Computer Systems Science & Engineering
DOI:10.32604/csse.2022.021433
Article

Tech Science Press

Securing Privacy Using Optimization and Statistical Models in Cognitive Radio Networks

R. Neelaveni[1,*], B. Sridevi[2] and J. Sivasankari[3]

[1]Department of Electronics and Communication Engineering, MNM Jain Engineering College, Chennai, 60009, India
[2]Department of Electronics and Communication Engineering, Velammal Institute of Technology, Chennai, 602001, India
[3]Department of Electronics and Communication Engineering, Ultra College of Engineering and Technology, Madurai, 625104, India
*Corresponding Author: R. Neelaveni. Email: rneelaveniphd@gmail.com

Received: 03 July 2021; Accepted: 16 August 2021

Abstract: Cognitive Radio Networks (CRN) are the possible and ideal solution for meeting the spectrum needs of next-generation communication systems. CRN is a promising alternative approach that allows spectrum sharing in many applications. The licensed users considered Primary Users (PU) and unlicensed users as Secondary Users (SU). Time and power consumption on security issues are considered degrading factors in performance for improving the Quality of Service (QoS). Irrespective of using different optimization techniques, the same methodology is to be updated for the task. So that, learning and optimization go hand in hand. It ensures the security in CRN, risk factors in spectrum sharing to SU for secure communication. The objective of the proposed work is to preserve the location of the SU from attackers and attain the clustering of SU to utilize the resource. Ant Colony Optimization (ACO) is implemented to increase the overall efficiency and utilization of the CRN. ACO is used to form clusters of SUs in the co-operative spectrum sensing technique. This paper deals with threat detection and classifying threats using parameters such as unlikability, context privacy, anonymity, conditional traceability, and trade-off. In this privacy-preserving model, overall accuracy is 97.4%, and it is 9% higher than the conventional models without Privacy-Preserving Architecture (PPA).

Keywords: Attacks; secondary users; cognitive radio networks; security

1 Introduction

Ever-increasing bandwidth demand in wireless communication initiates CRN to improve spectrum utilization. CRN allows the unlicensed SU to utilize PU spectrum without interference if the user was not using it as per Federal Communications Commission (FCC) regulatory policies. Many research models are available to measure the security threats [1] in CRN based on classes of vulnerabilities. Since CRN learned about the environment by being aware of the users, the Privacy-Preserving Algorithms (PPA) protect the network against interferences. Even though the algorithm secures the network, they do not present methodologies to determine the type and extent of privacy protection. Since PPA implementation increases the efficiency against security threats, it is insufficient to provide access and manage the attacks in the spectrum sharing process. It deals with specific security and privacy framework in CRN [2]. For providing accountable security within CRN entities, the theoretical model first addresses the risk factors in the spectrum sharing to SU. Efficient PPA is proposed experimentally for secured communication in the network. The improved ACO enhances security parameters. It improves efficiency, spectrum utilization, threat detection, and classification. The classification improvement is through unlikability, context privacy, anonymity, conditional traceability, and trade-off. The proposed framework identifies the threats, which affect the privacy factors in CRN by monitoring the environment. A better trade-off in privacy protection increases the overall efficiency of the system [3].

The intense utilization of wireless devices and their services increases the spectrum scarcity problem in wireless communication. CRN is a promising alternative approach that allows spectrum sharing in many applications. The licensed users are considered as PU and unlicensed users as SU. These SUs are permitted to utilize the licensed user spectrum without interference, improve spectrum utilization, and reduce the spectrum scarcity crisis in wireless communication. Many real-time applications like vehicular networks, and smart cities, have CRN implementations. The dynamic spectrum access in CRN improves the utilization and provides various spectrum opportunities such as interference management, device heterogeneity, and energy efficiency. Generally, CRN uses two approaches for SU to utilize the available spectrum based on the available information, such as spectrum sensing and geolocation database [4].

