International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Combating PUE Attack in Cognitive Radio Networks using RSSI Based EKF and UKF

Kattaswamy Mergu

Abstract: ***The problem of spectrum scarcity in wireless communication can be reduced by Cognitive Radio (CR) technology in which the spectrum holes or unused spectrum can be allocated to the secondary or unlicensed users. But the major problem in CR is providing security. Various security issues are present at different layer. One of the major wide spread security issue in the cognitive radio is the Primary user emulsion attack in which the malicious secondary user emulated as primary user to get spectrum resources for a long time. One of way to avoided PUEA is, by obtaining the location of malicious user. The conventional location detection techniques such as time of arrival, time difference of arrival and direction of arrival, will give better performance when the user is stationary. Even though Received Signal Strength Indicator along RF fingerprint technique gives the better location of mobile user but it requires the more hardware. Hence the cost is high.***

In this paper, the author proposed an algorithm to locate the attacker using EKF and UKF with RSSI. In this algorithm, the initial position of user can be obtained by Received Signal Strength Indicator. This initial position integrated to EKF and UKF to track the location of primary user, which is a mobile user so that PUE Attack can be identified and avoided. The author also compares the performance of Extended Kalman Filter with Unscented Kalman Filter by Matlab software.

Keywords : Cognitive Radio, Extended Kalman Filter, Primary User Emulsion Attack, Received Signal Strength Indicator, Unscented Kalman Filter .

I. INTRODUCTION

In the last two decades, the applications of WCN increasing rapidly, which leads to a problem of spectrum scarcity. Cognitive Radio technology provides the best solution to the problem of spectrum scarcity. Cognitive Radio technology is a dynamic spectrum access technique, which allocates the unused spectrum or spectrum holes to the secondary users(also called unlicensed users) by a technique called spectrum sensing [1].

According to [2], users can be divided into primary users, having licensed spectrum band and secondary users, having no licensed spectrum band. In [3], to obtain the spectrum opportunity, each individual secondary user under goes through a cognitive cycle , involving spectrum sensing, analysis, spectrum decision and transmission. In [4], the main task of physical layer of cognitive radio is spectrum sensing. In [4], the main task of physical layer of cognitive radio is spectrum sensing. There are many spectrum sensing techniques, some of important techniques are discussed in [2].

As we know that, cognitive radio is open yo everyone. Hence, providing security to the users is the major challenging task. The possible security issues at various layers in OSI model of CRN are, PUEA, jamming attack, spectrum sensing data falsification, control channel saturation DOS attack, sink hole attack, hello food attack and lion attack. Among the all the attacks, the PUE attack is a wide spread attack and affects the CRN very savior [5].

The possibility of PUEA is at physical layer, in which the malicious secondary user provides the false information to the other secondary users that, the channel will be used by a PU. Hence the SUs within the transmission range will be that a PU is active, and vacate the channel. The scenario of PUE attack is as shown in Fig. 1. PUE attack can be categorized as selfish attack and malicious attack [6].

i. Selfish Attack: the attacker imitates the characteristics of primary user and prevents the other users to attain the maximum spectrum resources.

ii. Malicious Attack: the attacker confuses the other secondary users by sending false observations. Hence the opportunistic spectrum sharing can be disturbed and the attacker not to exploits the spectrum for its own use.

Some impacts on PUE attacks on Cognitive Radio Network are, wastage of bandwidth, connection unreliability, denial of service(DOS), quality of service (QOS) degradation and interference of SUs with Pus.

Some of the traditional techniques for SUs to identify the signal from Pus, that includes Energy Detection, location verification and feature detection [7].

i. Energy Detection: energyof the signal can be measured at each anchor node and comparing with that obtained from true Pus. However, it fails to detect the advanced PUE attack i.e. when either PUE or PU is a mobile user.

ii. Location Verification: Location Verification technique is again categorized into Distance Ratio Test (DRT) and Distance Difference Test (DDT) [8]. DRT uses the received signal strength based method, in which the received power can be measured. Based on the power received the primary user/ attacker location can be estimated and where as DDT uses the regular location based methods such as TOA, TDOA and DOA.

