February, 2014

Robust Asynchronous Authentication Protocol for Secure Cognitive Spectrum Sharing

Fatty Salem
Maged Ibrahim, *Helwan University*
I. Ibrahim

Robust Asynchronous Authentication Protocol for Secure Cognitive Spectrum Sharing

Fatty M. Salem*, Maged H. Ibrahim, and I. I. Ibrahim

Department of Electronics, Communications and Computers, Helwan University

1, Sherif st., Helwan, Cairo, Egypt

E-mails: fatty4com@hotmail.com, mhii72@hotmail.com, iibrahim@softhome.net

Abstract

Cognitive Radio is a regulated technique for opportunistic access of idle resources and it is expected that the golden service of spectrum sharing to be achieved via the TV white space. The successful deployment of cognitive radio networks and the realization of their benefits depend on the assignment of essential security challenges to resist the system misuses. In this paper, to prevent Primary User Emulation attack, we propose an authentication protocol based on the deployment of multiple stages of stationary "helper" nodes. Helper nodes are serving as bridges, they can detect the presence of the primary user, and enable secondary users to verify the cryptographic signatures included in their signals. However, we propose to distinguish each TV tower with a unique ID to be used to prevent wormhole attack asynchronously. We also illustrate the secure interactions between cognitive radio's entities to solve the problem of replay and wormhole attacks, and Byzantine failures problem.

Keywords: Cognitive Radio Networks; Primary User Emulation; Wormhole Attack; Replay Attack; Byzantine Failures.

1. Introduction

With the rapid development of wireless communication technology, the radio spectrum shortage problem is emerged. Consequently, Cognitive Radio (CR) technology (Mitola, 2000; Gabriella et al., 2008) has become a promising technology to increase the efficiency of spectrum utilization. Cognitive radios, which are "intelligent" radios, can learn from the environment and adapt their transmission/reception frequencies and parameters. Through adaptive change parameter settings for the study and decision-making, it can improve spectrum utilization and communication efficiency. In a cognitive radio network, unlicensed users (secondary users) are allowed by FCC (2008) to access licensed bands on a noninterference basis to legacy spectrum users (primary users).

To avoid interfering with Primary Users (PUs), Secondary Users (SUs) should sense the spectrum to detect whether a PU is using the spectrum or not. There are three main approaches for PU detection: energy detection, matched filter and feature detection (Ikuma et al, 2008; Kim and Shin, 2008; Bhargavi and Murthy, 2010; Ziafat et al, 2011). In Energy Detection (ED), SUs detect the PU's signal based on the sensed energy. It estimates the presence of the signal by comparing the received energy with a known threshold derived from the statistics of the noise. Furthermore, Matched-filtering is known as the optimal method for PU detection when the transmitted signal is known. Moreover, in feature

detection, SUs exploit the periodicity in the received primary signal to identify the presence of PU's signal.

Unfortunately, all previous detection methods couldn't provide a trustworthy result. If a malicious SU wants to gain an unfair use of the PU's idle spectrum or if the adversary tries to prevent SUs from accessing the spectrum, they can emulate the PU's characteristics when sending its own signals. This type of attack is called Primary User Emulation (PUE) attack (Chen et al, 2008; Chen et al, 2009; Hao and, 2012).

Another types of attacks that may threaten CR are wormhole and replay attacks. In wormhole attack (Hu et al, 2003), an attacker may receive packets at one point in the network, forward them and relay them to another point in the network. On the other hand, in replay attack (Chandrashekar and Lazos, 2010), an attacker may store information without authorization and then retransmit it to trick the receiver into unauthorized operations.

Many proposed approaches suggest that Distributed Spectrum Sensing (DSS) enhances sensing accuracy and reduces the need for very sensitive sensing technology, which can be costly (Weiss and Jondral, 2004; Mishra, 2006; Shankar et al, 2005) when compared with individual spectrum sensing. However, DSS raises a security concern: Byzantine failures which may be caused by either malfunctioning sensing terminals or Spectrum Sensing Data Falsification (SSDF) attacks. In either case, incorrect spectrum sensing data is reported to the fusion center, which can affect the accuracy of the sensing decision.

Although CR technology improves efficiency of spectrum utilization, PUs usually do not gain from opening up the spectrum in the opportunistic spectrum access. Hence, Federal Communication Commission (FCC 2003) states that "no modification to the incumbent system (i.e., primary user) should be required to accommodate opportunistic use of the spectrum by secondary users". As a result, any solution that requires changes to PUs is not desirable.

2. The Model

In this section, the system and the adversary models are described.

2.1. System Model

Entities in CRs are classified into four categories:

- **Primary Users (PUs):** They are the licensed users who are assigned with certain channels. However, following the FCC rules, no modifications are permitted to PUs to provide secure communication in CRNs. Here, the PU is a TV tower and, like a number of TV towers, it transmits its signals with an Effective Radiated Power of 1000 kW (like WCTV and KTVY towers).
- **Secondary Users (SUs):** They are the unlicensed users who are allowed to use the channels assigned to a PU only when they do not cause any harmful interference to the PU. The FCC limits the personal/portable devices to 50 milliwatts (mW) Equivalent Isotropically Radiated Power (EIRP) with no antenna gain, except that when operating on a channel adjacent to a TV station or other licensed station/service and within the protected coverage area of that service, operations will be limited to 40 milliwatts.
- **Helper Nodes (HNs):** They are stationary nodes serving as "bridges". They can detect the presence of the PU, and enable SUs to verify the cryptographic signatures included in their signals. In our proposed protocol, we classified HNs into two levels. HNs in the first stage are close to the PU and responsible for detecting the presence of the primary signals. HNs in the second stages are distributed over the coverage area of the PU and responsible only for delivering the spectrum information to SUs. Finally, to securely communicate with SUs, HNs are initialized with public/private keys and certificates from a certificate authority.

