International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014
ISSN 2091-2730

Cognitive Radio Networks: Defense against – PUEA

M.Mohamed Faisal

Asst.Prof /CSE,Anna University-chennai, faisalcsesrvec@gmail.coml ,9688110199.

Abstract— A latest communication technology is Cognitive Radio Network that network in which an un-licensed user can use a unbound channel in a spectrum band of approved user. Primary User Emulation Attack (PUEA) is one of the major threats to the spectrum sensing, which reductions the spectrum access probability. The primary user emulation attacks in cognitive radio networks in an un-licensed digital TV band. A reliable AES-assisted DTV scheme, in which an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve accurate identification of the authorized primary users. When combined with the analysis on the autocorrelation of the received signal, the presence of the malicious user can be detected accurately whether or not the primary user is present. The AES-assisted DTV scheme, the primary user, as well as malicious user, can be detected with high accuracy and low false alarm rate under PUEA.

Keywords— Cognitive Radio Network, Primary User Emulation Attack, DTV, AES-encrypted, DSA, CR networks, HDTV.

1. Introduction

In a cognitive radio network, a licensed user is called the primary user, whereas an unlicensed user is named the secondary user (1). If secondary users sense that primary users do not transmit, they can then use the spare spectrum for communications; otherwise, secondary users detect the presence of primary users and will restrain from transmitting. In this way, secondary users can make use of precious spectrum without interfering with the transmission of primary users. The existence of cognitive networks is justified by the fact that many spectra are not fully used by their dedicated users, and therefore allowing secondary user's access will give the opportunity to fully use the bandwidths and provide more spectrums to users. This is particularly true when part of the bandwidth is reserved for applications that have not yet been developed. The time necessary for such applications to come on to market may be long or may simply never occur and precious bandwidth may simply be wasted for a substantially long period.

Cognitive networks are radio networks where each band of frequency is occupied by two groups of users: the primary users that form the primary network and the secondary users that form the secondary network. The primary users are supposed to have priority over the secondary users: i.e. the performance of the primary network should be protected against the traffic of the secondary network. By protection we mean that the performance of the primary network should be guaranteed independently of the demand from the secondary network(2). Besides, the throughput and possession of the secondary network should vanish when the traffic load of the primary network increases. In other words the secondary users are only allowed to take the blank periods left by the primary users.

The problem is that the protocol used by the primary users, in short the primary protocol, often comes after a standardization process that ignores the secondary users. The connotation is that the design of the secondary protocol is sometimes harder and more costly than the design of the primary protocol because the secondary protocol must indeed embed the features of the primary protocol in order to knowledgeably give priority to primary user.

The cognitive radio technology will enable the users to determine which portions of the spectrum is (1) available and detect the presence of licensed users when a user operates in a licensed band (spectrum sensing), (2) select the best available channel (spectrum management), (3) coordinate access to this channel with other users (spectrum sharing), and (4) vacate the channel when a approved user is detected (spectrum mobility).

The main functions of Cognitive Radios are:

(i) Spectrum Sensing: It refers to detect the vacant spectrum and sharing it without harmful interference with other users. It is an important requirement of the Cognitive Radio network to sense spectrum holes, detecting primary users is the most efficient way to detect spectrum holes.

(ii) Spectrum Management: It is the task of capturing the best available spectrum to meet user Communication requirements. Cognitive radios should decide on the best spectrum band to meet the Quality of Service requirements over all available spectrum bands, therefore spectrum management functions are required for Cognitive radios, these management functions can be classified as:

• Spectrum analysis

• Spectrum decision

(iii) Spectrum Mobility: It is defined as the process when a cognitive radio user exchanges its frequency of operation. Cognitive radio networks target to use the spectrum in a dynamic manner by allowing the radio terminals to operate in the best available frequency band, maintaining seamless communication requirements during the transition to better spectrum.

(iv) Spectrum Sharing: It refers to providing the fair spectrum scheduling method, one of the major challenges in open spectrum usage is the spectrum sharing.

2. AES-assisted DTV scheme

AES-assisted DTV scheme: The primary user generates a AES-encrypted reference signal (pseudo-random). It is used as the sync bits in the field sync segments remain unchanged for the channel estimation purposes. At the receiving end, the reference signal is regenerated for the detection of the primary user and malicious user.

