Journal of
Sensor and Actuator Networks

MDPI

Article

Primary User Emulation Attacks: A Detection Technique Based on Kalman Filter

Zakaria El Mrabet [1,*], Youness Arjoune [1], Hassan El Ghazi [2], Badr Abou Al Majd [3] and Naima Kaabouch [1]

[1] Department of Electrical Engineering, University of North Dakota, Grand Forks, ND 58202, USA; youness.arjoune@und.edu (Y.A.); naima.kaabouch@und.edu (N.K.)
[2] National Institute of Posts & Telecommunication, Rabat 10100, Morocco; elghazi@inpt.ac.ma
[3] Department of Mathematics, Mohammed V University, Rabat 1014, Morocco; b.abouelmajd@fsac.ac.ma
* Correspondence: zakaria.elmrabet@und.edu; Tel.: +1-701-885-2113

Received: 18 April 2018; Accepted: 13 June 2018; Published: 4 July 2018

Abstract: Cognitive radio technology addresses the problem of spectrum scarcity by allowing secondary users to use the vacant spectrum bands without causing interference to the primary users. However, several attacks could disturb the normal functioning of the cognitive radio network. Primary user emulation attacks are one of the most severe attacks in which a malicious user emulates the primary user signal characteristics to either prevent other legitimate secondary users from accessing the idle channels or causing harmful interference to the primary users. There are several proposed approaches to detect the primary user emulation attackers. However, most of these techniques assume that the primary user location is fixed, which does not make them valid when the primary user is mobile. In this paper, we propose a new approach based on the Kalman filter framework for detecting the primary user emulation attacks with a non-stationary primary user. Several experiments have been conducted and the advantages of the proposed approach are demonstrated through the simulation results.

Keywords: cognitive radio; primary user emulation attacks; mobile primary user; Kalman filter; received signal strength

1. Introduction

Cognitive radio (CR) technology is a viable solution that addresses the problem of the spectrum scarcity [1]. It enables secondary users to sense, dynamically adjust their transmission parameters, and access the idle frequency channels (spectrum holes) without causing any harmful interference to the primary users [2]. Due to the unreliable nature of the wireless communication, cognitive radio networks can be subject to various cyber-attacks which can have a negative impact on their performance [3–5]. Examples of these attacks include asynchronous sensing attacks [3], primary user emulation (PUE) attacks [5,6], spectrum sensing data falsification (SSDF) attacks [6,7], and jamming attacks [8,9].

A PUE attack targets the CR physical and MAC layers and is considered as one of the most severe attacks in which a malicious user emulates the transmission characteristics of the primary user (PU) and mimics its behavior to mislead legitimate secondary users. Such an attack can create a harmful interference to the primary user and prevent other secondary users from using the idle spectrum frequency channels [5,6]. There are two types of primary user emulation attackers [10]: selfish and malicious. The purpose of the selfish attacker is to use and selfishly exploit an idle frequency channel without sharing it with other legitimate secondary users. The malicious attacker, on the other hand, aims at causing a denial of service in cognitive radio networks and preventing secondary users from accessing the available frequency channels.

Several approaches have been proposed to cope with the PUE attacks [11–24]. For instance, the authors of Reference [11] proposed an energy-based detection approach to detect the source of the signal and decide if it is emitted by a legitimate primary user or an attacker. In their approach, each secondary user measures the power level of the received signal and compares it to that from a legitimate PU. The authors of Reference [12] proposed a belief propagation framework based on a Markov random field to detect the primary user emulation attacker. Each secondary user decides whether the signal is coming from a legitimate primary user or not using the energy detection technique then calculates the belief and exchanges it with other secondary users. If the average of the belief values is lower than a predefined threshold, then the signal is coming from a malicious user, otherwise, it is coming from a legitimate user. However, techniques based on energy detection are not efficient in distinguishing between noise and signal, and they suffer from a high probability of false alarm [13].

Feature-based techniques, such as autocorrelation and matched filter [14,15], are also inefficient in distinguishing between the PU signals and those of the PUE attacker. For instance, the authors of Reference [16] used the cyclostationary feature of the transmitter's signal to detect the source of the incoming signal. However, this technique is not efficient in detecting malicious users which can mimic the primary user signal features. In Reference [17], the authors proposed a radio-frequency fingerprinting detection technique. In this technique, the transmitter is identified based on some unique radiometric features extracted from its analog signals. In another paper [18], the authors proposed a detection technique using the characteristics of wireless channels. As the statistical property of the wireless channel between the transmitter and the receiver is unique in a wireless environment, this feature is used as a radio fingerprint to detect the primary user emulation attacker. However, radio fingerprinting based approaches require additional hardware or software to implement. In addition, these techniques are inefficient in identifying the primary user signal effectively since the characteristic of the noise introduced by the hardware is random.

Other techniques have been proposed to estimate the position of the transmitter and compare the estimated position with the known position of the primary user. The authors of Reference [19] proposed a time difference of arrival (TDoA) based approach to estimate the position of the transmitter. In this approach, the time elapsed between the transmission of the signal and the reception of the reply is used to estimate the location of the transmitter. Though TDoA can estimate more accurately the transmitter position than other techniques, it requires a tight synchronization between the transmitters and the receivers, which is challenging. In Reference [20], the authors proposed an angle of arrival based approach for detecting the transmitter's position. In this approach, the direction of the received signal is measured at different reference nodes, then by applying the triangulation technique, the transmitter location can be estimated. However, this technique is affected by the multipath phenomenon [21]. The authors of Reference [22] proposed a mitigation approach to distinguish the primary user signal from other signals via an energy-efficient localization technique and channel parameter variance. The authors of Reference [23] proposed a model based on the trilateration, the received signal strength (RSS), and the particle swarm optimization to increase the detection accuracy of the primary user emulation attacker. All the previously mentioned techniques do not deal with uncertainty which affects the measurements. The authors of Reference [24] proposed a Bayesian model and trilateration technique for detecting the primary user emulation attack position. Based on the received signal strength, the Bayesian decision theory is used to deal with the uncertainty related to the primary user environment and increase the detection accuracy of the primary user position.