- **Certificate authority (CA):** It is responsible for deploying the HNs and loading them with necessary public/private keys, certificates parameters and certificates. Moreover, CA is responsible for providing SUs with a database of all registered TV towers and their IDs signed with its private key.

2.2. Adversary Model

A secure cognitive radio authentication protocol must withstands the following types of possible attacks:

- **Primary User Emulation (PUE) Attack:** The objective of the adversary is to deny using licensed spectrum to other SUs in CRN by emulating PUs' signals. A PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack (Chen and Park, 2006):
  - ***Selfish PUE attacks:*** In this attack, an attacker's objective is to maximize its own spectrum usage. When selfish PUE attackers detect a fallow band, they prevent other SUs from using that band by transmitting signals that emulate the signal characteristics of PU's signals.
  - ***Malicious PUE attacks:*** The objective of this attack is to obstruct the dynamic spectrum access process of legitimate SUs; that is, prevent legitimate SUs from using fallow licensed spectrum bands, causing denial of service. Unlike a selfish attacker, a malicious attacker does not necessarily use fallow spectrum bands for its own communication purposes. However, both attacks could have disruptive effects on CRNs.
- **Wormhole Attack:** A wormhole attack is a type of attack that usually occurs by two malicious nodes via an out-of-band connection in which the first adversary receives or eavesdrops packets at one area and then tunnels them to the next adversary that is located in another point of the networks through a long-range directional wireless link or even by using direct wired link (Çayırcı and Rong, 2009).
- **Replay Attack:** A replay attack is a type of attack that uses a previously recorded or captured message to gain access to somewhere one is not authorized to be or to trick receiver into false identification or authentication.

3. Existing Tools

In this section, the Digital Signature Algorithm and the Weighted Sequential Probabilistic Ratio Test are reviewed.

3.1. Digital Signature Algorithm

The Digital Signature Algorithm (DSA) is a part of the National Institute of Standards and Technology (NIST) Digital Signature Standard (DSS 1994). The DSS signature scheme can be summarized as follows:

Key Generation: Let p and q be large prime numbers, where $q|(p-1)$ and let $g \in Z_p^*$ be an element of order q. The private key $x \in_R Z_q^*$ is chosen randomly and the public key y can be computed, where:

$$g = h^{(p-1)/q} \bmod p. \quad (1)$$

$$y = g^x \bmod p. \quad (2)$$

Signature Algorithm: Let $H(m)$, be a hash of the message to be signed. The signer picks a random number $k \in_R Z_q^*$, calculates $k^{-1} \bmod q$, and sets:

$$r = g^{k} \bmod p \bmod q. \tag{3}$$

$$s = k^{-1}(H(m) + xr) \bmod q. \tag{4}$$

The pair (r,s) is a signature of m.

Verification Algorithm: A signature (r,s) of a message m can be publicly verified by computing:

$$v = (g^{(H(m)\cdot s^{-1})} \cdot y^{(r\cdot s^{-1})} \bmod p) \bmod q. \tag{5}$$

If $v = r$, then the message is accepted; otherwise the message is rejected.

3.2. Weighted Sequential Probability Ratio Test (WSPRT)

The Byzantine failures problem can be caused by malfunctioning sensing terminals or spectrum sensing data falsification (SSDF) attacks. Each case could affect the accuracy of the sensing decision. We suggest the Weighted Sequential Probability Ratio Test (WSPRT) (by Chen et al, 2008) to improve robustness against Byzantine failures. WSPRT is composed of two steps; the first step is a reputation maintenance step, and the second step is the actual hypothesis test. In the reputation maintenance step, a sensing terminal's reputation ratings are allocated based on the accuracy of a sensing terminal's sensing. The reputation value is set to zero at the beginning; whenever its local spectrum sensing report is consistent with the final sensing decision, its reputation is incremented by one; otherwise it is decremented by one. Under this rule, assuming N_i's reputation value is r_i, the last sensing report N_i sent to data collector N_0 is u_i, and the final decision is u, then r_i is updated according to the following relation: $r_i \leftarrow r_i + (-1)^{u_i+u}$.

