IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Detection Of Primary User Emulation Attack in Cognitive Radio Networks Based On TDOA using Grey Wolf Optimizer

Aasia Rehman

Dept. of Computer Sciences, Kashmir University, Srinagar, India

**Corresponding Author: aasiya.rehman77@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i2.332337 | Available online at: www.ijcseonline.org

Accepted: 16/Feb/2019, Published: 28/Feb/2019

Abstract—Cognitive Radio is a technology that overcomes the problem of spectrum shortage by embedding the wireless devices with an intelligent agent to make the opportunistic use of available white spaces in the radio environment. However due to ubiquitous nature of cognitive radio networks, it is sensitive to a number of security threats which disturbs the overall performance of cognitive radio networks. The main goal of this paper is to thwart one of the security threats in Cognitive Radio Networks known as Primary User Emulation Attack. Primary User Emulation Attack is one of the most popular Dynamic Spectrum Access attack. In this paper we are detecting the primary user emulation attack based on TDOA values using Grey Wolf Optimizer. Simulation results show that Grey Wolf Optimizer is more accurate than using the Particle Swarm Optimization Algorithm for mitigation.

Keywords—*Cognitive Radio Network;Primary User Emulation Attack;Grey Wolf Optimizer;Particle Swarm Optimization;Dynamic Spectrum Access; Time Difference Of Arrival;*

I. INTRODUCTION

In CR Networks the allocation of frequency bands are organized by Federal Communication Commission (FCC). FCC allocates the spectrum bands to licensed users known as Primary Users, however major portion of spectrum band remain un-utilized most of the times as shown in the *Fig. 1*. This underutilization of spectrum, demands the development of Dynamic Spectrum Access methods which allows the unlicensed users to use the 'white spaces' of the licensed spectrum. Over the years FCC, has made flexible and extensive use of accessible spectrum by using the cognitive radio technology [1].

Cognitive Radio Technology is an evolving technology that enables the wireless devices to make use of white spaces of licensed spectrum for communication purposes however it should not cause any interference to the licensed user's communication. In order to find the white spaces within the licensed band, cognitive radio undergoes a process known as cognitive process which includes observe (sensing), reasoning (analysis), modification (adaptation) and act (communication)phases [2] as depicted in *Fig. 2*. Sensing and communication

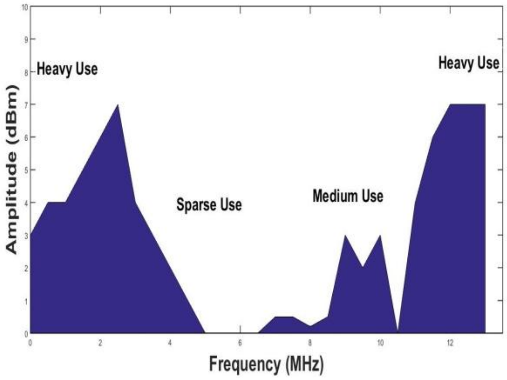

Fig. 1 Spectrum Usage

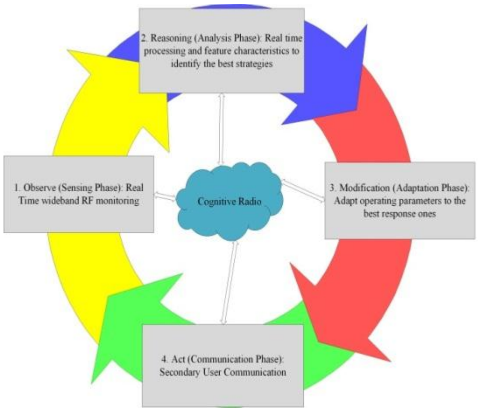
2. Reasoning (Analysis Phase): Real time processing and feature characteristics to identify the best strategies
1. Observe (Sensing Phase): Real Time wideband RF monitoring
Cognitive Radio
3. Modification (Adaptation Phase): Adapt operating parameters to the best response ones
4. Act (Communication Phase): Secondary User Communication

Fig. 2 Cognitive *Process for Cognitive Radio Networks*

phases are the most critical phases as they are most sensitive to security attacks e.g. while performing sensing the secondary device can be attacked by spoofing signals in white spaces by an intruder to impersonate the primary user's. Also when secondary devices utilize white spaces, the attacker can introduce jamming signals to halt the packet transmission during communication phase [2]. The phase's, analysis and adaptation are not mush sensitive to security attack and they depend on the sensed data received after sensing phase. Cognitive Radio Technology introduces entirely new classes of attacks including Primary user emulation attack, Spectrum sensing data falsification attack, jamming etc. because of its dynamic and ubiquitous spectrum availability. Mitigation techniques are developed to thwart these security attacks in cognitive radio networks for their better performances.

