Optimised Levenshtein centroid cross-layer defence for multi-hop cognitive radio networks

Davanam Ganesh | Thummala Pavan Kumar | Malchi Sunil Kumar

1 Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, AP, India
2 Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, AP, India
3 Department of Computer Science and Engineering, Sree Vidyantkerth Engineering College, Tirupati, AP, India

Correspondence
D. Ganesh, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, AP, India.
Email: dgani05@gmail.com

Abstract
Cognitive radio networks (CRN) make use of dynamic spectrum access to communicate opportunistically. Unlicensed users severely affect the spectrum sensing outcomes in CRN. Primary user emulation attack (PUEA) and spectrum sensing data falsification (SSDF) have become a paramount concern in CRNs. It is especially challenging when both masquerading (in the physical layer) and falsification (in the data link layer) occur by providing false spectrum reports. Existing methods to detect such attacks cannot be utilised in scenarios with multi-hop CRN. In this study, to mitigate attack against PUEA and SSDF, a method called optimised sensing and Levenshtein nearest centroid classification (OS-LNCC) for multi-hop CRN is presented. First, a network model for multi-hop CRN is designed. Next, a probable density optimal logical sensing model is designed to alleviate the problems related to falsification of spectrum reports. Here, the falsification of spectrum reports is overcome by exploiting dual factors, that is, probability for false alarm and probability for detection according to the departure rate of primary user (PU). With these dual factors, optimal logical sensing is made, therefore improving the throughput with minimum delay. Finally, each cognitive radio (CR) user evaluates its current sensing information to existing sensing classes through the Levenshtein distance function. Based on quantitative variables, the prediction function of each sensing class is measured using nearest centroid (NC) classifier and the sensing report is classified into either presence or absence of PU. These predictive classes are then integrated at the fusion centre so that robust mitigation against PUEA and SSDF is made. Computer simulation outputs show that OS-LNCC method performs better than the conventional methods using metrics such as sensing delay by 47%, percentage of error in prediction by 46% and throughput by 45%.

1 | INTRODUCTION

Cognitive Radio (CR) is one of the methods employed to address the issues related to insufficiency radio spectrum. In CR technology, there is a possibility of malicious users (MUs) accessing the radio frequencies across a spectrum hole. As MUs are not primary group of users for using CR technology, it poses a challenge to the exploitation of spectrum prediction. Thus, the users are classified into two types in CRN. Primary users (PUs) that take the specific part of the radio spectrum by holding an authority, and secondary users (SUs) that use the specific portions of the radio spectrum. With this, the licensed users only access resources and share information freely, anytime anywhere in CRN. The CR device senses the network which finds out the free channels and decides the channel to use. As far as cognitive cycle is concerned, spectrum sensing is the most crucial step, where an SU back off upon sensing a signal from a PU. During this stage, either attacker either acts as PUs or provide false observations in turn affecting both the PUs as well as SUs.

A PRO active-based learning MAC protocol (PROLEMUs) that provided resistance to two different attacks, namely, primary user emulation attack (PUEA) and spectrum sensing data falsification (SSDF) attack was presented in [1].

Learning-based predictive algorithm was designed here towards DoS attack in CRN. Here, three different models were...
1.1 Motivation and contribution

In CRNs, PUEA and SSDF are a major concern. Recently, several research works have been developed for multi-hop CRN by using machine learning models. But, an inter-domain hand-off communication and other emerging attacks were not considered. In conventional methods, the SD and the percentage of error in prediction to avoid complexity are not solved. In this study, probable density logical-OR rule is used to detect the attack by using probability function; and the Levenshtein distance function along with the Levenshtein distance function is used in this study as a means to classify between normal and MU, therefore contributing to spectrum detection accuracy at minimum time.
significant manner in the recent few years. In [9], an in-depth discussion of channel assignment mechanisms including different functionalities for CRNs is presented. At first, an overview was given to both CRNs and wireless networks. Then, the several aspects and limitations in the channel assignment were also discussed. In this context, neural network and multi-resolution analysis [10] were integrated to improve spectral efficiency and data rate of CRs. An overview of security threats and challenges concerning CRN was proposed in [11]. The impact of SU node transmission on channel capacity scaling factor based on maximum concurrent multi commodity flow (MCMCF) was designed in [12] to ensure fairness. Yet another Bayesian learning approach for both detection and mitigation was presented in [13] to achieve desired trade-off between security and performance for taming cross-layer attack. Another spectrum mobility management model was proposed in [14] with the objective of improving spectral sensing accuracy and channel holding time. Detecting and defeating attacks in cross layer to increase network efficiency were presented in [15]. A double adaptive thresholding scheme to distinguish the legal and MUs using Dempster–Shafer (DS) evidence theory was proposed in [16]. Here, analysis between probability and false alarm detection was also made. An integrated scheme [17] using adaptive modulation with coding (AMC) was carried out in the physical layer and rate adaptation (RA) in the MAC layer. This resulted in offering optimised throughput. A secure routing based on the trust value was employed in [18] to lessen the attack in CRN. This was said to be achieved by monitoring the nodes’ forwarding behaviours as malicious nodes were said to be identified based on the nodes’ trust. With this design consideration, routing selection-based model was integrated with spectrum allocation.

