

Regressive Schnorr Signature Based Deep Belief for Secured Data Routing In Cognitive Radio Network

T. Sundar^{1*}, A. Senthilkumar²

¹Research Scholar, Department of Computer Science, Periyar University, Salem, Tamil Nadu, India - 636011.

²Assistant professor, Department of Computer Science, Thiruvalluvar Government Arts College Rasipuram, Tamil Nadu, India - 637401.

KEYWORDS:

Cognitive Radio Network,
Secure Data Routing,
Poisson Regressive Analysis,
Schnorr Signature,
Deep Belief Network

ARTICLE HISTORY:

Received: 14.12.2025
Revised: 18.01.2026
Accepted: 10.02.2026

DOI:

<https://doi.org/10.31838/NJAP/08.02.11>

ABSTRACT

Wireless communication technology, called, Cognitive Radio Network (CRN) permits lesser users to approve networks lacking nosy with main users. Data routing is a confront in CRNs due to different features of CR mechanism, to name a few being, dynamic spectrum frequency bands in CRN, compromising network performance and presence of malicious nodes, therefore reducing the overall network performance. Therefore, secure and reliable routing becomes major issue for this type of network. In order to overcome this issue, a secure data routing method employing deep learning called Regressive Trust-aware Schnorr Signature based Deep Belief Network (RTSS-DBN) in CRN is proposed. It involves the four different layers namely, one input layer, two hidden layers and one output layer for secured data routing in CRN. Initially, number of cognitive radio nodes is considered as input in the input layer. In order to handle the security issues in CRN to enhance the data confidentiality rate, we planned two novel processes, such as authentication process and shifted spectrum sensing process in two hidden layers for secure data routing. In the first process (i.e. first hidden layer), we describe an authentication mechanism to sense the mean CR users or malicious users and removed them in the ultimate sensing decision. The CRN based on a secure linear sensing model using Poisson Regressive Analysis function. In the second process (i.e. second hidden layer), a novel sensing mechanism based on discrete logarithm function designed to examine a wideband spectrum with a high probability of detection rate employing Schnorr Signature Cryptographic is proposed. Finally with high detection results are sent to the output layer therefore ensuring secure data routing in CRN. The performance validation of RTSS-DBN method in CRN is discerned under distinct processes. The results of simulations described that the proposed RTSS-DBN method significantly addressed on data confidentiality rate, packet delivery ratio with reduced end-to-end delay and routing overhead, therefore ensuring robust security.

Author's e-mail: admin.sundar@gmail.com, senthilkumarmca76@gmail.com

How to cite this article: Sundar T, Senthilkumar A, Regressive Schnorr Signature Based Deep Belief For Secured Data Routing In Cognitive Radio Network, National Journal of Antennas and Propagation, Vol. 8, No. 2, 2026 (pp. 131-143).

1. INTRODUCTION

The emergence of 6G wireless communication guarantees enhancements in signal coverage, latency, data rates and so on. Secure routing protocols on the basis of optimization techniques have been designed over the past few decades to ensure reliable message delivery while sustaining high standards of security and privacy. Integrating cognitive radio with deep learning techniques has proven to be an efficient mechanism for generating secure communication channels.

A Reinforcement Learning-based Ensemble Regression (RL-ER) method was introduced in [1] to spectrum sensing along with channel state information prediction model employing MLP-KF. By combining Quantum Key Distribution with Public Key Infrastructure, robust dual layer authentication with improved prediction accuracy and minimal error rate was said to be established. In addition, by applying Quantum-Inspired Bat Optimization with Elliptic Curve ensured minimal encryption and decryption time. Despite improvements observed in terms of prediction accuracy, error rate with minimal

encryption/decryption time. But it didn't care about routing overhead or end-to-end latency. To concentrate on the end-to-end delay and routing overhead experienced in the routing of data, Poisson Regressive Trust-based Authentication is implemented in our study through Deep Belief Network through which by merely transmitting trusted classified nodes to the subsequent processing, goals are attained.

ODL-MUDSS in CRN In [2], It was suggested to use optimal deep learning to detect malicious users. The overall goal of ODL-MUDSS approach identified on automatic classification of the malicious users. Here too DBN was predetermined to allow precise identification of malicious users. In addition, authentication and intrusion rate recognition performance of DBN was enhanced using SCSSO algorithm and boosting the overall precision results. Though several performance improvements in terms of accuracy, authentication/intrusion rate along with computation time was ensured, however data confidentiality rate and packet delivery ratio was not concentrated. To address on the data confidentiality and improved packet delivery ratio Schnorr Signature Cryptography-based Secure Data Routing is designed that only ensuring authenticity between sender and receiver, achieves the objective

Repair based communication infrastructure with adjustable transmit rates of primary user packets in CRNs developed in [3]. In this case, PU packets were utilised to ensure recovery high-speed gearbox during system repair and low-speed gearbox during system breakdown. Also, a 3DMC and queuing model was designed to separate time for identifying system capability. The designed mechanism minimized the blocking rate and increased the throughput of data packets. Despite minimization of communication failure and ensuring repair in an advanced stage, the complexity level was not reduced.

