IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 3, March 2017

A Database Assisted Detection against Primary User Emulation in Cognitive Radio Network

T. Selvapriya[1], S. Sharmila[2], M. Sindhuja[3], V. Sinthuja[4], C. Jayasri[5]

UG Student, Final Year ECE, A.V.C College of Engineering, Mannampandal[1,2,3,4]

Assistant Professor of ECE, A.V.C College of Engineering, Mannampandal[5]

Abstract: CR is a promising technology for next generation wireless networks in order to efficiently utilize the limited spectrum resources and satisfy the rapidly increasing demand for wireless applications and services. Security is a very important but not well addressed issue in CR networks. In this article we focus on security problems arising from PUE attacks in CR networks. We present a comprehensive introduction to PUE attacks, from the attacking rationale and its impact on CR networks, to detection and defense approaches. In order to secure CR networks against PUE attacks, a two level database-assisted detection approach is proposed to detect such attacks. Energy detection and location verification are combined for fast and reliable detection. An admission control based defense approach is proposed to mitigate the performance degradation of a CR network under a PUE attack. Illustrative results are presented to demonstrate the effectiveness of the proposed detection and defense approaches.

Keywords: cognitive radio, spectrum sensing, Primary User Emulation Attack, protocol.

1. INTRODUCTION

Cognitive radio (CR) is an enabling technology to effectively address spectrum scarcity, and it will significantly enhance spectrum utilization of future wireless communications systems. In a CR network, the secondary (or unlicensed) user (SU) is allowed to opportunistically access the spectrum “holes” that are not occupied by the primary (or licensed) user (PU). Generally, the SUs constantly observe the spectrum bands by performing spectrum sensing. Once a spectrum “hole” is discovered, an SU could temporarily transmit on this part of the spectrum. As a consequence, scarce spectrum resources are shared in a highly efficient and resilient manner between the primary network and the CR network.

Among all the key technical problems of CR networks, security is a crucial but not well addressed issue. In all the main functionalities of CR networks such as spectrum sensing, spectrum mobility, spectrum sharing, and spectrum management, the CR network has been shown to be strategically vulnerable [1].The typical attacks on CR networks may include denial of service (DoS) attacks, system penetration, repudiation, spoofing, authorization violation, malware infection, and data modification. These attacks cause potential threats to the information confidentiality, integrity, and availability of the CR network[12]. Effective defense approaches are urgently needed to secure CR networks and deal with these attacks.

Nowadays, security threats and their countermeasures have been studied as one of the most important topics in the research area of CR technology [2]. In this article we mainly focus on the security problems arising from primary user emulation (PUE) attacks in CR networks.

2. PUE ATTACK AND THEIR CLASSIFICATION

PUE attacks are known as a new type of attacks unique to CR networks, in which the attackers may modify their radio transmission frequency to mimic a primary signal, thereby misguiding the legitimate SUs to erroneously identify the attackers as a PU.

The presence of PUE attacks may severely influence the performance of CR networks. This article aims at presenting a comprehensive introduction to PUE attacks, from the attacking principle and its impact on CR networks to detection and defense approaches. In order to secure CR networks, we propose a database-assisted detection approach and an admission control based defense approach against PUE attacks. The remainder of the article is organized as follows. The next section illustrates the principles of PUE attacks, and introduces its classification and impacts on CR networks. We then describe existing detection measures for PUE attacks.

A two level database-assisted detection approach is proposed. Energy detection and location verification are combined for both fast and reliable detection. Then we discuss the defense approaches against PUE attacks, where a guard channel based admission control is adopted to defend against PUE attacks. Finally, the conclusions of the article are presented.

3. CLASSIFICATION OF ATTACKERS

Since the security problem caused by PUE attacks was identified, different types of PUE attacks have been studied. We now introduce different types of PUE attackers associated with their classification criteria.

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 3, March 2017

Selfish Attacker:
The attacker's objective is to maximize its own spectrum usage. Here, the goal of the attacker is to increase its share of spectrum resources. This attack carried out between two attackers and establishes a dedicated link between the malicious PUE**.**

Malicious attacker:
The attacker's objective is to obstruct secondary user's access to the spectrum. In malicious PUE attackers try to prevent the legitimate secondary users from using the holes found in the spectrum.