In the sensing process, the SUs sense the idle channels through the fusion centre, and then it avails the channel without any interference to the PU. In contrast, the database-driven model uses the database of spectrum information maintained by the commercial service providers. It creates a query to the service providers about the available channel information and transmits the parameters to the SU based on the geolocation. FCC specifies the database-driven model as a primary model for CRN as it uses geolocation, especially on large scale applications. The responsibility and complexity in spectrum policies push the CRN to update the system so that the SU utilizes the network [5].

Additionally, if there is a policy change in database providers, it is easy to update SU devices. Secondary users provide their local information for availing the list of channels, and databases reveal the information of SUs. It gives priority based on urgency and allocates spectrum. Many protocols are available for information retrieval and secure the location privacy of SUs. However, it needs high computation cost and time overheads to provide reliable service and privacy to the SUs. In the location-based spectrum database sharing process, the chance of utilizing the spectrum by malicious SUs is more as it does not have any verification methods for location proof. So, the Malicious Users (MU) falsify their location to access the database for available channels using false information, then occupy the channels and gain benefits creating problems for the PUs as interference. The nodes categorize themselves into two cases based on the probability of MU. The first MU sends false information due to the device failure, and the SU is an intentional interference user that deliberately modifies the system's operation. For interfering with the bands, these users report tampered spectrum sensing information to the data fusion centre and collapse the algorithm, which reduces the system's performance [6].

Conventional fusion algorithms identify the first malicious user with their high probability of attack and fail to determine the second category. Very few protocols are available for information retrieval, which uses location verification through access points. Nevertheless, the implementation cost of such protocols is high and not suitable for all environments.

2 Existing Works

Many research models are available to measure the security threats [7] in CRN based on classes of vulnerabilities. Since CRN learned about the environment by being aware of the users, the PPA protects the network against interferences. Even though the algorithm secures the network, it does not present methodologies to determine the type and extent of privacy protection. Since implementing privacy-preserving models increases efficiency against security threats, it is insufficient to access and manage the attacks in the spectrum sharing process. The theoretical model first addresses the risk factors in the spectrum sharing to SU to provide accountable security within CRN entities. Efficient PPA is proposed experimentally for secured communication in the network.

Adaptive cluster-based techniques implemented in the literature [8] propose a voting system between intra and inter clusters. The voting helps to detect malicious SUs that induce Spectrum Sensing Data Falsification (SSDF) attacks. A *k*-means clustering based on partitioning of medoid separates the features or channel state information aggregated from different sensing devices to group them into clusters. Observed merit in the adaptive cluster-based method is that it is adequately tested against various SSDF attacks. At the same time, its predecessors are valid only for a given type of SSDF. The term variety includes collaborative or cooperative sensing scenarios [9]—energy detection methods used to detect PU activity in the experimentation. A two-level sensing scheme to defend against SSDF attacks has been presented in the literature [10], where the first stage is to scrutinize the sensed information for the presence of any malicious nodes, which may try to inject false information, and the second stage is to implement an SSDF robust sequential ratio probability test enabled fusion block.

2.1 Privacy Based Preservation Protocols

Previously, numerous privacy-preserving protocols were available in the research environment to maintain the privacy of database information of MU [11]. Among them, *k*-anonymity, Private Information Retrieval (PIR), and cuckoo filter are familiar in protecting the privacy of SUs. The *k*-anonymity privacy protection protocol uses volunteers for forwarding query messages of SUs so that the database could not identify the user who preserves its privacy. However, this method needs high communication overhead and many volunteers to collect queries from SUs. In some cases, it loses its privacy protection to the SUs. In PIR based model, the SUs obtain the channel information from a dataset without sending the geographical location so that it switches channels frequently according to the channel requesting message [12]. Due to this, changing the PIR model could not protect the privacy of the SUs location. The last cuckoo filter-based protocol uses a filter to compress the spectrum information and query the channel information to the server. The available channel information is shared with the query server and SUs in the network [13]. Nevertheless, it creates false positive and false negative rates if the query server results are incorrect, which fails in preserving the privacy of SUs information.