In this paper we mainly focus on detection of PUE attack. PUE attack is among the most popular Dynamic Spectrum Access attacks [3]. The primary system is authorized to use a particular spectrum band at any time. But when they are not using the assigned band it can be utilized by the CR users. The CR users must employ algorithms for sensing the spectrum to determine whether the primary system is using the band or not. Here the intruder can induce an attack by simply using a signal which is equivalent to the primary system that forces the spectrum sensing algorithms to generate faulty results. This makes the CR users to free the band because of the results of algorithm which makes them conclude that the primary system is currently using the spectrum. Thus the intruder can utilize the spectrum. This is known as the primary user emulation attack also sometimes called as sensory manipulation attack [3]. In this paper, the PUE attack is detected by using number of cooperative secondary users which sends their sensed data to the base-station. The base-station uses the correlation method to retrieve the TDOA (time difference of arrival) measurements which determines the position of the transmitter and is related with the known location of Primary User to reveal whether the sender is the attacker or a Primary User. In order to reduce the error of estimating the location of transmitter the optimization algorithm known as Grey Wolf Optimizer is applied, which minimizes the non-linear least square cost function [4].

II. RELATED WORK

In the literature various techniques have been proposed to detect the presence of primary user emulation attacker. Energy based detection technique was proposed in [5] [6] in which an unlicensed user was able to identify the signals from only another unlicensed user but cannot identify the PU signals. Hence, whenever the unlicensed user encounters a signal that is recognizable by it, it is presumed to be the signal from another unlicensed user. However if the signal cannot be identified by the unlicensed user it is considered to be from primary user. The authorsin [7-10] recommended a detection technique depending on feature extraction where the unlicensed users try to extract the particular features of the sensed signal. Thus, in these methods the unlicensed users are capable of identifying the innate features of the primary user signals due to which they are able to differentiate among the primary user signals and the secondary user signals. In [11] [12]the authors proposed a passive anti-PUE technique, known as dogfight in frequency bands where the secondary users randomly select the channel for sensing and mitigate the primary user emulation attack. In [13-17] the authors proposed the detection techniques based on analytical models known as Neyman-Pearson composite hypothesis test and a Wald's sequential probability test. In [18] the authors suggested a technique that combines the cryptographic signatures with link signatures to differentiate the genuine PU signals from the PUE attacker signals. In [19] the authors suggest a LocDef (localization-based defense) to determine if the received signal is from the PU or the attacker by calculating the location of the signal transmitter and analyzing its signal characteristics and then comparing its location with the known location of the PU.

III. DETECTION OF PRIMARY USER EMULATION ATTACK

Primary User Emulation Attack is the attack where the adversary transmits the primary-user-alike signals while the secondary users are sensing the spectrum thus sending away the secondary users as they cannot differentiate among primary user signals and the adversary's signals [12]. In this paper we are using the TDOA measurements to obtain the location of transmitter [20]. TDOA is defined as the difference between TOA obtained by two or more devices and TOA is defined as the measure of space among the device to be identified and the reference device. For obtaining the location of the transmitter, two TDOA measurements are required, which locates the transmitter on the intersection point of the two hyperboloids. However in actual atmosphere these hyperboloids seldom intersect. This error in estimating the location can be reduced to a great extent by the help of optimization algorithms. This paper uses an approach known as Grey Wolf Optimizer that reduces the error in estimating the location of the transmitter by minimizing the non-linear least square cost function [4].

Suppose (x, y) is the location of the sender which is in the range of n destinations at locations (x_i, y_i) where $i \epsilon [1, n]$ and the reference user called the base-station is at the origin (0,0) that has the location of the primary transmitters. The TDOA value $\tau_{i,}$ obtained from the pair formed by i and the base-station is shown in (1) [20] as a function of (x, y) [20]

$$F(x, y) = \frac{\sqrt{(x-x_i)^2+(y-y_i)^2}-\sqrt{(x)^2+(y)^2}}{v_p}(1)$$

The detection of PUEA has three main steps:

- Comparing the features of received signal with the primary user and the secondary user signal features.
- Applying the localization method based on TDOA using Grey wolf optimization technique to obtain the location of the transmitter.
- Compare the obtained location with the known location of the primary user and decide whether it is primary user or PUE attacker.