An ideal attack approach was introduced in [4] covers both known and unknown fusion rule scenarios, in order to optimise the risk. Cooperative sensing's energy efficiency was increased by using a combinatorial optimisation approach. Additionally, by combining reinforcement learning and graph neural networks, a deep learning method was discovered to improve the system's energy efficiency. A good deal was however done in regard to the energy efficiency; the throughput was also not enhanced by ideal attack.

In [5], Multi-layer Hyper-Graph (MLHG) was utilized using modeling networks and flat graph model to generate large graph size. Each group of CR devices represented by a hyper-edge and each layer represented the approved channel. The MLHG was employed to optimize the end-to-end network throughput, transmission rate, licensed users activity, jammers activity and times sharing. There was, however, a failure to minimize the computational complexity.

In, security minded robust resource allocation was constructed where energy harvesting cognitive radio networks between two transmitters in the channel gains and battery energy value are studied [6]. Utilising a time-switching protocol, the primary entry point used green resource energy to transmit data and energy to SAP. By using the power-domain non-orthogonal multiple access approach, SAP has enhanced the primary network's security of data transmission by primary network frequency band. Nevertheless, there was no decrease in the computation's cost.

CRNs are anticipated to play a main function towards encountering the mushrooming traffic requirement more than wireless systems. For real-time process, CR is specially integrated with AI and ML algorithms with aim of allocating in an intelligent fashion. In [7], A survey of the most advanced machine learning approaches in CRs is created. A survey of spectrum access security exploiting blockchain was presented in [8]. An overview of secure federated learning mechanisms for CRN was investigated in [9]. CRNs integrate features of both ad-hoc networks with CRs to no difficulty diverse types of communication scenarios. However, these networks are dependent to repeated attacks both from internal and external adversaries. The DL methods contributed to answer these attacks but bear from lack of network scalability and complexity. As a result, their constrained IP tracing potentialities make them unsuitable for real-time organization.

A review imparting perception into prospective solutions that can be of service to the foundation for evolution of future B5G/6G services was investigated in [10]. A systematic literature review on CRN and ML techniques towards spectrum sensing and security aspects were presented in [11]. Yet another security constraint mechanism was addressed in [12] employing particle swarm and continuous genetic algorithm. To ensure high spectrum sensing and security process performance, careful consideration should be given to the selection of a suitable sensing matrix and recovery method.

A novel chaotic compressive spectrum sensing (CSS) mechanism was designed in [13] to mutual CRNs because of Chebyshev sensing matrix and Bayesian recovery by Laplace prior to give both secure and reliable spectrum recognition. Despite improvement observed in terms of security and detection rate, however, packet collision ratio was not focused. To address on this aspect, an optimal channel selection method using Q-learning was proposed in [14] in concurrence with clustering algorithm. This in turn not only ensured packet delivery ratio but also reduced packet collision rate substantially. By, the packet delivery ratio and packet collision rate were improved. But security was failed to ensured.

A blockchain mechanism for ensuring security employing deep convolution neural network (dCNN) was presented in [15]. With this dNN not only reduced the communication delay but also enhanced security extensively. To sum the discussion, despite several methods were involved in secure data routing in cognitive radio network systems, these methods lack in detecting data confidentiality rate with minimal routing overhead. It is further noted that procedures that utilized DL methods falters at generating improved PDR and minimum end-to-end delay.

The motivation of research work by proposing a secure data routing method employing deep learning called Regressive Trust-aware Schnorr Signature based Deep Belief Network (RTSS-DBN) in CRN. This effectively achieved the end-to-end delay and data confidentiality by only distribution the trusted classified nodes for data routing and facilitate enhanced packet delivery ratio with minimal routing overhead based on a discrete logarithm function by ensuring authenticity between sender and receiver. The performance evaluation of RTSS-DBN method is determined under diverse measures. In summary; the major contributions of the learn are listed as follows.

- To develop a RTSS-DBN method for conducting secure data routing using an authentication mechanism to perceive the malicious CR users and remove them in ending sensing decision process and design high probability of detection rate via Deep Belief Network.
- To perform authentication process employing Poisson Regressive Analysis function based on a secure linear sensing model, therefore guarantee the better packet delivery ratio and minimum end-to-end delay.
- To execute Schnorr Signature Cryptographic mechanism based on a discrete logarithm function for performing authenticity between sender and receiver and then proceeding with data routing between them, therefore, reducing end-to-end delay and improving data confidentiality.
- To assess the efficiency of the proposed RTSS-DBN technique by assessing the main metrics such as the end-to-end delay reduction, improved data confidentiality, improved packet delivery ratio, and reduced routing overhead.

1.1 Paper Organization

In the present work, the paper is organized based on methods involved in identifying secure data routing by using efficient DL techniques. While, research on traditional methods together with their outcomes obtained is done on related domain with different methods and research gaps are also presented in Section 2. Moreover, section 3 suggests materials and methodology executed in the proposed Regressive Trust-aware Schnorr Signature based Deep Belief

Network (RTSS-DBN) in CRN. In section 4, the results achieved by proposed RTSS-DBN method are discussed. The comparative analysis of existing methods with proposed method described in Section 5. Finally, the conclusion of the proposed RTSS-DBN method is provided in Section 6.

