Malicious User Detection in Cooperative Environment in Cognitive Radio Networks

Sripriya. N1, Geetha Ramani. J2

1PG Scholar, ECE Dept, SNS College of Technology
Coimbatore, India
sriprn@gmail.com

2Assistant Professor, ECE Dept, SNS College of Technology
Coimbatore, India
geetharamanij@yahoo.co.in

Abstract: Cognitive radio efficiently utilizes the unused spectrum for secondary usage without interfering a primary licensed user. In cooperative environment, a primary licensed user can share spectrum occupancy information with a secondary user to enable dynamic spectrum access. However, a secondary user needs to verify accuracy of the spectrum occupancy information and it comes the legitimate primary users. Without the verification, a malicious user can falsify the spectrum occupancy information. This can result interference to the primary users and minimize available spectrum for the secondary usage. Proposed technique verifies that the source of the spectrum occupancy information is from the legitimate primary user thereby maximizing the spectrum utilization efficiency and minimizing any interference to the primary licensed users.

Keywords: Cognitive Radio (CR); Primary User (PU); Secondary User (SU); Cooperative Spectrum Sensing; Security

1. Introduction

Spectrum is the lifeblood of communication systems. Without spectrum there is no electromagnetic communication. The radio frequency spectrum is the medium between the transmitters and receivers in wireless communication. The radio spectrum is becoming scarce due to the increasing growth of the wireless communication technology and the high requirement of capacity and data rates for various applications.

Spectrum Sensing is a key step used in cognitive radio network. Basic requirement of cognitive radio is to scan the radio frequency spectrum and determine fallow bands which can be used in an opportunistic manner to increase spectrum efficiency. The most efficient way to identify white space is to detect primary users. Primary user network & secondary user network are physically separate from each other. Secondary users do not get direct feedback from the primary users about their transmission. So in order to detect to primary user transmission the secondary users have to depend on their sensing ability to. There are two different types of spectrum sharing scenarios. They are:

- Cooperative scenario
- Non-cooperative scenario

In cooperative scenario, a primary user provides secondary users with all information regarding the occupancy of the spectrum and about the unused spectrum so that the secondary users make use of that unused spectrum and keep away from the occupied spectrum. In the non-cooperative scenario, a secondary user needs to sense the spectrum for the unused spectrum and use that spectrum band without causing any interference to the primary user. In the cooperative scenario, a malicious user can masquerade as the primary user and provide false information to the secondary user regarding the occupancy of the spectrum, such as the spectrum is unoccupied and the secondary user can use though the primary user occupies the spectrum. With the information the information provided, the secondary user tries to occupy the spectrum and as a result, interference takes place between the primary user and secondary user. In some cases, the malicious user informs the secondary user as the spectrum is occupied even though the spectrum is free and as a result the spectrum is not utilized either by primary user or by secondary user. Because of these issues, a secondary user must make sure that the information regarding the occupancy of the spectrum is provided by a legitimate primary user. Proposed scheme identify that the information is provided by legitimate users.

2. Cooperative spectrum sensing

Under fading or shadowing, received signal strength can be very low and this can prevent a node from sensing the signal of interest. Noise can also be a challenge when energy detection is used for spectrum sensing, although there are spectrum sensing techniques that are robust in the presence of noise, such as feature detection approaches. Due to a low signal-to-noise ratio (SNR) value, the signal of interest may not be detected.

The idea of cooperative spectrum sensing is the collaboration of nodes on deciding the spectrum band used by transmitters emitting the signal of interest. Nodes send either their test statistics or local decisions about the presence of the signal of interest to a decision maker, which can be another node. Through this cooperation, the unwanted effects of fading, shadowing and noise can be minimized. This is because a signal that is not detected by one node may be detected by another. There are two forms of cooperation in spectrum sensing: hard combination and soft combination.