The existing localization techniques assume that the primary user position is fixed and known. Thus, each secondary user derives the position of the transmitter based on the received power and then compares it to the known position of the legitimate PU in order to verify if the transmitter is the legitimate PU or an attacker. However, in wireless communication networks where the primary user is mobile, such as cognitive radio ad hoc networks, the existing techniques produce inaccurate results since the position of the primary user varies over time. Therefore, in this paper, we propose a localization approach to detect the primary user emulation attacks in the case of mobile primary

users. The proposed approach is based on the Kalman filter framework for tracking the position of the primary user then the transmitter received power is used to derive the position of the transmitter before comparing it to the position estimated by Kalman filter.

The Kalman filter has been applied in several contexts including robotics vision, wireless sensor network, and tracking moving objects [25–35]. For instance, in Reference [25], the authors used the Kalman filter for robot mobile localization purpose. In Reference [26], the Kalman filter was applied for face tracking; and in Reference [27] the authors used the Kalman filter for tracking balls in the robotics vision field. Other applications of the Kalman filter have been proposed in the field of wireless sensor networks. For example, in Reference [28], the authors proposed an approach based on the Kalman filter combined with the Maximum Likelihood Estimation for tracking nodes in wireless sensor networks. The authors of Reference [29] proposed a routing protocol called SEARCH that predicts the destination in advance using the Kalman filter so that the route is extended and packets are reliably delivered to their destinations. In Reference [30], the authors used the Kalman filter for tracking the Global Navigation Satellite System signal. In Reference [31], the authors proposed an approach based on Kalman filtering combined with the particle swarm optimization algorithm for calculating the motion vectors of moving objects. To the best of our knowledge, this is the first application of the Kalman filter for tracking the PU position and detecting the PUE attacker in the cognitive radio context.

The remainder of this paper is organized as follows. In Section 2, we describe the proposed localization approach based on the Kaman filter. In Section 3, we first present the metrics used for evaluating the proposed approach's performance, then we discuss some examples of results and compare the proposed approach with the RSS-based location technique. Finally, some conclusions are drawn in the last section.

2. Methodology

The proposed approach is based on the Kalman filter framework for tracking the primary user location and deciding if the incumbent signal is emitted by a legitimate primary user or from an attacker. Figure 1 shows the flowchart of the proposed approach. In this approach, the primary user position is tracked using the Kalman filter [28], then the distance, d_{kfi} between a node i and the legitimate primary user is estimated. Next, the received power of the transmitter is used to calculate the distance, d_{pi} between the node i and that transmitter using the Free Space Path Loss Equation. If the difference between d_{kfi} and d_{pi} is greater or equal to a predefined threshold τ, then the transmitter is an attacker. Otherwise, it is a legitimate primary user.

In this work, we assume that the primary user is moving in a two-dimensional field and its state is described by its position and its velocity. In addition, we assume that the initial position of the primary user is known to the secondary users. The state of the primary user is represented as

$$x_k = \left[x(k)\ y(k)\ v_x(k)\ v_y(k)\right]^T \tag{1}$$

where $(x(k),\ y(k))$ are the coordinates of the primary user position at the time t_k and $(v_x(k),\ v_y(k))$ are the velocities of the primary user in x and y-directions at time t_k, respectively. In addition, we assume that the movement of the primary user is locally linear within the sampling interval time. Thus, its motion can be modeled as

$$x_{k+1} = A_k x_k + B_k u_k + \ w_k \tag{2}$$

where A and B represent the transition matrix and the control matrix, respectively. u_k is the acceleration of the primary user and w_k is a white Gaussian noise with zero mean and covariance matrix Q, which is given by

$$Q = \begin{bmatrix} {\sigma^2}_{wx} & 0 \\ 0 & {\sigma^2}_{wy} \end{bmatrix} \tag{3}$$

where $\sigma^2{}_{wx}$ and $\sigma^2{}_{wy}$ are the covariances of wx and wy which correspond to the acceleration noise of the primary user along the X-axis and Y-axis, respectively.

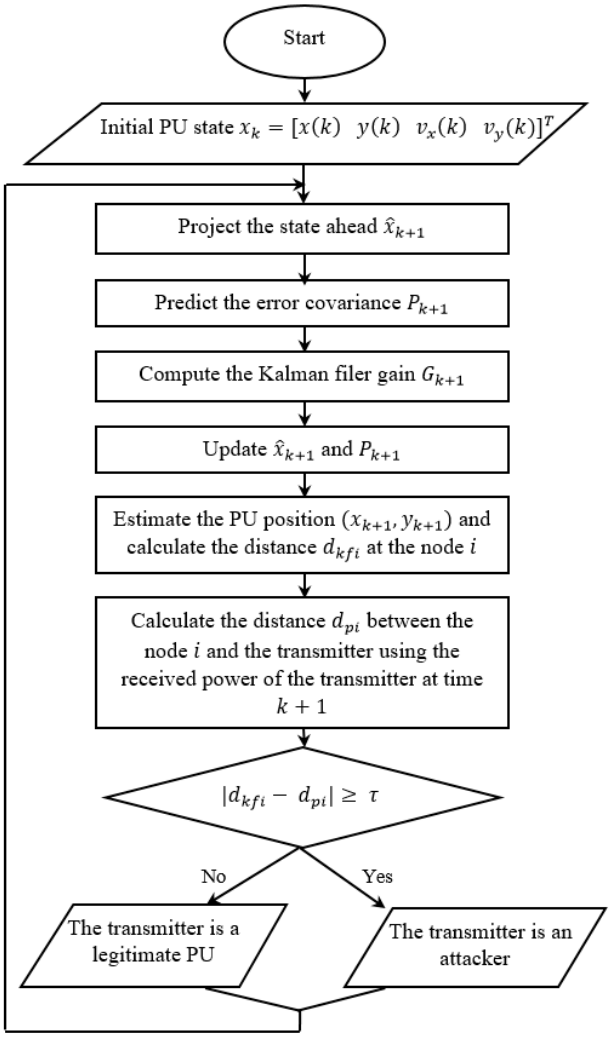

Figure 1. Flowchart of the proposed approach.