Finally, trusts were utilised to build obtained path trusts and delay for deciding suitable routing decisions. Attack in TCP and MAC layers was presented in [19] along with the defence mechanism based on round trip time (RTT) to improve throughput. A collaborative approach was designed in [20] utilising cluster analysis to achieve high spectrum accuracy. Channel hopping-based defence method was discussed in [21] to lessen the PUEA in CRN. Different attacks that occurred in the physical layer were analysed and studied in [22]. The detection method and encounter measures were exploited to defend the attacked CRN. A novel scheme to defend against the PUE attacker was presented in [23] by using adaptive Bayesian learning automaton algorithm. A distributed method based on the uncoordinated frequency hopping technique was developed in [24] to mitigate the PUE attack. Trust-based multi-hop cooperative spectrum sensing (CSS) method was discussed in [25] to defend against SSDF attack. A novel hybrid optimisation was designed in [26] to detect the spectrum in CRN. In [27], new CSS method was employed with less delay. Also, soft CSS was described in [28] to perceive the occurrence of PUEA. It effectively lessens the error probability in CRN. In [29], CRN with CSS is applied to handle the issues of sensing, grouping and decision making. A generic Byzantine attack model was introduced in [30] to obtain the condition that constructs the fusion centre (FC) blind. A non-cooperative game-theory approach was presented in [31] for overcoming the Byzantine attack problem to understand an effective Byzantine defence in CSS. A generic soft attack model was introduced in [32] from malicious behaviours. A generalised attack model was used to compute the attack cost and benefit, and cost-benefit trade-off issues. A generalised soft Byzantine attack model was developed in [33] to examine attack strategies in the absence of any defence, in terms of the attack strength and probability. A classical trust-value-based CSS algorithm was used to carried attack strategies and estimate the security of Byzantine attacker. In light of the standard international telecommunications union (ITU) recommendations, a rain fading channel model was introduced in [34] to investigate the interference level at the FS receiver considering the channel statistical properties, propagation losses and antenna patterns. ITU recommendations were considered for the antenna patterns and off-axis emission limits, where the rain attenuation is viewed as the simplified factor in modelling the channel fading distribution, and two representative antenna patterns are employed. A novel cognitive satellite-terrestrial network with interference temperature constraint was presented in [35]. A heavier shadowing severity of the satellite interference link results is used to minimise the outage probability. A secure and trusted routing and handoff mechanism were introduced in [36] to improve the network delay and overhead. However, the inter-domain handoff communication was not considered. A novel localisation approach was introduced in [37] for identifying the PUE emulation attack with integrating the trilateration and RSSI techniques. A double adaptive thresholding technique was introduced in [38] to deal with distinguished legitimate users, doubtful and MUs. A machine learning algorithm named support vector machine (SVM) was presented for categorising the legitimate SU and MUs. A novel cognitive user emulation attack (CUEA) was developed in [39] to efficiently mitigate the attack, but the designed system failed to consider the other emerging attack.

As explained above, many methods were addressing the issue of providing defence against attack in CRN. Critical issue in CRN is to plan a proper defence mechanism in the existence of attack, and capturing the physical and data link layer characteristics with single hop network. The SD ignores the percentage of error in prediction to avoid complexity and are not solved in conventional methods. Considering this issue converts the difficulty to multi-hop problem that needs a non-traditional customised solution method. In this study, a novel machine learning model called OS-LNCC method for multi-hop CRN is presented to solve this problem.

3 | OS-LNCC FOR MULTI-HOP CRN

The open characteristics of cognitive radio networks (CRNs), a security vulnerability, is exploited with dissimilar types of attacks which is launched in the process of CSS, namely, PUEA and Byzantine attack called SSDF. PUEA is one of the most challenging attack types in the part of PU. In this section, cross-layer defence architecture against two different attacks, namely, PUEA and SSDF under multi-hop CRN using novel machine learning method is proposed. Figure 1 shows the block
diagram of OS-LNCC method for multi-hop CRN. As shown in the Figure 1, a defence mechanism for cross-layer attack using novel machine learning model is presented. In this study, two layers, namely, physical layer (i.e. PUEA attack) and data link layer (i.e. SSDF attack) and the corresponding attacks in this layer are analysed and a defence architecture is presented accordingly. First, probable density optimal logical sensing model is designed to provide mechanism to mitigate against SSDF with higher throughput and minimum SD. Next, a robust algorithm called LNCC is designed for classification or emulation between normal and malicious CRN users (i.e. CRN nodes) made at the fusion centre, therefore contributing to robustness against PUEA attack. Thus, the normal users are identified and information shared across the network. To start with, the network model for multi-hop CRN is designed followed by the presentation of the elaborate description of the OS-LNCC method.