Iii. Feature Detection: it uses the energy detection to identify the existing users. Then it employs cyclostationary to extract the features of the user then fed into artificial neural networkfor detection of PUEA.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Kattaswamy Mergu*, Ph.D Scholor, Electronics and Communication, Sri Satya Sai University of Technology and Medical Sciences, Sehore, Madhya Pradesh India. Email: kattaswamy@gmail.com

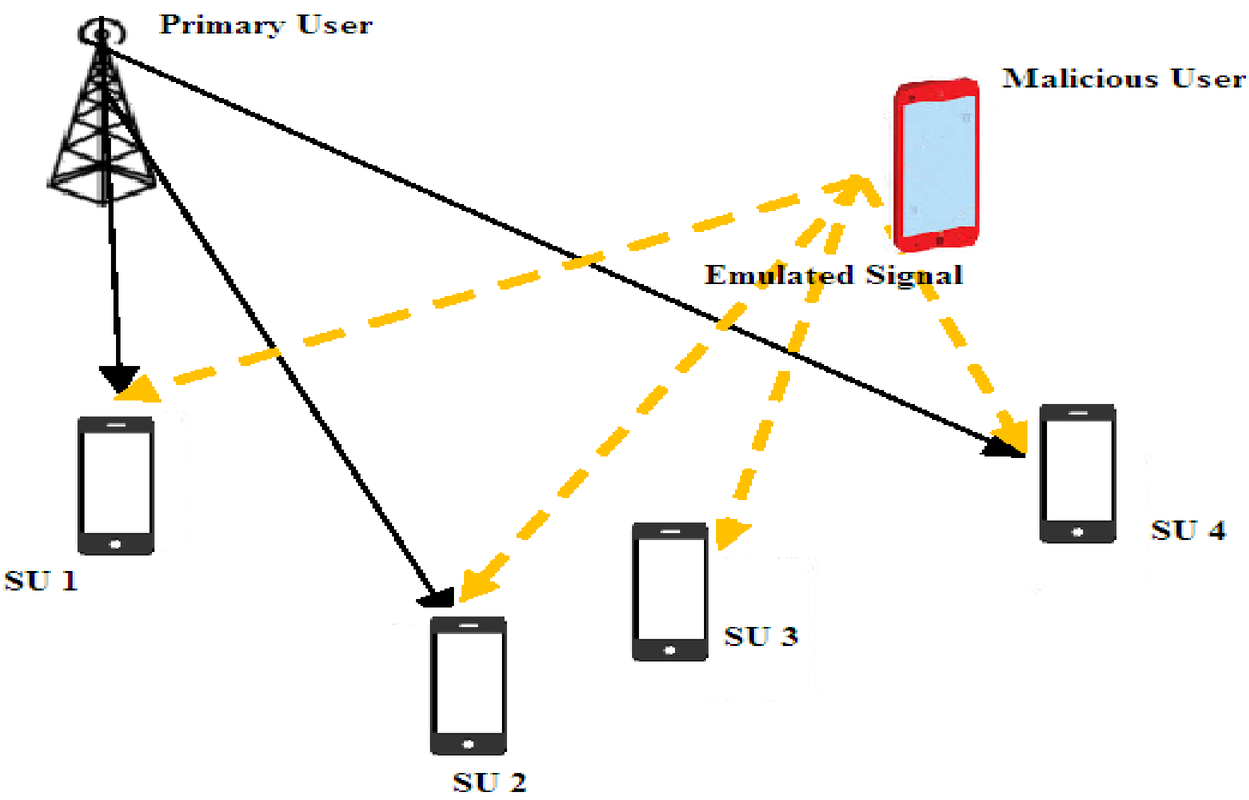

Figure 1. Scenario of PUE Attack [5]

This paper presented an algorithm based on location verification technique. The author integrates the RSS with EKF and UKF to detect the primary user/attacker.

II. RELATED WORK

A. Fingerprint based Localization Method

It is the most popular localization method comparing to all other because of its high accuracy [9]. Fingerprint-based localization having two phases- training phase and test phase.

i. Training Phase: In this phase, first we collect the RSSIs of PUs from all the beacons. These collected RSSIs are placed along with their location points in the RSSI database . These location coordinates generally referred as reference points.

ii. Test Phase: In this phase, data from each beacons is collected and calculated the RSSIs of PU.