The transition and the control matrix are given by

$$A_k = \begin{bmatrix} 1 & 0 & \Delta t_k & 0 \\ 0 & 1 & 0 & \Delta t_k \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B_k = \begin{bmatrix} \frac{\Delta tk^2}{2} \\ \frac{\Delta tk^2}{2} \\ \Delta t_k \\ \Delta t_k \end{bmatrix} \tag{4}$$

where $\Delta t_k = t_{k+1} - t_k$ is the sampling interval time between two successive measurements at t_{k+1} and t_k. The measurement model z_k adopted is given by

$$z_k = Cx_k + v_k \tag{5}$$

where C is the measurement matrix and v_k is the measurement noise which is a white Gaussian noise with zero mean and covariance matrix R. C is given by

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \tag{6}$$

During the first process of Kalman filter, the state of the primary user $\hat{x}_{k+1}$ and its associated covariance error matrix P_{k+1} at time t_{k+1} are predicted using the following equations

$$\hat{x}_{k+1} = A_k \hat{x}_k + B_k u_k \tag{7}$$

$$P_{k+1} = A_k P_k A_k^T + Q_k \tag{8}$$

where $\hat{x}_k$ is the primary user state at time k, P_k is the covariance error matrix at time k, and A_k^T is the transpose of transition matrix A at time k. During the update process of Kalman filter, the estimated state and its covariance error matrix at time $k+1$ are updated and corrected using the Kalman filter gain G_{k+1} as follows

$$G_{k+1} = P_{k+1} C^T \left(C P_{k+1} C^T + R \right)^{-1} \tag{9}$$

$$\hat{x}\prime_{k+1} = \hat{x}_{k+1} + G_{k+1}(z_k - C\hat{x}_{k+1}) \tag{10}$$

$$P\prime_{k+1} = P_{k+1} - C\hat{x}_{k+1} P_{k+1} \tag{11}$$

where C^T is the transpose matrix of the measurement matrix C, $\hat{x}\prime_{k+1}$ is the updated state of the primary user state at $k+1$, and $P\prime_{k+1}$ is the updated covariance error matrix P_{k+1}. Once the coordinates of the primary user position $(x_p,\ y_p)$ are estimated using the Kalman filter, the distance d_{kfi} between a fixed position of an anchor node $(x_i,\ y_i)$ and the primary user can be obtained using the following equation

$$d_{kfi} = \sqrt{\left(x_p - x_i\right)^2 + \left(y_p - y_i\right)^2} \tag{12}$$

In order to verify if the incoming signal is emitted by a legitimate primary user or by an attacker, a distance d_{pi} between the transmitter and a node i is required. This distance can be obtained from the received power signal of the transmitter using the Free Space Path Loss Equation [24]:

$$P_r = \frac{P_t G_t G_r \lambda^2}{\left(4\pi d_{pi}\right)^2} \tag{13}$$

where P_r is the received power, P_t is the transmitted power, G_r is the antenna gain of the receiver, G_t is the antenna gain of the transmitter, λ is the wavelength, and d_{pi} is the distance between an anchor node i and the transmitter. Equation (13) can be expressed in dB as

$$P_r(dB) = -10\alpha log_{10}\left(d_{pi}\right) + A \tag{14}$$

where α is the propagation path loss exponent and A is expressed as

$$A = 10log_{10}\left(P_t G_t G_r \lambda^2\right) - 20log_{10}(4\pi) \tag{15}$$

The received signal strength at an anchor node i can be impacted by the noise, Equation (14) can be written as

$$P_r(dB) = -10\alpha log_{10}\left(d_{pi}\right) + A + n_i \tag{16}$$

where n_i is a white Gaussian noise that follows the normal distribution $N\left(0,\ \sigma^2\right)$. Thus, the distance d_{pi} can be estimated as

$$d_{pi} = 10^{\frac{(A + n_i - p_r)}{10\alpha}} \tag{17}$$

By comparing the difference between the estimated distance d_{kfi} and d_{pi} at an anchor node i to a predefined threshold τ, the transmitter is considered as a primary user emulation attacker if the $\left|d_{kfi} - d_{pi}\right| \geq \tau$ and as a legitimate primary user when the $\left|d_{kfi} - d_{pi}\right| < \tau$.

3. Experiments and Results

To evaluate the performance of the proposed approach, a simulation of a primary user emulation attack scenario in a virtual cognitive radio network was performed using Matlab. The experiments were carried out on an Intel Core(TM) i7-6700 CPU @ 3.40 GHz 3.41 GHz, 16 GB RAM with a windows 10 64-bit Operating system. In the simulated scenario, we assume that there is a legitimate primary user, a PUE attacker, several secondary users along with some anchor nodes. We assume that the initial position of the primary user is known to the secondary users. Each anchor node gathers the measurements related to the primary user positions and share the results with the secondary users to track the movement of the primary user. These anchor nodes are positioned at specific positions while the secondary users are randomly deployed to simulate a real-world network scenario. Table 1 gives the simulation parameters used in this paper along with the positions of the anchor nodes, the initial position of the PU, and the position of the PUE attacker.