2. RELATED WORKS

Security in the physical layer is one of the most paramount aspects as far as cognitive radio networks (CRNs) are concerned owing to energy of spectrum access which stretches out to questions of defensive receptive information. Leading comparison to established methods of encryption used on higher layers, security in physical layer uses certain essential wireless channel features. It makes certain to signals cannot be decoded even when they have been episodic via eavesdropper.

To ensure secure communication with energy-efficient mechanism, an energy consumption model via collaborative spectrum sensing with reduced energy utilization and improved throughput was proposed in [16]. Yet another method to provide security employing two-level shared key authentication mechanism was designed in [17] for CRN. Here, only based on the common authentication among main and minor users greatest capacity channel was shared with better secrecy. But, the congestion failed to focus. To address this problem, [18] proposed an Optimized Energy Efficient Secure Routing Protocol to guarantee improved throughput.

Wireless communication based on CRNs is organized with the intent of selecting the most pertinent channel between accessible alternatives with the objective of optimizing spectrum resource usage. Nevertheless, spectrum sharing in CR network has a number of drawbacks and hence data transmissions are susceptible to security attacks due to the reason that licensed and unlicensed users sharing same network.

In [19], An energy efficient Deep Belief Network routing protocol, which is aimed at improving the transmission of data across the path chosen. Also, for effective data communication, an optimization method employing Mantaray Foraging Optimization (MRFO) algorithm was presented to improve packet delivery rate. A review of methods to mitigate security threats employing DL method was described in [20]. A hybrid integration of ML and DL employing LSTM and ELM for achieving temporal features from spectral data and to develop energy, distance for better sensing performance was investigated in [21].

In [22], dynamic radiospectrum management by taking into consideration the multi-criteria algorithm for provide security and QoS of secondary user's usage was achieved. Here, a multi-agent system model obtaining autonomous learning and focus on a spirited

cognitive environment was considered with developed security. But, throughput of data packets was not concentrated. To achieve on this aspect, a three-dimensional Markov chain was designed in [23] with adjustable transmission rate. In [24], A motion-optimization-based, traffic-driven clustering routing scheme was developed to minimize the energy that is used during routing. Allocation of spectrum in an arbitrary fashion permits secondary users (SU) to access frequency band for transmission in a temporary fashion by detecting spectrum hole when authorized primary user (PU) is not utilizing authorized frequency band. Nevertheless, cooperative spectrum sensing also new security problems, to name a few being, data falsification, PU emulation attacks, channel blockings and so on. A Multi-layer Hyper-Graph for improved throughput with secured routing was designed in [25]. A holistic survey of data privacy and security concerns for processing large amounts of data was investigated in [26].

With the objective of addressing the issues of shortage occurring in spectrum resource, a district autonomous security cooperative spectrum sensing process utilizing trust value as a major factor was designed in [27] in cognitive radio to recognize malicious node attacks. Yet another chicken swarm optimization method for focusing on the probability of detection rate was designed in [28]. In [29], a secure routing model based

on trust factor was introduced by using route decision algorithms. Distributed reinforcement learning was applied in [30] for allocating spectrum in an arbitrary fashion.

3. METHODOLOGY

Cognitive Radio Networks (CRNs) are utilized whenever there arises a requirement for selecting intelligent channel. Employing CR the trans-receiver transmits the examine the signals on CRN to confirm if the network is free or not. Upon successful completion of the scan process, secure data routing is designed on network. To various guarantee secure data routing state-of-the-art methods are proposed to optimize prediction accuracy, precision with minimal computation and encryption/decryption time. As optimizing these different metrics, there is positive security loop holes created in CRNs. Owing to these onwards loop holes, data routing capabilities of CR nodes get precious as malicious users authority unacceptable signatures therefore compromising the entire network. This work presents a secure deep learning-based routing process in CRN, referred to as Regressive Trust-aware Schnorr Signature-based Deep Belief Network (RTSS-DBN), to deal with these problems. Figure 1 shows the design of the RTSS-DBN approach.