In the hard combination scheme, local decisions of the nodes are sent to the decision maker. The major advantage of the hard combination scheme is that it requires only one bit of overhead. Additionally, it only requires a low-bandwidth
channel by which the decisions are sent. In the soft combination scheme, nodes send their sensing information directly to the decision maker without making any decisions. The decision is made at the decision make by the use of this information. Soft combination provides better performance than hard combination, but it requires a wider bandwidth for the control channel. It also requires more overhead than the hard combination scheme. In proposed scheme, three-bit hard combination scheme is used.

Figure 1 shows a functional block diagram of proposed cooperative spectrum sensing and localization scheme. All nodes apply coarse resolution sensing to obtain a quick examination of the spectrum of interest. Three-bit hard combination combines the coarse resolution sensing results to detect the signals in the air and to determine the frequency bands that need to be exhaustively inspected. Fine resolution sensing is applied to these frequency bands to narrow down the spectral bands of the signals in the air. Localization block is to estimate the position and EIRP of the transmitters emitting these signals, given the RSS and relative node position values.

For finding the locations of the transmitters, the decision maker applies the wavelet-based MRSS scheme.

To evaluate the performance of the RSS based localization scheme, mean square error (MSE) for position and the average absolute power estimation error (PEE) are used.

\[
MSE = \frac{1}{N_{\text{sim}}} \sum_{n=1}^{N_{\text{sim}}} \sqrt{(x - x_{\text{est},n})^2 + (y - y_{\text{est},n})^2} 
\]

\[
PEE = \frac{1}{N_{\text{sim}}} \sum_{n=1}^{N_{\text{sim}}} |P_t - P_{\text{est},nt}|
\]

Figure 2 shows the flowchart for signal source verification. Sensed signal is verified whether it is from legitimate user or from malicious user. If the characteristics, location and power level matches that of primary user then the signal is from trustworthy user else it is concluded that it is from untrustworthy user.

In proposed technique, distance between a cognitive user and other users is calculated based on location coordinates as well as received power level. If the distance calculated with both of these techniques matches, then the user is a trustworthy user. In other case, it would be considered malicious user. Relative trustworthiness of a user is given by

\[
\rho = \min \left( \frac{d_1}{d_2}, \frac{d_3}{d_4} \right)
\]

Based on the noise level, the distance calculated with received power level may not be very accurate. However, statistically, the distance calculated with both of the methods
3. Results

Simulation is carried out in MATLAB. Figure 3 depicts the effect of number of nodes cooperating on detection percentage at three different SNR values. Lower detection percentage is obtained when SNR is low.

Figure 3: Detection Percentage

Figure 4 depicts the plots of the position estimation MSE versus number of nodes for different values of number of samples when $\sigma=3$.

Figure 4: MSE VS Number of Nodes

Figure 5 shows the effect of the number of nodes on position estimation MSE for different values of $\sigma$ when the number of samples is 200.

Figure 5: MSE VS Number of Nodes

Figure 6 shows the effects of number of nodes on average absolute power estimation error for different values of number of samples.

Figure 6: PEE VS Number of Nodes

Figure 7 shows the effects of number of nodes on average absolute power estimation error for different values of standard deviation $\sigma$.

Figure 7: PEE VS Number of Nodes

Figure 8 shows the noise in between received signal power and distance (SNR=-24dB).

Figure 8: Received Signal Power

Figure 9 shows the trustworthiness of a user. If the SNR value increases, the trustworthiness increases. If the trustworthiness reaches to 1, then we can conclude that we are communicating with the primary user and not with the malicious user. Even if the trustworthiness is approximately equal to 1, we can trust the primary user, because there may be some interfering noise that will reduce the trustworthiness. Malicious user’s trustworthiness remains constant at 0.6, even though the SNR value increases.
Figure 9: Trustworthiness of a user

4. Conclusion

1. Through the proposed scheme, Wavelet-based multi-resolution spectrum sensing (MRSS) and received signal strength (RSS)-based localization methods were adapted to implement spectrum sensing and localization. With these methods
   - Signal detection performance is maximized
   - Accuracy of position is maximized
   - Power estimation with minimal computation complexity

2. Proposed technique verifies the source of information is from legitimate primary user and not from a malicious user masquerading to be a primary user (Primary User Emulation Attacker).

References