3.1 Network model

In this study, a multi-hop CRN consisting of \( m \) PUs (i.e. \( m \) Primary Users) and \( n \) SUs (i.e. Secondary Users) is taken into consideration and specific spectrum bands are assigned to PUs. On the other hand, the SUs do not possess any licensed or authorised channels and transmit DP in an opportunistic manner when identifying that the spectrum bands are not possessed by the PUs or the spectrum band is free. Each SU node \( n_i \) possess a set of available channels which includes both data transmission channel \((DTC)\) and common control channel \((CCC)\). From the name itself, \( DTC \) refers to data transmission and is denoted as given below:

\[
C_i = \{c_1, c_2, ..., c_m\}
\] (1)

From the above Equation (1), \( c_1, c_2, ..., c_m \) corresponds to the set of available channels. On the other hand, \( CCC \) is utilised for negotiation between the PUs and SUs. Therefore, at any instance, a link is said to be established between SU \( n_i \) and \( n_j \), if the following condition prevails:

\[
CCC \in C_i \cap C_j
\] (2)

With the above said assumptions as given in Equations (1) and (2), a network model with multi-hop CRN is designed and shown as follows. In the networking scenarios, with multi-hop CRN as basics, Figure 2 shows two centralised PU networks, where \( n \) ST transmitters SU–T with one FC are employed in the presence of two centralised PU transmitters PU–TP networks. On one hand, SU–T carry out spectrum sensing to discover PU–T condition. Then broadcast their corresponding sensing results to fusion centre FC.

3.2 Probable density optimal logical sensing

SSDF attack [1] sends false observation causing DoS in a specific spectrum, therefore reducing the throughput. However, with falsified reports sent through the users, the performance of spectrum allocation is degraded. To address this issue, in this study, a probable density optimal logical sensing model is designed to reduce the falsification of spectrum reports by means of STATLOG. A mechanism is designed where a joint
The optimisation problem is resolved to extend the throughput based on the probable density logical-OR rule imposed on the primary network. Figure 3 given below shows the optimal logical sensing attained in the presence of SSDF attack by means of STATLOG function.

The source $SU - T$ generates $DP$ and sends them to the destination node in multi-hop manner via intermediate $SUs–T$. Each $PU–T$ communicates with the PU base station (BS) with the aid of spectrum bands and intermediate $SUs–T$. Each hop DP is transmitted via the $PU$ spectrum band when the spectrum band is idle and then send the corresponding sensing decisions to $FC$. The $FC$ in turn makes an optimal decision based on the integration of local sensing decisions.

Let us further consider that the obtained signal is sampled at frequency $f_s$. If $PU–T$ is active, the obtained signal at the $PU–T$ is represented as given below:

$$H_1 = y(n) = s(n) + \varepsilon(n) \quad (3)$$

From the above Equation (3), $s(n)$ and $\varepsilon(n)$ refer to the PUs signal and the noise factor, respectively, and is termed as $H_1$. On the other hand, if $PU–T$ is inactive, the received signal at $PU–T$ is represented as given below:

$$H_0 = y(n) = \varepsilon(n) \quad (4)$$

From the above Equation (4), $\varepsilon(n)$ refers to the noise factor and is termed as $H_0$. Here, mean and variance are represented as $\mu_0$ and $\sigma_0$ for $H_0$, and mean and variance are represented as $\mu_1$ and $\sigma_1$ for $H_1$. Then, the probability for false alarm $Prob_{FA}$ and probability for detection $Prob_D$ are represented as given below:

$$Prob_{FA} = Q \left[ \frac{\alpha - \mu_0}{\sigma_0} \right] \quad (5)$$

$$Prob_D = Q \left[ \frac{\alpha - \mu_1}{\sigma_1} \right] \quad (6)$$

From the above Equations (5) and (6), $Q$ and $\alpha$ represent the $Q$-function for multi-hop CRN with mean and variance for both $H_0$ and $H_1$, respectively. Finally, an optimal decision rule based on the probable density logical-OR rule is made:

$$Prob_{E4} = 1 - \prod_{i=1}^{M} \left( 1 - Prob_{E4,i} \right) * \Theta_{dr} \quad (7)$$

$$Prob_D = 1 - \prod_{i=1}^{M} \left( 1 - Prob_{D,i} \right) * \Theta_{dr} \quad (8)$$

From the above Equations (7) and (8), $Prob_{E4}$ denotes the probability for false alarm and $Prob_D$ represents the probability for detection, $Prob_{E4,i}$ represents the users probability for
false alarm, \( Pr_{D,i} \) denotes the users probability for detection. Probability of \( Pr_{D,i} \) and \( Pr_{FA,i} \) are computed based on the departure rate \( \theta_{dr} \) to improve the attack detection rate. In the probable density logical-OR rule, when one of the decisions decides that there is a PU, then the final decision decides that there is a PU along with the departure rate \( \theta_{dr} \). With this, an optimal decision is made by the fusion centre thereby mitigating spectrum falsification. The pseudo code representation of probable density optimal logical sensing is given below.