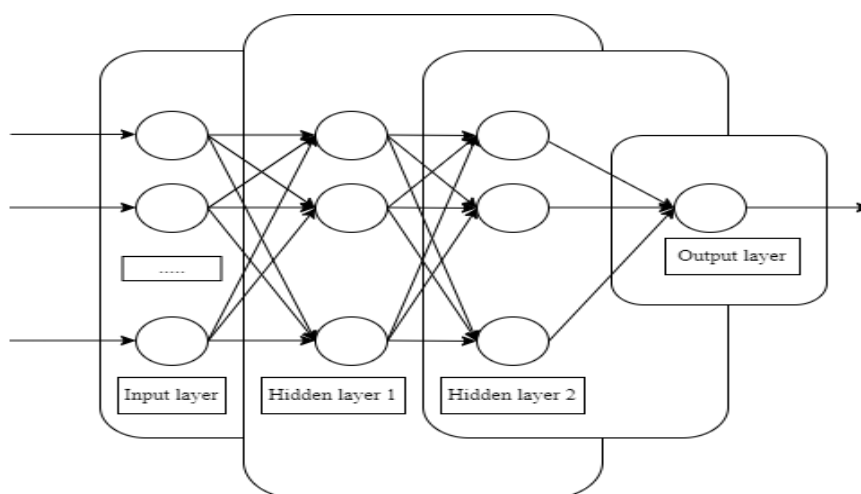


Fig. 1. Structure of RTSS-DBN method

From above figure 1, the RTSS-DBN method is split into three layers for secure data routing in CRN. Different numbers of cognitive users are considered as input in the input layer. Followed by which different numbers of cognitive users are sent to first hidden layer. In first hidden layer, Poisson Regressive Analysis is performed to categorize the cognitive user nodes into normal or malicious based on their behavior (i.e., trust value). After that the classified cognitive user nodes (i.e. normal/malicious) are sent to the second hidden layer. In the second hidden layer Schnorr Signature Cryptographic Data Transfer is performed with normal

sensor nodes to enhance the data routing security via key generation, signing and verification process. Finally secure data routing between cognitive user nodes are said to be ensured.

3.1 System model of Secured Data Routing in CRN

Figure 2 given below shows the system model followed for secured data routing in CRN including ' m ' primary user's symbolized as ' $PU = \{PU_1, PU_2, \dots, PU_m\}$ ' and ' n ' is denotes the secondary users ' $SU = \{SU_1, SU_2, \dots, SU_n\}$ ' respectively.

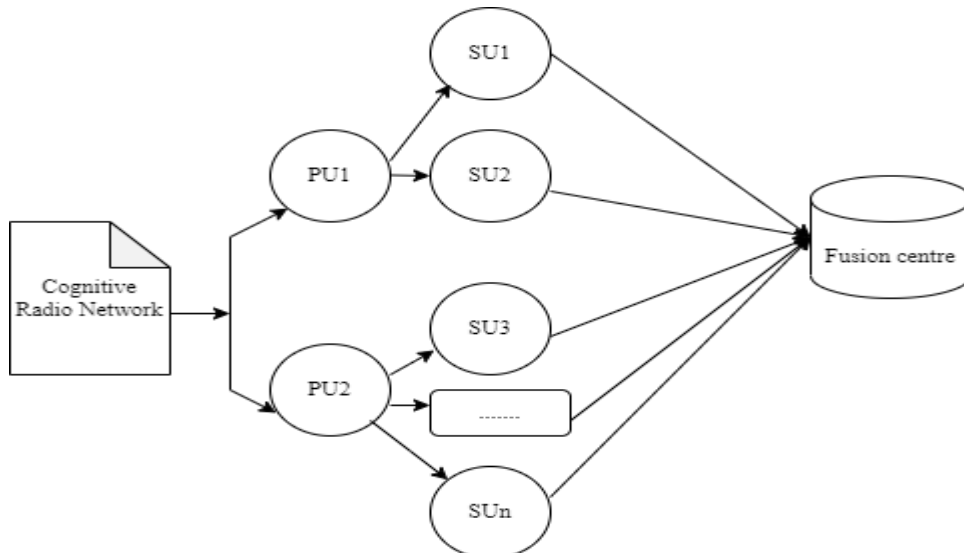


Fig. 2. System models of secured data routing in CRN

Above figure 2, described in the system model two primary users and secondary users are connected to a fusion center to structure secure data routing in CRN. The primary user ‘PU’ is appropriated to broad-band channel involves the ‘L’ non-overlapping frequency bands $\{f_1, f_2, \dots, f_l\}$. Let $H_{1,l}^{PU}$ and $H_{0,l}^{PU}$ signified as the hypothesis that ‘l – th’ frequency band is engaged by primary user ‘PU’ and ‘l – th’ frequency band is obtainable for secondary user ‘SU_j’. The secure data routing is performed to over common fusion center ‘FC’. Here two different phases are involved in the design of secure data routing, i.e., local spectrum sensing (LSS) phase and energy-efficient scheduling (EES) phase respectively. The channel gains for LSS links ‘PU_i → SU_j’ and EES links ‘SU_j → FC’ are denoted by $h_{P_i S_j}$ and $h_{S_j F}$ correspondingly.

3.2 Local spectrum sensing and Energy-efficient scheduling

To start with, cognitive radio nodes along with Local spectrum sensing (LSS) phase and Energy-efficient scheduling (EES) phase are considered as input in the input layer.

3.2.1 Local spectrum sensing (LSS) phase

After formation of SUs into group with each SU assigned with a specific frequency channel, every SU carried the local spectrum sensing (LSS) on its assigned channels. Over the LSS channel the received signal at ‘SU_j’ is formulated as,

$$Rec_i^{LSS} = h_{P_i S_j} SV + \varepsilon_i^{LSS}$$

In equation (1) ‘SV’, is the transmitted signal vector from the ‘PU’ primary user and ε_i^{LSS} is symbolized the noise vector at secondary user ‘SU_j’ over the LSS channel.

