Toward Secure Centralized Spectrum Sensing by utilizing Geographical Information

Chi-Yuan Chen\(^1\), Yao-Hsin Chou\(^2\), Han-Chieh Chao\(^{1,3,4}\), and Chi-Hsiang Lo\(^4\)

\(^1\)Department of Electrical Engineering, National Dong Hwa University, Taiwan
\(^2\)Department of Computer Science and Information Engineering, National ChiNan University, Taiwan
\(^3\)Institute of Computer Science & Information Engineering, National Ilan University, Taiwan
\(^4\)Department of Electronic Engineering, National Ilan University, Taiwan

Email: hcc@niu.edu.tw

Abstract—Spectrum utilization becomes more and more important while new techniques keep increasing and the spectrum bands remain finite. Cognitive Radio (CR) is a revolutionary technology to make use of the spectrum more effectively. In order to avoid the interference to the primary user, spectrum sensing must be sensitive. Cooperative Spectrum Sensing (CSS) is one way to increase the reliability of spectrum sensing. The information fusion technique is a key component of CSS. In this paper, we adopt a grid-like model for CR networks, and we utilize geographical information with reputational weights to propose a two-level fusion scheme called Secure Centralized Spectrum Sensing (SCSS). The simulation results show that as the attackers present high density aggregation at some areas, the correct sensing ratio of SCSS is increasing as well even when the number of attackers is very large.

Keywords—Cognitive Radio, Cooperative Spectrum Sensing, Centralized Spectrum Sensing, Information Fusion, Geographical Information.

I. INTRODUCTION

Today’s wireless networks are regulated by a fixed spectrum assignment policy, i.e. the spectrum is regulated by governmental agencies and is assigned to license holders or services on a long term basis for large geographical regions. The spectrum usage is concentrated on certain portions of the spectrum while a significant amount of the spectrum remains unutilized. This phenomenon would limit the growing of new technologies in wireless network. Dynamic spectrum access is proposed to solve these current spectrum inefficiency problems, and program aimed to implement the policy based intelligent radios is known as Cognitive Radios (CRs) \[16\]. CRs tried to share spectrum bands with the primary users \[1\]. There are two ways to share the spectrum band with primary users \[2\]: 1) Price-based sharing of spectrum and 2) Opportunity sharing of spectrum. The former could be realized when the primary network is willing to sell its spectrum hole to CR systems when it is not in use. In this case, the CR systems could be implemented in a simpler way and could guarantee no interference to primary users. Unfortunately it is not commonly be used by CR systems. For the latter approach, CR units utilize the spectrum band without the permission of primary networks. Spectrum sensing is the most important technique in this scheme.

In order to coexist with primary users without any interference, CRs have to be more sensitive than conventional radios. Without the awareness of primary networks, there is no connection or communication between CRs and primary networks directly. Secondary users (also called CRs) could only sense the spectrum band which might be used by primary users independently, secretly, and quietly. The security problem for CRs and Spectrum Sensing is rarely considered. However, such security problems cause serious impact on the fairness and efficiency for CRs. In this paper, we propose a two-level information fusion scheme called Secure Centralized Spectrum Sensing (SCSS) against the Spectrum Sensing Data Falsification (SSDF) attacks. We have three major contributions: 1) Utilizing the geographical information with reputational weights to reduce the impact of SSDF attacks, 2) While attackers present high density aggregation at some area, the correct sensing ratio increases. 3) The collection of geographical information without any signaling cost.

II. RELATED WORKS

Assuming that no secondary user would use the spectrum during spectrum sensing, we could decide spectrum between the two hypotheses \[6\]:

\[
x(t) = \begin{cases} 
H_0 & n(t) \\ 
H_1 & h \cdot s(t) + n(t) 
\end{cases}
\]

where \(x(t)\) is the complex signal received by CR, \(s(t)\) is the transmitted signal of the primary user, \(n(t)\) is the additive white Gaussian noise (AWGN), \(h\) is the complex gain of an ideal channel. The null hypothesis \(H_0\) states that no licensed user is detected, and the alternative hypothesis \(H_1\) indicates that primary user signal is detected. Such transmitter detection techniques could be classified into: energy detection \[3\], matched filter detection \[4\], and cyclostationary feature detection \[5\].

A. Cooperative Spectrum Sensing

Spectrum sensing in CR would be challenged by some uncertainties such as channel fading or shadowing. The low received signal strength is not enough for CR to detect whether the primary user exists or not. The impact of noise uncertainty is also important. A prior knowledge of noise is required during sensing, but it’s not available in practice. Because of

This research was partly funded by the National Science Council of the R.O.C. under grants NSC 98-2219-E-197-001 and NSC 98-2219-E-197-002
such channel uncertainties, spectrum sensing must be sensitive enough to overcome such uncertainties. On the other hand, hidden terminal problem is also a threat to CR. If a secondary node is out of the range of primary transmitter and may generate false decisions, it will interfere the primary user.