With the design consideration of multi-hop CRN using probable density optimal logical sensing algorithm, two different objectives, that is, minimising the SD and maximising the throughput are said to be attained. To start with, in this algorithm, to design cross-layer defence architecture with the objective of minimising the falsification of spectrum in multi-hop CRN, two hypotheses with PU active and inactive model are measured. At first, departure rate of \( PU-T \) is initialised. Next, PU and SUs with available channel, the two hypotheses are measured for each CRN node. When the PU is in active state, the first hypothesis is measured. The second hypothesis is measured when the PU is in an inactive state. In the next step, the probability of false alarm rate is calculated, then probability of detection is computed. The probability of false alarm rate and detection is computed based on the departure rate of PU. In the last step, the probable density logical-OR rule is employed to acquire the optimal decision rule. Here, an optimal decision regarding the spectrum sensing is made at the fusion centre with minimum delay, therefore reducing the SSDF attack with an improved throughput with less complexity. With this, the information is freely transmitted anywhere in the network without any data loss.

3.3 LNCC model

In a PUEA, an attacker [1] poses as a PU for executing the broadcasting in licensed spectrum bands that evades other SUs to exploit services. With proper classification mechanism, normal and MU can be differentiated so that only normal user makes transmission in a licensed frequency, making room for SU also.

The proposed study employs Levenshtein distance calculation to represent the features of user signal which is then fed into the NC classifier for classification and is called as the LNCC model. In this study, the LNCC model is initiated through determining the energy for predicting the users on the spectrum band. Then, the energy received at the \( i_{th} \) CR user at the \( k_{th} \) sensing area is written as given below:

\[
S_{ik} = \sum_{n=1}^{N} F_{ik} (j) \]  

(9)

From the above Equation (9) \( F_{ik}(j) \) represents the energy sample received by the \( k_{th} \) sensing area for the corresponding \( i_{th} \) CR user with \( N \) representing the total number of samples. With the above energy detection function given in Equation (9), this study employs NC, an LNCC, that categorises the observations into diverse classes by means of quantitative variables. NC classifies a test instance, in LNCC, the current sensing report as obtained from Equation (9) into one of several NC classes by majority voting. The vote is then updated for estimating the distance among sensing results. As far as CRN is concerned, it is highly impossible to say which results are more similar. So, similarity between the two sensing reports has to be obtained. The classification surface is split into diverse centroids and the distance of the present sensing result to each of the centroids is identified.

Let \( Dis (a_{1},C) \) represent the distance where \( C \) denotes the centroids given by \( C \in C_{1}, C_{2}, \ldots, C_{n} \). The distance is measured to each of the centroids representing either \( H_{0} \) or \( H_{1} \). Based on the measured distance, the current sensing result is categorised either to \( H_{0} \) or \( H_{1} \). First, the distance calculation is made by using the Levenshtein distance and then NC classifier is employed for classification. The Levenshtein distance computes exact distance within vectors. The collaborative virtual sensing used by [2] differs from each other due to the deadline. So, in this study, focus is made on evaluating the similarity among sensing results through the Levenshtein distance where it analyses the distance of current sensing result and the sensing classes. The Levenshtein distance between sensing results \( u \) and \( v \) (length \([a]\) and \([r]\)) is mathematically expressed as given below:

\[
Lev_{uv} (|a|,|q|) = \begin{cases} 
\max (p,q) & \text{if } \min (p,q) = 0 \\
\min Lev_{uv} (p - 1, q) + 1 & \text{if } Lev_{uv}(p,q) = 1 \\
\min Lev_{uv} (p, q - 1) + 1 & \text{if } Lev_{uv}(p,q) = 0 \\
\min Lev_{uv} (p - 1, q - 1) + 1 & \text{if } p \neq q
\end{cases} 
\]  

(10)
EXPERIMENTAL SETUP

Performance evaluation of SD

Here, actual decision is given to the test sensing reports is calculated. Therefore, OS-LNCC alleviates attack against PUEA and SSDF in CRN.

4 EXPERIMENTAL SETUP

The proposed OS-LNCC is compared with existing methods [1, 2, 5, 16]. To evaluate OS-LNCC, network simulator (NS2) is used. The metric used for this evaluation is SD, percentage of error in prediction and throughput. The evaluation is conducted on a network size of 1000 * 1000 m area with the packet size set as 2500 bytes. Number of packets broadcasted per session is set as 500. The total available spectrum is set to be 54–72 MHz. The bandwidth usable by CRs is constrained to be 2, 4 and 6 MHz [2]. The bandwidth of the CCC is set as 2 MHz.

The simulation results are analysed by using probable density optimal logical sensing and LNCC models in OS-LNCC. Initially a visual interface for network topology is presented. Then, the sensing model is employed to offer the optimal decision about the spectrum sensing. This aids to lessen the SSDF attack. In addition, LNCC model is applied to observe the behaviour of PU and thus detect the MUs or attackers in CRN. This is performed with the help of computing Levenshtein distance function where the distance between test and training sample sensing reports is calculated. Therefore, OS-LNCC alleviates attack against PUEA and SSDF in CRN.