The hypothesis test step of WSPRT is based on Sequential Probability Ratio Test (SPRT) (by Varshney, 1997). The idea of WSPRT is to modify the likelihood ratio used in the SPRT so that the decision variable also takes a sensing terminal's reputation into consideration. The new decision variable is:

$$W_n \leftarrow \prod_{i=0}^{n} \left(\frac{P[u_i \mid H_1]}{P[u_i \mid H_0]} \right)^{w_i} \tag{6}$$

Where w_i is defined as the weight of N_i and is a function of r_i : $w_i = f(r_i)$. The function of w_i and $f(\cdot)$ is as follows:

$$w_i = f(r_i) = \begin{cases} 0 & r_i \le -g \\ \dfrac{r_i + g}{\max(r_i) + g} & r_i > -g \end{cases} \tag{7}$$

The variable g(> 0) is used to ensure that enough weight is allocated to a sensing terminal that has a slightly negative reputation value. The fusion decision is based on the following criterion:

$$\begin{cases} W_n \ge \eta_1 \Rightarrow \text{accept } \mathrm{H}_1 \\ W_n \le \eta_0 \Rightarrow \text{accept } \mathrm{H}_0 \\ \eta_0 < W_n < \eta_1 \Rightarrow \text{take another observation} \end{cases} \tag{8}$$

The values of η_1 and η_0 are decided by $\eta_1 = \dfrac{1 - P_{01}}{P_{10}}$ and $\eta_0 = \dfrac{P_{01}}{1 - P_{10}}$. Where P_{01} and P_{10} are the tolerated false alarm probability and the tolerated missing probability, respectively.

4. The Protocol

In this section, the steps of the spectrum authentication protocol are described, i.e., the authentication of the PU signal at the first stage of HNs, its evaluation, and the interaction between CR's entities for secure broadcasting of spectrum status information.

4.1. PU Signal Authentication at HNs (First Stage)

Our objective is to enable SUs to decide whether a received signal is from a PU or not in the presence of various types of attacks. A key component of our approach is a set of 'helper' nodes placed within the coverage area of the PU (which is a TV tower in our system). Though we cannot modify to PUs due to the FCC constraint, we can put necessary mechanisms on each HN, including the use of cryptographic signatures.

We consider a network of SUs distributed over a large area, the IEEE 802.22 standard is designed to provide broadband wireless access services in a large area (typically 33 km radius). HNs in the first stage measure the power of the received signal using simple sensors due to their simplicity. The outcome of sensing by node HN_i is P_r, which represents an estimate of the received primary power at node HN_i. In dB, this is written as $P_r = P_t - PL$ where P_t is the transmitting power and PL is the pass loss.

The average large-scale path loss for an arbitrary transmitter-receiver (T-R) separation d, is expressed as a function of the path loss at a reference distance d_0 by using a path loss exponent, n. The reference path loss is calculated using the free space path loss formula given by friis free space equation (1964) or through field measurements at distance d_0:

$$PL(d_0)dB = 10\log\left[\frac{G_t G_r \lambda^2}{(4\pi)^2 d^2}\right] \tag{9}$$

Measurements have shown that at any value of d, the path loss $PL(d)$ (in dB) at a particular location is random and distributed log-normally about the mean distance-dependent value. That is:

$$PL(d)\ \ dB = \overline{PL}(d_0) + 10n\log(d/d_0) + X_\sigma \tag{10}$$

Where X_σ is a zero-mean Gaussian distributed random variable (in dB) with standard deviation σ (also in dB) reflecting the attenuation caused by fading. In case of no fading, this variable is 0.

σ is a parameter that typically range between *2–6 dB* and the path loss exponent n depends on the environments as shown in table 1.

Table 1: Pass Loss Exponents for Different Environments

Environment	**Pass loss exponent, *n***
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed Urban cellular radio	3 to 5
In building line of sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

Free space reference distance that is appropriate for the propagation environment. In large coverage cellular systems, 100 m reference distances are commonly used whereas in microcellular systems, much smaller reference distances (such as *10 m* or *1 m*) are used. We assume that close-in-reference distance is d_0 *=100 m*. For urban area cellular radio, we consider the path loss exponent is n=3.

HNs detect the power level of the received signals, if the power level exceeds a certain threshold γ, HNs decide that the received signal is that of the PU; otherwise HNs decide the presence of attacker.

Now, we need to determine the distance between the PU and the HNs at the first stage, and the threshold of the received signal power level, based on the requirements of probability of false alarm (i.e., an idle channel is detected as busy), and probability of missing (i.e., a busy channel is detected as idle).

4.2. Protocol Evaluation

To evaluate our proposed protocol, we first give the mathematical model of the received signal power, and then show the performance of the proposed authentication scheme in terms of the probability of false alarm and the probability of missing.

According to the log-normal path loss model in Eq. (10), since *PL(d)* is a random variable with a normal distribution in *dB* about the distance-dependent mean, so is $P_r(d)$, and the Q-function or error function (*erf*) may be used to determine the probability that the received signal level exceeds (or falls below) a particular level. The Q-function is defined as:

$$Q(z) = \frac{1}{\sqrt{2\pi}} \int_z^{\infty} \exp(-\frac{x^2}{2}) dx = \frac{1}{2}\left[1 - erf(\frac{z}{\sqrt{2}})\right] \tag{11}$$