2.2 Location-Based Verification Protocols

The problem of location verification of SUs in data-driven CRN is that SUs must provide proof about their geolocation to obtain channel information for secure communication. Access points verify the query SU's location using PIR based protocol. If the access points communicate directly to the SUs, it generates a signature as location proof. Topology-aware techniques, Delay-based Location Verification, Delay-based Internet Protocol geolocation, Client Self-Geolocation, Inference-based Approaches are examples of location-based verification protocols [14].

In public key cryptography-based algorithms, the access points must provide location proofs. Without access point proofs, the cryptography algorithms will not share information about the channel to the user. This method is also much expensive and unsuitable for all environments. Apart from preserving privacy, identifying the risk is also an essential issue in maintaining secure communication and privacy preserved CRN [15].

3 Proposed Work

The objective of the proposed work is to preserve the location of the SU from attackers and attain the clustering of SUs to utilize the resource.

3.1 Risk in Privacy-Preserving of Cognitive Radio Networks

The vital responsibility in identifying the risk is to protect the information from inference attacks. The following management process for identifying the risk involves five unique models to detect threats and to provide safe spectrum sharing with guaranteed access to SU:

Step 1. Risk monitoring
Step 2. Risk identification
Step 3. Risk analysis
Step 4. Risk assessment
Step 5. Risk management

It provides better trade-off and protection against spectrum sharing and utilization of CRN. Few actions considered as a threat in the risk monitoring process are as follows:

- Accessing the operational channel of requisite
- Accessing multiple channels
- Accessing more resources
- Freezing the allocated spectrum resources
- Increasing query rate for spectrum access
- Accessing resources with high transmit power.

3.2 Proposed Privacy-Preserving Architecture

The risk in the received signal is determined by analyzing the SNR (Signal to Noise ratio) [16,17], which is derived from the transmitted power of the received signal and the interference power of the received signal. The interference power and transmitted power are evaluated from the path loss and shadowing effect of the movement. When the received signal, SNR, goes below 0 dB, the risk is high.

a. Generally, the spectrum manager involves risk monitoring by observing the anomalous patterns of SUs spectrum requests. At a specific routine time, the spectrum manager monitors the level of risk by queries, moves of SU for identifying the risk. Considering secondary query identification as suspicious activity, the spectrum manager makes it a threat. Once any privacy threat is detected, the system manager gets alert, triggering the next step. Based on the threshold level, the spectrum manager identifies the risk. The system reacts and triggers the risk identification process if a single SU or many MU crosses the threshold.

b. If the spectrum manager observes any suspicious activities, it triggers the next step as risk identification. Once the risk is acknowledged, it is essential to obtain the attack occurrence and its impact. The probability of inference occurrence is defined using Bayes probability. Initially, it computes the probability of inference, and then it analyses the attack history for query rates, spectrum load, and other events.

c. These impact values are analyzed further with suitable privacy measures for the next observation level in risk analysis. The system loaded with geographic location is calculated during the identification process based on the inference attacks, and their impacts on the system are shown in Eq. (1).

$$P(H|E) = \frac{P(E|H)}{P(E)}P(H) \tag{1}$$

For privacy protection, an impact function is derived based on the parameters such as distance, time, and frequency to correlate these parameters. Finally, it updates the probability of inference as a hypothesis function, where H is the hypothesis for inference attack, and E is the observed error event. This error event is considered an indicator of an inference attack. While implementing the updated probability, it gives P(H|E) as posterior probability, P(H) as prior probability, and P(E) as the probability of an observed event. Based on Bayesian analysis, the posterior and prior probability are considered shreds of evidence of the attack. It triggers the re-evaluation of risk identification for updating the possibility.

d. The risk assessment determines the risk level of the system, thereby calculating the impact of risk.

The impact factor, i(E), is calculated as follows, Eq. (2)

$$\mathrm{i(E) = (iD(E)iT(E)iF(E))t} \tag{2}$$

The above impact factor is a vector function, and to simplify the vector, binary values are considered, such as 1 for impact and 0 for other cases. If the event occurs and has only time and location, it becomes (0 1 1)t. On obtaining the likelihood and impact values, the system starts the risk assessment process for quantifying the level of risk. This quantification process helps to determine the risk consequences and privacy factors. For risk assessment, the interference risk is a parameter, and its calculation is given in Eq. (3):

$$\mathrm{ir(E) = l(E)(E)} \tag{3}$$

where *ir* (E) is the risk inference after observing the event and $l(E)$ is the likelihood ratio of the event. The spectrum manager uses various levels of risk values for each sensitive change.

