Received: October 13, 2020. Revised: November 24, 2020.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Detection and Prevention of Primary User Emulation Attack in Cognitive Radio Networks Using Secure Hash Algorithm

Rajagopala Medpur VasanthaReddy[1]* **Sanjeev Channabasappa Lingareddy[2]**

[1]*Department of Computer Science, Alpha College of Engineering, Bengaluru,*
Affiliated to Visvesvaraya Technological University, Belagavi, India
[2]*Department of Computer Science, Sri Venkateshwara College of Engineering, Bengaluru,*
Affiliated to Visvesvaraya Technological University, Belagavi, India
* Corresponding author's Email: raju.medpur@gmail.com

Abstract: Cognitive radio network is enormously used to improve the spectrum utilization by enabling the dynamic spectrum access. The performance of the cognitive radio network is affected due to the denial of service caused by the primary user emulation attack. This primary user emulation attack restricts the spectrum access opportunity of secondary users. In this research, the integration of Secure Hash Algorithm -1 (SHA-1) and neural network (i.e., soft computing method) is proposed to avoid the primary user emulation attack. The Received Signal Strength (RSS) and Direction of Arrival (DoA) are used to achieve the localization between the primary and secondary users. The main objective of the proposed method is to minimize the loss ratio during the communication process. The performance of the RSS-DoA-SHA method is analyzed in terms of routing overhead, End-to-End Delay (EED) and loss ratio. The proposed RSS-DoA-SHA method is compared with two existing methods such as RSS-Angle of Arrival (AOA) method and Hybrid Routing Algorithm - Symmetric Key Cryptography (HRA-SKC) method to evaluate the performance measures. The end to end delay of the proposed method for 500 PU is 1ms, it is less when compared to the RSS-AOA method.

Keywords: Cognitive radio network, Direction of arrival, Primary user emulation attack, Received signal strength, Secondary user, Secure hash algorithm.

1. Introduction

Cognitive Radio Network (CRN) is used throughout the world due to its capacity of solving the issue between the restricted spectrum supply and spectrum demand from the growing wireless applications and services [1]. The two classes of the CRN are the Primary User (PU) and cognitive or Secondary Users (SU), in which the PU has the license to use the certain frequency of the radio spectrum. The SU exist on the cognitive radio doesn't have any license, but it uses the PU's frequency without creating any disturbance to the transmission of PU [2-4]. Generally, the Cognitive Radio (CR) used in different applications such as smart grid communications, dynamic spectrum admittance, intellectual convey systems, civic safety systems and cooperative networks [5]. The spectrum sensing is used in the Cognitive Radio (CR) to identify the unused bands (i.e., white spaces) and these unused bands are used to accomplish the data transmission. The CR eliminates the band and this CR is operated in another white space, when the primary signal is discovered in the CR's operating range [6,7].

This spectrum sensing provides less accurate solution in identification of the spectrum holes, but this spectrum sensing based identification is inexpensive and highly flexible method in wide network range [8]. In the development and distribution of CR, the security is considered as a challenging constraint due to the coexistence of the cognitive radio users with different licensed users [9] [10]. The spectrum sensing also considered as a challenging task due to the usage of different

DOI: 10.22266/ijies2021.0430.12

modulation, data rates and transmission power by the PU [11]. One of the major security threat in the CRN is Primary User Emulation (PUE) attack [12]. In PUE attacks, the attacker copies the PU signals which results in false alarms at spectrum sensing phase as well as the SUs are restricted from using the available channel. Therefore, the malicious attackers are significantly minimized the performances of the SUs [13, 14]. Moreover, the malicious attacker occupies an entire licensed spectrum or it misuses valuable licensed channels [15]. The major contributions of this paper are given as follows:

- The localization among the PU and SU are obtained using the RSS and DoA. The RSS and DoA calculations are used to identify the SUs entered in the range of PU.
- The secure hash algorithm-1 and neural network are used to generate the hash code to validate the SU from the PUE attackers.
- The performance of the proposed RSS-DoA-SHA method in CRN is analyzed by varying the number of primary and secondary users.

The overall organization of the paper is given as follows: The literature survey related to the analysis of CRN under PUE attacks is given in Section 2. The problem statement found from the literature along with the solution is given in Section 3. The proposed RSS-DoA-SHA method based secured CRN is clearly described in Section 4. Section 5 describes the results and discussion of the RSS-DoA-SHA method. Finally, the conclusion is made in Section 6.

2. Literature survey

Elghamrawy and Hassanien [16] presented the hybrid Genetic Whale Optimization Algorithm (GWOA) to improve the spectrum utilization and detect the PUE attacks. The PU and PUE were detected by comparing the two predefined thresholds with the SU's received signal energy. The balance among the exploitation and exploration phases was obtained by integrating the mutation and crossover of GWOA with whale optimization algorithm which was used to detect the optimal solution. This GWOA was obtained better detection probability against PUE attacks. The number of generations considered in the GWOA was high, which increased the delay during the PUE identification.

Madbushi [17] developed the chaotic tag-based sequencing to detect the PUE attack in the CRN. The cognitive base station was used to monitor a look-up table-based challenge sequence which was used as a defense against the PUE attack. Moreover, the tag-based chaotic communication system was used for the remaining attackers of the CRN. The node was referred as safe node, when the signal received by the receiver was in the suitable BER range. If the attacks were identified by the trust based mechanism, then the attacks were blocked and removed from the CRN. However, the delay was increased while increasing the number of nodes in the CRN.

Elghamrawy [18] presented the hybrid Genetic Artificial Bee Colony (GABC) algorithm to optimize the spectrum usage based on the PUE attack detection and improvement in the detection probability. The optimal solution was obtained based on the exploitation and exploration characteristics of the GABC algorithm. The existence of the PU and PUE were identified using the two predefined thresholds in the GABC. The effect of false spectrum sensing alarm created by the malicious users was minimized using the GABC. The detection probability was increased, only when the GABC has higher amount of generations.