The probability of detection (i.e., the PU's signal is correctly identified) is the probability that the received signal power level exceeds a certain value which can be calculated from the cumulative density function as:

$$\begin{aligned} P_D &= \Pr[P_r(d) \geq \gamma] = Q\left[\frac{\gamma - \overline{P_r}(d)}{\sigma}\right] \\ &= \frac{1}{2} - \frac{1}{2} erf\left[\frac{\gamma - \overline{P_r}(d)}{\sigma\sqrt{2}}\right] \\ &= \frac{1}{2} - \frac{1}{2} erf\left[\frac{\gamma - \left[P_t - (\overline{PL}(d_0) + 10n\log(d/d_0))\right]}{\sigma\sqrt{2}}\right] \end{aligned} \tag{12}$$

The probability of missing can be calculated from:

$$\begin{aligned} P_M &= \Pr[P_r(d) < \gamma] = 1 - P_D \\ &= \frac{1}{2} + \frac{1}{2} erf\left[\frac{\gamma - \left[P_t - (\overline{PL}(d_0) + 10n\log(d/d_0))\right]}{\sigma\sqrt{2}}\right] \end{aligned} \tag{13}$$

When placing HNs (in the first stage) at distance *d = 3,000 m*, the relations between the threshold γ and the probability of detection, and the probability of missing are shown in Figure 1 and 2.

The threshold γ can be determined based on the requirement for the probability of missing P_M or the probability of false alarm P_f . For practical applications, the IEEE 802.22 standard suggests both probabilities of false alarm and missing be less than 0.1 in terms of detecting PUs (Cordeiro et al, 2006). Herein, a stricter requirement that $P_M \leq 0.02$ was assumed, and thus from Figure 1 and 2, the threshold γ could be determined to be 11 watt to

keep the probability of detection more than 0.98 and the probability of missing less than 0.02 (at σ=*4dB*).

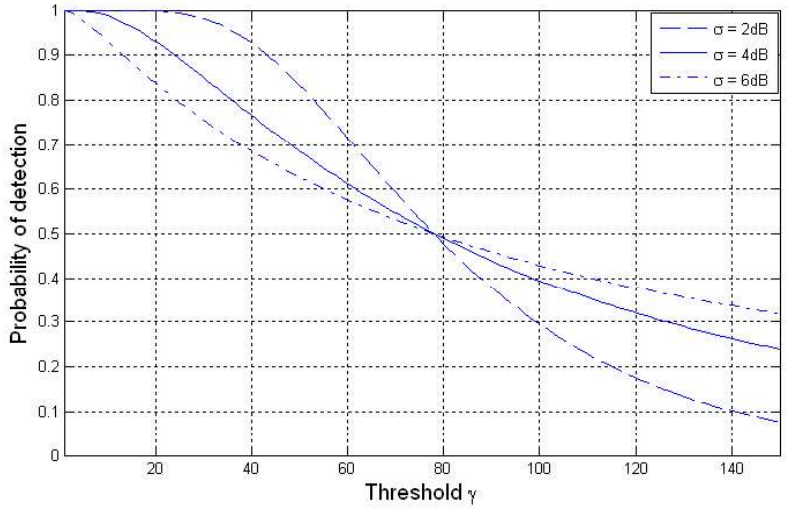

Figure 1: Probability of detection versus threshold γ

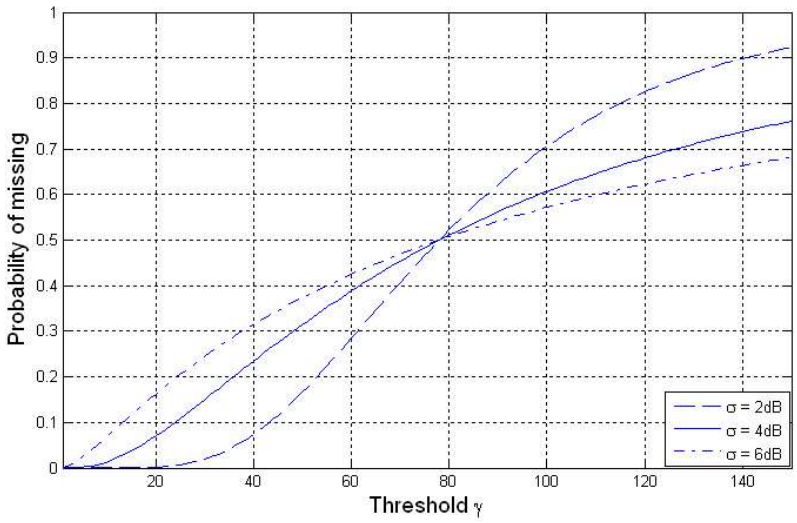

Figure 2: Probability of missing versus threshold γ

Following the FCC rules (2003), the unlicensed users are assumed to have a maximum transmission output power that is within the range from a few hundred milliwatts to a few watts. Fixed devices will be allowed to operate at up to 1 watt (W) transmitter output power and with a gain antenna to achieve 4 Watt EIRP. Hence, at the maximum permissible transmitting power (4 Watt EIRP), Figure 3 shows the probability of false alarm versus the distance between the attacker and the first level of HNs at different values of standard deviation. Herein, a stricter requirement that $P_f \leq 0.02$ was assumed, and thus the attacker should be placed at *4 m* (at minimum) away from the first stage of HNs at *4dB* standard deviation to keep the required low level of the probability of false alarm.