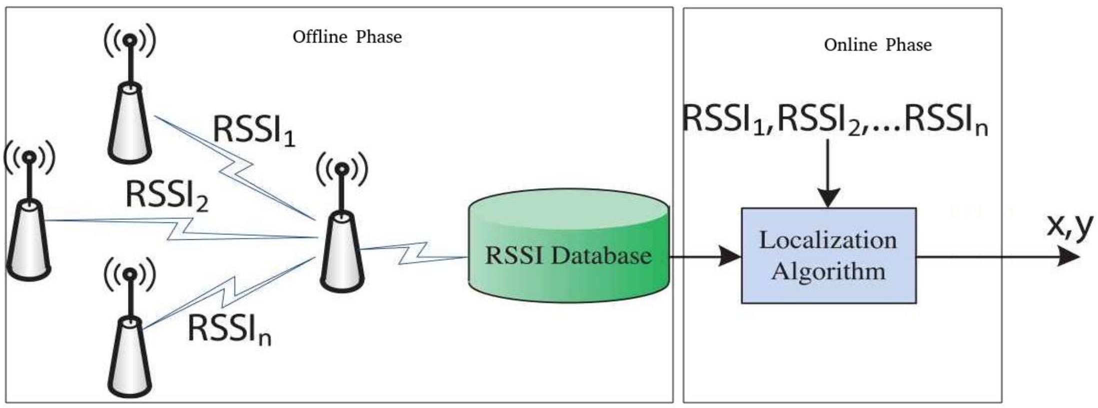

Figure 2: RSSI based Fingerprint location detection method [9]

If the characteristics of RSSIs measured in the test phase matches with the training phase, then the user is a PU otherwise it is an attacker. The major problem of this is, it requires more hardware and large database to store the RSSIs. Hence the cost is high.

B. Detection based on Kalman filter with RSSI

Zakaria El Mrabet proposed a technique [10] based on location verification using kalman filter with RSSI. In this method, first the position of PU is continuously tracked and the distance can be measured from all the beacon nodes.

Secondly, the distance from each beacon node can be measure by using RSSI. Then, the difference of these two distances is compared to a defined threshold value. If the difference between the distances is less than the threshold it is a PU otherwise it is an attacker.

III. PROPOSED SYSTEM

In [11], the author assumed that the system of interest is linear. But in many cases, the systems of interest are nonlinear by nature and another problem is initial position of system should be known priorly. Hence the estimation of PU will be erroneous. There are several extensions to the kalman filter such as EKF, UKF and so on. In this paper, the author proposes an algorithm to track PU signal using EKF and UKF, which gives better results for nonlinear systems comparing with traditional kalman filter. The author also given solution for initial position problem by using RSSI. The block diagram of location detection based on EKF/UKF and RSSI is as shown in figure 3.

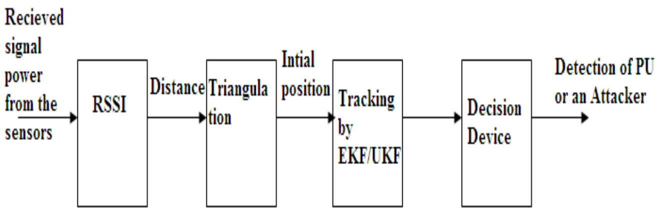

Figure:3 Location detection based on EKF/UKF and RSSI

A. EKF

In this method, the observation equations are first linearized. The linearization can be carried out by means of their Taylor series expansion [13].

Assuming that, the process noise and measurement noise are additive white nosie.

Consider the model as

$$x_n=f(x_{n-1},n-1)+q_{n-1} \quad (1)$$

$$y_n=h(x_n,n)+r_n \quad (2)$$

Where x_n- state vector
y_n- measurement vector

$q_{n-1}\sim N(0,Q_{n-1})$ process noise vector

$r_n\sim N(0,R_n)$ measurement noise vector

$f(\bullet)$, – the dynamic model function

$h(\bullet)$, – the measurement model function

Extended Kalman Filter having two phases such as, prediction phase and update phase. The proposed algorithm given in details as follows

Step 1: Intialize (x_{n-1}, P_{n-1}, q_{n-1}, r_n)

