Location Detection Model for Primary User Emulation Attacks Avoidance in Cognitive Radio Networks

Diafale Lafia
Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife, Nigeria
dlafia@pg-student.oauife.edu.ng

Mistura Sanni
Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife, Nigeria
msanni@oauife.edu.ng

Rasheed Adetona
Department of Mathematics
Obafemi Awolowo University
Ile-Ife, Nigeria
adetonara@oauife.edu.ng

Bodunde Akinyemi
Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife, Nigeria
bakinyemi@oauife.edu.ng

Ganiyu Aderounmu
Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife, Nigeria
gaderun@oauife.edu.ng

***Abstract* - Cognitive Radio Networks (CRNs) have been developed to improve the usage of the spectrum in an opportunistic manner. The coexistence mechanisms among secondary users and legitimate users of the spectrum are defined. A specific feature of CRNs is that it is prone to various kinds of attacks and failures that can compromise the security and performance of the network. This study developed a Time Difference of Arrival (TDoA) -based technique for locating Primary User Emulation (PUE) attackers and minimizes the estimation error in detecting the location in Cognitive Radio Networks. The simulation results show that the proposed model has improved accuracy in avoiding primary user emulation attacks with fewer errors. It was concluded that the proposed location model with respect to minimizing estimation errors could be used for primary user emulation attack avoidance in Cognitive Radio Networks.**

Keywords: Cognitive radio, primary user emulation attacks, location detection, TDoA, network

I. INTRODUCTION

Cognitive Radio (CR) technology is developed to be an implementation of the dynamic spectrum access paradigm [1]; [2]. Based on the result, cognitive radio can sense its surrounding environment and decides and adjusts its parameters without external intervention. Cognitive radio can also sense the presence of the primary user automatically and autonomously. When a CR user identifies a Primary User (PU) transmitting in the spectrum, it has to leave the spectrum and search for another which is idle or has a hole in the spectrum that is unoccupied by any primary user. All secondary users can access the spectrum without any priority [3].

Remote Method Invocation (RMI) is one of the key elements of the framework for implementing cognitive functionality. These specific features of cognitive radio predispose the network to threats. This paper proposes a Time Difference of Arrival (TDoA) -based method for the transmitter's location. The physical location of radio frequency transmission sources has been a hot topic for many years in wireless applications. Time Difference of Arrival is a method that implements the differences in time of arrival measures for a given signal's source at two or more pairs of nodes. TDoA can be used in IEEE 802.22 networks for locating an attacker [4]. This paper focused on how TDoA ideally works and how to apply it in locating Primary User Emulation (PUE) attackers in cognitive radio networks.

II. RELATED WORKS

Mobile and network-based are the two main techniques for location detection. In the first one, a global positioning system is used to give the position of a network user. This method relies on GPS satellites' information in time which is not limited to detecting an attacker. In the second technique, distance (transmitter-receiver) estimation is used [4]. This technique relies on Received Signal Strength, Angle of Arrival, and Time of Arrival.

In [5], the received signal strength-based technique is developed to determine the distance in a line of sight. The transmitter can be located by measuring several users' Received Signal Strenght (RSS) when the path loss is known. However, this technique is limited in dynamic networks due to shadowing and signals with multipath. The consequence of shadowing in the RSS-based technique is the proportionality between the variance and its range [6].

In ToA, signal propagation time estimates the distance between the transmitter-receiver. In [7], a test signal is sent to locate a user while it awaits the response to locate the two users. The user's cooperation is required in ToA, which makes this technique unsuitable for CRNs to locate an attacker.

In [8], a belief propagation-based technique was proposed. Secondary Users (SUs) determine the location and compatibility function, then the results are shared with all CR users that execute the belief function iteratively. When the results converge for all CR users, the attacker is detected, and its signal's features and parameters are broadcasted in the network. Since transmission time and the transmitted signal strength are unknown, the location verification approach is deployed using the difference of the RSS at the CR users' level. At least four CR users are needed to localize the attacker.

In [14], the Distance Difference Test (DDT) is proposed using the relative phase difference of the received signals. The distances between PU and two location verifiers (LVs) are determined. To the difference of distance, the signal's phase shift of the LVs is used. Distance Ratio Test (DRT), using RSS, relies on a large-scale propagation model because the fluctuations caused by small-scale fading in RSS are not considered. Both DDT and DRT form the transmitter verification scheme.