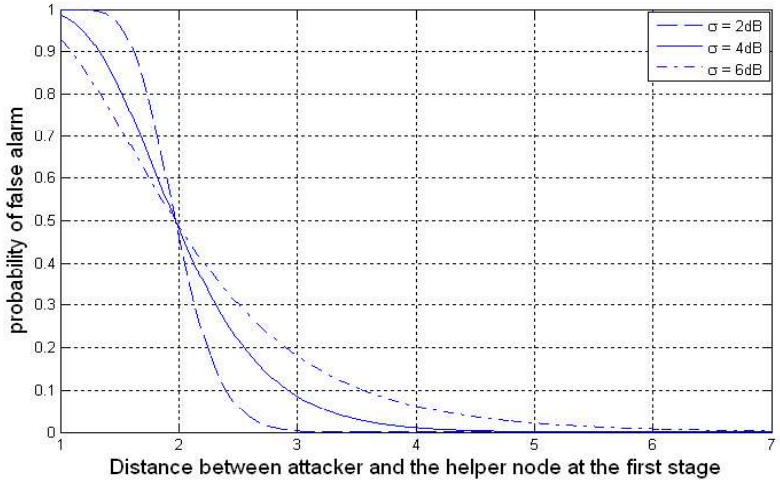

Figure 3: Probability of false alarm versus distance between attacker and first stage of HNs

4.3. Interactions between CR's Entities in Our System

Our proposed PU authentication scheme is depending on a first stage of HNs placed physically close to a PU, however HNs are physically bound to PU which is a TV tower covering an area of several kilometers (Wild and Ramchandran, 2005). Hence, HNs are NOT able to deliver spectrum information directly to all SUs in the coverage area of the tower due to the power constraint mandated by the FCC.

To solve this problem, we propose to distribute HNs in next stages over the coverage area of the TV tower. HNs in the first stage are responsible for (1) authenticating the PU's signal based on the received power level measurement, and (2) broadcasting spectrum status information to HNs in the next stages and/or to SUs. However, HNs in the next stages act as repeaters forwarding the received spectrum information to next stage of HNs and/or to SUs inside their coverage area. The idea is similar to the primary user authentication scheme (Salem et al, 2012) to resist against PUE attack. However, the scheme proposed by Salem et al (2012) hadn't discussed wormhole and replay attacks.

In the previous proposed authentication protocols (Chandrashekar and Lazos, 2010; alem et al, 2012), synchronization of common sequence numbers among all nodes in the network becomes a must to withstand replay attacks. While numerous methods were proposed using a packet leash technique (Hu et al, 2003; Safi et al, 2009) to detect and defend against the wormhole attack. The leashes can be grouped into geographical and temporal. In geographical leashes, all nodes should have knowledge of its own location in the network and insecure synchronized clock. Whenever a node sends the data packet, it includes its own recent location and transmission time in header. Therefore, the receiver can predict the neighbor relation by calculating the distance between itself and the sender. In temporal leashes, all nodes calculate the expiration time of each packet by using light's velocity and append this expiration time in the packet's header. Destination compares its own arrival time and expiration time in the packet to detect the wormhole attack. Such protocols depend on GPS (Global Positioning System) technology to determine nodes' location, however GPS technology is considered expensive or unusable because of the environment.

Unlike sensor networks which consist of autonomous nodes with limited battery and of base stations, CR is being intensively investigated for opportunistic access to the TVWS, where TV towers have a fixed location and energy level of hundreds of thousands of Watts. For this, the IEEE 802.22 standard (Stevenson et al, 2005) is designed to provide broadband wireless access services in a large area (typically *33 km* radius and in some instances base

station coverage may extend to *100 km*). Hence, it is not necessary to determine the SUs' accurate locations using GPS technology to determine by which TV tower SUs are covered. For example, it is adequate for a SU to determine that it is located in Florida to identify that it is covered by WCTV tower. Hence, we propose in our system to distinguish each TV tower with a unique ID (or area ID), and provide all SUs with a data base of all TV towers and their IDs. However, one may think about the amount of memory required to store such data base where SUs are mobile users with a little memory, but it is worth mentioning that there are only *65* registered TV towers in the entire United States as an example.

In our proposed protocol, each HN periodically sends the spectrum information to the next stage of HNs, however SUs first poll the HN's in the neighborhood by broadcasting a random number. Using power level detection, each helper node HN_i in the first stage constructs an occupancy vector V_i indicating the set of channels where legitimate PUs are active. V_i is an m-bit vector (m is the number of channels of the system) and the j^{th} bit of V_i is set to one if channel j is currently occupied; Otherwise, it is set to zero. The TV spectrum sensing process is repeated at the HNs at the frequency mandated by the FCC (e.g., every 2 seconds) (2008).

Now, we aim to describe interactions between CR's entities in our proposed protocol:

Interactions between CA and HNs: For each HN_i, the CA runs the key generation algorithm to generate a Public/Private key pair (Pu_{HNi}, Pr_{HNi}) with the certificate $cert_{HNi}$ for each HN_i. Where $cert_{HNi}$ is simply the signature of CA on $(Pu_{HNi} \,||\, AID)$ using CA's private key Pr_{CA}, where $cert_{HNi} = \{(Pu_{HNi} \,||\, AID), sign_{CA}(Pu_{HNi} \,||\, AID)\}$ and AID is the area ID. Hence, the CA provides each HN_i with $(Pr_{HNi}, cert_{HNi})$.

