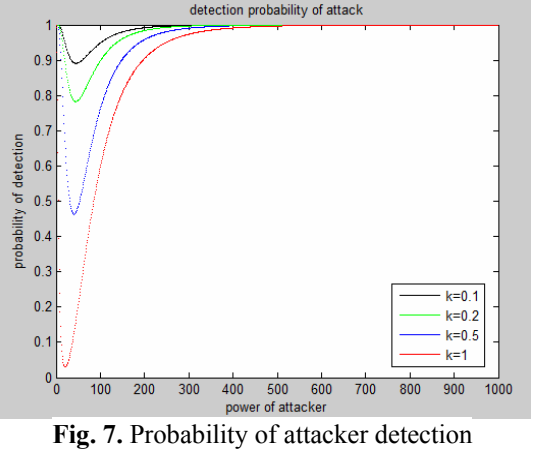

Fig. 7. Probability of attacker detection

In this figure, we see that selection of smaller value of k, can result in higher probability of detection. Note that, selection of very small value for k, will result in erroneously detection of primary user signal as the signal of the attacker.

5. COCULUTION

Cognitive radio is a revolutionary technology that makes significant progress in the effective use of the frequency spectrum. Inherent nature of this technology creates the chance for the attacker in these networks. This vulnerability that created due to the inherent nature of cognitive radio technology, can severely impact on the safety and quality of service in these networks. In this paper, we focus on the primary user emulation attack. In this paper, we proposed a method for reducing the effect of primary user emulation attack in cognitive radio networks. In this method, we benefit of the energy detection based spectrum sensing that is a simplest method of spectrum sensing and with merge this method with our scheme, we can effectively reduce the effect of primary user emulation attack. With runs some simulation, we examine the performance of this scheme. The simulation results show that this proposed scheme can effectively detect this kind of attacks.

REFERENCES

[1] Danda B. Rawat and Gongjun Yan, **"Spectrum Sensing Methods and Dynamic Spectrum Sharing in Cognitive Radio Networks: A Survey,"** *International Journal of Research and Reviews in Wireless Sensor Networks*, March 2011.

[2] M Nekovee, **"Dynamic spectrum access — concepts and future architectures,"** *BT Technology Journal*, April 2006.

[3] K.C. Chen, Y.J. Peng, N. Prasad, Y.C. Liang, S. Sun, **"cognitive radio network architecture: trusted network layer structure,"** *National science council*, Taiwan *ROC*, 2008.

[4] Rehan Ahmed and Yasir Arfat Ghous, **detection of vacant frequency bands in cognitive radio**, *Blekinge Institute of Technology ph.d thesis*, May 2010

[5] Beibei Wang and K. J. Ray Liu, **"Advances in Cognitive Radio Networks: A Survey,"** *IEEE communication society*,2008

[6] K. Chen, P. Chen, N.R. Prasad, Y. Liang, and S. Sun, **"Trusted cognitive radio networking,"** *presented at Wireless Communications and Mobile Computing*, 2010, pp.467-485.

[7] Y. Liu, P. Ning, and H. Dai, **"Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures,"** *In Proceedings of the 2010 IEEE Symposium on Security and Privacy*, pages 286–301, 2010.

[8] O. Le´on, J. Hern´andez-Serranoand M. Soriano, **"Securing cognitive radio networks,"** *international journal of communication systems*, 2010.

[9] 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.

[10] Shrestha Junu,Sunkara Avinash Thirunavukkarasu Balaji, **Security in Cognitive Radio**, San Jose State University ph.d thesis, 2010

[11] Goldsmith, **Wireless Communications**, Cambridge University Press, 2005.

[12] Alfred Asterjadhi and Michele Zorzi, **"JENNA: a Jamming Evasive Network coding Neighbor-discovery Algorithm for Cognitive Radio Networks,"** *IEEE international conference on communication*, 2010.