III. METHODOLOGY

A. Time Difference of Arrival (TDoA)

In the TDoA, the time difference of arrival is used to estimate the location. Using two nodes, the time difference is represented by a hyperbolic curve. The intersection of three hyperbolas can be accepted as the transmitter location if at least four nodes receive the signal [9]. The accuracy is a function of timestamp precision at the receiver's side. The timestamp, in turn, depends on signal bandwidth [10].

For the transmitter's location purpose, all nodes (CR users) in the CRN perform sensing and send the result to the Base Station (BS), which is in charge of deciding the existence or not of a PU. When a transmitter is detected, CR users (at least two) execute the location technique procedure to identify the transmitter. The synchronization between CR nodes and BS must be tight for this location. Several synchronization techniques in literature [11] can be used in CRN. However, these techniques are limited because a microsecond of errors can lead to hundreds of meters of difference. The proposed technique can be summarized in five steps: starting process (start of recording); sending of well-known predefined marker signal by the BS to every CR node; sending of recordings with the marker by the CR nodes to the BS and synchronisation; assuming the BS at (0,0), the elapsed time can be defined as in expression (1) [4] with *i* being the anchor node receiving the marker, *(x,y)* its position and *vp* the propagation velocity, and deriving location estimation (TDoA derivation).

$$\Delta t_i \frac{\sqrt{x_i^2+y_i^2}}{v_p} \qquad (1)$$

B. TDoA Measurement Model

In a CRN of N well-known positioned CR users, assuming the propagation paths between CR user and source are line-of-sight (LOS), assuming the range measurement of noise n_i; i = 1; 2;…; N is independent and follows a Gaussian distribution with zero mean and variance σi^2, the TDOA measurement model is given in expression (2) [12]:

$$t_{i1} = \frac{1}{v_p}\|u - s_i\| - \frac{1}{v_p}\|u - s_1\| + n_{i1}, \text{ i=2,…..,N} \qquad (2)$$

where s_1 is the reference sensor, v_p is the known propagation speed, u is the source position, s_i the position of the *i*th sensor, and n the noise.

C. Synchronization

Lightweight Time Synchronization (LTS) is used in this case. It allows obtaining specific precision with little overhead. Two algorithms are developed: the first for CR users requesting forchronization, and the second proactively synchronizes all CR users. For the two algorithms, a BS is required as a reference. A proactive algorithm constructs spanning trees with the BS at the root. CR users utilise round-trip synchronization to synchronize with the parents. When a CR user needs synchronization, a request is sent to the BS using a routing scheme. For overhead reduction purposes, CR users demand pending synchronization. If the response is positive, the synchronization is established with the neighbor instead of processing to an independent multi-hop synchronization with the BS[13].

IV. SIMULATION

The simulation was carried out using MATLAB R2016a on a Dell Latitude E7440 laptop (8G ram, processor Intel core i5 2.6GHz). The base station is assumed to be at (0,0), and the position of all nodes participating in the cooperative detection is well known. The distance is measured in meters, and the network range considered is a square of 100m as a side length. The propagation velocity is 10m/µs with variant noise. The different simulation results are shown in Figures 1-3.