The assessment of the risk factors based on Tab. 1 triggers the risk analysis process for the next step, quantifying the process. Based on the levels of privacy, inference changes are marked complications. Considering the status and policies for SU preference, the system decides the threshold value in the privacy-preserving process. The threshold management process uses data mining techniques for preserving the data from attacks.

f. Finally, risk management uses analyzed parameters and summarizes the overall risk impact. The Uncertainties like the number of SU, distance, and power are considered for prior probabilities and are used to analyse posterior probabilities in finding the SNR.

Table 1: Risk inference values used in assessment process

Range (%)	State
0–25	Low
25–50	Medium
50–75	High
75–100	Critical

3.3 Ant Colony Optimization

All the ant aims to move towards the food in the correct path. The pheromone determines the proper path. Optimized ant colony optimization is used to form clusters of SUs in the co-operative spectrum sensing technique. Cluster formation is done based on the distance with a radius of 0.5 for each cluster. Similarly, all the SU aims to move towards the same network/spectrum in the correct path. The proper path is determined by the present position and the following position expressions; if the next position is better, it is updated to the SU to move in the same direction so that the ants will move randomly to increase their convergence rate; this interaction behaviour of ants makes them identify the distance between the neighbours based on the Euclidian distance. The probability of assigning values to the transition represents the feasible and non-feasible vertex in the processing module. The pheromone trace set used in the proposed model details the pheromone level for possible transition (*i*) from the present position to the next position. This update on every change helps to make the correct decision in the future. These characteristics are related to optimize the risk in PPA. Once the risk management process finalized the data with risk and its impact values, the optimization process again improves the impact values through its parameters—the cluster formation in optimized ant colony optimization secured by *k*-anonymity, which considers the distance range parameter. The distance ranges are classified as State 1 as least distance, State 2 as a minimum, State 3 as a medium, State 4 as high, to State 5 as very high. It is generally related to the data and convergence along with coefficient parameters in observing the ant behaviour. The location updating process is calculated from the random distribution factor as in the following, Eq. (4)

$$\overrightarrow{l_{j,t}} = \vec{l}_{i,t} + \mathrm{Re}al * Rand\ \mathrm{int}[-1,\ 1] \tag{4}$$

Updating the new position is done by analyzing the stability of the present position and unique position. If the strength of position $\overrightarrow{\mathrm{l_j}}$ is better than the present position $\overrightarrow{\mathrm{l_i}}$ the new position is updated.

$$\overrightarrow{l_{j,t}}(n+1) = \vec{l}_{i,t}(n) + (\overrightarrow{l_{j,t}}(n) - \vec{l}_{i,t}(n)) * Rand\ int[0,\ 1] \tag{5}$$

This step is frequently repeated to update the position over every displacement, as Eq. (5). If the position $\overrightarrow{\mathrm{l_j}}$ is not identified even after performing the above steps, then all possible iterations are done to attain the best position from the present position. This behaviour given as ANT forward movement of one step is represented in Eq. (6).

$$\overrightarrow{\mathrm{l_{j,t}}}(\mathrm{n}+1) = \vec{\mathrm{l}}_{\mathrm{i,t}}(\mathrm{n}) + \left(\frac{\overrightarrow{\mathrm{l_{j,t}}}(\mathrm{n}) - \vec{\mathrm{l}}_{\mathrm{i,t}}(\mathrm{n})}{\varphi_{\mathrm{i,t}}}\right) *\mathrm{Rand}\ \ \mathrm{int}[0,\ 1] \tag{6}$$

If the $\overrightarrow{\mathrm{l_i}}$ Position of AF '*i'* follows the best $\overrightarrow{\mathrm{l_b}}$, then the ants will move randomly to increase their convergence rate. This interaction behaviour of ants makes them identify the distance between the neighbours based on the Euclidian distance. The center obtained previously is calculated based on the intra-cluster. The function minimum is given in Eq. (7).