3.2.2 Energy-efficient scheduling (EES) phase

Second with the completion of LSS phase, SUs are planned to carry out the sensing in a time-division way with energy-efficient scheduling. With aim of detailing the accessibility of frequency bands within transmission range of ‘PU’, let us describe a SIR of length ‘L’, where bits ‘0’ and ‘1’ is frequency band being utilized and frequency band being offered. Let assume they represent two energy thresholds ‘ $E_{1,i}(l)$ ’ and ‘ $E_{2,i}(l)$ ’ where ‘ $E_{1,i}(l) < E_{2,i}(l)$ ’. Furthermore ‘ SIR_i^{LSS} ’ denote the SIR measured at ‘SU_j’ over the LSS channel ‘ $h_{P_i S_j}$ ’. Then, Energy-efficient scheduling (EES) phase for the ‘l – th’ element of ‘ SIR_i^{LSS} ’ is mathematically stated as given below.

$$SIR_i^{LSS}[l] = \begin{cases} 0, & \text{if } [Rec_i^{LSS}[l]] \geq E_{2,i}(l) \rightarrow h_{1,l}^{SU_j} \\ 1, & \text{if } [Rec_i^{LSS}[l]] < E_{1,i}(l) \rightarrow h_{0,l}^{SU_j} \\ \varphi [Rec_i^{LSS}[l]], & \text{otherwise} \end{cases} \quad (2)$$

From the above equation (2) ‘ $\varphi[.]$ ’ denotes the energy estimation of an observed signal that is being forwarded to the fusion center for further processing.

Dissolving the security issue in CRN and in the process of trying to improve data confidentiality, we suggest two new processes: an authentication process and a shifted spectrum sensing process, to be carried out in a two-layer concealment, which data is being transferred safely.

3.3 Poisson Regressive Trust-based Authentication

Poisson Regressive CRN designed with ‘i’ nodes classified into ‘X’ normal nodes (SUs) and ‘Y’ MUs, which assist with a fusion center ‘FC’ to carry out the spectrum sensing process in the first hidden layer. Previous to arriving at final decision pertaining to

spectrum occupation, all CRN users, comprising SUs and MUs, at first performed an authentication process based on Poisson Regressive Analysis, to verify their reliability. After that, once the following FC has achieved its classification, every user is either known as a trusted user or malicious user and the classified nodes are sent to the second hidden layer. Figure 3 given below shows the flow diagram of Poisson Regressive Trust-based Authentication model.

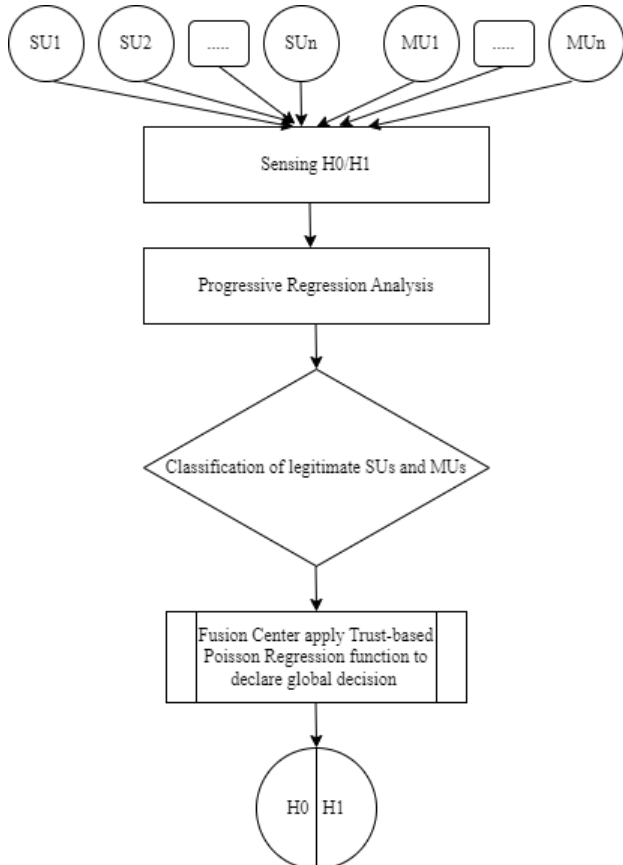


Fig. 3. Flow diagram of Poisson Regressive Trust-based Authentication

As illustrated in the above figure with the presence of secondary users SUs and malicious users MUs a Poisson Regressive Trust-based Authentication model is applied according to the frequency band presence ‘ H_1 ’ or frequency band absence ‘ H_0 ’. Followed by which classification of legitimate SUs and malicious MUs are performed according to the trustworthiness of node. Finally, the fusion centre applies Poisson Regressive Analysis function to declare global decision regarding the classified normal and malicious nodes.