Arun and Umamaheswari [19] developed the adaptive learning-based attack detection to detect and avoid the PUE attack using the transmitter's received power. The low power PU and different adversaries were detected by adopting the cyclo stationary feature in the learning process. Additionally, the transmission time and distance variance were estimated to improve the learning process which enhances the communication rate of SU and signal classification rate. The throughput of the SU and high detection were obtained by distinguishing the malicious PU and low spectrum using the learning case. However, the computational complexity was high due the use of cyclo stationary feature detection in CRN.

Sharifi [20] presented the Cooperative Sensing Scheme (CSS) with Attack-Aware Threshold Selection (AATS) to detect the malicious PUE attack. The probabilities of the PUE attack fake signal in both the existence and nonexistence of the licensed PU signal were evaluated to determine the optimal threshold. This optimal threshold was used to minimize the total error probability and enhance cooperative sensing performance. Moreover, this AATS doesn't require any specific feature or physical position of the PU signal. This AATS was required high amount of sensing intervals to identify the optimal threshold to improve the CSS performance.

Li and Wang [21] developed the queueing-game-theory for analyzing the behavior of the SU. Here, the CRN was analyzed under two types of misbehavior users such as Malicious Misbehavior Users (MMUs)

Received: October 13, 2020. Revised: November 24, 2020.

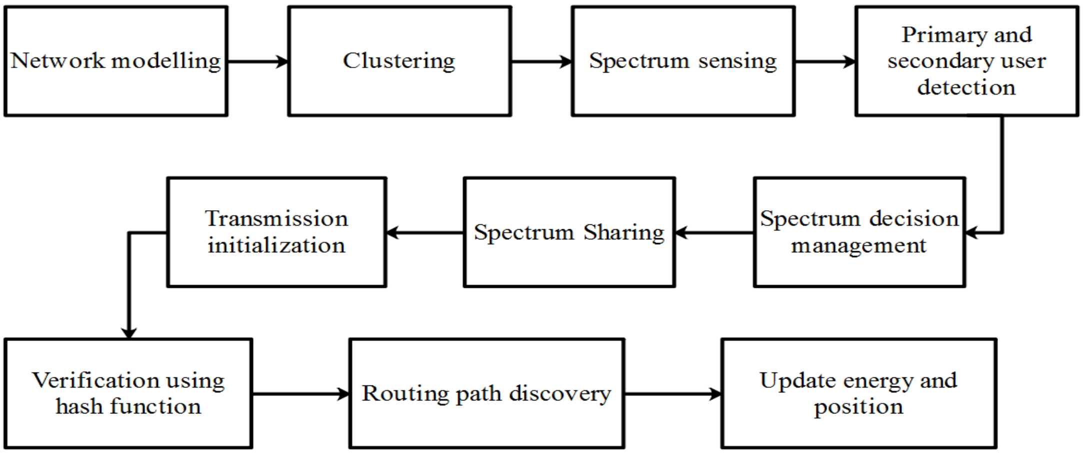
Network modelling
Clustering
Spectrum sensing
Primary and secondary user detection
Spectrum decision management
Spectrum Sharing
Transmission initialization
Verification using hash function
Routing path discovery
Update energy and position

Figure. 1 Block diagram of RSS-DoA-SHA method

and Selfish Misbehavior Users (SMUs). The Nash equilibrium joining strategy was obtained and SU's efficiency was enhanced using the noncooperative behavior. Next, the fee was imposed on the SU to avoid the gap among the socially optimal strategies and individual equilibrium. The SU was forced to leave the system, when the PUE attack was generated by the MMU.

Yadav [22] presented the analysis of throughput for CRN under PUE attack. The hybrid spectrum access scheme and joint impact of the PUEA were considered to develop the analytical expression for analyzing the throughput. The increment in PU's tolerable peak interference and higher transmit power were enhanced the SU's throughput. But, the higher attacker strength and probability of presence attacker reduces the throughput performances of SU.

Singh and Singh [23] developed the Range based primary user localization technique for detecting the PU's position along with the transmit power. The PU localization was accomplished using the RSS and Angle of Arrival (AOA). The Range based PU localization was mainly depending on the information received from only 2 SUs which used for accomplishing the process of localization. Here, RSS was utilized to determine the distance between the PU and SU. After applying the Trilateration method based distance calculation, the AOA was utilized for selecting the possible locations of the PU. This RSS-AOA method doesn't consider any security mechanism to avoid the malicious attackers in the CRN.

Khasawneh, M., Azab, A. and Agarwal, A. [24] presented the Hybrid Routing Algorithm (HRA) to identify the optimal path based on the Belief Level (BL), the probability of PU presence, and the channel cost. The Cluster Head (CH) was selected based on the higher BL using the fusion center of the CRN. Next, the HRA routing combined spectrum sensing and spectrum management phases. The Symmetric-Key Cryptography (SKC) was used to encrypt the message transferred among different network nodes in spectrum sensing and spectrum management phase. Hence, the HRA decreased the time required during the route establishment and minimized the maintenance cost. However, the processing time of the CH was increased due to the increment in the amount of SUs in the CRN.

3. Problem statement

Current issues related to the CRN are stated in this section and it also explains how the RSS-DoA-SHA method overcomes the problems faced in the CRN. The issues faced by the CRN are mentioned as follows:

The high amount of generations required by the GWOA [16] increases the delay while differentiating the PU from PUE attack. Next, the delay in the CRN is increased along with an increment in the number of nodes [17]. The CRN with higher delay shows that the data transmission time between the users of the CRN is high during the PUE attack detection. The number of generations in the GABC [18] is required to be higher to achieve the higher PUE detection probability. Moreover, the RSS-AOA [23] doesn't use any security mechanism to prevent the CRN from the PUE attack. The CRN without any security mechanism causes the packet drop through the CRN.