4. IMPACT ON CR NETWORKS

Figure 1 shows a typical scenario of a PUE attack. There are two primary base station. Let's consider first primary base station (BS) is transmitting in channels f1, f2 and f3 to the PU receivers. Channels f6, f7 and f8 are idle. By observing this, SU1, SU2, and SU3 are allowed to use these three idle channels for transmissions.

However, the appearance of a PUE attacker, say, EU2, may block the SUs from using an idle channel. EU2, may, for example, mimic the primary signal in channel f8. Once the attack succeeds, SU1 and SU3 are misled to evacuate channel f8 and the link between them is interrupted. The Second primary Base station is occupying channels f4 and f5, while SU4 and SU5 are using channels f9 and f10, respectively. PUE attackers EU3 and EU4 are emulating the primary signals in channels f11 and f12, respectively. In this situation, suppose that SU4 and SU5 need to find channels to connect with the cognitive base station (BS). If attackers EU3 and EU4 cannot be correctly identified, SU4 and SU5 will find no vacant channels and hence may not be able to communicate with the cognitive BS.

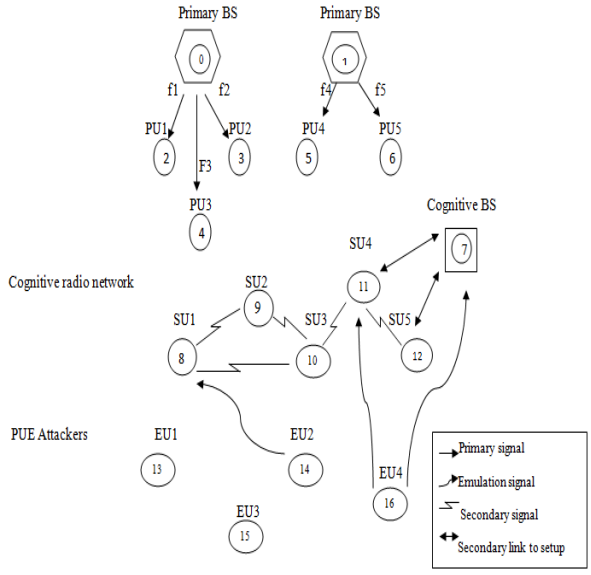

Figure 1.Illustration of PUE attacks in the CR networks.

The above two examples describe two different attacking cases. The first example illustrates the case in which the PUE attacker attacks the in-service SUs and seizes one of their channels, causing interruption of some of the SU services. The second example illustrates the case in which the PUE attackers occupy the idle channels and waste the spectrum opportunities of the SUs.

CONDITIONS FOR SUCCESSFUL PUE ATTACKS:

In a CR network to better understand PUE attacks and facilitate the design of countermeasures, we summarize these essential conditions as follows.

No PU-SU Interaction:
There is no interaction between the primary and the secondary networks. This is a necessary condition for a successful PUE attack. Otherwise, if the legitimate SUs are allowed to exchange information with the PUs, a PU verification procedure could be designed to easily detect a PUE attack. In most cases this condition holds.

PU and SU Signals Have Different Characteristics:
The primary and secondary networks use wireless signals with different characteristics, i.e. using different modulation modes and different signal statistical features. An SU receiver is inherently designed only for the secondary signal but unable to demodulate and decode the primary signal. The PUE attackers take advantage of this fundamental condition to emulate the primary signal that is unrecognizable for the legitimate SUs.

Primary Signal Learning and Channel Measurement:
To emulate the primary signal, the attacker has to track and learn the characteristics of the primary signal. For an advanced attack, the attacker may also estimate the power level as well as the channel conditions to generate more tricky transmitting signals.

Avoiding Interference with the Primary Network:
Although this is usually a primary concern for the SUs, it is also an important condition that the PUE attackers have to comply with. Attackers, especially the selfish ones, should carefully monitor the behaviors of PUs so as not to cause extra interference with the primary network.

IMPACT OF PUE ATTACKS ON CR NETWORKS

The presence of PUE attacks causes a number of problems for CR networks. The list of potential consequences of PUE attacks follows.