For primary trust evaluation, a SU node obtains information regarding its adjacent nodes’ behavior pertaining to a designated task. The trustworthiness of the adjacent nodes’ is obtained in terms of the rate at which packets are forwarded by them. Let ‘ $U_{i,j}^l$ ’, ‘ $V_{i,j}^l$ ’ is the number of packets forwarded from SU ‘ i ’ to ‘ j ’ with additionally from SU ‘ j ’ to its consecutive adjacent nodes’ at time instance ‘ t_i ’ respectively.

$$PT_{i,j}^l = \frac{U_{i,j}^l}{V_{i,j}^l} \tag{3}$$

From the above equation (3), the primary trust value, ‘ $PT_{i,j}^l$ ’ measured by node ‘ i ’ for its adjacent node ‘ j ’ on the basis of node ‘ i ’ scrutiny at time instance ‘ t_i ’. In the midst of inadequate information exchange between nodes, secondary trust measurement parallel to primary trust aids the accuracy by increasing the accuracy of trust evaluation. With the assumption that the total number of adjacent nodes are ‘ $AN_{i,j}$ ’, then the secondary trust measured by ‘ SU_i ’ for ‘ SU_j ’ at time instance ‘ t_i ’ is obtained as given below.

$$ST_{i,j}^l = \frac{\sum_{z=1}^{AN_{i,j}} PT_{z,j}^l}{AN_{i,j}} \tag{4}$$

From the above equation (4) the secondary trust value ‘ $ST_{i,j}^l$ ’ is measured by taking into considerations the primary trust value results ‘ $PT_{z,j}^l$ ’ and the corresponding adjacent nodes are ‘ $AN_{i,j}$ ’ respectively. Then employing the primary trust results and the secondary trust results the overall trust value based on the behavior is obtained as given below.

$$T_{i,j}^l = PT_{i,j}^l + ST_{i,j}^l \tag{5}$$

Finally by employing a secure linear sensing model using the Poisson Regressive Analysis function trustworthiness is established where malicious are eliminated them in the final sensing decision. The Poisson Regressive Analysis function to detect malicious user is calculated as,

$$Prob_{t_i} [k] = \frac{e^{-\lambda t_i} (\lambda t_i)^k}{k!} \tag{6}$$

In equation (6), the probability of seeking ‘ k ’ trustworthiness of secondary users in time ‘ t ’, is calculated by taking into thought event rate ‘ λ ’ (i.e. number of secondary users per unit time) and total event rate ‘ k ’ (i.e. overall number of secondary users for simulation) respectively.

3.4 Schnorr Signature Cryptography-based Secure Data Routing

Finally, the proposed method secures routing requests and reply messages by encrypting them using the Schnorr Signature Cryptographic technique for each classified trusted user. The proposed technique is designed in such a manner so as to maximize security level of routes for each classified trusted user via second hidden layer. In the second process (i.e. second hidden layer), a novel sensing mechanism based on a discrete logarithm function to scan a wideband spectrum for each classified trusted user with a high probability of detection rate employing Schnorr Signature Cryptographic is

designed. By employing Schnorr Signature Cryptographic technique the packet for each classified trusted user is routed through a network while safeguarding it from attacks by only ensuring authenticity of replies. To be more specific by only ensuring authenticity of request and replies between trusted users (i.e. sender/receiver) packets are routed securely using Schnorr Signature Cryptographic technique in CRN. The Schnorr Signature Cryptographic-based secured data routing being a digital signature ‘ $DS = (KG, Sig, Ver)$ ’ comprises of three processes, namely, key generation, signing and verification.

3.4.1 Key Generation

In Key Generation ‘ KG ’ process a pair of public key and secure keys are generated for each classified trusted user ‘SUs’ on the basis of the security parameter input ‘ $1z$ ’. On one hand the public key ‘ $PubK$ ’ is aired on an open channel whereas the secret key or private key ‘ $PrivK$ ’ is kept secret by the classified trusted user ‘SUs’ or cognitive user. Let us select a generator ‘ $Gen \leftarrow \mathbb{G}[Arb]$ ’ and generate arbitrary value ‘ $rnd \leftarrow \mathbb{Z}_q^*[Arb]$ ’. Then, adjust ‘ $x_1 = Gen^{rnd}$ ’ and ‘ $x_2 = x_1^{rnd}$ ’ and select hash function along with the public and secret or private key as given below.

$$H: \{0,1\}^* * \mathbb{G} * \mathbb{G} \rightarrow \mathbb{Z}_q \tag{7}$$

$$PubK \rightarrow (Gen, x_1, x_2) \tag{8}$$

$$PrivK \rightarrow (rnd) \tag{9}$$

From the above equations (7), (8) and (9), secret key or private key ‘ $PrivK$ ’ is retained by the classified trusted user ‘SUs’ while the public key is symbolized as ‘ $PubK$ ’ is used for further processing.

3.4.2 Signing

Following the key generation process, the classified trusted sender user ‘SUs’ encrypts the packet ‘ DP ’ by using classified trusted receiver user public key. Given a packet ‘ $DP \in \{0,1\}^*$ ’ and secret key or private key ‘ $PrivK$ ’ as input, a random salt (i.e. in addition to hash function a password is included to defend against

attacks) ‘ $RS \leftarrow \mathbb{Z}_q^*$ ’. Then, following functions are evaluated to generate digital signature.

$$P = Gen^{RS} \tag{10}$$

$$Q = x_1^{RS} \tag{11}$$

$$f = H(P, Q, DP) \tag{12}$$

$$Sign = (rndf + RS) \tag{13}$$

Finally, with the above intermediate functions according to (10), (11), (12) and (13), the digital signature is generated a given below.

$$\sigma = (f, Sig) \tag{14}$$

With the above generated digital signature along with the packet, the classified trusted sender user sends it to the receiver through intermediate node.