In order to detect the attackers, all the secondary users first observe the spectrum and then transmits the observed data to the base-station. The base-station collects the sensed data from the secondary users and then applies the correlation technique to obtain the TDOA measurements which requires tight synchronization. A collection of TDOA measurement, results in non-linear set of equations with multiple solutions [20] which is an issue of optimization that we are solving using the Grey Wolf Optimizer. The error in time of arrival values is assumed to be normal random variable with variance obtained by using the Cramer-Rao Lower Bound (CRLB) [21] providing a lower bound on free channel with several paths. In TDOA, since every measurement is the deviation of two TOA values, any measurement among a node i and the base-station can be defined as [20] $\tau_i = N$ (f_i (x, y)) $\sigma_i^2+\sigma_0^2$ where [20]

$$\sigma_i^2 \geq 1/8\Pi^2.B^{2\cdot}\,SNR_i \qquad (2)$$

σ_i is the measure of variance from node i and σ_0 is the measure of variance from BS. B is the bandwidth and SNR_i is the signal to noise ratio at device i. In IEEE 802.22, Hata model for suburban areas have been suggested for path loss computations [22]. Thus SNR_i at node i can be modeled as in equation (3) [20] where ΔL_p in (4) is path loss and SNR_0 is the BS signal to noise ratio [20] and d_i and $d_0$are the distances between the transmitter to the device i and the base station respectively. h_p is the antenna height.

$$SNR_i = SNR_0 - \Delta L_p\ (dB) \qquad (3)$$

$$\Delta L_p\ (dB) = [44.9\text{-}6.55(h_p)]\ \log(d_i / d_0) \qquad (4)$$

Non-Linear Least Square Function: The main aim of non-linear least square is to minimize the sum of squares of error on estimating the location which can be designated as:

$$\hat{X} = \mathit{arg}\min J_{NLS,\ TDOA}(\hat{X}) \qquad (5)$$

The output of the above equation is the attacker's location, and here $J_{NLS,\ TDOA}(\hat{X})$ is the objective function and can be represented as under [23]:

$$\text{JNLS, TDOA}(\hat{X}) = \sum_{i=1}^{N}(r_{TDOA,i} - \sqrt{(\tilde{x} - x_i)^2 + (\tilde{y} - y_i)^2} + \sqrt{(\tilde{x} - x_0)^2 + (\tilde{y} - y_0)^2})$$

$$= (r_{TDOA}\text{-}f_{TDOA})^T * (r_{TDOA}\text{-}f_{TDOA}) \qquad (6)$$

IV. Grey Wolf Optimizer

Grey Wolf Optimizer proposed in [24] by Seyedali Mirjalili, Seyed Mohammad Mirjalili and Andrew Lewis is a meta-heuristic optimization algorithm encouraged from grey wolves. Meta-heuristic methods are the most popularly used methods in various fields particularly in computer sciences over the last two decades [24]. It is because meta-heuristic methods are fairly simple, flexible, derivation free and prevents local optima [24]. Grey Wolf Optimizer imitates the leadership hierarchy and hunting techniques from Grey Wolves. Also few important steps namely hunting, seeking for victim, surrounding and attacking the victim are carried out [24].

Grey Wolf is from the Canidae family who desire to live in groups of size 5-12 on an average. The leadership hierarchy of Grey Wolves is shown in *Fig. 3*. At the top of hierarchy are the males and females called alphas (α) which are the decision makers of the group like decision about hunting, sleeping etc. Alpha wolves are also known as dominant wolves since their decision are to be followed by all the group members. At the second level the wolf is known as beta (β) wolf. These are the subordinates for alphas that help them in making the decisions for the group [24]. The beta wolf can be male or female and is one of the most suitable wolf incase alpha wolf passes away or becomes old to lead. At the lowest level is the omega (ω) wolf which is dominated by all other wolves. And then there is a delta (δ) wolf which is not the alpha, beta or omega wolf. They need to follow alpha and beta wolves but they can dominate omega wolves. They include elders, hunters, scouts and care takers [24].