Where x_{n-1}, P_{n-1} are intial values obtained from RSSI

Step 2: Prediction Phase

$$\hat{x}_n^{-}=f(x_{n-1},n-1)\text{ ---------------- }(3)$$

$$P_n^{-}=F_x(x_{n-1},n-1)P_{n-1}F_x^T(x_{n-1},n-1)+q_{n-1}\quad(4)$$

Step 3: Update Phase

$$v_n=y_n-H_x(x_n^{-},n)\text{ ---------------- }(5)$$

$$s_n=H_x(x_n^{-},n)P_n^{-}H_x^T(x_n^{-},n)+r_n\text{ -------- }(6)$$

$$Gain\ Update\ K_n=P_n^{-}H_x^T(x_n^{-},n)\text{ ------- }(7)$$

$$x_n=x_n^{-}+K_n v_n\text{ ---------------- }(8)$$

$$P_n=P_n^{-}-K_n s_n K_n^T\text{ ---------- }(9)$$

where

$$[F_x(x,n-1)]_{j,j'}=\frac{\partial f_j(x,n-1)}{\partial x_{j'}}\Big|_{x=n}$$

$$[H_x(x,n)]_{j,j'}=\frac{\partial h_j(x,n-1)}{\partial x_{j'}}\Big|_{x=x}$$

Step 4: return x_n, P_n

B. UKF

One of the drawbacks of EKF is, in most of the cases the calculations of Jacobian and Hessian matrices can be very difficult process and secondly, when predict and update function of f and h are high order in non-linearity, the performance of EKF can be degraded. The Kalman Filter, which is suitable for high order non-lineasystems, is Unscented Kalman Filter.

In this method, forming gaussian approximation can be done by Unscented Transformation (UT) [14]. The main advantage of UT is, having better capturing strength on higher order moments caused by the non-linear transform.

In UT, we choose sigma points deterministically, which are in a fixed number. These sigma points propagate through the non-linear function g and estimate the moments of the transformed variable from them.

Consider the model equations as follow

$$x_{n+1}=F(x_n,u_n,v_n)\text{ ---------- }(10)$$

$$y_n=H(x_n,k_n)\text{ ------------- }(11)$$

Similar to KF and EKF, UKF also having two phase: Prediction Phase and Update Phase.

Step 1: Intialize $\left(\hat{x}^a_0,\ P^a_0,\ W^{(m)}_0, W^{(c)}_0\right)$

Where $\hat{x}^a_0$ - is the intial state vector obtained from RSSI

P^a_0 - is the intial covariance of state vector obtained

$W^{(m)}_0$ - intial weights of average values

$W^{(c)}_0$ - intial weights of covariance matrix

Step 2: Calculation of sigma points

$$\chi^a_{n-1} = \left[\hat{x}^a_{n-1}\ \ \hat{x}^a_{n-1} + \Gamma\sqrt{P^a_{n-1}}\ \ \hat{x}^a_{n-1} - \Gamma\sqrt{P^a_{k-1}}\right] \quad (12)$$

where $\Gamma = \sqrt{L+\tau}$

τ - composite scaling function

L-Dimension of the state

Step 3: Time update

$$\chi^x_{n|n-1} = F\left(\chi^x_{n-1}, u_{n-1}, (\chi^v_{n-1})\right) --- (13)$$

$$x^-_n = \sum_{i=0}^{2L} W^{(m)}_i \chi^x_{i,n|n-1} ------- (14)$$

$$P^-_k = \sum_{i=0}^{2L} W^{(c)}_i \left(\chi^x_{i,n|n-1} - \hat{x}^-_n\right)\left(\chi^x_{i,n|n-1} - \hat{x}^-_n\right)^T$$

----------(15)

$$Y_{n|n-1} = H\left(\chi^x_{i,n|n-1}, \chi^n_{n-1}\right) ------ (16)$$

$$y^-_n = \sum_{i=0}^{2L} W^{(m)}_i Y_{i,n|n-1} --------- (17)$$

Step 4: Measurement update

$$P_{\tilde{y}_n, \tilde{y}_n} = \sum_{i=0}^{2L} W^{(c)}_i \left(Y_{i,n|n-1} - \hat{y}^-_n\right)\left(Y_{i,n|n-1} - \hat{y}^-_n\right)^T$$