Solution:

In this RSS-DoA-SHA method, RSS and DOA are used for the precise estimation of the SU which are entered in the PU's range. The combination of SHA-1 algorithm and neural network is used to generate the hash function and the generated hash function is attached to the users of the CRN. The SUs are considered as valid user only when the hash function between the users are matched together which minimizes the packet drop in the CRN. Therefore, this hash function minimizes the complexity in the PUE attack identification. Moreover, the lesser computations of the localization of SU and SHA-1 help to minimize the delay during communication.

4. RSS-DoA-SHA method)

In this RSS-DoA-SHA method, the combination of SHA-1 algorithm and neural network is used to accomplish the security between the users of the CRN. Here, the localization of users is achieved by using the RSS and DOA. The main phases accomplished in the CR technology are spectrum sensing, decision, sharing and handoff/ mobility. Since, the CR technology uses the cognitive engines for occupying the idle spectrum band released by the PU. The block diagram of the RSS-DoA-SHA method is presented in Fig. 1.

4.1 System model of cognitive radio network

In this RSS-DoA-SHA method, the RSS and DoA are estimated by the CR device to detect the signal of the SU without using any information about the data communication. Each CR is installed with an antenna and the features of the antenna is modified into the measurements in N possible different sectors. The system model of CRN is presented in Fig. 2.

In this CRN, the radiation pattern is used to describe the sector of the CRN and PU signal's attenuation is described as DoA function using the radiation pattern. The radiation pattern ($p(\varphi - \upsilon_n)$) is only based on the DoA of the PU signal (φ) and n^{th} sector's orientation (υ_n). The main beam of the antenna is approximated for simplifying the radiation pattern model by Gaussian like shape. Eq. (1) shows the radiation pattern of the CRN model.

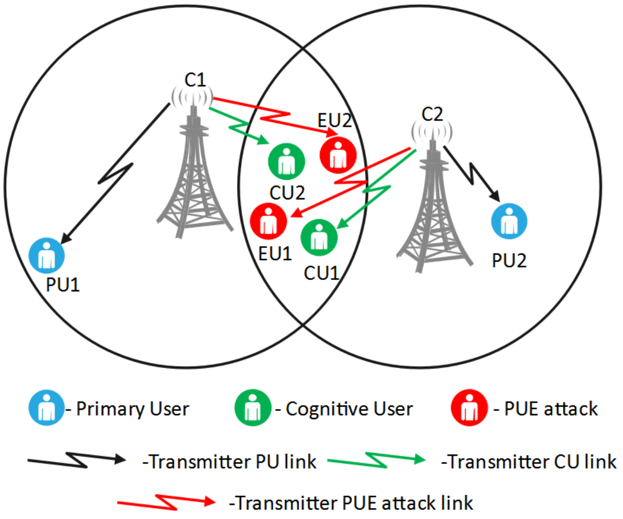

Figure. 2 System model of CRN

$$p(\varphi) = \exp\left(-[M(\varphi)]^2/\beta\right) \quad (1)$$

Where, $M(\varphi)$ is utilized to limit the input angle in the range of $[-\pi, \pi]$ and it is expressed as $M(\varphi) = mod_{2\pi}(\varphi + \pi) - \pi$ as well as β represents the beam width. In this CRN, the spacing among the sectors i.e., $\Delta\upsilon = {}^{2\pi}/_{N}$ is considered as constant which shows that the n^{th} sector orientation is $\upsilon_n = n\Delta\upsilon$. The side sector suppression (b_s) is used instead of characterizing the radiation pattern through the beam width. The b_s is defined as attenuation and this attenuation arrived in the n^{th} sector's orientation (υ_n). Moreover, the attenuation is recognized in the adjacent sectors $n-1$ and $n+1$, i.e., $b_s = p(\Delta\upsilon)$. The number of overlap among the neighboring sectors and independent sectors are identified using the side sector suppression. Next, the output beamwidth is detected using the Eq. (2).

$$\beta = -(2\pi)^2[N^2 \ln(b_s)]^{-1} \quad (2)$$

The A amount of complex samples are successively switched and received by each sector in the measurement period that totally generates $N \times A$ complex samples. Next, the baseband complex received signal caused from the sector n with $a = (n-1)A + 1 \dots nA$ of sample index range is expressed in the following Eq. (3).

$$x(a) = p(\varphi - \upsilon_n)s(a) + \omega(a) \quad (3)$$

Where, additive noise considered as circular symmetric complex Gaussian is represented as $\omega(a)$. Similarly, the noiseless portion of the received signal of the PU is referred as circular symmetric complex Gaussian ($s(a)$).

The aforementioned assumptions show that the differentiation among the signal of the PU and noise is difficult at the CR. Hence, the evaluations of the DoA (φ) and RSS (γ) are mainly depends on the received energies. Eq. (4) is used to calculate the n^{th} sector's power.

$$\epsilon_n = \frac{1}{A}\sum_{a=(n-1)A+1}^{nA} |x(a)|^2 \quad (4)$$

The Gaussian distribution is used for approximating the energies to moderate the higher values of A. The Gaussian distribution values of the energy (ϵ_n) are mean (μ_n) and variance (σ_n^2) which are shown in the Eqs. (5) and (6) respectively.

$$\mu_n = \sigma_w^2 + \rho_n \gamma \quad (5)$$

$$\sigma_n^2 = \frac{1}{A}(\sigma_w^2 + \rho_n \gamma)^2 \quad (6)$$

Where, $\rho_n = [p(\varphi - v_n)]^2$ and σ_w^2 is the variance of the noise $\omega(a)$.