The primary steps for hunting by Grey Wolves are [24]:

- Discovering, running after and approaching the victim
- Following, surrounding and harassing
- Attacking the victim

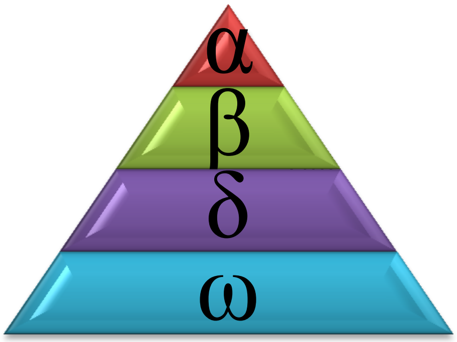

Fig. 3Leadership Hierarchy of Grey Wolf

In GWO α is treated as the first best solution and β and δ are treated as the 2nd and 3rdbest solutions respectively. The left out solutions are considered as ω. GWO algorithm performs optimization using alpha, beta and delta whereas omega follows them.

GWO Algorithm [24] is as under:

```
Algorithm: Grey Wolf Optimizer
Input: Max_Iterations, Population of Wolves $X_i$ (i= 1, 2…. n), A, C, a and t =1
Compute the fitness of each individual using equation (6)
        $X_\alpha$, the first finest individual
        $X_\beta$, the 2nd finest individual
        $X_\delta$, the 3rd finest individual
While (t <Max_Iterations)
    For i= 1 to size_of Population of wolves
        every individual modify the location of the present individual
End for
Modify values of A, C and a
Compute the fitness of all individuals using equation (6).
Update $X_\alpha$, $X_\beta$, and $X_\delta$
T = t+1
End while
Output: $X_\alpha$
```

Here the output of the algorithm i.e. X_α, is the estimated location of the transmitter with minimum localization error. *Fig 4* depicts the flowchart for Grey Wolf Optimizer Algorithm

Some important points about GWO are as follows:

- The leadership hierarchy defined in [24] helps the grey wolf optimizer to store the best solution achieved so far.
- The encircling method introduced by [24] determines a round carved neighborhood surrounding the solutions that can be further expanded to larger amplitudes as a hyper sphere.
- The arbitrary parameters A and C help the solutions to have hyper spheres with distinct radius.
- The hunting technique defined in [24] permits the candidate solutions to identify the possible position of the prey.
- The dynamic values of a and A ensure exploration and exploitation.
- The transformation between exploration and exploitation is guaranteed by the changing values of A and a.
- Half of the iterations are dedicated to exploration and other half to exploitation with reducing values of A.
- Grey Wolf Optimizer have two important parameters to be fine-tuned that are a and C.

V. RESULTS AND DISCUSSIONS

In this paper, we are using cumulative distributive function and mean square error to evaluate the accuracy of the used technique i.e. Grey Wolf Optimizer for detection of primary user emulation attack using the MATLAB tool. IEEE 802.22 network is used with TV tower

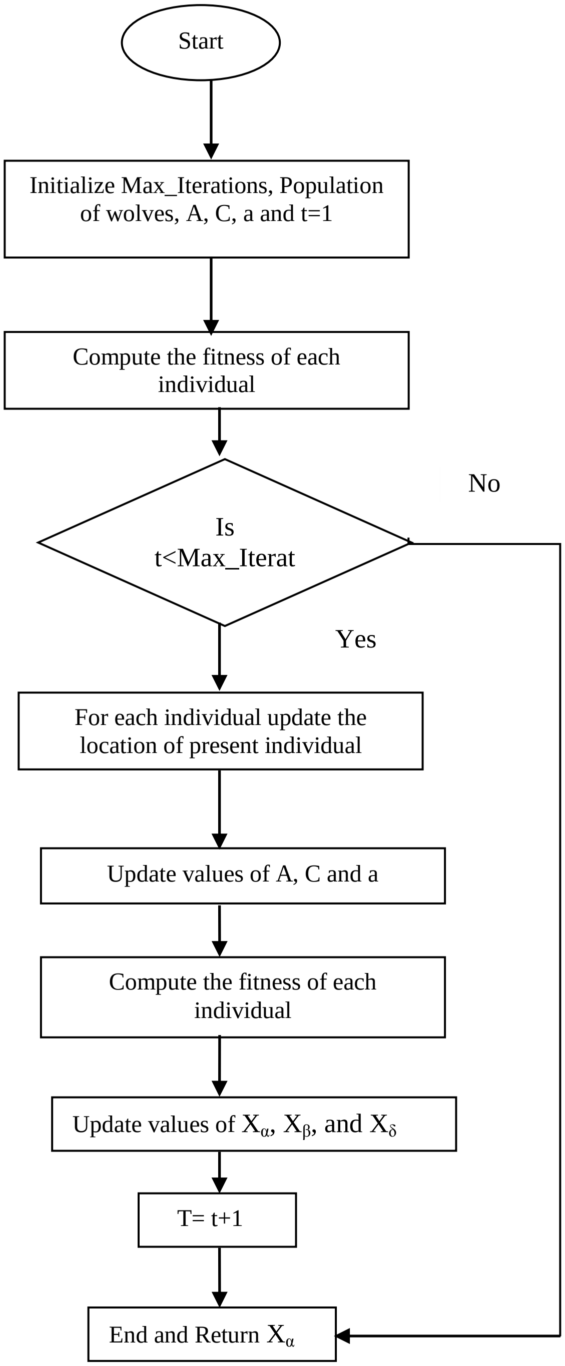
Start
Initialize Max_Iterations, Population of wolves, A, C, a and t=1
Compute the fitness of each individual
Is t<Max_Iterat
No
Yes
For each individual update the location of present individual
Update values of A, C and a
Compute the fitness of each individual
Update values of Xα, Xβ, and Xδ
T= t+1
End and Return Xα