Table 1. The simulation parameters.

Parameter	Value/Range
Transmission power	150 W
Transmitter antenna gain	12 dB
Receiver antenna gain	4 dB
Frequency	2400 MHz
Path loss exponent	2
SNR	Range [−20, 20]
Initial position $(x(k),\ y(k))$ of the PU at $k = 0$	(1400, 1400)
Coordinates of the anchor nodes positions	(500, 500); (500, 1000); (500, 1500); (1000, 15,000); (1500, 1500); (1500, 1000); (1500, 500); (1000, 500); (725, 1000); (1225, 1000); (1000, 725); (1000, 1225); (1225, 1500); (725, 1500); (1225, 500)
Position of the PUE attacker	(1470, 1470)
Coordinates of the secondary users positions	(750, 1350); (1200, 1400); (1300, 650); (800, 1000); (700, 750); (1000, 1100); (850, 650); (1400, 1100); (1450, 1200); (1400, 600); (1450, 850);

Due to a number of random variables used in the proposed approach, including the noise affecting the acceleration, the measurement, and the signal, the Monte Carlo technique was used to handle the uncertainty in the simulation. The proposed approach was extensively tested and evaluated using several metrics including the probability of detection, the probability of false alarm, the probability of miss detection, and the error function. The results of the proposed approach were compared to those of the RSS-based localization technique.

The probability of detection, P_d, corresponds to the number of times where the primary user emulation attacker signal is correctly classified as an attack divided by the total number of attacks. It is given by

$$P_d = \frac{Number\ of\ PUE\ detections}{Total\ number\ of\ attacks} \tag{18}$$

The probability of false alarm, P_{fa}, corresponds to the number of times where the legitimate primary user signal is wrongly classified as an attack divided by the total number of legitimate signals. It is expressed as

$$P_{fa} = \frac{Number\ of\ false\ detected\ attack}{Total\ number\ of\ legitimate\ signals} \tag{19}$$

The probability of miss detection, P_m, corresponds to the number of times where an attack is incorrectly classified as a normal signal divided by the total number of attacks. It is given by

$$P_m = \frac{Number\ of\ miss\ detected\ attacks}{Total\ number\ of\ attacks} \tag{20}$$

The error function calculates the error between the estimated and the actual trajectory of the primary user. It is given by

$$\text{Error function} = \frac{1}{n}\sum_{i=1}^{n}(X - X')^2 \tag{21}$$

where X is the actual trajectory, X' is the predicted trajectory, and n is the number of collected measurements.

Examples of results are given in Figures 2–9. Figure 2 illustrates the error function versus the measurement noise. As it can be seen from this figure, this function remains almost constant when the measurement noise values are less than 0.02, and it increases exponentially after that value. For measurement noise values equal to 0.2 and 0.07, the error function is 0.1 and 0.11, respectively. When the measurement noise is greater than 0.3, the error function increases exponentially. For instance, when the measurement noise is equal to 7, the error function is equal to 10 and when this measurement noise increases to 8.5, its corresponding error function value rises to 15. These results suggest that measurements noise values that are less than 0.2 are the optimal values for the experiments since they reduce the error between the actual and the predicted trajectory leading to a better estimation of the primary user position. Thus, we selected 0.05 for conducting the remaining experiments.

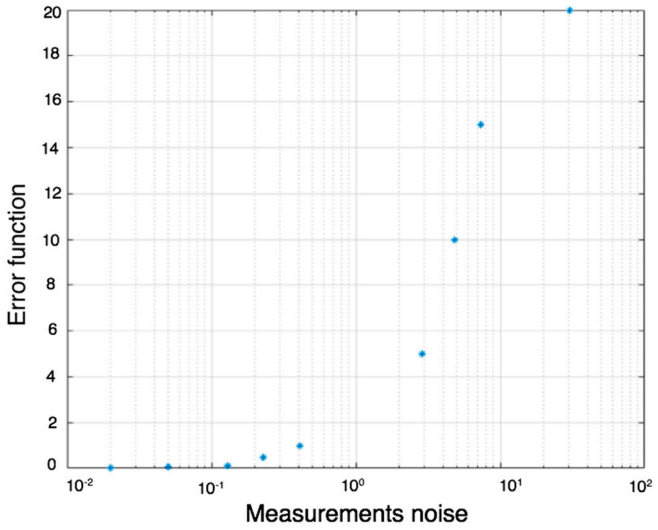

Figure 2. Error function as a function of the measurement noise.

Figures 3 and 4 show the scenario used for simulating the mobile primary user, the fixed PUE attacker, secondary users, and anchor nodes. In Figure 3, the red symbols represent the measurements collected by the anchor nodes regarding the movement of the primary user. Due to the measurement noise, these collected measurements are not precise enough to accurately predict the primary user trajectory. From Figure 4, it can be seen that after using the optimal measurement noise value selected previously, which is 0.05, and by applying the Kalman filtering process, the predicted trajectory is close to the actual one. These results suggest that the secondary users can use the collected measurements with the Kaman filter to accurately predict the position of a mobile primary user.