4.1.1 Cramer-rao bounds

The CRB is generally a lower bound on the covariance matrix of the unbiased estimator. The CRB is achieved as Fisher Information Matrix (FIM)'s inverse for the calculation of $L \times 1$ parameter vector ($\boldsymbol{r}$) with the $M \times 1$ vector ($\boldsymbol{\epsilon}$). The FIM is calculated using the Eq. (7).

$$\boldsymbol{F}_{i,j} = -E\left(\frac{\partial^2}{\partial \boldsymbol{r}_j \partial \boldsymbol{r}_k} \ln[f(\boldsymbol{\epsilon}|\boldsymbol{r})]\right), j, k = 1, \dots, L \quad (7)$$

Where, the posterior probability distribution of $\boldsymbol{\epsilon}$ with $\boldsymbol{r}$ is represented as $f(\boldsymbol{\epsilon}|\boldsymbol{r})$.

The $M = N$ energies $\epsilon = [\epsilon_1, \epsilon_2, \dots, \epsilon_N]^T$ are used to calculate $\boldsymbol{r} = [\varphi, \gamma]^T$ at $L = 2$. The posterior probability distribution given in Eq. (8) is calculated using the Eqs. (5), (6) and Gaussian distribution of the energy distribution.

$$f(\boldsymbol{\epsilon}|\boldsymbol{r}) = \frac{1}{(2\pi)^{\frac{N}{2}} |\boldsymbol{Q}|^{\frac{1}{2}}} exp\left\{-\frac{1}{2}(\epsilon - g)^T Q^{-1}(\epsilon - g)\right\} \quad (8)$$

Where, $g = [\mu_1, \mu_2, \dots, \mu_N]^T$ and $Q = [\sigma_1^2, \sigma_2^2, \dots, \sigma_N^2]^T$.

4.1.2 Calculation of DoA and RSS using MaxE estimator

In this RSS-DoA-SHA method, the MaxE estimator is used to calculate the DoA and RSS. The maximum power calculated by the MaxE estimator and orientation of connected sector are used to calculate the DoA as shown in Eq. (9). Next, the RSS is calculated based on the difference between the noise variance and maximum energy which is shown in Eq. (10). This MaxE estimator has less computational complexity and it gives better performance than the other estimators.

$$\hat{\varphi}_n = \{v_j | j = \arg\max_j \epsilon_j\} \quad (9)$$

$$\hat{\gamma}_n = \max_j \epsilon_j - \sigma_w^2 \quad (10)$$

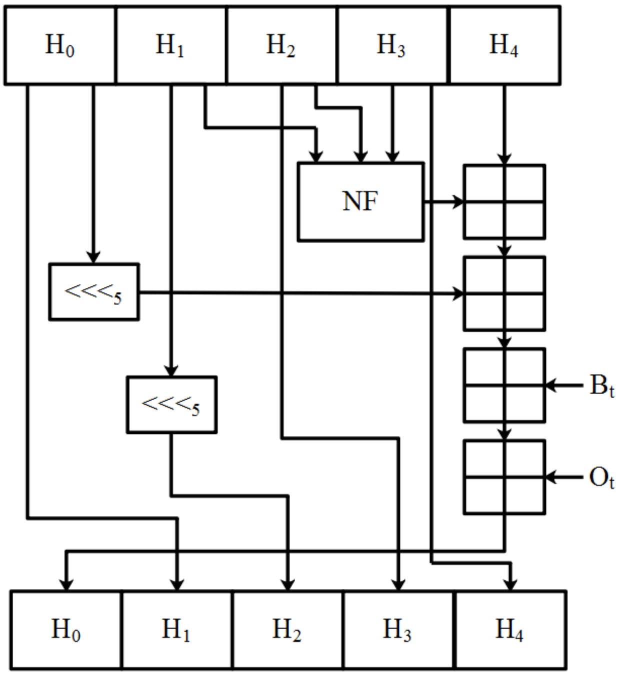

Figure. 3 Architecture of one way SHA-1

This RSS and DoA are used to identify the SU which is entered into the cluster of the PU. Then this SU is validated as normal user based on the hash function generated from the SHA 1.

4.2 Generation of hash function using SHA and neural network

The combination SHA 1 and neural network is used to generate the hash function to classify the normal users from the malicious attackers (i.e., PUE attacks). The SHA 1 is generally used in different applications and protocols to improve the security from the malicious attackers. In this RSS-DoA-SHA method, the generated hash function is stored in the users of the CRN for identifying the malicious attackers. The one way SHA-1 iteration is shown in the following Fig. 3.

Where, 32 bit words of state are H_0, H_1, H_2, H_3 and H_4; nonlinear function is NF; B_t and O_t are the derived from the message block and round constant respectively; step number is represented as t.

The SHA – 1 used to secure the CRN users by generating the 160-bit hash value as message digest. Next, this value is minimized as hexadecimal number with the length of 40 digits.

The steps processed in the SHA-1 are given as follows:

1. Bits padding: The padding is inserted at the end of the message length is 64bits and multiple of 512.

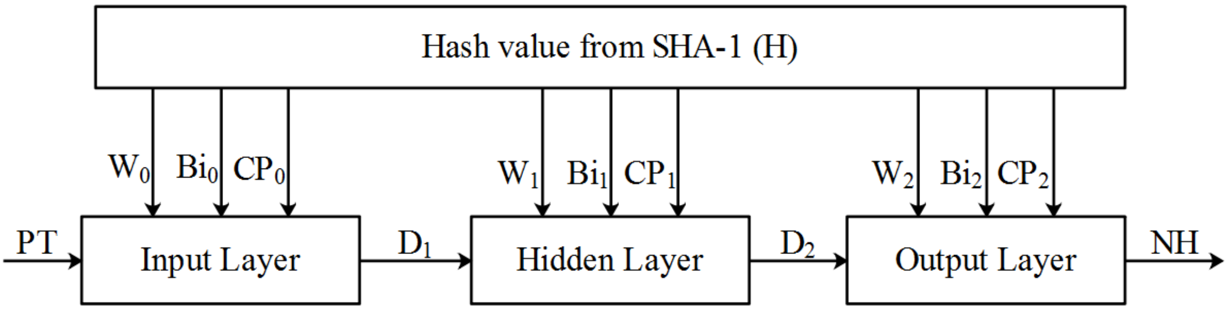

Figure. 4 Structure of neural network based hash function generation

2. Appending length: The excluding length is calculated.
3. The input is divided into 512 bit blocks.
4. Initialization of chaining variables: Five chaining variables of 32 bit are initialized.
5. Processing of blocks: 1. Copy the chaining variables, 2. Separate the 512 into 16 sub blocks and 3. Process 4 rounds of 20 steps.