*Fig. 4*Flow Chart *Grey Wolf Optimizer* as primary transmitter and receivers. Each experiment is run for 500 simulations. The performance of suggested method known as Grey Wolf optimizer is compared with the Particle Swarm Optimization Algorithm. Some of the assumptions and parameters used are as follows:

- Base-station is assumed to be at origin
- Secondary users ranging from 10 to 100 are randomly distributed over 30 * 30 km^2 area
- Primary user is placed outside the cognitive radio network at position (50000m, 50000m) with 30 to 150 km far from the base-station
- Position of primary user is known to the base-station,
- Primary user emulation attacker is located at (8000m, 1000m) when within the network and at (50000m, 0m) when located outside the network
- Hata model is used for channel path,
- Signal to noise ratio changes from -10dB to 10dB
- Lower and Upper bounds are taken as [-10000, -10000] and [10000 10000] respectively
- Bandwidth as 6MHz
- Antenna height is taken as 1.5 m.
- Maximum number of iterations = 200
- Size of population = 50
- Inertia weight for PSO, w = 0.9

Fig. 5 depicts the CDF vs. Distance Error plots for Grey Wolf Optimizer and Particle Swarm Optimization Algorithms using non-linear least square (NLS) as the fitness function with SNR$_0$= -10dB and number of secondary users equal to 100. The graph clearly demonstrates that GWO-NLS outperforms PSO-NLS e.g. at CDF= 0.7, the error is 10m and 20 m for GWO and PSO respectively.

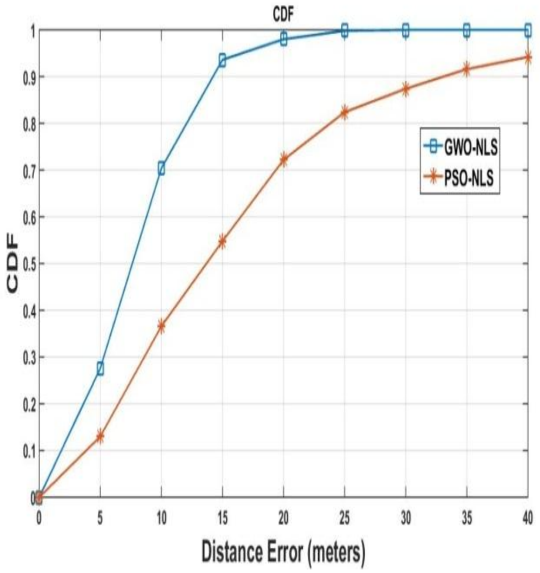

*Fig. 5 CDF vs. Distance Error*PUEA inside CRN at (8000m, 1000m)

Fig. 6 illustrates the variation of distance error with the increase in signal to noise ratio with secondary devices equal to 10. It is clear from the graph that GWO-NLS is more accurate than the PSO-NLS.