Cooperative spectrum sensing is a possible way to solve these threats mentioned above. By cooperation within secondary users, more information could be taken during spectrum sensing. This kind of sensing technique can be implemented either in a centralized or in a distributed way [2, 6]. In the centralized approach, as illustrated in Fig. 1, the CR base-station receives all the sensing information from the secondary users and determines the state of spectrum. Then the local results are sent to a CR base station that performs data fusion and determines the final spectrum sensing result. The sensing terminals may return different results due to some reasons such as the distance between the primary user and the sensing terminals, shadowing, or fading. Each time a secondary user requests an access of a certain spectrum, a permission of the CR base station is needed. The cost of this scheme might be expensive, but it’s effective to manage to spectrums and by considering reputation of node. Distributed approach requires exchange of observations among all the secondary users. Each secondary user plays a role of fusion center, and chooses the best channel from the available spectrum, based on the local data available to them (often from the neighbor nodes). This scheme could be easier implemented with low cost, but it’s hard to manage and some collision might be happened.

![Figure 1. Centralized Spectrum Sensing Model.](image)

**B. Threats to Cognitive Radios**

**Incumbent Emulation (IE) attacks [7]:** Incumbent users have the higher priority than secondary users to use the spectrum. A malicious secondary user could transmit signals that emulate the characteristics of an incumbent to gain the higher priority. If the primary transmitter has a fixed location, such as TV systems, it could be verified by comparing the location and signal power between the incumbent signal and the detected signal. However for another type of mobile incumbent user, it’s a more difficult problem. Radio environment map (REM) is a possible solution. By comparing its observed location and the activities stored in the REM database, it’s possible to verify mobile incumbent user.

**Spectrum Sensing Data Falsification (SSDF) attacks [7]:** Another threat to Cooperative Spectrum Sensing is that attackers may send false results to a data collector, and the fusion center would make a wrong decision. Therefore, the fusion scheme must be robust enough.

**C. Data Fusion Techniques**

SSDF attacks would undermine the optimality of the test and potentially cause miss detection or false alarm instances. These data fusion techniques treat all the terminals indiscriminately, and applying some schemes to filter the data is needed. Some basic data fusion techniques have been studied. In order to compare with existing techniques, we simply discuss Weighted Sequential Probability Ratio Test [8] below. Other basic fusion techniques could be found in Decision fusion [13, 8], Bayesian detection [14, 8], and The Neyman-Pearson test [15, 8] for further reading.

**Weighted Sequential Probability Ratio Test [8]:** WSPRT is composed of two steps. The first step is a reputation maintenance step. A sensing terminal’s reputation rating is allocated based on the accuracy of its sensing results. The reputation value is set to zero at the beginning; whenever its local spectrum sensing report by node i is consistent with the final sensing decision, its reputation is incremented by one; otherwise it is decremented by one. In the second step, hypothesis test of WSPRT is based on Sequential Probability Ratio Test (SPRT) [9]. The decision variable is also takes a sensing terminal’s reputation into consideration. $W_n = \prod_{i=0}^{n} \left( \frac{P[i|H_1]}{P[i|H_0]} \right)^{w_i}$. (2)

$n$ is a variable and can be different from $m+1$. The $w_i = f(\tau_i)$, where $f$ is a function to estimate the weight $w_i$ of node $i$ by considering reputation $\tau_i$, and $f(\cdot)$ is defined as following:

$$f(\tau_i) = \begin{cases} 0 & \tau_i \leq -g \\ \frac{\tau_i + g}{\max(\tau_i) + g} & \tau_i \geq -g \end{cases}, \quad (3)$$

where the variable $g(>0)$ is used to meet the requirement of ensuring that enough weight is allocated to a sensing terminal.

All the schemes above need the same knowledge of a priori probabilities i.e., $P[u_i|H_1]$ and $P[u_i|H_0]$. But in practice such data may not be available. Even if such data is available, because a priori probabilities change with a sensing terminal’s location, empirical data would need to be re-collected every time the sensing terminal moves to a different location.