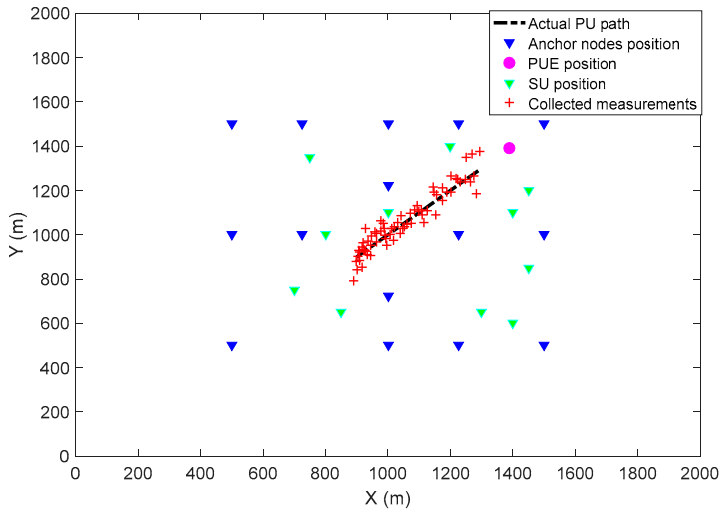

Figure 3. Simulation scenario of the mobile primary user the fixed primary user emulation attacker, secondary users and anchor nodes. The red symbols represent the collected measurements gathered by the anchor nodes.

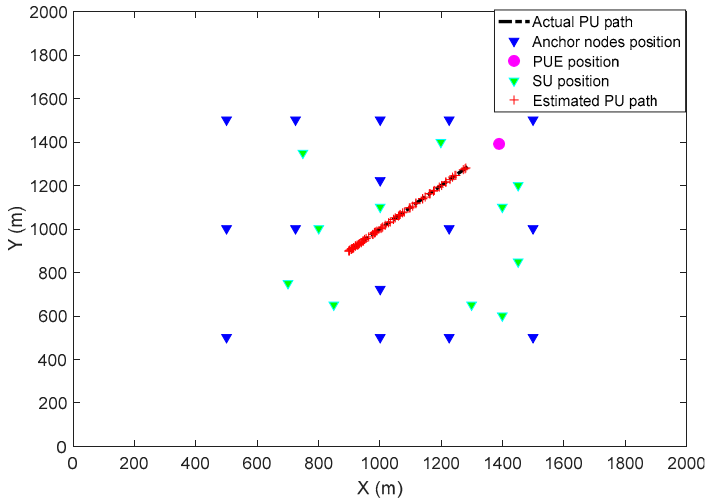

Figure 4. Simulation scenario of the mobile PU, the fixed PUE, SUs, and anchor nodes. The red symbols represent the predicted PU path after applying Kalman filtering with an optimal measurement noise value.

Figure 5 shows the probability of detection as a function of the distance, d_{pu_pue} between a mobile primary user and a primary user emulation attacker for different SNR values. As one can see, the probability of detection increases as the distance between the primary user and the attacker increases. For example, for an SNR value of -10 dB, the probability of detection is equal to 37% when the distance between the primary user and the attacker is 50 m, but this probability increases to 60% when the distance is equal to 100 m. In addition, this figure shows that the probability of detection increases with the increase of SNR values. For instance, for a distance of 50 m between the PU and the PUE attacker, the probability of detection is equal to 37%, 80%, 96%, 99.2%, and 99.7%, for SNR values corresponding to -10 dB, -5 dB, 0 dB, 5 dB, and 10 dB, respectively.

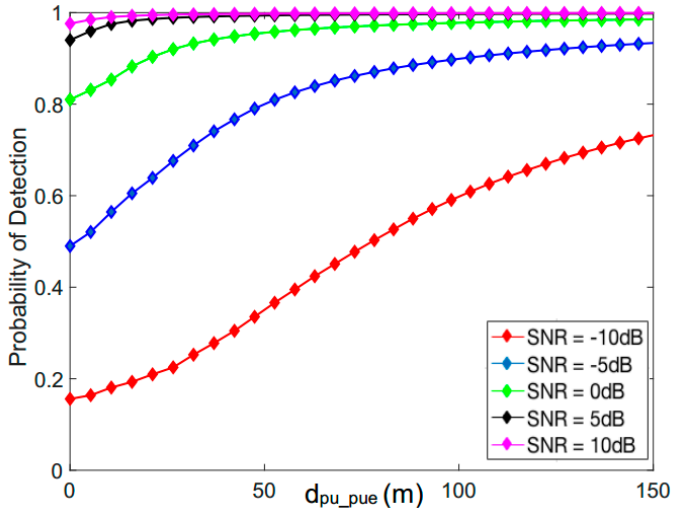

Figure 5. Probability of detection as a function of the distance d_{PU_PUE} between a mobile PU and a PUE.

Figure 6 shows the probability of detection as a function of the probability of false alarm for a distance d_{pu_pue} = 30 m between the primary user and the primary user emulation attacker. As it can be observed, the probability of detection increases with the increase in the probability of false alarm. For example, for an SNR value of −15 dB and with a probability of false alarm of 10%, the probability of detection is 16%, but when the probability of false alarm increases to 30%, the probability of detection is equal to 61%. In addition, with the increase of the SNR value, the probability of detection increases. For instance, with a probability of false alarm of 2%, the probability of detection is equal to 39%, 63% 90%, 99%, and 100% for SNR values corresponding to −15 dB, −10 dB, −5 dB, 0 dB, and 5 dB, respectively.

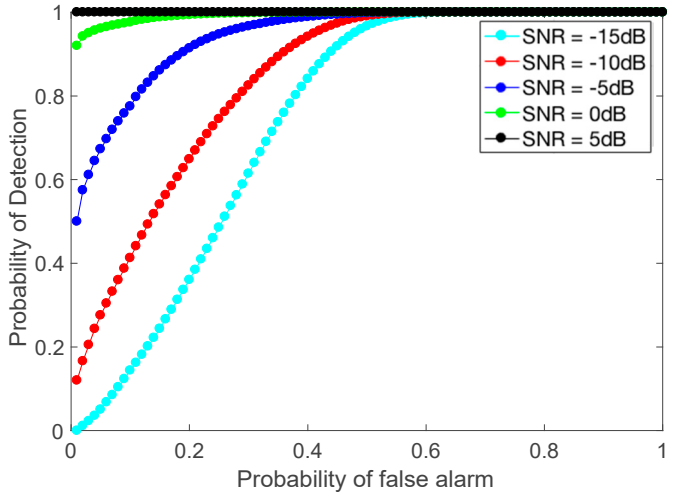

Figure 6. Probability of detection as a function of the probability of false alarm for d_{PU_PUE} = 30 m.