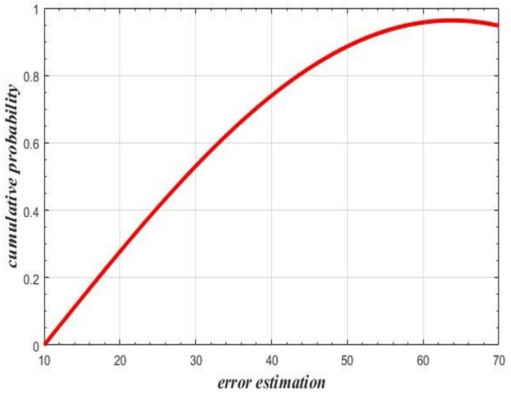

Fig. 1. Cumulative probability

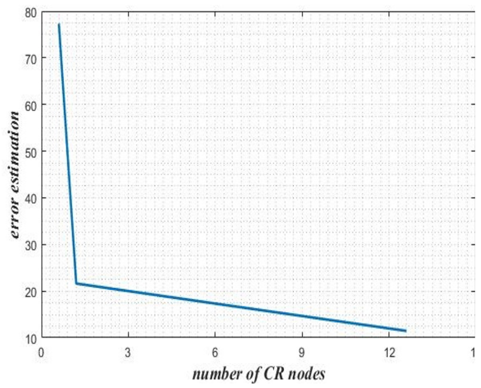

Fig. 2. Error estimation with respect to the number of CR node

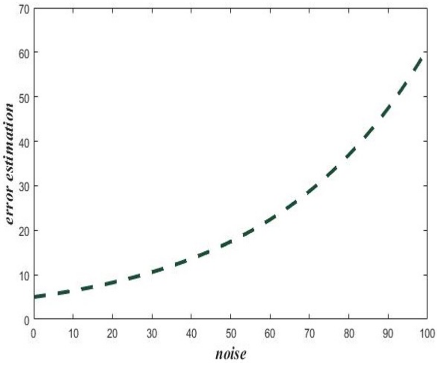

Fig. 3. Error estimation with respect to noise

V. DISCUSSION

The simulation results show that the probability of locating a transmitter increases with the error estimation (Figure 1); thus, the farther the signal source from the well-known position, the better the attacker's detection. The cumulative probability reaches 0.97 when the error estimation distance exceeds 70m in cooperative detection such as TDoA—the more nodes involved, the lesser the error. Figure 2 shows that the distance of estimation error decreases with the number of CR nodes. The error estimation distance decreases from 70m when the number of CR nodes is 1 to 12m when the number of CR nodes goes beyond 12. The results in figure 3 show that the spectrum noise affects the error estimation in a direct relationship. In a noise-free spectrum, the estimation error is 7.5m which increases to 60m when the noise reaches 100 W/Hz The probability of locating the source of the signal is a function of the number of CR nodes, the estimation error, and the spectrum noise.

VI. CONCLUSION

This paper explicitly presents a location detection method to avoid primary user emulation attacks in cognitive radio networks. The proposed technique is based on TDoA and Lightweight Time Synchronization method to estimate the position location. The proposed solution has been simulated, and the provided performance evaluation shows the goodness of the proposed method. The attacker can be located with less error, and the location process is accurate. For future work, multiple attackers can be considered.

REFERENCES

[1] J. Mitola (1999). Cognitive radio for flexible mobile multimedia communications. In proceedings of 1999 IEEE International Workshop on Mobile Multimedia Communications, (MoMuC'99), pp. 3-10.

[2] D. Deepa and D. Sumita (2018). An intelligent resource management scheme for SDF-based cooperative spectrum sensing in the presence of primary user emulation attack. Computers & Electrical Engineering, pp. 555-571.

[3] Z. Jin, S. Anand and K. Subbalakshmi (2009). Detecting primary user emulation attacks in dynamic spectrum access networks, In Proceedings of the IEEE International Conference on Communications, pp. 1- 5.

[4] O. León, J. Hernández-Serrano and M. Soriano (2012). Cooperative detection of primary user emulation attacks in CRNs. Computer Networks, 56(14), pp. 3374-3384.

[5] N. Patwari, J. Ash, S. Kyperountas, A. O. Hero III, R. Moses and N. Correal, (2005) Locating the nodes: cooperative localization in wireless sensor networks, IEEE Signal Processing Magazine 22 (4) 54–69,

[6] R Chen., J.M. Park and J. Reed, (2008). Defense against primary user emulation attacks in cognitive radio networks, IEEE Journal on Selected Areas in Communications 26 (1) 25–37,

[7] N. Goergen, T. Clancy and Newman T., (2010). Physical layer authentication watermarks through synthetic channel emulation, IEEE International Symposium on New Frontiers (DySPAN), pp. 1–7.

[8] A. Bensky, (2016) Wireless Positioning Technologies and Applications, second ed., Artech House

[9] H. Sallouha, A. Chiumento and S. Pollin, (2017). Localization in long-range ultra-narrow band IoT networks using RSSI, in: IEEE International Conference on Communications,

[10] S. Pandey and P. Agrawal, (2006) A survey on localization techniques for wireless networks, Chinese Institute of Engineers 29 (7) 1125

[11] Z. Dai, G. Wang, X. Jin, and X. Lou (2020) Nearly Optimal Sensor Selection for TDOA-Based Source Localization in Wireless Sensor Networks, IEEE Transactions on Vehicular Technology, pp 1-12.

[12] J.V. Greunen and J. Rabaey (2003). Lightweight time synchronization for sensor networks. In 2nd ACM International Workshop on Wireless Sensor Networks and Applications, pages 11–19.

[13] Chen R., Park J. M. and Reed J. H. (2008), Defense against primary user emulation attacks in cognitive radio networks, IEEE Journal: Selected Areas of Communication, 26 (1), pp. 25-37

[14] R Chen. and J. M. Park (2006), Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks, Networking Technologies for Software Defined Radio Networks, SDR'06, 1st IEEE Workshop, pp. 110-119.