WSPRT propose an approach to calculate the probabilities based on the log-normal shadowing path loss mode. The log-normal shadowing path loss model can be represented as:

$$PL(d) = PL(d_0) + X_\sigma = PL(d_0) + 10l \log \left( \frac{d}{d_0} \right) + X_\sigma. \quad (4)$$

$d$ is the transmitter-receiver distance, $PL(d)$ is the path loss as a function of $d$, $PL(d_0)$ is the mean of $PL(d)$, $X$ is a zero-mean Gaussian distributed random variable with standard deviation, $d_0$ is a close-in reference distance which is determined from measurements close to the transmitter, and $l$ is the path loss exponent which indicates the rate at which the path loss increases with distance. All items in the equation are in $dB$.

The received power $P_r = P_t - PL(d)$, where $P_t$ is the transmitted power, and both $P_r$ and $P_t$ are in $dB$. Assuming the
receiver uses an energy detector with a detection threshold \( r \), the a priori probabilities under \( H_2 \) can be computed as:

\[
P(u_i = 1|H_2) = P(P_r > r|H_2) = P(X_i < P_t - PL(d) - r)
\]

\[
= Q \left( \frac{r - P_t + PL(d)}{\sigma} \right) \quad (5)
\]

\[
P(u_i = 0|H_2) = 1 - P(u_i = 1|H_2) = Q \left( \frac{P_t - r - PL(d)}{\sigma} \right) \quad (6)
\]

In the above derivations, \( (P_r > r) \) represents the condition that an energy detector detects a received signal, \( P_r \) is replaced with \( P_t - PL(d) \), and \( PL(d) \) is replaced with the expression shown in (4). When hypothesis \( H_0 \) holds, \( P_r = n_0 \), where \( n_0 \), can be regarded as a Gaussian noise power with mean \( n_0 \) and standard deviation \( n \). Similarly the a priori probabilities under \( H_0 \) can be computed as:

\[
P(u_i = 1|H_0) = Q \left( \frac{r - n_0}{\sigma} \right), \quad (7)
\]

\[
P(u_i = 0|H_0) = Q \left( \frac{n_0 - r}{\sigma} \right). \quad (8)
\]

The advantage of this approach is that the calculation method utilizes the physical location of a sensing terminal. Thus, when a sensing terminal moves to a different location, a priori probabilities can be immediately calculated without waiting to collect new empirical data.

III. SECURE CENTRALIZED SPECTRUM SENSING (SCSS)

A. System model of SCSS

In order to strengthen the correction of spectrum sensing, we adopt the centralized spectrum sensing model to our system. The system model is shown in Fig.2. A fusion center called CR base station is needed, and the proposed Secure Centralized Spectrum Sensing (SCSS) is implemented as an information fusion mechanism inside. The sensing terminal is denoted as \( N_k (0 \leq k \leq m) \). During the observation time, every sensing terminal \( N_k \) starts to listen whether the incumbent signal exists or not and returns the result as \( u_k \). The CR base station takes these sensing results into account. By adopting these two proposed weights includes the Geographical Weight and the Reputation Weight, so that the CR base station could make a final decision \( u \). Whenever any secondary user attempts to use the spectrum band, it must send a request to the CR base station. After receiving the request, the CR base station retrieves sensing result \( u_k \) from each sensing terminal. According to all the retrieved \( u_k \), the CR base station determines whether the CR area is occupied and return the status \( H_0 \) or \( H_1 \) to the secondary user.

In order to improve the correctness of spectrum sensing (especially in the areas far from the primary transmitter), and to increase the difficulty of attacking, we take the geographical information into account while aggregating the sensing information. With the aid of multiple antennas (Sectorised Antennas and Angle-of-Arrival estimation algorithms) and employing Time-Difference-Of-Arrival (TDOA), the CR network area can be divided into several grids as shown in Fig.3 [10]. In the center is the CR base station, and from the center to the outside, we assigned every circle a number \( i \) in turn. For each pizza-like segment, we assigned a number \( j \) to each one clockwise. Finally, we can use \( G(i,j) \) to represents each grid. Grids are too small for the inner circle, so we combine these grids into one grid.

\[ u = \prod_{k=0}^{n} \left( \frac{P[u_k|H_1]}{P[u_k|H_0]} \right)^{w_k} \]

(9)

where \( n \) is the number that the CR base station takes for fusion. A global decision value \( S_n \) is defined for the final spectrum state as following:

\[
S_n = \prod_{k=0}^{n} \left( \frac{P[u_k|H_1]}{P[u_k|H_0]} \right)^{w_k} ,
\]

(9)

where \( n \) is the number that the CR base station takes for fusion. The sensing information fusion will stop until:

\[
S_n \geq \eta_1 \quad \rightarrow \text{accept } H_1
\]

\[
S_n \leq \eta_0 \quad \rightarrow \text{accept } H_0
\]

\[
\eta_0 \leq S_n \leq \eta_1 \quad \rightarrow \text{take another sample}
\]

(10)