----------------(18)

$$P_{x_n, y_n} = \sum_{i=0}^{2L} W^{(c)}_i \left(\chi_{i,n|n-1} - \hat{x}^-_n\right)\left(Y_{i,n|n-1} - \hat{y}^-_n\right)^T$$

-----------------(19)

$$Gain\ Update\ K_n = P_{x_n y_n} P^{-1}_{\tilde{y}_n \tilde{y}_n} ----- (20)$$

$$\hat{x}_n = x^-_n + K_n\left(y_n - \hat{y}^-_n\right) --------- (21)$$

$$P_n = P^-_n - K_n P_{\tilde{y}_n \tilde{y}_n} K^T_n ---------- (22)$$

Step 5: return x_{n+1}, P_{n+1}

C. Proposed Algorithm

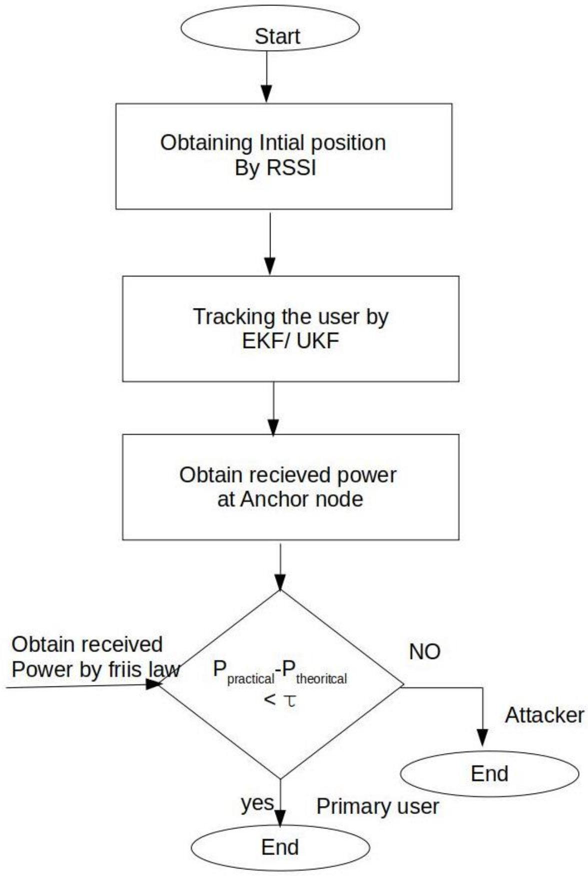

Figure 4: Flow chart of Location detection based on EKF/UKF and RSSI

Step 1: Collecting the received power of each user at each beacon.

Step 2: From the received power estimate the distance from anchor node to the user by using path loss model

$$d_{rssi} = 10^{\frac{RSSI-A}{10\eta}} ------------- (23)$$

Step 4: Find initial position of the user by triangulation method. Let (X, Y) are initial values.

Step 5: Track the user by EKF/UKF, assuming (X,Y) are initial values.

Step 6: Find the final position and the power received ($P_{practical}$) at final position.

Step 7: Find the power by using Friis equation

$$P_{theoritical} = \frac{P_t G_t G_r}{(4\pi\lambda d)^2} ----------- (24)$$

Step 8: If $|P_{practical} - P_{theoritical}| < \gamma$, the user is a primary user , else an PUEA

IV. RESULT AND DISCUSSION

The main objective of this paper is defense against primary use emulsion attack by finding the location of the primary user. Here the author proposes an algorithm based on Extended Kalman Filter and Unscented Kalman Filter. The initial positions of the filter is estimated by Received Signal Strength Indicator (RSSI).

The set up for this experiment is as follows. Firstly, we assumed Bluetooth mobile user as a primary user. We obtained the RSSI values. Then we estimated distance between the anchor node and the Bluetooth mobile user by path loss model.

By using triangulation method we estimated the initial position the primary user. These estimated initial values are given to both EKF and UKF. Then the process of tracking can be done continuously. The received power at final position is compared with the power obtained by friis formula. The proposed algorithms with necessary mathematical expressions are also explained clearly. Figure 5 shows the RSS vs the distance between the anchor node and primary user. It is clearly understood that, as the RSS is increasing the distance

Figure 6 and 7 shows the how tracking of primary user taken place by both EKF and UKF filters. It is observed that both non-linear filter follows the almost exactly same as the original path. The author also compares the performance of EKF and UKF by means of RMSE as shown in fig.8. It is clearly observed that, the RMSE value of UKF is less than that compared with the RMSE value of EKF. Suppose if we observe at time 40secs the RMSE value of EKF is 0.0075 where as the RMSE value UKF is 0.0065.