$$\varnothing(\mathrm{z_1, z_2,\ z_{3,}} \ldots \mathrm{z_n}) = \sum_{\mathrm{i}=1}^{\mathrm{n}} \left(\iint_{\mathrm{x^3}}^{\alpha} \parallel \mathrm{Z_i} - 1 \parallel *\varphi(\mathrm{i})/2 \right) \tag{7}$$

The probability of assigning values to the transition represents the feasible and non-feasible vertex in the processing module. The pheromone trace set used in the proposed model gives the details about the pheromone level for possible transition *(i, j)* from the present position to the next position. This update on every change helps to make the correct decision in the future. These characteristics are related to the optimization of risk in PPA. Once the risk management process finalizes the data with risk and its impact values, the optimization process improves the impact values through its parameters. The presence of inference and its impacts affecting the system performance is evaluated. The entire system eliminates such assumptions using necessary actions and preserves the spectrum and user information from the MU based on the above evaluation. The algorithm is for ACO for optimization. It initializes a set of PU and SU and computation of threshold corresponding to the pheromone trail left by the ants. Whenever the input received signal (PU/SU) has a strength less than or greater than the given threshold, the direction of the search process is changed. The search is for the optimal spectrum. The pseudo-code for the proposed model is summarized below.

```
Step 1. Input
        Unavoidable channel ($ch_u$)
        Predefined thresholds for distance $thr_{dis}$
        Location of the SU $loc_{sec}$
        The initial level of the SU $T_{sec}$
Step 2. Output:
        Updated level of the $SU = T_{sec}$
        Termination of the connection Term
Step 3. Initialization:
        Term = False, $T_{sec} = T_0$
        Initialize population size,
Step 4. Generate random variables on a continuous trail
Step 5. Compare stability factor and strength
Step 6. Select better strategy policy
Step 7. While S→REQ access to $CH_u$ and $T_{sec} > Thr_{dis}$
Step 8. If Dist ($loc_{sec}$) $< thr_{dis}$
Step 9. Then $T_{sec} = T_{sec} - t$
Step 10. End
Step 11. Else If Dist ($loc_{sec} > thr_{dis}$ Then $T_{sec} = T_{sec} - 2t$
Step 12. End
Step 13. End
Step 14. Change next location
Step 15. The parameters are $\rho_{2,}\ \rho_{3,\ldots}\rho_n$
Step 16. For random points $u^t$,   $t = 1,\ 2,\ \ldots.L_l$  $t = 1$ to $L_l$
Step 17. Compute integer values $L_{swarm} = int(\rho_4 L)$
Step 18. If $L_{swarm} > 0$ then
Step 19. For $i = 1$ to $L_{swarm}$
Step 20. Move and create a suitable connection to the set
Step 21. $Z_\alpha = z(p^i_\alpha,\ q^j_\alpha)$
Step 22. If $Z_\alpha < Z_m$ Then replace the corresponding position into a new one from the function value
```

4 Results and Discussions

The experimental model is a one attack system in collaboration with two attackers. The proposed PPA permits access to resources based on SU positions. It is assumed that the attackers are in an operational zone and are known to channel information. Experimentations are done for the same attacks for the proposed privacy-preserving and non-privacy-preserving models. The system performance obtained using step values is evaluated through the interference attacks. The plot on the impact of privacy uncertainty over queries for both algorithms is in Fig. 1.