2.1 DTV Transmitter

The DTV transmitter obtains the reference signal as follow: first, generating a pseudo-random (PN) sequence, then encrypting the sequence with the AES algorithm. Note that a pseudo-random sequence is first generated using a Linear Feedback Shift Register (LFSR) with a secure initialization vector (IV). Once sequence is generated, it is used as an input to the AES encryption algorithm and a 256-bit secret key is used for the AES encryption so that the maximum possible security is achieved(3).Denote the PN sequence by x, then the output of the AES algorithm is used as the reference signal, which can be expressed as:

$$s = E(k, x) \quad ..(1)$$

Here k is the key, and $E(\cdot, \cdot)$ denotes the AES encryption operation. The transmitter then places the reference signal s in the sync bits of the DTV data segments.

The secret key can be generated and distributed to the DTV transmitter and receiver from a trusted 3rd party in addition to the DTV and the CR user. The 3rd party serves as the authentication Centre for both the primary user and the CR user, and can carry out key distribution. To prevent impersonation attack, the key should be time varying.

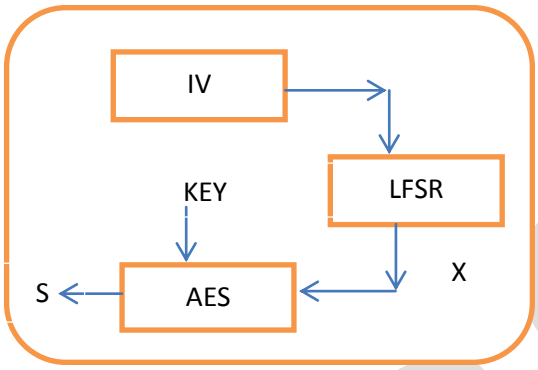

Fig. 1.DTV Transmitter.

2.2 DTV Receiver

The receiver regenerates the encrypted reference signal, with the secret key and IV that are shared between the transmitter and the receiver(3). A correlation detector is employed, where for primary user detection, the receiver evaluates the cross correlation between the received signal r and the regenerated reference signal s; for malicious user detection, the receiver further evaluates the auto-correlation of the received signal r.

The cross-correlation of two random variables x and y is defined as:

$Rxy = < x, y > = E\{xy *\}$..(2)

PUEA, the received signal can be modeled as :

$r = \alpha s + \beta m + n$..(3)

Where s is the reference signal, m is the malicious signal, n is the noise, α and β are binary indicators for the presence of the primary user and malicious user, respectively. More specifically, α = 0 or 1 means the primary user is absent or present, respectively; and β = 0 or 1 means the malicious user is absent or present, respectively.

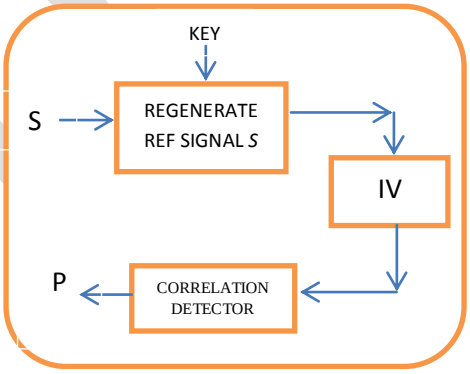

Fig. 2.DTV Receiver.

1) Detection of the Primary User: To detect the presence of the primary user, the receiver evaluates the cross-correlation between the received signal r and the reference signal s,

$$Rrs = < r, s > = \alpha < s, s > + \beta < m, s > + < n, s > = \alpha\sigma 2s \text{ ..(4)}$$

Where σ2s is the primary user's signal power, and s, m, n are assumed to be independent with each other and are of zero mean. Depending on the value of α in , the receiver decides whether the primary user is present or absent.

2) Detection of the Malicious User: For malicious user detection, the receiver further evaluates the auto-correlation of the received signal r,

$$Rrr = < r, r > = \alpha 2 < s, s > + \beta 2 < m, m > + < n, n > = \alpha 2\sigma 2s + \beta 2\sigma 2m + \sigma 2n \text{ ..(5)}$$

Where σ2m and σ2 n denote the malicious user's signal power and the noise power.