3.4.3 Verification

Finally in the verification process, the receiver node by only ensuring authenticity of reply decrypt the cipher packet and obtain the original packet. To verify digital signature ‘ $\sigma = (c, Sig)$ ’ of a packet ‘ DP ’ the following intervening functions are evaluated.

$$P' = Gen^{Sig} x_1^{-f} \tag{15}$$

$$Q' = x_1^{Sig} x_2^{-f} \tag{16}$$

In the end, the validity or verification is performed using digital signature to ensure authenticity of replies by the receiver node as given below.

$$H(P', Q', DP) \equiv f \tag{17}$$

From the above equation (17) only upon the successful validity, secured data routing is ensured via second hidden layer. Finally high detection results are sent to the output layer therefore ensuring secure data routing in CRN. This in turn ensures secured data routing at the output layer in CRN. The pseudo code representation of a Regressive Trust-aware Schnorr Signature based Deep Belief Network (RTSS-DBN) secure data routing method employing deep learning in CRN is given below.

Algorithm 1: Regressive Trust-aware Schnorr Signature based Deep Belief Network (RTSS-DBN) secure data routing

```

1: Initialize Primary Users 'PU = PU1, PU2, ..., PUm', Secondary Users 'SU = SU1, SU2, ..., SUn', 'm = 10', 'n = 100'
//Input layer
2: Formulate local spectrum sensing (LSS) according to (1)
3: Formulate energy-efficient scheduling (EES) according to (2)
//First hidden layer
4: Evaluate primary trust evaluation according to (3)
5: Evaluate secondary trust evaluation according to (4)
6: Evaluate overall trust value according to (5)
7: Compute Poisson Regressive Analysis function to detect malicious user according to (6)
8: Return normal users 'SU' and discard malicious users 'MU'
//Second hidden layer
9: For each normal users 'SU'
//Key Generation
10: Generate hash function according to (7)
11: Generate public key according to (8)
12: Generate private key according to (9)
//Signing
13: Generate intermediate functions according to (10), (11), (12) and (13)
14: Generate digital signature according to (14)
//Verification
15: Generate intervening functions according to (15) and (16)
16: If 'H(P, Q, DP) ≡ f'
17: Then authenticity successful
18: Go to step 24
19: Else
20: Authenticity is failed
21: Proceed with other set of cognitive users
22: End if
23: End for
//Output layer
24: Secure data routing between sender and receiver

```

As given in the above algorithm, a secure data routing in CRN, a pseudo code representation of sending packet across network while safeguarding it from attacks by ensuring its authenticity is presented. The entire pseudo code representation is separated into two sections, each consisting of four separate levels: an input layer, two hidden layers, and an output layer. The input layer of the simulation parameters listed in table 1 is initially acquired. Next, in the first hidden layer, Poisson Regressive Trust-based Authentication is carried out to confirm the reliability of users and based on the trust each user is either recognized as a trusted user or malicious user and the classified nodes are sent to the second hidden layer for further processing. In this way by only sending the trusted classified nodes for further processing, the end-to-end delay and data confidentiality rate is developed. Following which in the second hidden layer, Schnorr Signature Cryptography-based Secure Data Routing is conducted wherein the trusted user is permitted to initiate with the data routing process. Here, based on a discrete logarithm function to scan a wideband

spectrum only ensuring the authenticity between the sender and receiver data routing is accomplished between them. This in turn improves the packet delivery ratio with minimal routing overhead.

4. EXPERIMENTAL ANALYSIS

The experimental evaluation of proposed ELSTM-RPO method for the CRN generated using NS-3 simulation software. The total number of iterations is 50, and the population size or number of users is assumed to be 50. Reinforcement Learning-based Ensemble Regression (RL-ER), one of the few current methodologies, is compared to the suggested method [1]. and the Best Malicious User Detection for Spectrum Sensing Using Deep Learning (ODL-MUDSS) [2] in terms of different analyses such as authentication rate, data confidentiality rate, intrusion rate, and encryption/decryption time to establish the superiority of the developed method. The simulation parameters are provided in table.

Table 1 Simulation parameters

S. No	Parameters	Values
1	Simulation area	1000m*1000m
2	Number of secondary users	100
3	Number of primary users	10
4	Maximum node speed	10 m/sec
5	Total number of CR channels	8
6	Mobility model	Random mobility
7	Data rate	2 Mbps
8	Packet size	512 bytes
9	Simulation time	100sec
10	Number of iterations	10

5. Performance evaluation

Three algorithms, RTSS-DBN, RL-ER [1], and ODL-MUDSS [2] are used to simulate the proposed secure data routing algorithm. Its performance is then compared to the two other data routing algorithms on several metrics. Data confidentiality is a measure of how secure data packet is routed in CRN, while packet delivery ratio is a measure of how reliably data packets are routed in CRN. Here secure data packet routed refers to protecting against malicious users whereas reliable data packets focus on consistently performing data routing without taking into consideration the malicious user intent.