Bandwidth Waste:
The ultimate objective of deploying CR networks is to address the spectrum under-utilization that is caused by the current fixed spectrum usage policy. By dynamically accessing the spectrum "holes," the SUs are able to retrieve these otherwise wasted spectrum resources.

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 3, March 2017

However, PUE attackers may steal the spectrum "holes" from the SUs, leading to spectrum bandwidth waste again.

QoS Degradation:
The appearance of a PUE attack may severely degrade the quality-of-service (QoS) of the CR network by destroying the continuity of secondary service. Due to the fixed allocation of frequency bands, overall spectrum utilization is relatively low. Although certain frequencies experience severe congestion, in many locations large holes of unused spectrum exist. Therefore, regulators have realized that there is a need for an improved, more dynamic and efficient, mechanism for management of wireless resources.

Connection Unreliability:
If a real time secondary service is attacked by a PUE attacker and finds no available channel when performing spectrum handoff, the service has to be dropped. This real time service is then terminated due to the PUE attack. In principle, the secondary services in CR networks inherently have no guarantee that they will have stable radio resources because of the nature of dynamic spectrum access. The existence of PUE attacks significantly increases the connection unreliability of CR networks.

Denial of Service:
When a secondary user wants to transmit some data, it has to go through a request and acknowledgement process. However, if all the channels are occupied by the primary user emulators, the normal SU cannot even find a channel to send a request, so their service will be denied.

PERFORMANCE DEGRADATION DUE TO PUE ATTACKS:
We adopt the term saturation to characterize the state of a CR network in which all the channels are occupied by PUs, SUs, and PUE attackers, i.e. there are no idle channels, and the term outage characterizes the state of a CR network in which there is no spectrum band available for the common control channel (CCC). In a practical CR network, it is necessary to build up a CCC for exchanging control messages. The CCC might be established by using a dedicated radio transceiver and setting up an out-of-band fixed channel.

However, this is very difficult in a real CR network due to the additional cost of hardware and the assignment of a dedicated spectrum band. It is more likely that the CCC should be constructed by means of dynamic spectrum access. This implies that the CR network needs to maintain a stable channel as its CCC. Under PUE attacks, the CCC may also be attacked and disconnected. The system will be suspended in this case. Two new performance metrics are defined as follows.

• Outage Probability: The outage probability is defined as the probability that a CR network stays in the outage state in which there is no available spectrum band for constructing a CCC.

• System Recovery Time: The system recovery time is defined as the average time duration that a CR network (in the outage state) takes to acquire an available spectrum band as a CCC for delivering control messages. When the current CCC is no longer available due to the arrival of a PU or a PUE attack, it has to switch to a new channel. As a consequence, the CCC is disconnected only in the case that all of the channels are occupied by PUs or PUE attackers. In the saturation states with only one SU channel being used as the CCC, if a PU arrives and occupies the CCC, or if a PUE attacker successfully attacks the CCC, the CR network transitions to the outage state.

Figure 2(a)(b) shows the outage probability and the system recovery time in terms of the PUE attacking strength, i.e. the attack arrival rate. It is observed that both the outage probability and the system recovery time increase dramatically with an increase in attacking strength. Without PUE an attack, the outage probability is near zero and the recovery time is very short. In the case of a PUE attack, the outage probability is over 0.3 percent and the recovery time is nearly 2ms. Hence, the outage probability increases dramatically, and the recovery time is extended substantially, compared to the case in which there are no PUE attacks. These observations indicate that the existence of PUE attacks may seriously degrade the performance of a CR network. Detection and defense approaches against PUE attacks are becoming very critical to secure CR networks.