4.1 Performance evaluation of SD

A multi-antenna BS was introduced [40] to improve the secure transmission. In the BS, the imperfect channel state information (CSI) and statistical CSI of the link among the BS and satellite user are presented. A multi-antenna BS with two beamforming (BF) algorithms such as hybrid zero-forcing (HZF) and partial zero-forcing (PZF) was designed for statistical CSI cases for
TABLE 1  Sensing delay (SD) versus number of cognitive radio network (CRN) nodes

| Number of CRN nodes | SD (ms) (OS-LNCC) | PROLEMus | Deadline-based routing and spectrum allocation | CLVF | Double adaptive thresholding technique |
|---------------------|-------------------|----------|---------------------------------|-------|---------------------------------------|
| 50                  | 1.35              | 1.8      | 2.35                            | 2.63  | 3.01                                  |
| 100                 | 1.95              | 2.25     | 4.15                            | 4.15  | 5.32                                  |
| 150                 | 2.15              | 2.55     | 4.55                            | 5.02  | 5.64                                  |
| 200                 | 2.55              | 2.95     | 5.15                            | 5.67  | 5.91                                  |
| 250                 | 3.15              | 3.55     | 6.56                            | 7.02  | 7.43                                  |
| 300                 | 3.35              | 4.35     | 7.35                            | 7.92  | 8.15                                  |
| 350                 | 4.15              | 5.15     | 9.25                            | 9.87  | 10.6                                  |
| 400                 | 4.85              | 6.16     | 11.15                           | 12.03 | 12.82                                 |
| 450                 | 5.55              | 8.35     | 12.35                           | 12.88 | 13.43                                 |
| 500                 | 7.15              | 10.55    | 14.55                           | 15.01 | 15.96                                 |

Abbreviations: CLVF, cross layer verification framework; OS-LNCC, optimised sensing and Levenshtein nearest centroid classification; PROLEMus, PROactiveLearning-based MAC protocol.

overcoming the optimisation issue. SD refers to the time delay occurrence in the channel sensing phase. In other words, SD is referring the number of channels sensed through an SU prior to data broadcasting:

\[
SD = \text{Time} \left[ \text{Prob}_{E1} + \text{Prob}_{D2} \right] \times N
\] (13)

From the above Equation (13), SD is measured based on the time occurrence in the channel sensing phase, that is, \( \text{Prob}_{E1} \), \( \text{Prob}_{D2} \) and the number of CRN nodes \( N \). It is measured in terms of milliseconds (ms). Table 1 given below shows the SD values obtained by applying the Equation (13) for five different methods such as OS-LNCC, existing methods in [1, 2, 5, 16].

Figure 4 given above shows the graphical representation of SD using OS-LNCC, existing methods in [1, 2, 5, 16]. Ten different simulation runs were conducted and similar number of CRN nodes in the range of 50 to 500 for fair comparison. Here, the CRN nodes refer to the inclusion of PU and SU in CRN. From the figure, it is illustrative that the SD is in the increasing trend for all the five methods. With 50 number of CRN nodes considered for experimentation, the time consumed in channel sensing phase using OS-LNCC was found to be 1.35 ms, 1.8 ms for [1], 2.35 ms for [2], 2.63 ms for [5] and 3.01 ms for [16]. From this, it is inferred that the SD was identified to be lesser using OS-LNCC method when compared to [1, 2, 5, 16]. The existing method in [1] was used to detect the attack. But, it failed to provide better SD results. This is because of the incorporation of probable density optimal logical sensing algorithm. By applying this algorithm, the SD is even found to be better in the presence of multi-hop CRN. This is because of identifying two hypotheses, first, by applying the STALOG function, and then measuring the false alarm and detection by means of Logical OR rule. With this, the SD is said to be reduced using OS-LNCC method by 20% compared to [1], 52% compared to [2], 55% compared to [5] and 59% compared to [16].

4.2  Performance evaluation of percentage of error in prediction

Cross-layer attack first refers to the attack occurring at more than one layer. In OS-LNCC, the attack occurring in the physical layer called PUEA and attack occurring at the data link layer called SSDF are considered and defence mechanism is provided accordingly. During the provisioning of defence mechanism, certain amount of wrong predictions are also said to have taken place. Hence, the percentage of wrong detection is measured as given below:

\[
% \text{ of } Err_p = \frac{\text{Wrong}_p}{N} \times 100
\] (14)
TABLE 2 Percentage of error detection versus number of CRN nodes

| Number of CRN nodes | OS-LNCC | PROLEMus | Deadline-based Routing and Spectrum Allocation | CLVF | Double adaptive thresholding technique |
|---------------------|---------|----------|-----------------------------------------------|------|-----------------------------------------|
| 50                  | 8       | 14       | 22                                            | 26   | 38                                      |
| 100                 | 15      | 29       | 35                                            | 45   | 50                                      |
| 150                 | 25      | 35       | 40                                            | 47   | 60                                      |
| 200                 | 30      | 45       | 60                                            | 67   | 77                                      |
| 250                 | 40      | 55       | 75                                            | 81   | 90                                      |
| 300                 | 50      | 70       | 90                                            | 97   | 108                                     |
| 350                 | 55      | 78       | 105                                           | 109  | 116                                     |
| 400                 | 70      | 90       | 120                                           | 125  | 134                                     |
| 450                 | 85      | 105      | 130                                           | 138  | 143                                     |
| 500                 | 90      | 125      | 145                                           | 150  | 158                                     |

FIGURE 5 Graphical representation of percentage of error detection

From the above Equation (14), the percentage of error in prediction (% of $Err_p$) is measured based on the percentage ratio of samples of CRN nodes provided as input $N$ and the wrong predictions made $Wrong_p$ by the network. It is measured in terms of percentage (%). Table 2 given below shows the percentage of error detection values arrived at by applying Equation (14) for five different methods, OS-LNCC, existing methods in [1, 2, 5, 16].