The 160 bit hash value (H) generated from the SHA-1 is given as input to the neural network along with 128 bit plaintext data (PT). The hash key from the SHA-1 is separated into three different set of keys such as 1) W_0, Bi_0, CP_0 2) W_1, Bi_1, CP_1 and 3) W_2, Bi_2, CP_2, where W represents the weight value; Bi is the bias value and CP is the control parameter. At first, the XOR operation between the plain text and first key set W_0, Bi_0, CP_0 are carried out in the input layer. Next, the XORed value (D_1) is given as input to the hidden layer where the substitute operation is performed between the D_1 and 2nd key set W_1, Bi_1, CP_1 that produces output D_2. Finally, the concatenation operation is accomplished between the D_2 and 3rd key set W_2, Bi_2, CP_2 is performed in output layer to generate the new hash function (NH) with high randomness. The process of optimal hash function generation using neural network is presented in the Fig. 4.

The algorithm for the RSS-DoA-SHA method is given as follows

```
1. Initialize nodes.
2. Initialize PU & SU.
3. Allocate resources for PU & SU.
4. Neighbor node information collection.
5. Update energy, hash function and position.
6. Initialize source & destination node.
7. Generate hash function using SHA-1 and
   neural network.
8. Send route request (RREQ) to destination
   with hash function.
9. If (current node == destination node)
10. Send route reply (RREP) to source node.
11. If (DoA and Energy matched)
12. Check hash function.
13. If (Hash function of RREP == Hash function
    of RREQ)
14. Initialized packet forwarding (Go to step 17)
15. Else
Reject RREP (Go to step 6)
16. Else
Forward RREP to neighbour node (Go to step 9)
17. Update position and energy
```

In this RSS-DoA-SHA method, the RSS and DoA are used to achieve the localization of the users and the flowchart of the RSS-DoA-SHA method is shown in Fig. 5. Where, SHF and RHF are the source hash function and destination hash function respectively. Here, the DoA is computed using the maximum power and orientation of connected sector while the RSS is computed based on the difference between the noise variance and maximum energy. Next, the combination of SHA-1 and neural network is used to generate the hash function and the generated hash function is attached to the users of the CRN. This hash function is used to differentiate the normal user from the PUE attackers. This SHA-1 and neural network based PUE attack mitigation helps to minimize the loss through the CRN.

5. Results and discussion

The results and discussion of the cognitive radio network under PUE attack are described in this section. The RSS-DoA-SHA method is implemented and simulated in the MATLAB 2018a on the i5 desktop computing environment with 8 GB RAM. The RSS and DOA based localization of the SUs are used to determine the secondary users which are entered in the primary clusters. Additionally, the integration of SHA-1 algorithm and neural network

Received: October 13, 2020. Revised: November 24, 2020.

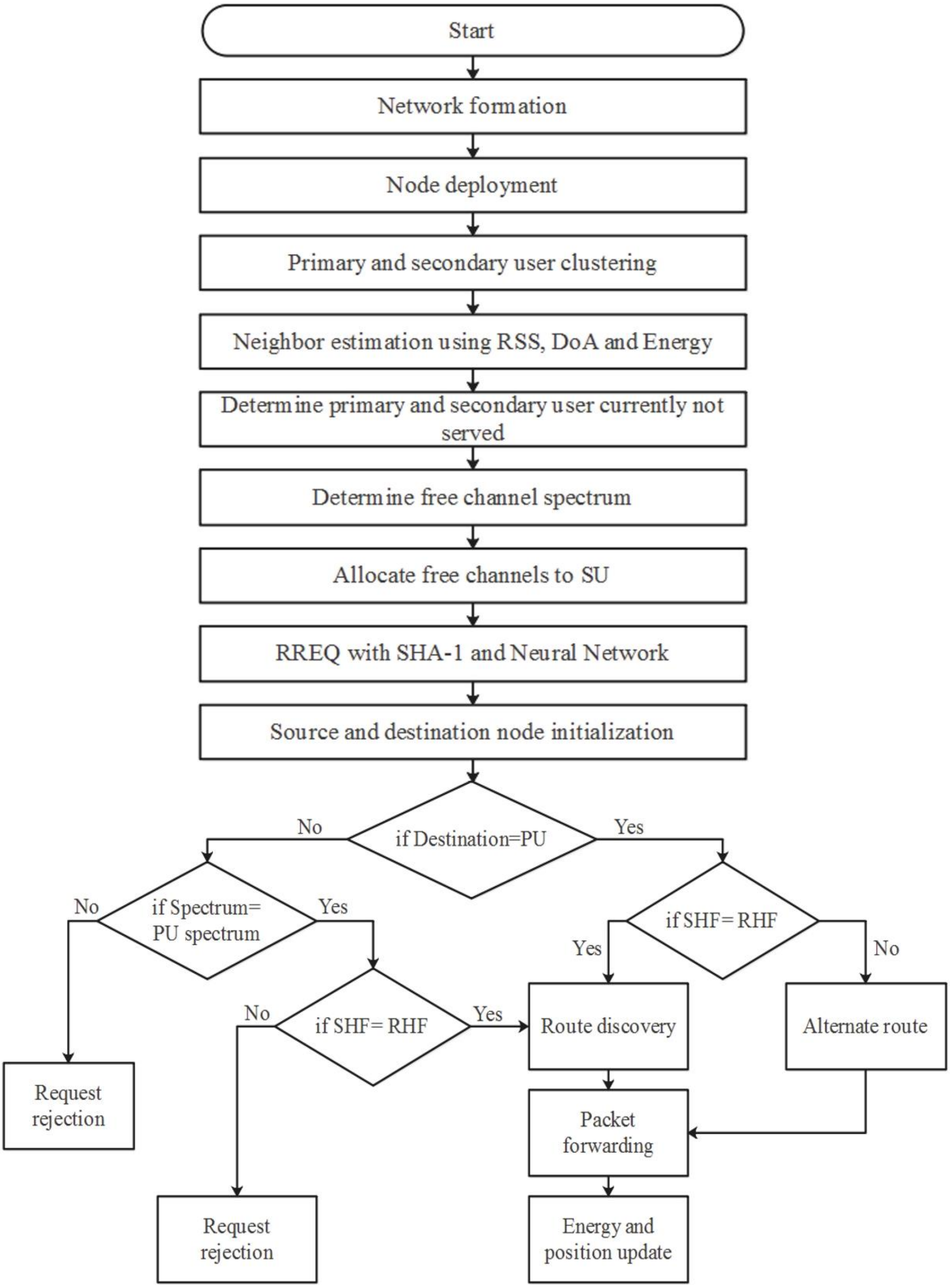
Start
Network formation
Node deployment
Primary and secondary user clustering
Neighbor estimation using RSS, DoA and Energy
Determine primary and secondary user currently not served
Determine free channel spectrum
Allocate free channels to SU
RREQ with SHA-1 and Neural Network
Source and destination node initialization
if Destination=PU
No
Yes
if Spectrum= PU spectrum
No
Yes
if SHF= RHF
Yes
No
if SHF= RHF
No
Yes
Request rejection
Route discovery
Alternate route
Packet forwarding
Request rejection
Energy and position update