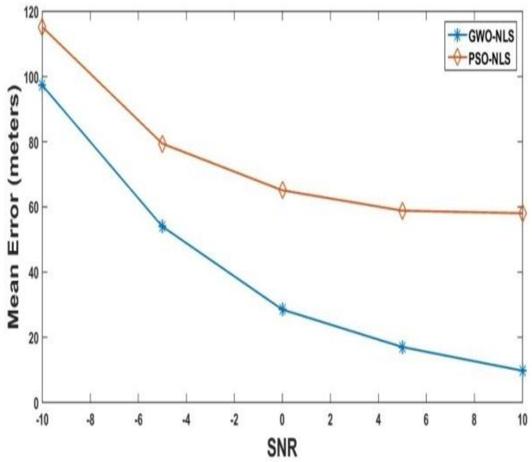

Fig. 6Mean Error vs. SNR PUEA at (8000m, 1000m)

*Fig. 7*shows the CDF vs. Distance Error plots for Grey Wolf Optimizer and Particle Swarm Optimization algorithms using non-linear least square (NLS) as the fitness function with primary user emulation attacker located outside the CR network at (50000m, 0m), SNR$_0$ = -10dB and number of secondary users equal to 100. The graph clearly demonstrates that GWO-NLS is more accurate than the PSO-NLS and also the detection of PUEA is difficult when it is located outside the network since it has larger distance error than when it is located inside it. When CDF = 0.6, the distance error is 110m and 200 m for GWO-NLS and PSO-NLS respectively.

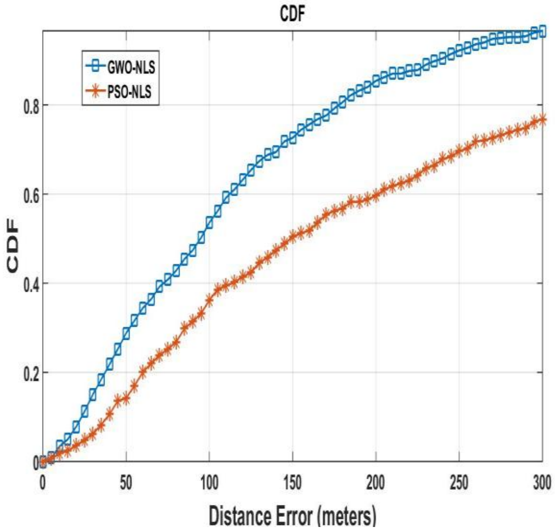

Fig. 7CDF vs. Distance Error PUEA outside CRN at (50000m, 0m)

VI. CONCLUSION

Cognitive Radio Technology over the years has been recommended as a radical solution for constructive use of the deficient spectrum bands in a robust and brilliant ways. The cognitive radio technology enables wireless devices with supplementary bandwidth, stable communication and adaptability for fast developing wireless applications by changing the operating frequency to the free licensed frequency and modifying the transmitting parameters according to the radio environment. In this paper we have used an optimization technique known as Grey Wolf Optimizer in addition to cooperative detection of primary user emulation attack based on TDOA values to minimize the error encountered in locating the attacker. Simulation results shows that the used technique, Grey Wolf Optimizer is more accurate than using the Particle Swarm Optimization Technique.

REFERENCES

[1] Beibei Wang and K. J. Ray Liu, "*Advances in Cognitive Radio Networks: A Survey*," IEEE Journal of Selected Topics in Signal Processing, vol. 5, no. 1, February 2011.

[2] Rajesh K. Sharmaand Danda B. Rawat, "*Advances on Security Threats and Countermeasuresfor Cognitive Radio Networks: A Survey*" IEEE Communications Surveys & Tutorials.

[3] T. Charles Clancy, Nathan Goergen, "Security in cognitive radio networks: threats and mitigation," 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008. Crown Com 2008, 2008, pp 1–8 (IEEE).

[4] H. Srikanth Kamath, L. M. Schalk, "*Primary User Localization Schemes in Cooperative Sensing*," International Journal of Computer Applications (0975 8887) Volume 105 - No. 13, November 2014.

[5] K.Challapali, S. Mangold, and Z. Zhong, "Spectrum agile radio:Detecting spectrum opportunities," Proceedings of the 6th AnnualInternational Symposium on Advanced Radio Technologies, March 2004.

[6] M.P.Olivieri, G. Barnett, A.Lackpour, A. Davis, and P. Ngo, "A scalable dynamic spectrum allocation system with interference mitigation forteams of spectrally agile software defined radios,"Proceedings of theIEEE International Symposium on New Frontiers in Dynamic SpectrumAccess Networks, November 2005.