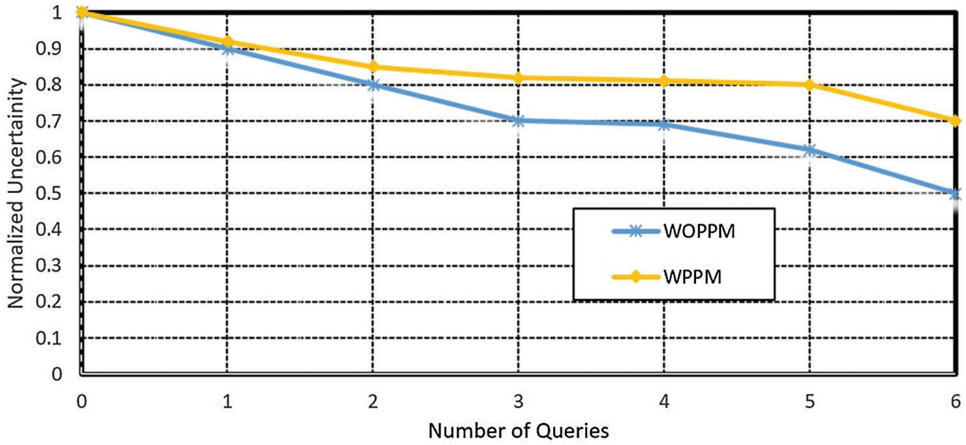

Figure 1: Impact of the uncertainty on privacy for an attack

From Figs. 2 and 3, the algorithm without PPA is in blue, and it decreases drastically over the REQ, while the proposed PPA in orange provides stable results for all the queries. Initially, it decreases due to the attack and improves the privacy factors with more significant perturbation in the last. The threshold defines the uncertainty in the experimentation model. These threshold values are utilized up to 100%, and the suitable uncertainty is plotted in Fig. 2 for fixed steps. The proposed model provides better results since the attacker depends on this threshold value. The model without having PPA fails as it does not maintain the threshold values for the queries. If the threshold value is high, then the Request (REQ) needed to infer is also high, which may provide a possible route to the attacker to interfere with the network. Fig. 3 is plotted for threshold values, and it is uncertain for adaptive steps. The proposed model uses a maximum threshold for each step in the process. The adaptive action changes frequently based on SU, and the attacker changes the user values and attacks the network.

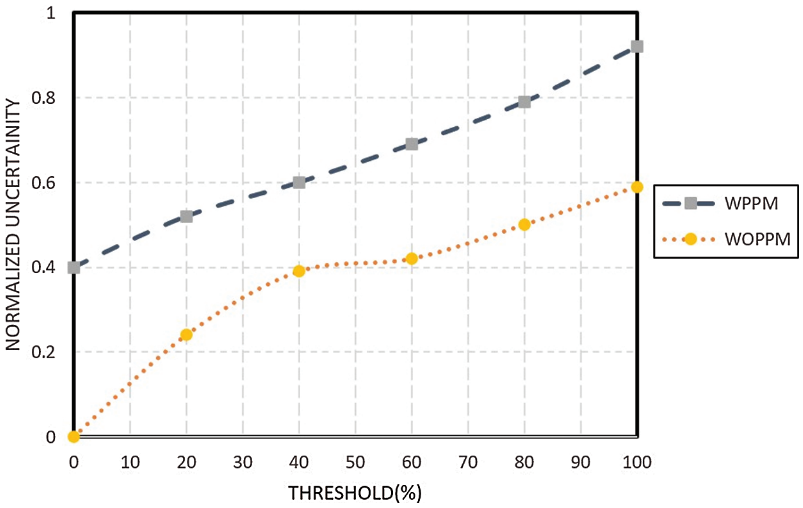

Figure 2: Comparison of the impact on privacy for attack (fixed step)

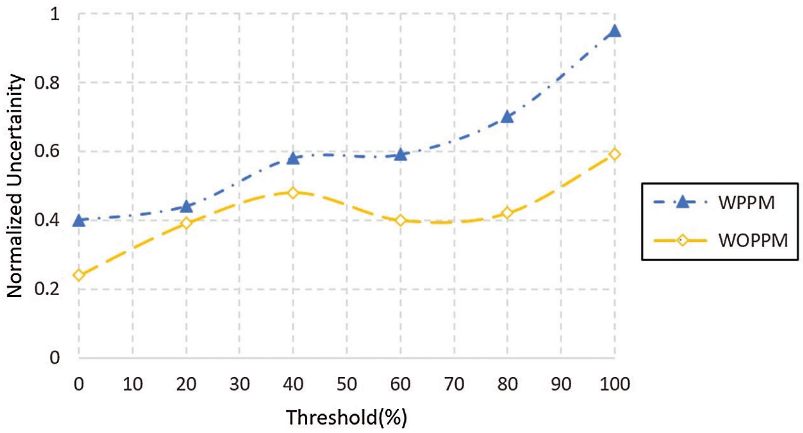

Figure 3: Comparison of the impact on privacy for attack (adaptive step)