3. Primary user emulation attack(PUEA):

One of the major technical challenges regarding spectrum sensing is the problem of accurately distinguishing primary user signals from secondary user signals. In cognitive radio networks, primary users possess the priority to access the channel, while secondary users must always relinquish access to the channel over to the primary user and ensure that no interference is generated. Consequently, if a primary user begins to transmit across a frequency band occupied by a secondary user, the secondary user is required to leave that specific spectral band immediately. Conversely, when there is no primary user activity present within a frequency range, all the secondary users possess equal opportunity to the unoccupied frequency channel (5). Based on this principle, there exists the potential for malicious secondary users to mimic the spectral characteristics of the primary users in order to gain priority access to the wireless channels occupied by other secondary users. This scenario is referred to in the literature as primary user emulation (PUE).

3.1 **PUE Example**

In this network, there are three normal secondary users, named D1, D2 and D3. They are communicating with each other using the "white space" channels. D1 and D2 are using Channel 1, D2 and D3 are using Channel 2, and D1 and D3 are using Channel 3. At this time, a malicious secondary user, i.e., a primary user emulator appears on Channel 3. Since this malicious secondary user mimics the spectral characteristics of the primary users, D1 and D3 think that there is a primary user transmitting on this channel. According to the criteria of dynamic spectrum access network, D1 and D3 have to leave Channel 3 immediately. However, the other two channels are both occupied by the other users right now, so they cannot find any other available channels to continue their communication, making the connection terminated.

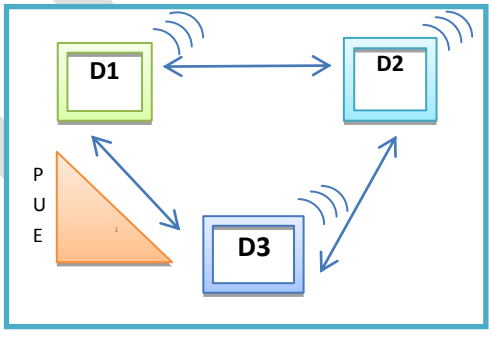

Fig. 3. Primary user emulation attack functions

.

3.2 Impact of PUE on DSA Networks:

There are several outcomes that can be incurred by PUE attacks in a dynamic spectrum access network:

• Unstable Connections: A network is frequently attacked by a primary user emulator, the secondary users in this network always have to leave their current channels and seek new channels. However, it is very likely that other channels are also occupied, so their connections have to be terminated.

• Spectrum Under-utilization: The original purpose of dynamic spectrum access is to address the problem of spectrum scarcity caused by FCC's fixed spectrum allocation.

In DSA, the secondary users can temporarily borrow unoccupied licensed spectrum (6). However, if there are several primary user emulators in the network; it is possible that all the available licensed channels are occupied by them, so the normal SU cannot find any channels to borrow. If it is the case, then the problem of spectrum scarcity is not solved at all.

• 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.

• Interference with Primary Users: Although the PUE attacks are solely aimed at secondary users, and the primary user emulators are supposed to obey the rule that they will not cause any interferences with the primary users. However, in a dynamic spectrum access network, the PU and SU exit in the same network, so any user's activates would have some impact on the others. Especially since primary user emulators mimic the spectral characteristics of the primary users, their transmission power is usually higher than that of the normal secondary users, so it can cause an interference with the primary users.

It is noted that PUE is different from traditional jamming in wireless networks. The malicious users do not aim to cause significant interference to the secondary users. The objective of the malicious users is to cause the secondary users to vacate the spectrum by having them believe that primary transmission is in progress. Thus, when PUE is successfully detected, the secondary users do not suffer degradation in the quality of their communication due to the transmission from the malicious users.

3.3 Classification of Attackers

Since the security problem caused by PUE attacks was identified, different types of PUE attacks have been studied (7).

We now introduce different types of PUE attackers associated with their classification criteria.