Figure. 5 Flowchart of the RSS-DoA-SHA method

is used to validate the SUs as normal or malicious attackers. The performance of the RSS-DoA-SHA method is analyzed in terms of routing overhead, EED and loss ratio. The RSS-DoA-SHA method is evaluated by varying the number of primary users and secondary users. Here, the RSS-DoA-SHA method is compared with RSS-AOA [23] and HRA-SKC [24] to show the effectiveness of the RSS-DoA-SHA method under PUE attack.

The performances analyzed in this RSS-DoA-SHA method is described as follows:

a. Routing overhead

Routing overhead is defined as the total amount of control packets generated by the primary user which is expressed in the Eq. (11).

$$Routing\ overhead = \sum_{k=1}^{c} R_k \qquad (11)$$

Where, R defines the amount of control packets and c defines the amount of source nodes which transmits the data packets.

b. End to end delay

EED is defined as the average time to transmit the packet through the CRN and this EED is expressed in the Eq. (12).

$$EED = \frac{1}{h}\sum_{k=1}^{h}\frac{D_k}{PR_k} \qquad (12)$$

Where, the packet's total delay is represented as D_k, amount of received packets is represented as PR_k and h is the application traffic.

c. Loss ratio

Loss ratio is defined as the ratio between the amount of lost packets and amount of transmitted packets. The loss ratio is expressed in the following Eq. (13).

$$Loss\ ratio = \frac{\sum_{k=1}^{c} PS_k - \sum_{k=1}^{c} PR_k}{\sum_{k=1}^{c} PS_k} \qquad (13)$$

Where, the amount of packets sent and received are represented as PS and PR respectively.

5.1 Performance evaluation by varying the number of secondary users

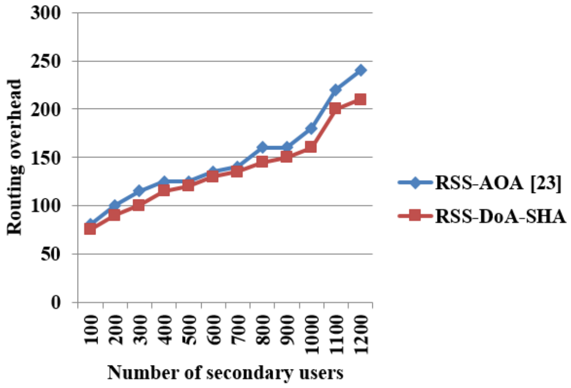

Figure. 6 Comparison of routing overhead for different SUs

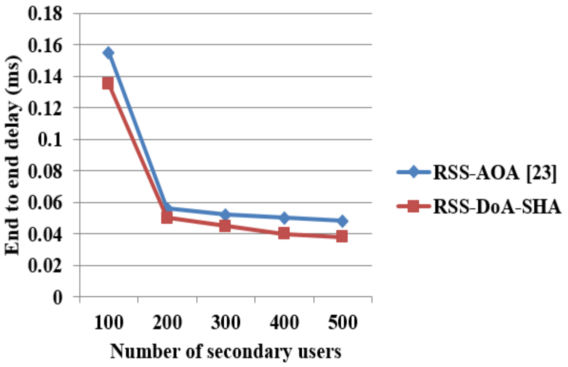

Figure. 7 Comparison of EED for different SUs

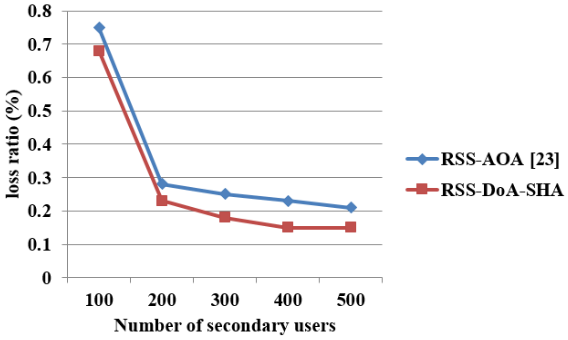

Figure. 8 Comparison of loss ratio for different SUs

The performance analysis of RSS-DoA-SHA method under PUE attacks with varying secondary users is described in this section. Here, the RSS-DoA-SHA method is compared with the RSS-AOA [23] in terms of secondary users are analyzed as routing overhead, EED and loss ratio. Here, the secondary users vary from 100-1200 to analyze the CRN.