Figure 5 given above shows the graphical representation of percentage (%) of error detection with respect to different number of CRN nodes considered at different time intervals and different sessions. As already mentioned that the CRN nodes used in the simulation refers to both the PU and SU in the CRN network, the percentage of error detection measured also differs and hence not said to be proportionately increasing. However, as the number of CRN node increases, percentage of error detection also increased. But it is found to be comparatively lesser when applied with OS-LNCC when compared to the existing methods [1, 2, 5, 16]. This is evident from the simulation. When 50 number of nodes was considered for simulation, the wrong predictions made during the overall defence architecture using OS-LNCC was found to be 4, 7 using [1], 11 using [2], 13 using [5] and 19 using [16]. The existing method [1] was used to find the bounds for prediction errors with Chernoff’s bounds. But, the error rate was not minimised. The reason is because of the application of probable density logical-OR rule, that also considers the departure rate $\theta_{dr}$ of PU with which the final decision is taken by the fusion centre regarding spectrum falsification. In addition, by using Levenshtein distance between two sensing reports, classification of PU and MU are made significantly. With this the percentage of error prediction is reduced using OS-LNCC method by 31% compared to [1], 46% compared to [2], 51% compared to [5] and 56% compared to [16].

4.3 Performance evaluation of throughput

Finally, the efficiency of the cross-layer defence architecture is measured based on the throughput rate. The throughput of CRNs is closely related to the spectrum sensing frame structure. Spectrum sensing frame structure is separated into local sensing time, cooperative time, and transmission time. The throughput of the CRN is depending on sensing method and it is offered as follows.

$$T = \frac{DRU \times Time_{CP}}{Time_{TS}}$$  \hspace{1cm} (15)

From the above Equation (15), the throughput rate $T$ is measured based on the data rate $DR$ of each cognitive user, $U$ unused channels as perceived by the SU, $Time_{CP}$ corresponding to the time period of the competing phase and $Time_{TS}$ referring to the time duration of the entire time slot. It is estimated in the unit of bits per second. Table 3 given below shows the throughput rate by applying Equation (15) for five different methods, OS-LNCC, existing methods [1, 2, 5, 16].
### Table 3: Throughput versus number of CRN nodes

| Number of CRN nodes | OS-LNCC | PROLEMus | Deadline-based routing and spectrum allocation | CLVF | Double adaptive thresholding technique |
|---------------------|---------|----------|-----------------------------------------------|------|---------------------------------------|
| 50                  | 22.4    | 16.8     | 14                                            | 12.01 | 10                                    |
| 100                 | 35.5    | 25.5     | 19.55                                         | 17.05 | 14.31                                 |
| 150                 | 41.35   | 30.15    | 26.15                                         | 25.24 | 20.26                                 |
| 200                 | 50.25   | 40.25    | 36.35                                         | 32.24 | 29.11                                 |
| 250                 | 66.156  | 55.35    | 49.15                                         | 45.23 | 41.34                                 |
| 300                 | 70.35   | 60.15    | 56.55                                         | 54.11 | 51.63                                 |
| 350                 | 75.15   | 68.35    | 60.25                                         | 56.13 | 53.26                                 |
| 400                 | 80.25   | 72.45    | 66.16                                         | 63.32 | 57.34                                 |
| 450                 | 85.55   | 80.15    | 74.35                                         | 70.31 | 68.23                                 |
| 500                 | 90      | 82.35    | 76.55                                         | 72.26 | 69.63                                 |

**Figure 6** Graphical representation of throughput

Figure 6 given above shows the graphical representation of throughput with respect to 500 different CRN nodes. In throughput measure, time period of the slot is taken as 0.050 ms and the time period of the contending phase for proposed method is 0.035 ms. The PUs channel utilisation factor is considered as 4 for all the five methods. The data rate of each channel is found to 8 ms for the proposed method. Hence, the throughput is observed as 22.4 bps for OS-LNCC method, 16.8 bps for [1], 14 bps for [2], 12.01 bps for [5] and 10 bps for [16]. Here, throughput is referred as the total data rate supposed by the CRN. From the figure, it is precise with wrong detection. The users in the CRN obtain a false notion that acquiring larger throughput rate. The existing method [2] was applied to higher resource utilisation. But, the method does not maximise the effective throughput. From the simulation values provided above, it proves that throughput estimation without considering optimal sensing and robust classification results offers a false result of performance. Evaluating the throughput rate of state-of-the-art methods, [1, 2, 5, 16], the throughput is improved in OS-LNCC method compared to [1, 2, 5, 16] as OS-LNCC method makes sure that a primary channel is sensed by only one SU and not by the MU by effective classification based on the LNCC. With this, the throughput rate using OS-LNCC method is found to be better by 21% compared to [1], 38% compared to [2], 51% compared to [5] and 68% compared to [16].