[7] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues inspectrum sensing for cognitive radios," Proceedings of the Thirty-eightAsilomar Conference on Signals, Systems, and Computers, November2004.

[8] L.P.Goh, Z.Lei, and F Chin, "Dvb detector for cognitive radio," Proceedings of the International Conference on Communications, page 64606465, Glasgow, Scotland, June 2007.

[9] Y.Qi, T.Peng, W.Wang, and R.Qian, " Cyclostationarity-based spectrumsensing for wideband cognitive radio," Proceedings of the 2009 WRIInternational Conference on Communications and Mobile Computing,page 107111, Washington, DC, USA, 2009.

[10] W.Xia, S.Wang, W.Liu, and W.Cheng, "Correlation-based spectrum sensing in cognitive radio," Proceedings of the 2009 ACM Workshop on Cognitive Radio Networks, page 6772, New York, NY, USA, 2009.

[11] H Li and Z Han, "*Dogfight in spectrum: Combating primary useremulation attacks in cognitive radio systems, part i: Known channel statistics*,"IEEE Transactions on Wireless Communications, 9(11):3566–3577, 2010.

[12] Husheng Li and Zhu Han, "*Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems-Part II: Unknown Channel Statistics*," IEEE Transactions on Wireless Communications, Vol. 10, No. 1, January 2011.

[13] S Anand, Z Jin, and KP Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks,"Proceedingsof IEEE Symposium on New Frontiers in Dynamic Spectrum AccessNetworks, Chicago, IL, USA, October 2008.

[14] Z Jin, S Anand, and KP Subbalakshmi, "Detecting primary user emulationattacks in dynamic spectrum access networks," Proceedings of IEEE International Conference on Communications, Dresden, Germany, June2009.

[15] Z Jin, S Anand, and KP Subbalakshmi, "*Mitigating primary useremulation attacks in dynamic spectrum access networks using hypothesis testing*," ACM SIGMOBILE Mobile Computing and Communications
Review, 13(2):74–85, 2009.

[16] Z Jin, S Anand, and KP Subbalakshmi, "Performance analysis of dynamicspectrum access networks under primary user emulation attacks," Proceedings of IEEE Global Telecommunications Conference, Miami,FL, USA, December 2010.

[17] Zituo Jin,"Primary user emulation attack in dynamic spectrum accessnetworks: threats, mitigation and impact," Licentiate dissertation, StevensInstitute of Technology, Hoboken, NJ, May 2012.

[18] Peng Ning Yao Liu and Huaiyu Dai,"Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures,"Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 2010.

[19] R.Chen, J.M.Park, and J.H. Reed,"*Defense against primary useremulation attacks in cognitive radio networks*,"IEEE Journal on SelectedAreas in Communications Special Issue on Cognitive Radio Theory andApplications, 2008.

[20] Olga Leon, Juan Hernandez-Serrano, Miguel Soriano, "*Cooperative Detection of Primary User Emulation Attacks in CRNs*," Computer Networks, Elsevier, Vol. 56, pp. 3374-3384, Sep. 2012.

[21] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch, H. Poor, Z.Sahinoglu, *Localization via ultra-wideband radios: a look atpositioning aspects for future sensor networks*, IEEE Signal Processing Magazine 22 (4)(2005)70–84.

[22] A. Eksim, S. Kulac, M. Sazli, Effective cooperative spectrum sensing inieee 802.22 standard with time diversity, in: International Conference on Advances in Computational Tools for Engineering Applications, ACTEA'09,2009,pp.528–531.

[23] Walid R. Ghanem, Mona Shokair and Moawad I. Desouky, "An improved Primary User Emulation Attack Detection in Cognitive Radio Networks Based on Firefly Optimization Algorithm," 2016, 33rd National Radio Science Conference (NRSC 2016), Feb 22-25, 2016, Aswan, Egypt.

[24] Seyedali Mirjalili, Seyed Mohammad Mirjalili and Andrew Lewis, "*Grey Wolf Optimizer*," Advances in Engineering Software 69 (2014) 46–61, Elsevier.

Authors Profile

Aasia Rehman is pursuing PhD in the PG Department of Computer Sciences at Kashmir University. She has been awarded M. Tech in CSE from Shri Mata Vaishno Devi University, Jammu and B. Tech from Kashmir University, Srinagar. Her areas of expertise include Cognitive Radio Networks, Wireless Networks and Machine Learning.