Secure broadcasting of authentic spectrum information to HNs in the next stages: HNs in the first stage are responsible for broadcasting spectrum status information periodically to HNs in the next stage. Each HN_i periodically transmits the following information: $\{(m_i \,||\, t_m) \,||\, sign_{HNi}(m_i \,||\, t_m) \,||\, cert_{HNi}\}$. Here, $sign_{HNi}(m_i \,||\, t_m)$ denotes the cryptographic signature of HN_i on the message $(m_i \,||\, t_m)$ where m_i is the vector V_i and t_m is the timestamp in the message. To prevent replay attack between HNs, the transmitted spectrum information has time limits to be updated. The time window width of the timestamp acceptance is determined according to the dynamic change of the spectrum which may be set from few seconds to several hours.

However, HNs in the next stages first check the correctness of timestamp in the received message then verify the authenticity and integrity of the received message by verifying the validity of the cryptographic signature $sign_{HNi}(m_i \,||\, t_m)$, the message that fails to be authenticated is discarded. If the message is verified, each HN_j in the next stage will retransmit the received spectrum information as follows: $(m_j \,||\, t_m \,||\, sign_{HNj}(m_j \,||\, t_m) \,||\, cert_{HNj})$

It is obvious that the clocks used by the communicating nodes are not precisely synchronized because HNs in the next stage will accept the received message as a fresh message if $(t_c\text{-}T\text{-}D \le t_m \le t_c+T)$ where t_c is the current time, the differences in clock values are less than some threshold value T and the messages sent from one device to another are subject to a maximum transit delay of D. Hence, the time of acceptance interval or the 'window of acceptance' is $[t_c\text{-}T\text{-}D,\ t_c + T]$.

HN-SU Interactions:

- SU → HN: Each SU generates a fresh random number N_c and sends *Request* to the nearest HNs. This random number is the challenge to HNs to resist against replay attack without the need to synchronize the network.
- HN → SU: The nearest HNs respond with the following information: $\{(m_i \,||\, N_c, sign_{HNi}(m_i \,||\, N_c), cert_{HNi}\}$.
- SU operates as follows:
  - It searches first for its legitimate AID* in its data base.

- It uses Pu_{CA} to extract the *AID* and Pu_{HNi} from each $cert_{HNi}$, then compares the extracted AID with the legitimate AID*. If they are the same, it continues the procedures; otherwise, it detects wormhole attacker and rejects the HN_i*'s* response.
- It then compares the extracted N_c with its generated N_c^*. If they are the same, it continues the procedures. Otherwise, it detects replay attacker and rejects the HN_i*'s* response.
- It then uses the extracted Pu_{HNi} to verify the signature $sign_{HNi}(m_i \,||\, N_c)$. If the signature is valid, it accepts m_i as a valid message; otherwise, it rejects the HN_i*'s* response.

Finally, it is possible for a HN to falsely detect a PU because of noise or interference in the wireless environment. Additionally, attacker may corrupt HNs and enforce them to send false spectrum sensing data. Many proposed schemes indicate that these problems can be addressed by distributing spectrum sensing. In our system, each HN acts as a sensing terminal that conducts local spectrum sensing and the local results are reported to a data collector. When a SU needs to conduct spectrum sensing, it becomes a data collector, collects local sensing reports from the nearby HNs, and executes data fusion and determines the final spectrum sensing result.

We suggest the WSPRT data fusion technique, that is more robust against Byzantine failures than the "OR" fusion rule, the "AND" fusion rule, and the "Majority" fusion rule (Pandharipande et al, 2005; Visotsky, 2005). SPRT may collect multiple reports from corrupted sensing nodes, which amplifies the effect of the attack. However, WSPRT makes a favorable tradeoff between data collection overhead and robustness of data fusion. Specifically, WSPRT improves the robustness of data fusion (against Byzantine failures) at the cost of requiring an increased number of local sensing reports.

5. Security Analysis

In this section, we evaluate the security of our proposed protocol.

PUE attack is prevented due to the deployment of multiple stages of HNs, and the performance evaluation of the proposed protocol is discussed in section 4.2.

HN's message fabrication attack: It stands for an attacker masquerading as a legitimate HNs by stealing or changing the message in a protocol. In our proposed protocol, if the attacker wishes to impersonate a HN, the attacker should forge the digital signature standard, which is assumed unforgeable, or send the stolen message. Moreover, if the adversary sends the stolen message to SU, then SU can detect that the message was used in another session by confirming the random number in that message. SU can detect the final spectrum sensing result and reject the reports received from corrupted HNs by running the existing weighted sequential probabilistic ratio test.

Replay Attack: Replay attack stands for an attacker storing a message in a previous session, then sending the stored message in the current session to masquerade as a legitimate HN. Our protocol is secure against this attack. The messages in our protocol are changed every session using a random number N_c. If SU sends a random number as a challenge to HN, HN sends a response that contains a signed challenge to SUs. Therefore, if the attacker sends the previous message to SU, SU can detect that the received message contains different random number ($N_c^* \neq N_c$) and hence, SU will immediately reject the received message. Thus, the attacker cannot attack our protocol by sending the previous message.