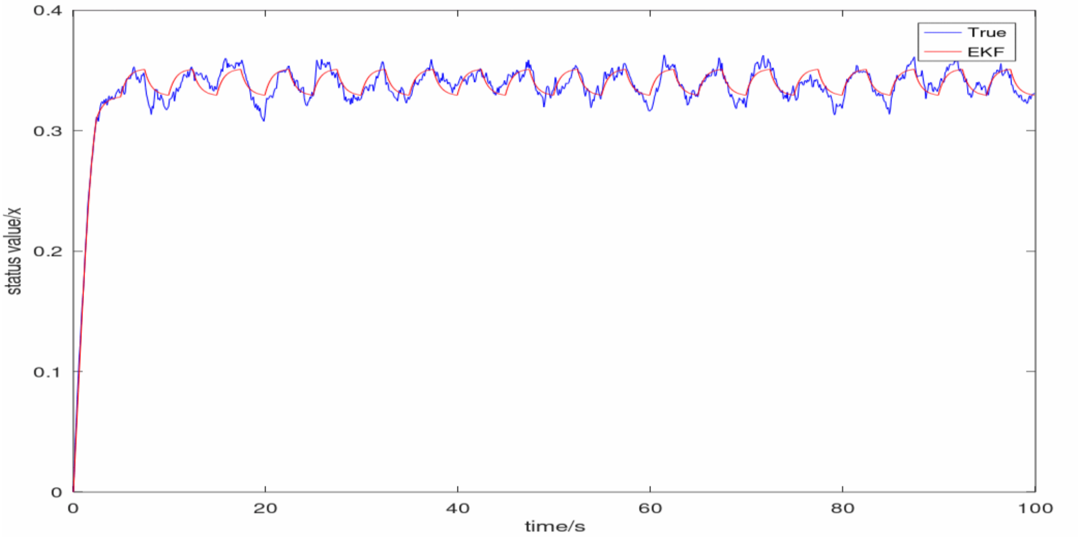

Figure 5: Received signal strength vs distance

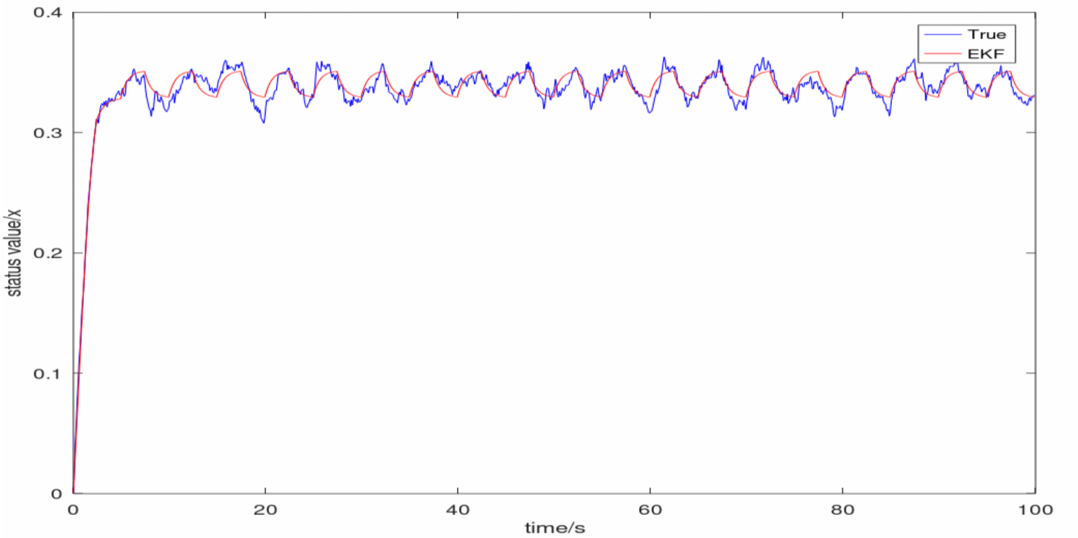

Figure 6: Location tracking by EKF

Retrieval Number: B3886129219/2019©BEIESP
DOI: 10.35940/ijeat.B3886.129219
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication