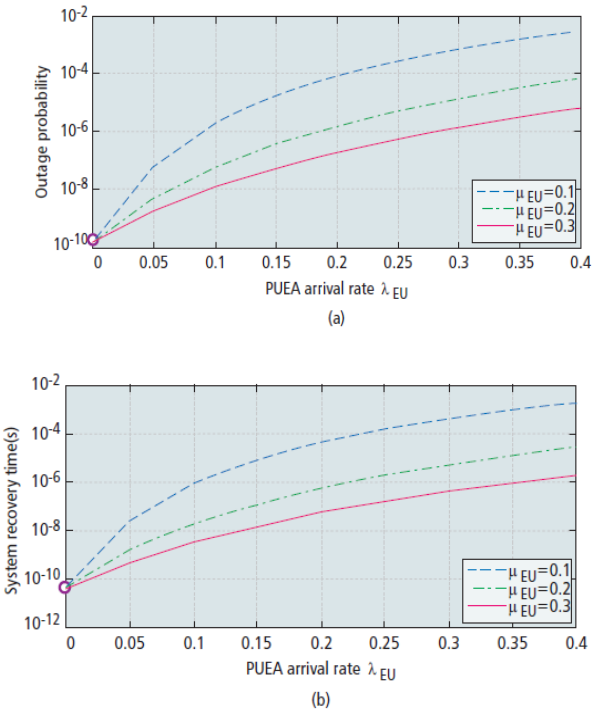

Figure 2. Outage probability and system recovery time

DOI 10.17148/IJIREEICE.2017.5313

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 3, March 2017

EXISTING DETECTION APPROACHES:

In the literature, some detection approaches against PUE attacks have been presented.

Energy Detection:

Energy detection is a simple but widely used approach for spectrum sensing in CR networks. It is also one of the basic approaches for the detection of PUE attacks. By measuring the power level of the received signal at the SU receiver and comparing it with that from the true PUs, the CR network can judge whether the signal comes from an attacker or not.

Drawback:

- A pure energy detector is not robust enough to tackle an advanced PUE attack.
- Poor performance in low SNR.

RSS-Based Detection:

RSS based localization techniques arise from the fact that there is a strong correlation between the distance of a wireless link and RSS. PUE attacks in CR networks without using any location information.

Drawback:

- This detection approach does not need dedicated sensor networks.
- High computational complexity.

Location Verification:

Two location verification schemes
are proposed in [3]. They are called distance ratio test (DRT) and distance difference test (DDT), respectively. In both schemes, dedicated cognitive nodes (SUs or a cognitive BS) with enhanced functionality are involved for location verification [12]. DRT uses a received signal strength (RSS) based method, where two dedicated cognitive nodes measure the RSS of the signal source and calculate the ratio of these two RSSs to check whether it coincides with their distances to the true PU (e.g. a TV broadcast tower). Using DDT, the arrival time of the transmitted signal from the source is measured by the two dedicated cognitive nodes.

Drawback:

- Verification performance is liable to the uncertainty of noise power.

A Database-Assisted Detection Approach:

Figure 4 shows our proposed database-assisted PUE attack detection approach, which has three key components: multi threshold fast energy detection, fingerprint-based location verification, and the two-level database.

In this approach a local database is integrated in each SU, while a global database is built up in the cognitive BS. The local database is used to store historical spectrum sensing data and the local detection decisions of each SU. The global database is used to collect and record all the SUs' spectrum sensing data and the local detection decisions, as well as the global detection decisions. The networks to be installed in affixed location and the BS is required to know its location. The location of the BS must be known to within a 15m radius while the location of CPE must be known to within a 100m radius. The main operations of the proposed detection approach are explained as follows.

Basic Operations:

We consider a system model in which there are one primary BS (e.g. the TV broadcasting tower) and multiple PUE attackers. In our model the attackers are static or quasi-static, i.e. moving very slowly.

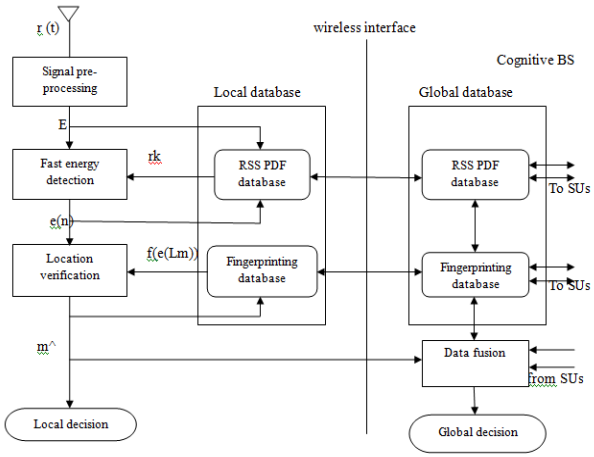

Figure 3. Proposed database assisted approach.