- Selfish & Malicious Attackers: A selfish attacker aims at stealing bandwidth from legitimate SUs for its own transmissions.
- Power-Fixed & Power-Adaptive Attackers: The ability to emulate the power levels of a primary signal is crucial for PUE attackers, because most of the SUs employ an energy detection technique in spectrum sensing. A power fixed attacker uses an invariable predefined power level regardless of the actual transmitting power of the Pus and the surrounding radio environment.
- Static & Mobile Attackers: The location of a signal source is also a key characteristic to verify the identity of an attacker. A static attacker has a fixed location that would not change in all round of attacks.

3.3.1 Impact of PUE attacks on CR Networks

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

• 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" are able to retrieve these otherwise wasted spectrum resources. 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 services. For instance, a malicious attacker could disturb the on-going services and force the SUs to constantly change their operating spectrum bands. Frequent spectrum handoff will induce unsatisfying delay and jitter for the secondary services.

• 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 resource because of the nature of dynamic spectrum access. The existence of PUE attacks significantly increases the connection unreliability of CR networks.

• Denial of Service: Consider PUE attacks with high attacking frequency; then the attackers may occupy many of the spectrum opportunities. The SUs will have insufficient bandwidth for their transmissions, and hence, some of the SU services will be interrupted. In the worst case, the CR network may even find no channels to set up a common control channel for delivering the control messages. As a consequence, the CR network will be suspended and unable to serve any SU. This is called Denial of Service (DoS) in CR networks.

• Interference with the primary network: Although a PUE attacker is motivated to steal the bandwidth from the SUs, there exists the chance that the attacker generates additional interference with the primary network.

4. DEFENCE AGAINST PUE ATTACK:

A reliable AES-encrypted DTV scheme, in which an AES-encrypted reference signals, is produced. It is used as the sync bytes of each DTV data frame. With the help of this a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver. It can then be used to accomplish precise detection of authorized PUs. This proposal necessitates no modification in hardware or system structure except of a plug-in AES chip. It can also be applied to today's DTV system directly to diminish PUEA, and achieve efficient spectrum sharing.

In the DTV system, the generated AES encrypted reference signal is also used for synchronization purposes at the authorized receivers. The proposed representation diminishes PUEA, enabling robust system operation, and guarantees resourceful spectrum sharing. The efficiency of the proposed approach is verified through both mathematical derivations. The PU generates a pseudorandom AES-encrypted reference signal there by highlighting that synchronization is definite in the proposed model.

4.1. EVALUATION FOR PRIMARY USER DETECTION

The system performance for primary user detection, under H0 and H1, through the evaluation of the false alarm rate Pf and the miss detection probability Pm. The false alarm rate Pf is the conditional probability that the primary user is considered to be present, when it is actually absent,

$$Pf = Pr(H1|H0) \quad ...(6)$$

The miss detection probability Pm is the conditional probability that the primary is considered to be absent, when it is present,

$$Pm = Pr(H0|H1) \quad ...(7)$$

4.2 EVALUATION FOR MALICIOUS USER DETECTION

The system performance for primary user detection(6), under H0 and H1, through the evaluation of False Alarm Rate and Miss Detection Probability for Malicious User Detection(7).Define P f,0 and P f,1 as the false alarm rate when α = 0 or α= 1, respectively,

$Pf,0 = Pr(H01|H00)$.. (8)

$Pf,1 = Pr(H11|H10)$..(9)

The overall false alarm rate is given by:

$Pf = P0Pf,0 + (1 - P0)Pf,1$ ... (10)

wherePO is the probability that ˆα = 0, i.e.,

$P0 = (1 - Pf)P(\alpha = 0) + Pm\,P(\alpha = 1)$... (11)

Similarly, the miss detection probabilities can be defined as Pm,0 and Pm,1, when the primary user is absent and present, respectively,

Pm,0= Pr(H00|H01). ..(12)

$Pm,1 = Pr(H10|H11)$....(13)

The overall malicious node miss detection probability is defined as:

$Pm = P0Pm,0 + (1 - P0)\,Pm,1$…(14)