Wormhole attack: It stands for an attacker capturing messages at one point in the network and replaying them to another separate point in the network. However, in our proposed protocol, we assign an AID for each area covered by the same PU (here it is a TV tower).

Therefore, if the attacker sends a forwarded message from a remote area to SU, SU can detect that the received message contains different AID ($AID^* \neq AID$). Thus, the attacker cannot attack our protocol by sending a forwarded message from a remote area.

SUs' privacy preserving: Privacy is primarily regarded as preserving the anonymity of a SU and/or the privacy of its location. As the collaborative spectrum sensing (Cand and Zhang, 2009; Wang et al, 2010) is regarded as a promising approach to improve the performance of spectrum sensing in CRNs, several new security attacks in collaborative spectrum sensing, which aim to compromise SU's location privacy by correlating their sensing reports and their physical locations. A number of protocols (Rifà-Pous and Garrigues, 2011; Blasco et al, 2012; Gao et al, 2012; Li, 2012) are proposed to preserve the privacy of SUs. However, these protocols affect the performance of the collaborative sensing and complicate the computation at the SUs as SUs are responsible for sensing the spectrum and delivering the sensing reports to the data fusion in the prior proposed protocols. However, in our proposed protocol, HNs are the entities responsible for delivering the sensing reports to the data fusion instead of SUs. Moreover, in our proposed protocol, the secure interaction between SUs and HNs doesn't require any public parameters of SUs to be used in the protocol.

6. Conclusion

Our proposed protocol provided primary user authentication to secondary users through helper nodes in order to maximize secondary users' transmission opportunity. In our proposed protocol, the distributed helper nodes over the coverage area of the primary users serve as bridges to enable secondary users to verify the cryptographic signature carried by helper nodes' signals, while helper nodes could authenticate the primary user's signals based on measuring the received power signal level which is the main disparity between primary user and any other entity in the cognitive radio network. Hence, it could eliminate the primary user emulation attack, and compared to prior work, our system can provide stricter requirements for probability of false alarm and probability of missing. The proposed protocol could resist against replay and wormhole attacks efficiently in the absence of helper nodes synchronization. Moreover, we can improve the robustness of data fusion against Byzantine failures relying on helper nodes for delivering spectrum sensing reports to the data fusion instead of secondary users as proposed in prior works. Hence, we can preserve the secondary users' privacy in our proposed scheme. The proposed protocol requires a little memory to secondary users to store the database, public keys, and several digital signatures.

References

[1] Bhargavi, D. and C.R., Murthy, C.R., 2010. "Performance comparison of energy, matched-filter and cyclostationarity-based spectrum sensing", *IEEE Eleventh International Workshop on Signal Processing Advances in Wireless Communications (SPAWC),* Marrakech, pp. 1-5.

[2] Blasco, M.J., H., Rifà-Pous, and C., Garrigues, 2012. "Review of robust cooperative spectrum sensing techniques for cognitive radio networks", *Wireless Personal Communications* 67, pp 175-198.

[3] Cand, S. and Q., Zhang, 2009. "Achieving cooperative spectrum sensing in wireless cognitive radio networks", *ACM MC2R, Special Issue on Cognitive Radio Technologies and Systems*13, pp. 14-25.

[4] Çayırcı, E. and C., Rong, 2009. "Security in Wireless Ad Hoc and Sensor Networks", London: Wiley.

[5] Chandrashekar, S. and L., Lazos, 2010. “A Primary User Authentication System for Mobile Cognitive Radio Networks”, *In the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL),* Rome, pp. 1-5.

[6] Chen, R., and J. M. Park, 2006. “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks”, *In IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, pp. 110-119.

[7] Chen, R., J.M., Park, and K., Bian, 2008. “Robust distributed spectrum sensing in cognitive radio networks”, *In Proceeding of IEEE INFOCOM, the 27th Conference on Computer Communications*, Phoenix, AZ, pp. 1876 - 1884.

[8] Chen, R., J.M., Park, and J.H., Reed, 2008. “Defense against primary user emulation attacks in cognitive radio networks”, *IEEE Journal on Selected Areas in Communications* 26, pp. 25–37.

[9] Chen, Z., T., Cooklev, C., Chen, C., Pomalaza-Raez, 2009. “Modeling primary user emulation attacks and defenses in cognitive radio networks”, *IEEE 28th International Performance Computing and Communications Conference (IPCCC),* Scottsdale, AZ, pp. 208 – 215.

[10] Cordeiro, C., K., Challapali, and M., Ghosh, 2006. “Cognitive phy and mac layers for dynamic spectrum access and sharing of tv bands”, *In Proceedings of the first international workshop on Technology and policy for accessing spectrum (TAPAS ’06),* New York, NY, USA, ACM, DOI: 10.1145/1234388.1234391.

[11] FCC. Second report and order and memorandum opinion and order, FCC-08-260, 2008.

[12] Federal Communications Commission, 2003. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies. ET Docket, (03-108).

[13] Friis, H.T., 1946. “A Note on a Simple Transmission Formula”, *In Proceeding of the IRE* 34, pp. 254–256.