Figs. 6, 7 and 8 shows the comparison of routing overhead, EED and loss ratio for varying SUs respectively and the proposed RSS-DoA-SHA method gives better performance than the existing RSS-AOA method [23]. For example, the routing overhead of the RSS-DoA-SHA method for 200 SU is 90, it is less when compared to the RSS-AOA [23]. The loss ratio of RSS-AOA [23] for 200 SU is 0.28% that is high when compared to the RSS-DoA-SHA method. The RSS-AOA [23] has less efficiency

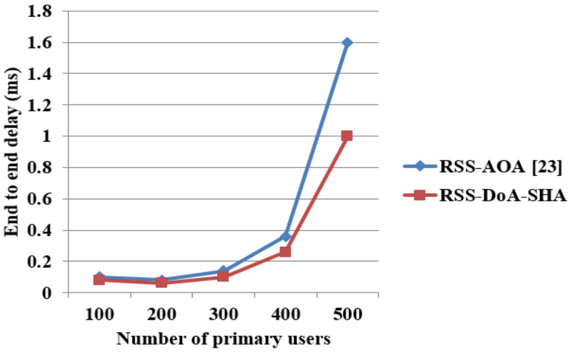

Figure. 9 Comparison of EED for different Pus

Table 1. Comparison of HRA-SKC and RSS-DoA-SHA

Number of secondary users	**EED (ms)**		**Packet loss ratio**		**Routing overhead**	
	HRA-SKC [24]	**RSS-DoA-SHA**	**HRA-SKC [24]**	**RSS-DoA-SHA**	**HRA-SKC [24]**	**RSS-DoA-SHA**
100	0.1	0.082	0.7	0.68	50	47
200	0.05	0.045	0.2	0.18	90	79
300	0.04	0.037	0.18	0.17	98	86
400	0.035	0.028	0.16	0.13	120	102
500	0.03	0.021	0.13	0.11	125	109

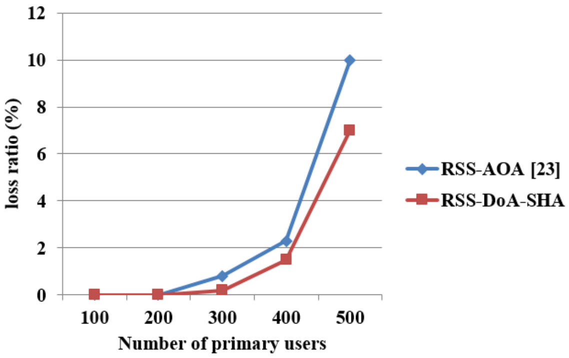

Figure. 10 Comparison of loss ratio for different PUs

because it doesn't have any security mechanism to prevent the CRN from the PUE attack. But, the RSS-DoA-SHA method with the integration of SHA-1 and neural network prevents the PUE attack which used to minimize the routing overhead and loss ratio.

5.2 Performance evaluation by varying the number of primary users

The performance analysis of RSS-DoA-SHA method under PUE attacks with varying primary users is described in this section. Here, the RSS-DoA-SHA method is compared with the RSS-AOA [23] in terms of secondary users are analyzed as EED and loss ratio.

The comparison of EED and loss ratio for different PUs is illustrated in the Fig. 9 and Fig. 10 respectively. Here, the primary users varied from 0-16 to analyze the CRN. The Fig. 9 and Fig. 10 shows that the RSS-DoA-SHA method achieves better performance than the RSS-AOA [23]. For example, the EED of the RSS-DoA-SHA method for 500 PU is 1ms, it is less when compared to the RSS-AOA [23]. The loss ratio of RSS-AOA [23] for 500 PU is 10% that is high when compared to the RSS-DoA-SHA method. The RSS-DoA-SHA method gives better performance due to the utilization of SHA-1 algorithm and neural network to prevent the CRN from the PUE attack.

5.3 Comparative analysis

This section shows the comparative analysis between the proposed RSS-DoA-SHA method and HRA-SKC [24]. For this comparison, the CRN of the RSS-DoA-SHA method is initialized with $100 \times 100\ m^2$ with 5% of SUs as malicious nodes.

Table 1 shows the comparative analysis of the HRA-SKC [24] and RSS-DoA-SHA for varying SUs i.e., from 100 to 500. From the Table 1, knows that the RSS-DoA-SHA method provides better performance than the HRA-SKC [24]. For example, the EED of the HRA-SKC [24] is increased due to the increased processing time of CH according to the number of SUs. However, the hash function generated by the SHA-1 and neural network improves the security against the PUE attacks. Therefore, the mitigation of the PUE attacks using the RSS-DoA-SHA method decreases the packet losses and increases the spectrum utilization during the communication.

6. Conclusion

CRN is generally implemented to enhance the communication reliability using the efficient and dynamic spectrum exploitation. But, the CRN is vulnerable to the PUE attacks that increases the failure probability of spectrum access. In this research paper, the hash function is generated and attached to the users of the CRN using the integration of SHA-1 and neural network which improves the security against the PUE attacks. The localization of the users is obtained using the RSS and DoA calculations. The maximum energy is mainly used to calculate the RSS and DoA. The mitigation of PUE attacks in the CRN using the integration of SHA-1 and neural network improves the spectrum utilization and minimizes the loss during communication. The RSS-DoA-SHA provides better performance than the RSS-AOA and HRA-SKC method. The EED of the RSS-DoA-SHA method is 1ms for 500 PU, it is less when compared to the RSS-AOA method. In the future, a deep neural network can be used to enhance the performances of CRN such as EED and packet loss ratio.