#### 4.4 Computational complexity

The amount of time taken to detect the MUs from the normal CRN nodes is referred as computational complexity. Computational complexity is calculated in terms of milliseconds (ms) with the mathematical formula shown in below:

\[
\text{Computational Complexity} = \text{Number of CRN node} \times \text{Time}
\]

From Equation (16), computational complexity is measured. Table 4 given below shows the computational complexity values arrived at by using the Equation (16) for five different methods, OS-LNCC, existing methods in [1, 2, 5, 16].

Figure 7 given above presents the graphical representation of computational complexity with respect to 500 different CRN.
nodes. From the graphical representation, existing methods in [1, 2, 5 16] obtain 3.32 ms, 2.52 ms and 2.37 ms, 2.20 ms of computational complexity, whereas 1.98 ms is achieved in proposed OS-LNCC method. From the above figure, OS-LNCC method results with better computational complexity. The results reported above confirm that with the increase in the time, computational complexity also increases. It minimises the time taken for the MUs. Hence, proposed OS-LNCC method attains reduced computation complexity by 30% compared to [1], and 18% compared to [2], 17% compared to [5] and 20% compared to [16].

5 | CONCLUSION

In this study, a novel OS-LNCC for multi-hop CRN is proposed as defence architecture for CRN with probable density optimal logical sensing model and LNCC are examined. Sensing a channel in the existence of multi-hop is examined to influence the throughput of the CRN. The algorithm for mitigating the spectrum falsification by means of STATLOG function along with the algorithm for significant classification between the CRN normal and MU by means of novel machine learning for reducing PUE is designed and thereby throughput of CRN is enhanced. In addition, the effectiveness of OS-LNCC method is analysed in terms of SD, percentage of error prediction and throughput. The simulation outcomes are clearly evident that the performance of OS-LNCC compared with conventional methods. Thus, OS-LNCC method enhances the percentage of error prediction, throughput, which increases the defence mechanism of CRN with minimum SD.

In this study, only the probability of attack detection and false alarm is considered. In future, we can consider the other network parameters such as data rate and overall network throughput at the presence of attackers. In addition, a more efficient method for considering jointly SSDF and PUEA attacks in a CR is still a foremost issue needing to be addressed. SSDF attack still poses significant performance degradation in CRN. In future, we can use some network’s parameters and classification methods to separate the MUs from the normal users to enhance the performance of the CRN.

REFERENCES

1. Patnaik, V.M., et al.: PROLEMus: A proactive learning-based MAC protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks. IEEE Trans. Cognit. Commun. Networking 5(2), 400–412 (2019)
2. Jagannath, J., et al.: Design and experimental evaluation of a cross-layer deadline-based joint routing and spectrum allocation algorithm. IEEE Trans. Mob. Comput. 18(8), 1774–1788 (2019)
3. Li, J., et al.: Security management based on trust determination in cognitive radio networks. EURASIP J. Adv. Signal Process. 1–16 (2014)
4. Meng, Y., et al.: Resource allocation and interference management for multi-layer wireless networks in heterogeneous cognitive networks. EURASIP J. Wireless Commun. Networking pp. 1–12 (2019)
5. Jagadeesan, S., Parthasarathy, V.: Design and implement a cross layer verification framework (CLVF) for detecting and preventing blackhole and wormhole attack in wireless ad-hoc networks for cloud environment. Cluster Comput. 299–310 (2018)
6. Manna, T., Misra, I.S.: Design, implementation and analysis of cognitive radio enabled intelligent WBAN gateway for cost-efficient remote health monitoring. Physical Communication, 35, pp. 100713. Elsevier (2019)
7. Darabkh, K.A., et al.: A–Z overview of the in-band full-duplex cognitive radio networks. Computer Communication 45, pp. 66–95. Elsevier (2019)
8. Hossain, E., et al.: Evolution and future trends of research in cognitive radio: a contemporary survey. Wireless Commun. Mobile Comput. 1–35 (2013)
9. Gupta, N., Dhurandher, S.: Cross-layer perspective for channel assignment in cognitive radio networks: A survey. Int. J. Commun. Syst. 1–19 (2019)
10. Rodriguez-Colina, E., Hernandez, C.A., et al.: Dynamic OFDM transmission for a cognitive radio device based on a neural network and multi-resolution analysis. Wireless Commun. Mobile Comput. 1–12 (2018)
11. Hlavacek, J.D., Chang, M.: A layered approach to cognitive radio network security: A survey. Computer Networks, pp. 414–436. Elsevier (2014)
12. Salah, A., et al.: Joint channel assignment and power allocation based on maximum concurrent multicolecumity flow in cognitive radio networks. Wireless Commun. Mobile Comput. 1–15 (2018)
13. Zhang, L., et al.: Tamming cross-layer attacks in wireless networks: a bayesian learning approach. IEEE Trans. Mob. Comput. 18(7), 1688–1702 (2019)
14. Koushik, A.M., et al.: Intelligent spectrum management based on transfer actor-critic learning for rateless transmissions in cognitive radio networks. IEEE Trans. Mob. Commun. 17(5), 1204–1215 (2018)