In a given moment and in a specific spectrum band (channel), only one of the attackers at most will emulate a primary signal. In the proposed approach, there are four main units in the SU: a signal pre-processing unit, a fast energy detector, allocation verifier, and a local database. The local database consists of two components: An RSS probability density function (PDF) database and a fingerprint database. The signal preprocessing unit receives the received signal $r(t)$ from the radio frequency (RF) unit as input. Let $x(t)$, h(t), and w(t) denote the transmitted signal, channel impulse response, and receiver thermal noise, respectively.

Let s(t) and s¢(t) denote the real PU signal and the PUE attack signal, respectively. Then the transmitted signal x(t) = $s(t)$ for the real PU signal, $s(t) = s¢(t)$ for the PUE attack signal, and $x(t) = 0$ when no signal is transmitted. The input signal is given by $r(t) = x(t) * h(t) + w(t)$. Let {tn} denote the sequence of sampling times and Ns the number of samples in one sensing period. After sampling, squaring, and aggregation, the signal pre-processing unit generates the sampled energy vector e = $e[n]$ (n = 1, 2… Ns) and the aggregated energy E. Then we have the sampled energy e[n] = r2(tn) and the aggregated energy E = S1 Ns e[n]. After that, the aggregated energy E is sent to the fast energy detector for comparison to the preset thresholds.

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 3, March 2017

If the comparison result indicates that there is no signal or it is a PUE attack signal, the detection procedure is terminated and the corresponding decision is made. Otherwise, the energy vector e[n], containing more detailed energy information, is sent to the location verification unit. The location of the source of the signal is estimated using Bayesian hypothesis testing. The estimated location ^*m* of the signal source is then transmitted to the cognitive BS for data fusion. The operations of the fast energy detector and location verifier are described below.

Multiple Thresholds Based Fast Energy Detection:

The goal of a fast energy detector is to quickly react to possible PUE attacks. The basic idea of a fast energy detector stems from conventional energy detection. In a conventional energy detector, there is only one energy threshold to distinguish the presence or absence of a primary signal. This single-threshold detector is not efficient for detecting a PUE attack signal. To distinguish a PUE attacker from a real PU, a fast energy detector sets up three energy thresholds, denoted by g0, g1 and g2.

Here, g0 < g1 < g2, and g0 is according to the original threshold in a conventional energy detector. If the input E < g0, it is decided that there is no PU or PUE attacker present. The two new thresholds g1 and g2 are used to distinguish the signals of a PU and a PUE attacker. If the input g0 < *E* < g1 or *E* > g2, it is decided that a PUE attack is detected. Otherwise, the received signal is initially diagnosed to be a PU signal. The location verifier will be launched for further examination. It is emphasized that using two energy thresholds to distinguish a PU from a PUE attacker is justified by the following fact. A PUE attacker tries to emulate the transmitting power of a real PU. However, it is very difficult for the attacker to fabricate a signal so that all of the SUs receive the signal with a power level similar to that of the real PU. By randomly assigning a few SUs to measure the received signal power, and letting these SUs know the signal power of the real PUs, a PUE attack could be discovered with a high probability.

Generally, the received energy E has the form of a chi square distribution. Since the number of samples is large in most cases, we can use the central limit theorem (CLT) to approximate the chi-square distribution by a Gaussian distribution.

Let H0, H1 and H¢1 denote the hypothesis of receiving no signal, a real PU signal, and a PUE attack signal, respectively. Let Pd (g1, g2) and Pf (g1, g2) denote the PUE attack detection and false alarm probabilities, respectively. We have

Pd (g1, g2) = Pr {g0 < E < g1|H1} + Pr {E > g2|H1}, and Pf(g1, g2) = Pr{E <g1|H1} + Pr{E > g2|H1}.