Figure 7 shows the probability of miss detection as a function of the distance d_{pu_pue} between a mobile primary user and a primary user emulation attacker. As expected, the probability of miss detection decreases as the distance between the PU and the PUE increases. For example, for an SNR value of −10 dB, the probability of miss detection is equal to 65% when the distance between the primary user and the attacker is equal to 50 m, but this probability drops to 41% when the distance increases to 100 m. In addition, this figure shows that when the SNR value increases, the probability of miss detection decreases. For example, with a distance of 110 m between the primary user and the

attacker, the probability of miss detection is equal to 37%, 10%, 5%, 1%, and 0% for SNR values of −10 dB, −5 dB, 0 dB, 5 dB, 10 dB, respectively.

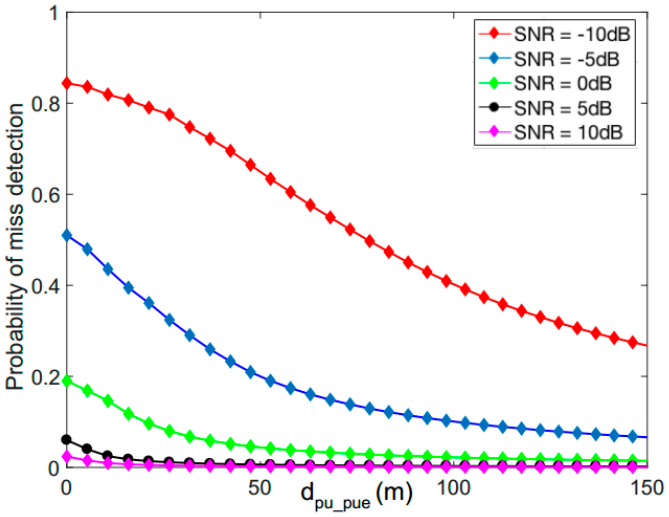

Figure 7. Probability of miss detection as a function of the distance d_{PU_PUE} between the mobile PU and a PUE.

Figure 8 shows a comparison between the proposed approach and the RSS-based localization technique in terms of the probability of detection as a function of distance with an SNR value of −10 dB. The RSS-based localization technique is selected for comparison purpose since it has been proposed in several previous papers [20,23,24]. This technique uses the transmitter received power to derive the position of the transmitter. The calculated position is combined with other techniques including Particle Swarm Optimization and the Maximum Likelihood estimation to optimize the detected location of the transmitter. This technique meets the Federal Communication Commission which states that no modification to the primary user system should be performed to accommodate the opportunistic use of the spectrum by secondary users. As shown in this figure, the probability of detection for the proposed approach, as well as the RSS-based localization approaches, is low when the attacker is in a close proximity to the legitimate primary user location. When the distance increases, the probability of detection of the proposed approach increases while it remains almost the same for the RSS-based localization technique. For instance, when the distance between the primary user emulation attacker and the primary user is equal to 50 m, the probabilities of detection of the proposed approach and the RSS-based localization technique are 24% and 16%, respectively. When the distance increases to 100 m, the probability of detection of the proposed approach increases to 49% while it remains equal to 16% for the RSS-based localization approach. This result suggests that it is challenging to detect the primary user emulation attacker when the attacker is in a close proximity to the legitimate primary user location. However, when the distance becomes larger, the proposed approach produces better results than the RSS-based approach because in this latter, the secondary users use the received signal strength to calculate the position of the transmitter then compare it to the fixed and known position of the legitimate primary user. Since the position of the primary user changes over time, this RSS-based approach produces inaccurate results in terms of the probability of detection.

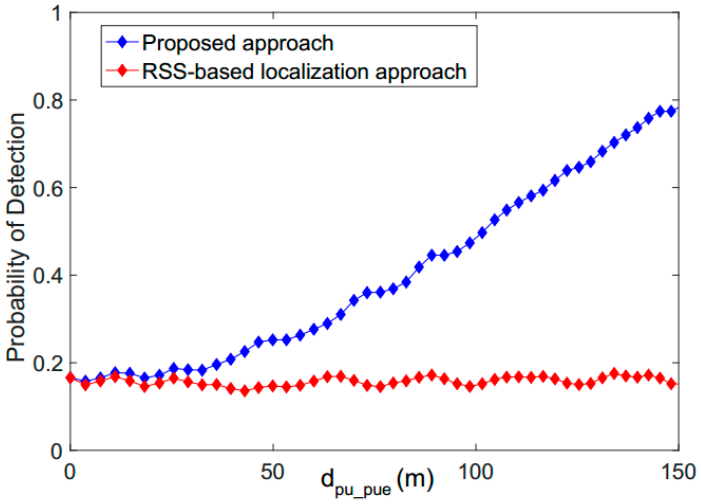

Figure 8. Comparison between the proposed technique and the RSS-based localization technique in terms of the probability of detection as a function of the distance.

Figure 9 illustrates a comparison between the proposed technique and the RSS-based localization technique in terms of the probability of miss detection as a function of the distance with an SNR value equal to −10 dB. As one can see, the miss detection probabilities of the proposed approach and the RSS-based localization technique are high when the attacker is close to the primary user location. As expected, when the primary user starts moving and the distance becomes larger, the probability of miss detection of the proposed approach decreases while it remains the same for the RSS-based localization technique. For example, when the distance is 50 m, the probabilities of miss detection of the proposed approach and the RSS-based localization technique are 76% and 84%, respectively. When the distance increases to 150 m, the probability of miss detection of the proposed approach decreases to 19% while it remains equal to 84% for the RSS-based localization technique.