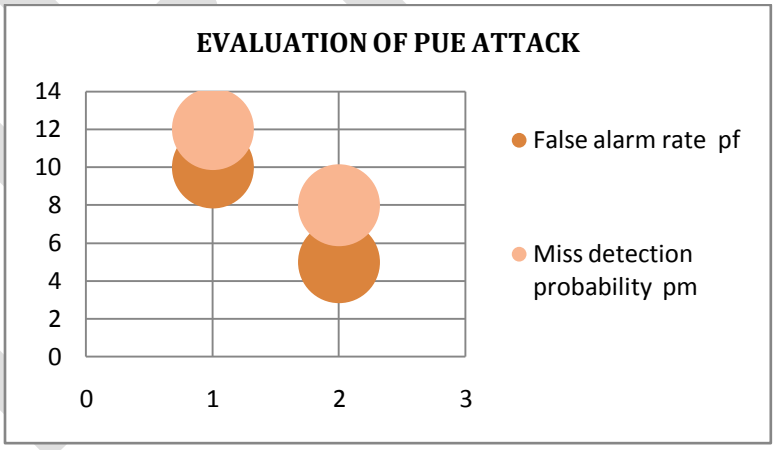

Fig. 4.Evaluation of primary user emulation attack.

5. CONCLUSION

A reliable AES-assisted DTV scheme was proposed for robust primary and secondary system operations under primary user emulation attacks. In the proposed scheme, an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and be used to achieve accurate identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. The practically feasible in the sense that it can effectively combat PUEA with no change in hardware or system structure except of a plug-in AES chip. Potentially, it can be applied directly to today's HDTV systems for more robust spectrum sharing. It would be interesting to explore PUEA detection over each sub-band in multi-carrier DTV systems.

REFERENCE:

[1] Ahmed Alahmadi, Mai Abdelhakim, JianRen, and Tongtong Li," Defense Against Primary UserEmulation Attacks inCognitive Radio Networks Using AdvancedEncryptionStandard"IEEE IFS,MAY2014,pp. 772-781.

[2] Deepa Das," Primary User Emulation Attack in CognitiveRadio Networks: A Survey", IRACST- IJCNWC,june – 2013,pp. 312-318.

[3] Ms. Shikha Jain," Emulation Attack in Cognitive Radio Networks: AStudy", IRACST- IJCNWC,apr – 2014,pp. 169-172.

[4] FCC, "Spectrum policy task force report," Federal Commun. Commission,Columbia, SC, USA, Tech. Rep. ET Docket No. 02-135, Nov. 2002.

[5] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrumaccess/cognitive radio wireless networks:A survey," Comput. Netw., Int. J. Comput. Telecommun.Netw., vol. 50,no. 13, pp. 2127–2159, Sep. 2006

[6] M. Thanu, "Detection of primary user emulation attacks in cognitiveradio networks," in Proc. Int. Conf. CTS, May 2012, pp. 605–608.

[7] R. Chen and J.-M.Park, "Ensuring trustworthy spectrum sensing incognitive radio networks," in Proc. IEEE Workshop Netw. Technol. Softw.Defined Radio Netw., Sep. 2006, pp. 110–119.

[8] R. Chen, J.-M.Park, and J. Reed, "Defense against primary useremulation attacks in cognitive radio networks," IEEE J. Sel. AreasCommun., vol. 26, no. 1, pp. 25–37, Jan. 2008.

[9] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primaryuser emulation attacks using belief propagation of location informationin cognitive radio networks," in Proc. IEEE WCNC, Mar. 2011,pp. 599–604.

[10] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary useremulation attacks in dynamic spectrum access networks," in Proc. IEEEInt. Conf. Commun., Jun. 2009, pp. 1–5.

[11] R. Chen, J. M. Park, and J. H. Reed, "Defense againstprimary user emulation attacks in cognitive radio networks,"IEEE Jl. on Sel. Areas in Commun.: Spl. Issue on CognitiveRadio Theory and Applications, vol. 26, no. 1, pp. 25-37, Jan.,2008.

[12] Z. Jin, S. Anand," Mitigating Primary User Emulation Attacks in DynamicSpectrum Access Networks using Hypothesis Testing", Mobile Computing and Communications Review, Volume 13, Number 2,pp-74-85.

[13] S. Anand, Z. Jin, and K. P. Subbalakshmi, "Ananalytical model for primary user emulation attacksin cognitive radio networks," Proc., IEEESymposium of New Frontiers in Dynamic SpectrumAccess Networks (DySPAN'2008), Oct.2008