Conflicts of Interest (Mandatory)

The authors declare no conflict of interest.

Received: October 13, 2020. Revised: November 24, 2020.

Author Contributions (Mandatory)

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] J. Li, Z. Feng, Z. Wei, Z. Feng, and P. Zhang, "Security management based on trust determination in cognitive radio networks", *EURASIP Journal on Advances in Signal Processing*, Vol. 2014, No. 1, pp. 48, 2014.

[2] K. Elangovan and S. Subashini, "Particle bee optimized convolution neural network for managing security using cross-layer design in cognitive radio network", *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-9, 2018.

[3] M. Patnaik, V. Kamakoti, V. Matyáš, and V. Řchák, "PROLEMus: A proactive learning-based MAC protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks", *IEEE Transactions on Cognitive Communications and Networking*, Vol. 5, No. 2, pp. 400-412, 2019.

[4] J. Guo and X. Zhou, "Secure distributed routing algorithm with optimizing energy consumption for cognitive radio networks", *Wireless Personal Communications*, Vol. 72, No. 4, pp. 2533-2550, 2013.

[5] C. V. Vivekanand and K. B. Bagan, "Secure Distance Based Improved Leach Routing to Prevent Puea in Cognitive Radio Network", *Wireless Personal Communications*, Vol. 113, pp. 1823–1837, 2020.

[6] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard", *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 5, pp. 772-781, 2014.

[7] J. Zhu, "Security-reliability trade-off for cognitive radio networks in the presence of eavesdropping attack", *EURASIP Journal on Advances in Signal Processing*, Vol. 2013, No. 1, pp. 169, 2013.

[8] N. Nguyen-Thanh, P. Ciblat, A. T. Pham, and V. T. Nguyen, "Surveillance strategies against primary user emulation attack in cognitive radio networks", *IEEE Transactions on Wireless Communications*, Vol. 14, No. 9, pp. 4981-4993, 2015.

[9] Y. Jararweh, H.A.B. Salameh, A. Alturani, L. Tawalbeh, and H. Song, "Anomaly-based framework for detecting dynamic spectrum access attacks in cognitive radio networks", *Telecommunication Systems*, Vol. 67, No. 2, pp. 217-229, 2018.

[10] C. Xin, and M. Song, "Detection of PUE attacks in cognitive radio networks based on signal activity pattern", *IEEE Transactions on Mobile Computing*, Vol. 13, No. 5, pp. 1022-1034, 2014.

[11] A. Karimi, A. Taherpour, and D. Cabric, "Smart traffic-aware primary user emulation attack and its impact on secondary user throughput under rayleigh flat fading channel", *IEEE Transactions on Information Forensics and Security*, Vol. 15, No. 1, pp. 66-80, 2019.

[12] D. T. Ta, N. Nguyen-Thanh, P. Maillé, and V. T. Nguyen, "Strategic surveillance against primary user emulation attacks in cognitive radio networks", *IEEE Transactions on Cognitive Communications and Networking*, Vol. 4, No. 3, pp. 582-596, 2018.

[13] N. T. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric bayesian classification", *IEEE Transactions on Signal Processing*, Vol. 60, No. 3, pp. 1432-1445, 2011.

[14] M. Dabaghchian, A. Alipour-Fanid, K. Zeng, Q. Wang, and P. Auer, "Online learning with randomized feedback graphs for optimal PUE attacks in cognitive radio networks", *IEEE/ACM Transactions on Networking*, Vol. 26, No. 5, pp. 2268-2281, 2018.

[15] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks", *IEEE Journal on Selected Areas in Communications*, Vol. 30, No. 10, pp. 1850-1860, 2012.

[16] S. M. Elghamrawy and A. E. Hassanien, "GWOA: a hybrid genetic whale optimization algorithm for combating attacks in cognitive radio network", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, No. 11, pp. 4345-4360, 2019.

[17] S. Madbushi, R. Raut, and M. S. S. Rukmini, "Trust establishment in chaotic cognitive environment to improve attack detection accuracy under primary user emulation", *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, Vol. 42, No. 3, pp. 291-297, 2018.

[18] S. M. Elghamrawy, “Security in cognitive radio network: defense against primary user emulation attacks using genetic artificial bee colony (GABC) algorithm”, *Future Generation Computer Systems*, Vol. 109, pp. 479-487, 2020.

[19] S. Arun and G. Umamaheswari, “An adaptive learning-based attack detection technique for mitigating primary user emulation in cognitive radio networks”, *Circuits, Systems, and Signal Processing*, Vol. 39, No. 2, pp. 1071-1088, 2020.

[20] A. A. Sharifi, M. Sharifi, and M. J. M. Niya, “Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach”, *AEU-International Journal of Electronics and Communications*, Vol. 70, No. 1, pp. 95-104, 2016.

[21] K. Li and J. Wang, “Optimal joining strategies in cognitive radio networks under primary user emulation attacks”, *IEEE Access*, Vol. 7, pp. 183812-183822, 2019.

[22] K. Yadav, B. Prasad, A. Bhowmick, S. D. Roy, and S. Kundu, “Throughput performance under primary user emulation attack in cognitive radio networks”, *International Journal of Communication Systems*, Vol. 30, No. 18, pp. e3371, 2017.

[23] A. K. Singh, and A. K. Singh, “Range-based primary user localization in cognitive radio networks”, *Procedia Computer Science*, Vol. 93, pp. 199-206, 2016.

[24] M. Khasawneh, A. Azab, and A. Agarwal, “Towards Securing Routing Based on Nodes Behavior During Spectrum Sensing in Cognitive Radio Networks”, *IEEE Access*, Vol. 8, pp. 171512-171527, 2020.