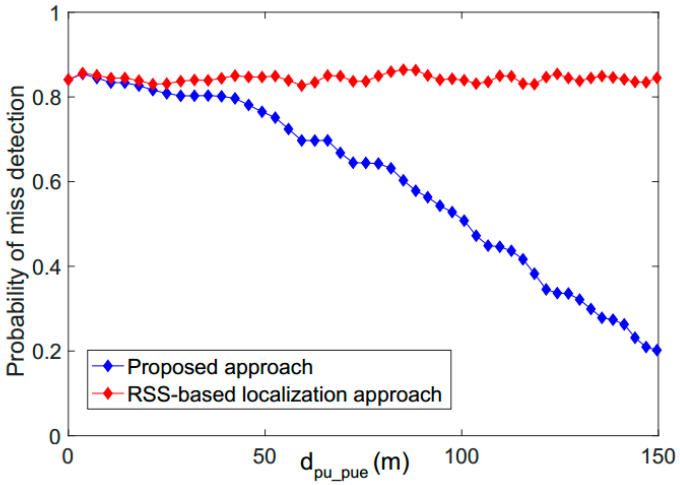

Figure 9. Comparison between the proposed technique and the RSS-based localization technique in terms of the probability of miss detection as a function of the distance.

4. Conclusions

Cognitive Radio networks are subject to several cyber-attacks. The primary user emulation attack is one of the most severe attacks that can impact the normal functioning of these networks. In this paper, we propose a new approach for detecting primary user emulation attacks with a non-stationary

primary user. A Kalman filter based technique is used for tracking and estimating the position of the mobile primary user, then the transmitter received power is used to derive the position of the transmitter before comparing it to that estimated by Kalman filter. Thus, secondary users can verify if the transmitter is a legitimate primary user or an attacker. Several experiments were conducted and the model was extensively tested and its results were compared to those of the RSS-based location approach. The results show that the proposed approach produces satisfactory results in terms of tracking the primary user in a non-stationary environment and it outperforms the RSS-based localization technique in terms of probability of detection and probability of miss detection. However, the proposed technique has a few limitations that need to be addressed in future works. These limitations include finding the initial coordinates of the primary user, handling the uncertainty in the measurements, and detecting an attacker that is in close proximity to the legitimate primary user position.

Author Contributions: Z.E.M., Y.A., and N.K. conceived and designed the experiments; Z.E.M. performed the experiments; Z.E.M., Y.A., and N.K. analyzed the data; Z.E.M. wrote the paper; N.K. revised and oversaw the project; N.K. provided the resources and financial support. H.E.G. and B.A.A.M. provided feedback.

Funding: Wireless Communications & Networking Lab, Electrical Engineering Department, University of North Dakota, USA.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kaabouch, N.; Hu, W.-C. Handbook of Research on Software-Defined and Cognitive Radio Technologies for Dynamic Spectrum Management. *IGI Glob.* **2014**. [CrossRef]
2. Masonta, M.T.; Mzyece, M.; Ntlatlapa, N. Spectrum Decision in Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1088–1107. [CrossRef]
3. Riahi Manesh, M.; Kaabouch, N. Security threats and countermeasures of MAC layer in cognitive radio networks. *Ad Hoc Netw.* **2018**, *70*, 85–102. [CrossRef]
4. Bhattacharjee, S.; Sengupta, S.; Chatterjee, M. Vulnerabilities in cognitive radio networks: A survey. *Comput. Commun.* **2013**, *36*, 1387–1398. [CrossRef]
5. Bouabdellah, M.; Kaabouch, N.; El Bouanani, F.; Ben-Azza, H. Network layer attacks and countermeasures in cognitive radio networks: A survey. *J. Inf. Secur. Appl.* **2018**, *38*, 40–49. [CrossRef]
6. Chaitanya, D.L.; Chari, K.M. Performance Analysis of PUEA and SSDF Attacks in Cognitive Radio Networks. *Comput. Commun. Netw. Internet Secur.* **2017**, 219–225. [CrossRef]
7. Sharifi, A.A.; Niya, M.J.M. Defense against SSDF attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach. *IEEE Commun. Lett.* **2016**, *20*, 93–96. [CrossRef]
8. Reyes, H.I.; Kaabouch, N. Jamming and Lost Link Detection in Wireless Networks with Fuzzy Logic. *Int. J. Sci. Eng. Res.* **2013**, *4*, 1–7.
9. Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks. *IEEE Trans. Smart Grid* **2017**, *8*, 2431–2439. [CrossRef]
10. Nguyen-Thanh, N.; Ciblat, P.; Pham, A.P.; Nguyen, V.T. Surveillance Strategies against Primary User Emulation Attack in Cognitive Radio Networks. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 4981–4993. [CrossRef]
11. Jin, F.; Varadharajan, V.; Tupakula, U. Improved detection of primary user emulation attacks in cognitive radio networks. In Proceedings of the 2015 International Telecommunication Networks and Applications Conference (ITNAC), Sydney, Australia, 18–20 November 2015; pp. 274–279.
12. Yuan, Z.; Niyato, D.; Li, H.; Song, J.B.; Han, Z. Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 1850–1860. [CrossRef]
13. Manesh, M.R.; Apu, M.S.; Kaabouch, N.; Hu, W.-C. Performance evaluation of spectrum sensing techniques for cognitive radio systems. In Proceedings of the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, New York, NY, USA, 20–22 October 2016; pp. 1–7.
14. Hector, R.; Subramaniam, S.; Kaabouch, N.; Hu, W.-C. A spectrum sensing technique based on autocorrelation and Euclidean distance and its comparison with energy detection for cognitive radio networks. *Comput. Electr. Eng.* **2016**, *52*, 319–327. [CrossRef]