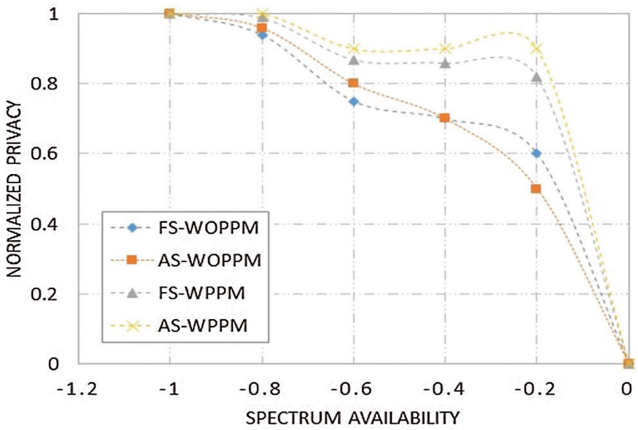

Figure 4: Spectrum availability *vs.* normalized privacy

The proposed model has better results for the dynamic environment than the model without PPA. The plot on normalized privacy and spectrum availability for both the models using fixed and adaptive step is in Fig. 4. From the figure, the model without having privacy-preserving delays in privacy issues is compared to the proposed PPA. Fig. 5 represents the ACO cloak area occupied by users, and Fig. 6 describes the ACO clustering based on the distance. Same-coloured users in it represent each cluster.