[14] Gabriella, M., Y., Hua, T., Kaiser, and X., Wang, 2008. “Cognitive Radio Technology”, *IEEE Signal Processing Magazine* 25, pp. 10 – 198.

[15] Gao, Z., H., Zhu, S., Li, S., Du, and X., Li, 2012. “Security and privacy of collaborative spectrum sensing in cognitive radio networks”, *IEEE Wireless Communications* 19, pp. 106 – 112.

[16] Hao, D. and K, Sakurai, 2012. “A Differential Game Approach to Mitigating Primary User Emulation Attacks in Cognitive Radio Networks”, *In IEEE 26th International Conference on Advanced Information Networking and Applications (AINA),* Fukuoka, pp. 495 – 502.

[17] Hu, C., A., Perrig, and D.B., Johnson, 2003. “Packet leashes: a defense against wormhole attacks in wireless networks”, *In Proceedings of 22th Annual Joint Conference of the IEEE Computer and Communications (INFOCOM),* pp. 1976–1986.

[18] Ikuma, T. and M., Naraghi-Pour, 2008. “A Comparison of Three Classes of Spectrum Sensing Techniques”, *In proceeding of IEEE global telecommunication conference (GLOBECOM),* New Orleans, LO, pp. 1-5.

[19] Kim, H. and K.G., Shin, 2008. “In-band spectrum sensing in cognitive radio networks: energy detection or feature detection? ”, *In Proceedings of the 14th ACM international conference on Mobile computing and networking MobiCom ’08,* New York, NY, USA, ACM, pp.14-25.

[20] Li, S., H., Zhu, Z., Gao, X., Guan, K., Xing, and Xuemin, 2012. “Location privacy preservation in collaborative spectrum sensing”, *In Proceedings of IEEE INFOCOM,* Orlando, FL, pp. 729 – 737.

[21] Mishra, S., A., Sahai, and R., Brodersen, 2006. “Cooperative sensing among cognitive radios”, *In proceedings of the IEEE International Conference on Communications,* Istanbul, pp. 1658 – 1663.

[22] Mitola, J., 2000. “Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio”, Dissertation, KTH Royal Institute of Technology, Stockholm, Sweden.

[23] National Institute of Standards and Technology, NIST FIPS PUB 186, (1994) Digital Signature Standard. U.S. department of Commerce.

[24] Pandharipande, A., J., Kim, D., Mazzarese, and B., Ji, 2005. “IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22”,. available at: http://www.ieee802.org/22/. Last accessed on August 12, 2013.

[25] Rifà-Pous, H. and C., Garrigues, 2011. “A secure and anonymous cooperative sensing protocol for cognitive radio networks”, *In Proceedings of the 4th international conference on Security of information and networks,* ACM, New York, NY, USA, pp. 127-132.

[26] Safi, S.M., A., Movaghar, and M., Mohammadizadeh, 2009. “A novel approach for avoiding wormhole attacks in VANET”, *First Asian Himalayas International Conference on Internet*, AH-ICI 2009, Kathmandu, pp.1-6.

[27] Salem, F.M., M.H., Ibrahim, E.A., Ali, 2012. “Secure Authentication Scheme Preventing Wormhole Attacks in Cognitive Radio Networks”, *Asian Journal of Computer Science and Information Technology* 2, pp. 52-55.

[28] Salem, F.M., M.H., Ibrahim, I.I., Ibrahim, 2012. “A primary user authentication scheme for secure cognitive TV spectrum sharing”, *International Journal of Computer Science Issue* 9, pp. 157-166.

[29] Shankar, S., S., Cordeiro, and K., Challapali, 2005. “Spectrum agile radios: Utilization and sensing architectures”, *In Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks,* Baltimore, MD, USA, pp. 160–169.

[30] Stevenson, C.R., C., Cordeiro, E., Sofer, and G., Chouinard, 2005. “RAN requirements”, IEEE 802.22-05/0007r46, Sep 2005.

[31] Varshney, P.K., 1997. “Distributed Detection and Data Fusion”, 1st edn Springer-Verlag New York, 1997.

[32] Visotsky, E., S., Kuffner, and R., Peterson, 2005. “On collaborative detection of TV transmissions in support of dynamic spectrum sharing”, *In Proceeding of IEEE DySPAN, First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks,* Baltimore, MD USA, pp. 338–345.

[33] Wang, B., K.J., Liu, and T.C., Clancy, 2010. “Evolutionary cooperative spectrum sensing game: how to collaborate?”, *IEEE Transaction on Communications* 58, pp. 890-900.

[34] Weiss, T.A. and F.K., Jondral, 2004. “Spectrum pooling: An innovative strategy for the enhancement of spectrum efficiency”, *IEEE Communications Magazine* 42, pp. S8-14.

[35] Wild, B. and K., Ramchandran, 2005. “Detecting primary receivers for cognitive radio applications”, *In Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks,* Baltimore, MD, USA, pp. 124–130.

[36] Ziafat, S., W., Ejaz, and H., Jamal, 2011. “Spectrum sensing techniques for cognitive radio networks: Performance analysis”, *In 2011 IEEE MTT-S International Microwave Workshop Series on Intelligent Radio for Future Personal Terminals (IMWS-IRFPT),* Daejeon, pp. 1-4.