Data Fusion Driven Location Verification:

The proposed location verification approach does not need any dedicated positioning sensors [5]. In particular, suppose that the global database has recorded the location fingerprints of *M* PUE attackers as well as that of the real PU. The location verification will specifically identify the source of the received signal from the real PU and the PUE attackers. The location verification consists of three main steps. In step one, the SUs observe the input energy vector e and estimate the location of the source by finding the best matching entry in their local databases. In step two, the SUs send the estimated location to the cognitive BS for data fusion. The cognitive BS makes a final decision and identifies the signal source. In step three, the cognitive BS updates the global database according to the gathered fingerprinting information from the multiple SUs. Updated information is also sent to the SUs' local databases. Location estimation using Bayesian hypothesis testing is described as follows. Let Lm (m = 0, 1, 2… *M*) denote the location of the signal source, where *L*0 corresponds to the real PU and *L*{1, 2, …, *M*} correspond to the attackers, respectively. The input energy vector e follows a parameterized probability density function with the parameter stored in the database. Specifically, the probability density function of e under the hypothesis that the source is located in *Lm* is denoted f(e|Lm). The estimation of the location of the source of the signal is given by,

$$\hat{m} = \underset{m=0,1,2,\ldots,M}{\arg\max}\ \pi_m f\left(e \middle| L_M\right)$$

Where πm is the a priori probability of the hypothesis that the source is located in Lm.

The estimated location ^m is sent as the local decision to the cognitive BS for data fusion. The data fusion rules that lead to various global decisions are explained below:

• True *PU:* If all local decisions are identical and L0, that is, ^m =0, the cognitive BS will decide that the signal source is the true PU.
• PUE attack in a known location: If all local decisions are identical and m OE L{1, 2, …, M}, the cognitive BS will decide that the source is the PUE attacker in location Lm.

The final decision will be sent by the cognitive BS to the SUs. Both the local and global databases will be updated when a PUE attack is detected, either by the fast energy detector or by the location verifier. In particular, in the fast energy detector, the energy thresholds will be re-computed. In the location verifier, the probability density functions of the energy vector will be updated. In addition, if a new location of a PUE attacker is detected, a new profile will be created to track this new attacker. The communication overhead to update the two level database is proportional to the frequency of PUE attacks.

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 3, March 2017

5. ILLUSTRATIVE RESULT

We consider a scenario where there are three PUE attackers located in positions L1, L2, and L3. The SUs are distributed in a circular field with radius 1 km. The primary BS is located in the center, while L1, L2, and L3 are, respectively, 100 m, 200 m, and 300 m away from the center. Figure 4 demonstrates the effectiveness of the proposed detection approach. The PUE attack detection probability is shown interms of the false alarm probability. In this example, we have shown two cases when the sampling parameter varies.

The comparison indicates that more samples lead to higher detection probability. We can observe that the farther the PUE attacker is located from the primary BS, the easier it is to detect it. For example, when Ns = 12 and Pf = 0.1 percent, the PUE attack detection probabilities are 0.93, 0.95, and 0.97 When the PUE attacks are performed from locations L1, L2,and L3, respectively. The results indicate that the proposed approach works effectively and is able to successfully detect the attacks.

Defense Approaches at Various Protocol Layers:
To defend against PUE attacks, Effective countermeasures can be taken at different layers of the communications protocol stack.

Physical-Layer Approach:
Physical-layer techniques such as source separation signal design, spread spectrum, and directional antennas can be employed to deal with the intended interference from malicious PUE attackers. The key in the design of an efficient physical layer countermeasure is to exploit the a priority knowledge about the characteristics of the primary signal and its dissimilarity with the interference signal.

MAC-Layer Approach:
Undetected PUE attacks will steal bandwidth from the CR network. To let the SUs maintain moderate QoS performance, radio resource management (RRM) strategies such as admission control, spectrum handoff, and spectrum scheduling should be studied.

Network-Layer Approach:
In cognitive ad hoc networks, once the locations of the PUE attackers are estimated, a position based cognitive routing strategy could be employed to deal with the PUE attacks. Those SUs that are located within the attacking range of the PUE attackers should be considered temporarily unavailable. End-to-end routing paths should be established without crossing the unavailable SU nodes.