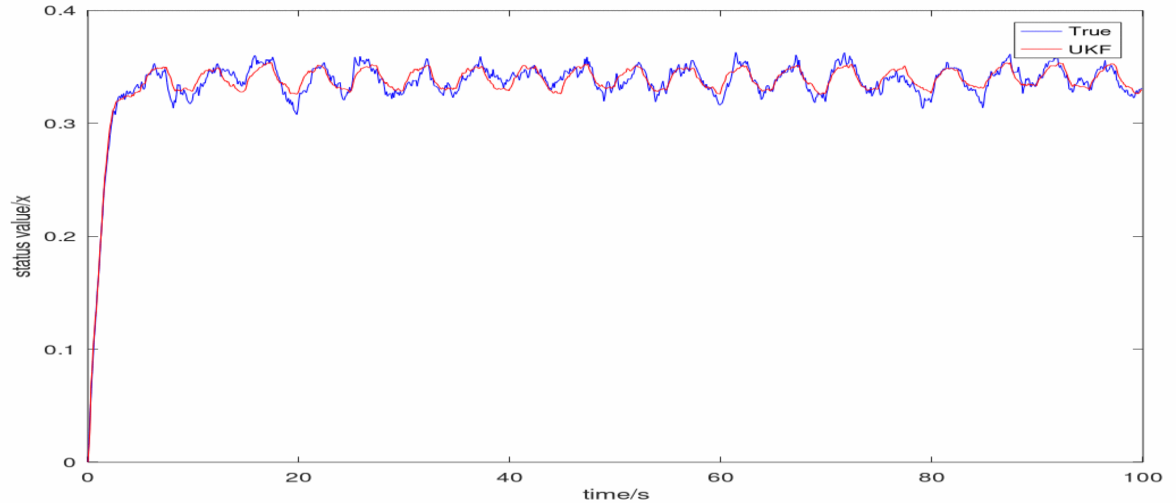

Figure 7: Location tracking by UKF

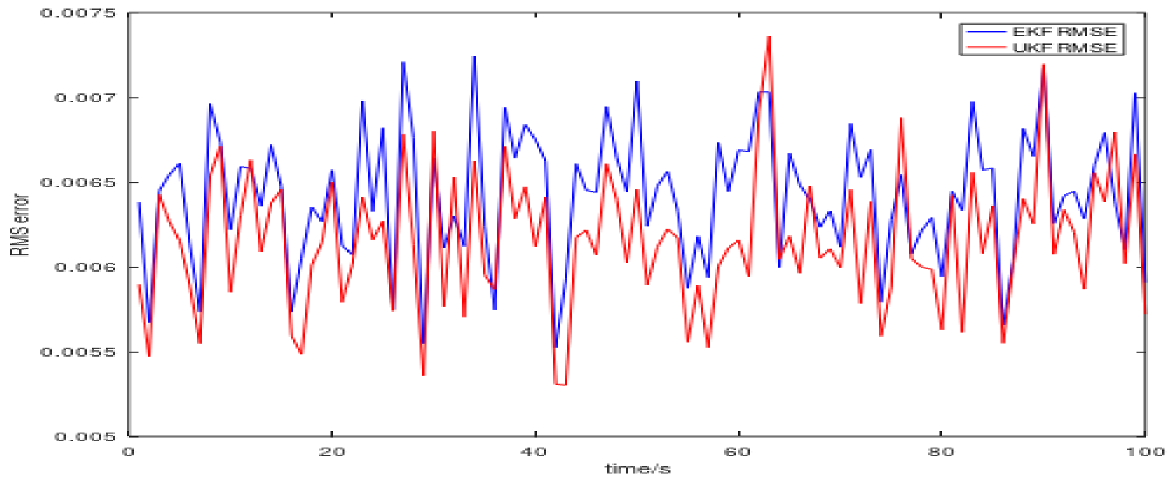

Figure 8: RMSE Comparisons of EKF and UKF

V. CONCLUSION

It is observed from figure 8, tthat the UKF performed well in locating the primary user as compared to that of EKF. It is also observed that UKF not required the complex jacobian matrix and UKF is accurate in first two terms of Taylor expansion whereas EKF is accurate in only first term of Taylor expansion. The limitation of EKF and UKF is, the noise which is assumed to be additive white gaussian noise. The performance of EKF and UKF is poor if the noise is non-white noise. Hence if the noise is non-white noise we can estimate the location user using a filter called “Particle Filter” which gives better results. In this paper, we assumed that only one primary user and estimated the location of that user and hence PUE attack can be avoided. Further this work can be extended to combat the PUE attack when multiple primary users are present.