15. Salahdine, F.; El Ghazi, H.; Kaabouch, N.; Fassi Fihri, W. Matched filter detection with dynamic threshold for cognitive radio networks. In Proceedings of the International Conference on Wireless Networks and Mobile Communications, Marrakech, Morocco, 20–23 October 2015; pp. 1–6.
16. Nguyen, N.T.; Zheng, R.; Han, Z. On identifying primary user emulation attacks in cognitive radio systems using nonparametric bayesian classification. *IEEE Trans. Signal Process.* **2012**, *60*, 1432–1445. [CrossRef]
17. Rehman, S.U.; Sowerby, K.W.; Coghill, C. Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios. *IET Commun.* **2014**, *8*, 1274–1284. [CrossRef]
18. Chin, W.L.; Tseng, C.L.; Tsai, C.S.; Kao, W.C.; Kao, C.W. Channel-Based Detection of Primary User Emulation Attacks in Cognitive Radios. In Proceedings of the IEEE 75th Vehicular Technology Conference, Yokohama, Japan, 6–9 May 2012; pp. 1–5.
19. Ghanem, W.R.; Shokair, M.; Desouky, M.I. An improved primary user emulation attack detection in cognitive radio networks based on firefly optimization algorithm. In Proceedings of the 33rd National Radio Science Conference, swan, Egypt, 22–25 February 2016; pp. 178–187.
20. Sichitiu, M.L. Angle of Arrival Localization for Wireless Sensor Networks. In Proceedings of the 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, Reston, VA, USA, 25–28 September 2006; pp. 374–382.
21. León, O.; Hernández-Serrano, J.; Soriano, M. Cooperative detection of primary user emulation attacks in CRNs. *Comput. Netw.* **2012**, *56*, 3374–3384. [CrossRef]
22. Sultana, R.; Hussain, M. Mitigating Primary User Emulation Attack in Cognitive Radio Network Using Localization and Variance Detection. In Proceedings of the First International Conference on Smart System, Innovations and Computing, Jaipur, India, 15–16 April 2018; pp. 433–444.
23. Fihri, W.F.; Arjoune, Y.; El Ghazi, H.; Kaabouch, N.; El Majd, B.A. A particle swarm optimization based algorithm for primary user emulation attack detection. In Proceedings of the IEEE 8th Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, 8–10 January 2018; pp. 823–827.
24. Fihri, W.F.; El Ghazi, H.; Kaabouch, N.; El Majd, B.A. Bayesian decision model with trilateration for primary user emulation attack localization in cognitive radio networks. In Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Marrakech, Morocco, 16–18 May 2017.
25. Yi, J.; Wang, H.; Zhang, J.; Song, D.; Jayasuriya, S.; Liu, J. Kinematic modeling and analysis of skid-steered mobile robots with applications to low-cost inertial-measurement-unit-based motion estimation. *IEEE Trans. Robot.* **2009**, *25*, 1087–1097. [CrossRef]
26. Tsai, C.Y.; Dutoit, X.; Song, K.T.; Van Brussel, H.; Nuttin, M. Robust face tracking control of a mobile robot using self-tuning Kalman filter and echo state network. *Asian J. Control* **2010**, *12*, 488–509. [CrossRef]
27. Birbach, O.; Frese, U. A multiple hypothesis approach for a ball tracking system. In Proceedings of the 12th International Conference on Computer Vision Systems, Liège, Belgium, 13–15 October 2009; pp. 435–444.
28. Xingbo, W.; Minyue, F.; Huanshui, Z. Target tracking in wireless sensor networks based on the combination of KF and MLE using distance measurements. *IEEE Trans. Mob. Comput.* **2012**, *11*, 567–576. [CrossRef]
29. Chowdhury, K.R.; Di Felice, M. A routing protocol for mobile cognitive radio ad-hoc networks. *Comput. Commun.* **2009**, *32*, 1983–1997. [CrossRef]
30. O'Driscoll, C.; Petovello, M.G.; Lachapelle, G. Choosing the coherent integration time for Kalman filter-based carrier-phase tracking of GNSS signals. *GPS Solut.* **2011**, *15*, 345–356. [CrossRef]
31. Ramakoti, N.; Vinay, A.; Jatoth, R. Particle swarm optimization aided Kalman filter for object tracking. In Proceedings of the 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, Kerala, India, 28–29 December 2009; pp. 531–533.
32. Eftekhar Azam, S.; Chatzi, E.; Papadimitriou, C. A dual Kalman filter approach for state estimation via output-only acceleration measurements. *Mech. Syst. Signal Process.* **2015**, *60*, 866–886. [CrossRef]
33. Eftekhar Azam, S.; Chatzi, E.; Papadimitriou, C.; Andrew, S. Experimental validation of the Kalman-type filters for online and real-time state and input estimation. *J. Vib. Control* **2017**, *23*, 2494–2519. [CrossRef]

34. Lourens, E.; Papadimitriou, C.; Gillijns, S.; Reynders, E.; De Roeck, G.; Lombaerta, G. Joint input-response estimation for structural systems based on reduced-order models and vibration data from a limited number of sensors. *Mech. Syst. Signal Process.* **2012**, *29*, 310–327. [CrossRef]
35. Lourens, E.; Reynders, E.; De Roeck, G.; Degrande, G.; Lombaerta, G. An augmented Kalman filter for force identification in structural dynamics. *Mech. Syst. Signal Process.* **2012**, *27*, 446–460. [CrossRef]