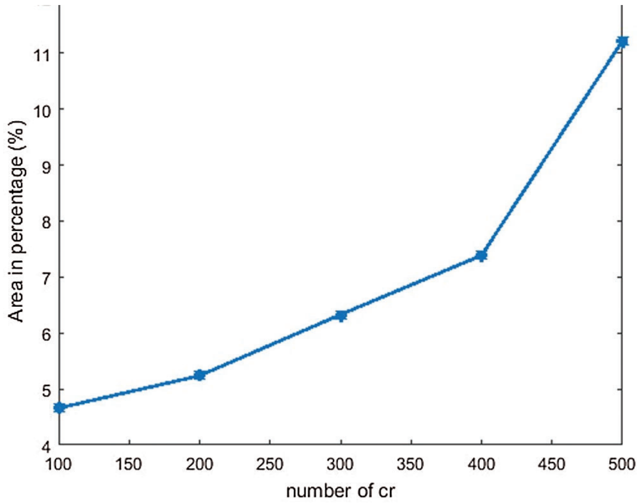

Figure 5: ACO cloak area occupied by users

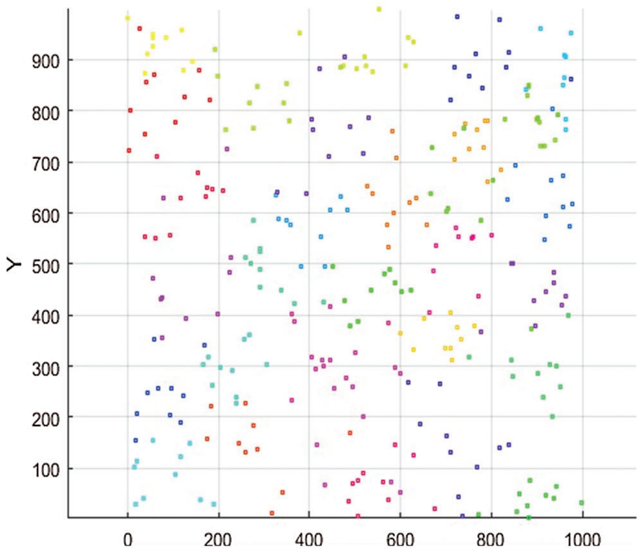

Figure 6: CRN users grouping

5 Conclusion

This chapter deals with the issues in privacy-preserving in CRN. The impact on user information privacy is defined based on the risk factors. A Privacy-Preserving Architecture designed with ACO increases the efficiency of the privacy model and is suitable for all environments. By applying this in spectrum resources, the trade-off between spectrum availability and privacy protection increases. Optimization helps to improve privacy as an objective function with a minimized set of constraining variables. Higher constraints are satisfied before the lower limitations through this improved ACO. Overall accuracy in preserving the privacy of the proposed model is 97.4%, which is 9% higher than the conventional model without having PPA.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. K. Sharma and D. B. Rawat, “Advances on security threats and countermeasures for cognitive radio networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[2] S. Ganeriwal and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” in *2nd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN ‘04)*, Washington DC, USA, pp. 66–77, 2004.

[3] H. Li and Z. Han, “Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems-part II: Unknown channel statistics,” *IEEE Transaction Wireless Communications*, vol. 10, no. 1, pp. 274–283, 2015.

[4] G. Yang, G. S. Yin, W. Yang and D. M. Zuo, “A reputation-based model for malicious node detection in WSN,” *Journal of Harbin Institute of Technology*, vol. 10, pp. 158–162, 2009.

[5] J. Jiang, G. Han, F. Wang, L. Shu and M. Guizani, “An efficient distributed trust model for wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.

[6] R. Chen, J. M. Park and J. H. Reed, “Towards secure distributed spectrum sensing in cognitive radio networks,” *IEEE Communication Magazine*, vol. 46, no. 4, pp. 50–55, 2008.

[7] Y. Wu and K. J. R. Liu, “An information secrecy game in cognitive radio networks,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 831–842, 2011.

[8] M. Dorigo, V. Maniezzo and A. Colorni, “Ant system: Optimization by a colony of cooperating agents,” *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 26, no. 1, pp. 29–41, 1996.

[9] B. Wang, Y. Wu and K. J. Liu, “Game theory for cognitive radio networks: An overview,” *Computer Networks*, vol. 54, pp. 2537–2561, 2010.

[10] J. Y. Zhang, A. Lei, J. T. Jia and L. Gao, “Improvement of the ant colony algorithm for solving TSP problems,” *Journal of Xidian University*, vol. 32, no. 5, pp. 681–685, 2005.

[11] P. Zhou, X. P. Li and H. F. Zhang, “An ant colony algorithm for job shop scheduling problem,” in *Proc. of the World Congress on Intelligent Control and Automation*, Hangzhou, P. R. China, pp. 2899–2903, 2004.

[12] M. Poturalski, P. Papadimitratos and J. P. Hubaux, “Formal analysis of secure neighbor discovery in wireless networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 6, pp. 355–367, 2013.

[13] A. Abdou, A. Matrawy and P. C. Oorschot, “CPV:Delay-based location verification for the internet,” *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 130–144, 2013.

[14] M. Trimble, “The future of cybertravel: Legal implications of the evasion of geolocation,” *Fordham Intellectual Property Media Entertainment Law Journal*, vol. 22, pp. 567–657, 2011.

[15] B. Sadkhan and D. M. Reda, “Security issues of cognitive radio network,” in *2nd Int. Conf. on Engineering Technology and its Applications (IICETA)*, *27-28 Aug. 2019*, Al-Najef, Iraq, pp. 117–122, 2019.

[16] R. Zhang, N. Wang, N. Zhang, Z. Yan, W. Lou *et al.*, “Priroster: Privacy-preserving radio context attestation in cognitive radio networks,” in *IEEE Int. Symp. on Dynamic Spectrum Access Networks (DySPAN)*, *11–14 Nov.*, Newark, NJ, USA, pp. 1–10, 2019.

[17] D. H. Tashman and W. Hamouda, “An overview and future directions on physical-layer security for cognitive radio networks,” in *IEEE Network*, vol. 35, no. 3, pp. 205–211, 2021.