REFERENCES

1. Rajesh K. Sharma, Danda B. Rawat,"Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A survey ,"IEEE Communication Surveys & Tutorials Vol. 17 No. 2, 2015, pp 1023-1043.
2. Kattaswamy Mergu, "Spectrum Sensing Using Neyman-Pearson Based Matched Filter Detection In Cognitive Radio Networks," Journal of Basic and Applied Research International, vol. 21,No.3, 2017, pp. 143-149.
3. Pinaki Sankar Chatterjee, "Detecting PUE Attack by Measuring Aberrational Node Behavior in CWSN ," Journal of Interconnection Networks, vol. 18,No.1, 2017, pp. 1-15.
4. A.S Kang, Renu Vig," Simulation Analysis of Prototype Filter Bank Multicarrier Cognitive Radio Under Different Performance Parameters," Indonesian Journal of Electrical Engineering and Informatics (IJEEI) vol. 3,No.3, 2015, pp. 157-166.
5. Shivanshu Shrivastava, A. Rajesh, P.K. Bora,"Defense against primary user emulation attacks from the secondary user throughput perspective," International Journal of Electronics & Communication (AEU) Vol 84, 2018, pp 131-143.
6. Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis,"A Survey on Security Threats and Detection
7. Techniques in Cognitive Radio Networks ," IEEE Communications Surveys & Tutorials, Vol 15, No.1 2013, pp. 428-445.
8. D. Pu, Y.Shi, A.V. Ilyashenku, and A.M Wyglinski, "Detecting Primary User Emulsion Attack in Cognitive Radio Networks ," in Proc. IEEE Global Telecommunications Conference, Dec 2011, pp. 01-05.
9. D.Eswara Chaitanya, G.Sasibhushana Rao, “Unknown radio source localization based on a modified closed form solution using TDOA measurement technique,” 4th International Conference on Recent Trends in Computer Science and Engineering , 2016, pp.184-189.
10. Santosh Subedi and Jae-Young Pyun, “Practical Fingerprinting Localization for Indoor Positioning System by Using Beacons Journal of Sensors,” Volume 2017, pp. 1-17.
11. Zakaria El Mrabet , Youness Arjoune, Hassan El Ghazi , Badr Abou Al Majd, and Naima Kaabouch, " Primary User Emulation Attacks: A Detection Technique Based on Kalman Filter," Journal of Sensor and Actuator Networks,2018,pp. 1-14.

12. A.UmaMageswari, J.Joseph Ignatious ,R.Vinodha," A Comparitive Study Of Kalman Filter, Extended Kalman Filter And Unscented Kalman Filter For Harmonic Analysis Of The Non-Stationary Signals," International Journal of Scientific & Engineering Research, Vol.3, No. 7, july 2012, pp. 1-9.
13. S. Konatowski & A. T. Pieniezny, "A comparison of estimation accuracy by the use of KF, EKF & UKF filters," WIT Transactions on Modelling and Simulation, Vol 46 , 2007, pp. 779-789.
14. Dai Hong-de, Dai Shao-wu, Cong Yuan-cai, Wu Guang-bin," Performance Comparison of EKF/UKF/CKF for the Tracking of Ballistic Target," TELKOMNIKA, Vol.10, No. 7, 2012, pp. 1537-1542.

AUTHORS PROFILE

Mr. Kattaswamy Mergu, pursuing Ph.D from Sri Satya Sai University of Technology and Medical Sciences in the department of Electronics and Communication Engineering, Mady Pradesh, India. He has published 10 international journals in various publications. He has 10 years of teaching experience in the department of ECE. His main research interest includes Cognitive Radio, Wireless Communication, Coding Theory and Antennas.