15. Wankhede, S.V., et al.: Design approach for cross layer attacks defence in cognitive radio. Int. Res. J. Eng. Tech. 2(4), 1–4 (2015)

16. Khan, M.S., et al.: A double adaptive approach to tackle malicious users in cognitive radio networks. Wireless Commun. Mobile Comput. 5, 1–9 (2019)

17. Arunachalam, M., Kandasamy, B.: Cross-layer design for downlink scheduling combined with call admission control in wireless networks. Wireless Commun. Mobile Comput. 2–8 (2017)

18. Zhang, G., et al.: Using trust to establish a secure routing model in cognitive radio network. PLoS One 10, 1–15 (2015). https://doi.org/10.1371/journal.pone.0139326

19. Nagireddygari, D., Thomas, J.: MAC-TCP cross-layer attack and its defense in cognitive radio networks. ACM 1–8 (2014)

20. Khasawneh, M., Agarwal, A.: A collaborative approach for monitoring nodes behavior during spectrum sensing to mitigate multiple attacks in cognitive radio networks. Secur. Commun. Netw. 1–16 (2017)

21. Ahmadfard, A., Jamshidi, A.: A channel hopping based defense method against primary user emulation attack in cognitive radio networks. Comput. Commun. 148, 1–8 (2019)

22. Salahdine, F., Kaabouch, N.: Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey. Phys. Commun 39, 101001 (2020)

23. Mahmoudi, M., et al.: Defense against primary user emulation attackers based on adaptive Bayesian learning automata in cognitive radio networks. Ad Hoc Networks 102, 102147 (2020)

24. Mahmoudi, M., et al.: Uncoordinated frequency hopping scheme for defense against primary user emulation attack in cognitive radio networks. Comput. Networks 163, 106884 (2019)

25. Khalunzedah, A., et al.: Trust-based multi-hop cooperative spectrum sensing in cognitive radio networks. J. Inf. Secur. Appl. 42, 29–35 (2018)

26. Supraja, P., et al.: Spectrum prediction in cognitive radio with hybrid optimized neural network. Mobile Networks Appl. 24, 357–364 (2019)

27. Hu, H., et al.: Efficient spectrum sensing with minimum transmission delay in cognitive radio networks. Mobile Networks Appl. 19, 487–501 (2014)

28. Emami, M., et al.: Soft cooperative spectrum sensing using quantization method in the presence of smart PUE attack. Mobile Networks Appl. 22, 650–659 (2017)

29. Prasad, R.G.P., Venkatesan, G.: Based multi-channel synchronized spectrum sensing in cognitive radio network with 5G. Mobile Networks Appl. 24, 327–339 (2019)

30. Wu, J., et al.: Generalized Byzantine attack and defense in cooperative spectrum sensing for cognitive radio networks. IEEE Access 6, 53272–53286 (2018)

31. Wu, J., et al.: Game-theory approach against Byzantine attack in cooperative spectrum sensing. J. Southeast Univ. (English Edition) 34(4), 423–429 (2018)

32. Wu, J., et al.: Cost-benefit tradeoff of Byzantine attack in cooperative spectrum sensing. IEEE Syst. J. 1–12 (2019)

33. Wu, J., et al.: Analysis of Byzantine attack strategy for cooperative spectrum sensing. IEEE Commun. Lett. 2990869. https://doi.org/10.1109/LCOMM.2020

34. An, K., et al.: Performance limits of cognitive uplink FSS and terrestrial FS for Ka-band. IEEE Trans. Aerosp. Electron Syst. 55, 2604–2611 (2019)

35. An, K., et al.: Outage performance of cognitive hybrid satellite terrestrial networks with interference constraint. IEEE Trans. Veh. Technol. 9394–9404 (2016)

36. Rathee, G., et al.: A Trust framework to detect malicious nodes in cognitive radio networks. Electronics 8, 1–9 (2019). https://doi.org/10.3390/electronics8111299

37. Fihri, F., et al.: A decision-making approach for detecting the primary user emulation attack in cognitive radio networks. Int. J. Commun. Syst. 1–15 (2019), https://doi.org/10.1002/dac.4026

38. Khan, M.S., et al.: A double adaptive approach to tackle malicious users in cognitive radio networks. Wireless Commun. Mobile Comput. 1–9 (2019). Article ID 2350694 doi.org/10.1155/2019/2350694

39. Khan, M.S., et al.: Support vector machine-based classification of malicious users in cognitive radio networks. Wireless Commun. Mobile Comput. 1–11 (2020). Article ID 8840948. doi.org/10.1155/2020/8840948

40. An, K., et al.: Secure transmission in cognitive satellite terrestrial networks. IEEE J. Sel. Areas Commun. 34, 3025–3037 (2016)

How to cite this article: Ganesh D, Kumar TP, Kumar MS. Optimised Levenshtein centroid cross-layer defence for multi-hop cognitive radio networks. IET Commun 2021;15:245–256. https://doi.org/10.1049/cm2.12050