Cross-Layer Approach:
A cross-layer design framework may be set up to defend against PUE attacks. In the framework, the behavior of the detected PUE attacks is observed at the physical layer and reported to the upper layers, such as the RRM mechanism at the MAC layer or the routing mechanism at the network layer. We emphasize that even the undetected PUE attacks could be estimated in the physical layer by considering the theoretically derived detection probability the control parameters of the upper layer are jointly optimized considering the existence of PUE attacks.

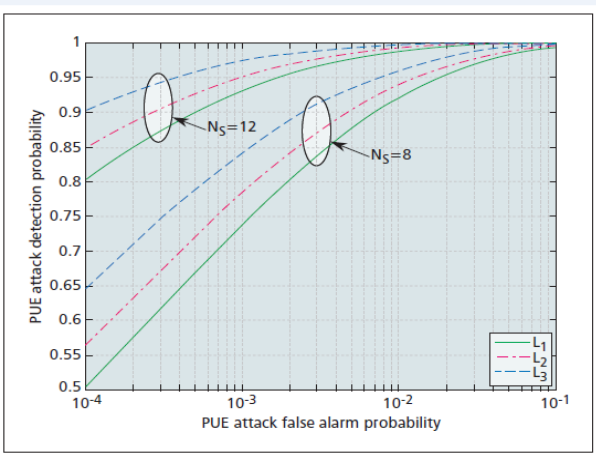

Figure 4. PUE Attack detection probability in terms of false alarm probability

6. CONCLUSION

This article focuses on the PUE attack security problem in CR networks. A comprehensive introduction to PUE attacks is presented and several technical challenges are discussed, including classification of attackers, conditions for successful PUE attacks, and impacts of PUE attacks on CR networks. After that, a database-assisted detection approach is proposed to efficiently discover PUE attacks. Multi-threshold fast energy detection and fingerprint-based location verification are integrated and driven by a two-level database. In addition, an admission control based defense approach is proposed to alleviate the impact of PUE attacks on the performance of CR networks. By reserving a portion of the channels for the handoff services, the dropping rate induced by successful PUE attacks can be clearly reduced. Illustrative results demonstrate that the reported detection and defense approaches are effective in discovering and defending PUE attacks in CR networks.

REFERENCES

[1] S. T. Zargar et al., "Security in Dynamic Spectrum Access Systems: A Survey," Proc. Telecommunications Policy Research Conf., Arlington VA, 2009.

[2] T. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," Proc. 3rd Int'l Conf. Cognitive Radio Oriented Wireless Networks (CrownCom 2008)

[3] R.Chen and J.-M. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," Proc. IEEE Workshop Networking Technologies for Software Defined Radio Networks, Sept. 2006.

[4] J. Mitola, Software Radios: Wireless Architecture for the 21st century, New York Wiley, 2000. Z. Chen et al., "Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 3, March 2017

Networks," Proc. Performance Computing and Communications Conference (IPCCC), 2009, IEEE 28th Int'l, Dec. 2009, pp. 208–15.

[5] S. Chen, K.Zeng, and P. Mohapatra, "Hearing is Believing: Detecting Mobile Primary User Emulation Attack in White Space," Proc. IEEE Int'l. Conf. Comput. Commun. Mini Conf., 2011.

[6] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks," IEEE Trans. Commun., vol. 60 , no. 9, 2012, pp. 2635–43.

[7] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," Proc. IEEE Int'l Conf. Commun. (ICC), 2009.

[8] D. Pu et al., "Detecting Primary User Emulation Attack in Cognitive Radio Networks," Proc. IEEE Global Telecommunications Conf., Dec. 2011.

[9] C. R. Stevenson et al., "IEEE 802.22: The First Cognitive Radio Wireless Regional Area Network Standard," IEEE Commun. Mag., Jan. 2009, pp. 130–38.

[10] Z. Gao et al., "Location privacy leaking from spectrum utilization information in database-driven cognitive radio network," in Proc. ACM Conf. Comput. Secur., 2012, pp. 1025–1027.

[11] Z. Gao et al., "Security and privacy of collaborative spectrum sensing in cognitive radio networks," IEEE Wireless Commun., vol. 19, no. 6, pp. 106–112, Dec. 2012.