5.1 Inferences

Spectrum sensing is critical: Accurate detection of presence of primary user is significant in identifying available spectrum holes that are crucial for secure data routing in a CRN. By employing Poisson Regressive Trust-based Authentication mechanism via Deep Belief Network in the proposed RTSS-DBN method, aids in addressing end-to-end delay and data confidentiality rate in a significant manner.

To protect data confidentiality, Schnorr Signature Cryptography mechanism is applied, while authentication mechanisms are designed in validating and analyzing the legitimacy of communicating nodes (i.e. cognitive sender and cognitive receiver nodes) within the network.

Trust management: Also identifying and circumventing probable malicious nodes or malicious users is critical for secure data routing, is achieved through trust management mechanisms (i.e., primary trust and secondary trust) that evaluate node behavior prior to the secure data routing process, therefore improving packet delivery ratio with minimal routing overhead.

5.2 Data confidentiality rate

Data confidentiality rate is evaluated to engage in analysis of low risk data routing in CRN. It is mathematically formulated as,

$$CR = \sum_{i=1}^N \frac{DP_{AAD}}{DP_i} * 100$$

From the above equation (18) the data confidentiality or confidentiality rate 'CR' is measured by taking into considerations the data packets involved in simulation process 'DP_i' and the number of data packets accessed by authenticated cognitive users 'DP_{ACU}'. CR is measured in percentage (%), advanced the data confidentiality or confidentiality rate better the efficiency of the method is said to be. Table 2 shows the data confidentiality rate of the proposed and existing methods. From Table 2, the proposed RTSS-DBN method data confidentiality rate for 50 data packets in 96%, which is significantly higher compared to the existing RL-ER [1] (88%), ODL-MUDSS [2] (82%). Therefore, it is clear to propose the RTSS-DBN method outperforms other conventional methods in data confidentiality rate.

Table 2 Comparative analysis of proposed RTSS-DBN method based on data confidentiality rate

Data packets	Data confidentiality rate (%)		
	RTSS-DBN	RL-ER [1]	ODL-MUDSS [2]
50	96	88	82
100	93.15	85.25	80.35
150	92	84.35	80
200	90.35	82.15	78
250	90	82	78.15
300	90.55	82.35	79
350	92	84.55	80
400	93.15	85.15	81.35
450	94.25	87	82
500	95	89	85

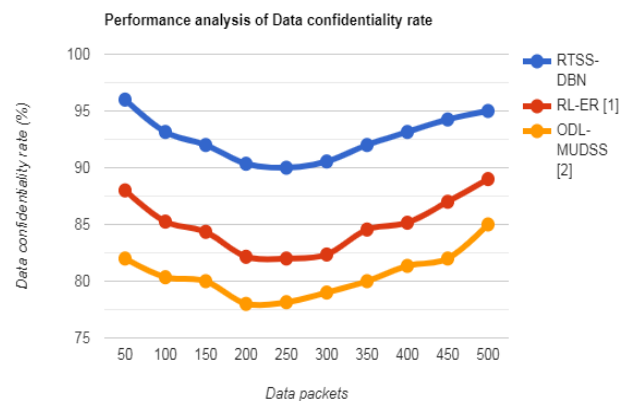


Fig. 4. Performance measurement based on data confidentiality rate

In figure 4, describe the compares our proposed RTSS-DBN method with RL-ER [1] and ODL-MUDSS [2]. It is obvious from figure to data confidentiality rate reduces when more data packets are present in network for being routed. However, the data confidentiality rate in the proposed RTSS-DBN method is better than that of the with RL-ER [1] and ODL-MUDSS [2] because the routes contain only trusted users whereas malicious users to have lower belief level are debarred. The reason due to the improvement in data confidentiality rate can be contributed to the authentication process followed employing Poisson Regressive Analysis. Only upon confirming with the reliability via primary and secondary trust value, authentication is ensured. This in turn improves overall data confidentiality using RTSS-DBN method by 9% and 15% compared to [1],[2].

5.3 Impact of End-to-end delay

End-to-end delay is defined as the total time taken by a packet to reach the destination node after being sent by the source node. A more precise measurement of end-to-end delay is used to determine the time required for all packets to reach the destination. The end-to-end delay is calculated as follows:

$$E2E = T_{i\ End} - T_{i\ Start}$$

In equation (19), the 'E2E' denotes the end-to-end delay based on end time it takes for a packet to receive destination 'T_{i End}' and start time it takes for a packet to propagate 'T_{i Start}'. It is measured in terms of seconds (sec). From Table 3, proposed RTSS-DBN method demonstrates a more efficient end-to-end delay process, taking only 5.35 sec to ensure secure data routing, with RL-ER [1] taking 7.16 sec and ODL-MUDSS [2], requiring 8.45sec.

Table 3 Comparative analysis of proposed RTSS-DBN method based on end-to-end delay

Number of users	End-to-end delay (sec)		
	RTSS-DBN	RL-ER [1]	ODL-MUDSS [2]
5	5.35	7.15	8.45
10	7.25	12.15	17.35
15	9	14.35	19.15
20	11.35	16.85	21.35
25	13	18.35	23.55
30	14.15	19.25	24.52
35	13.35	18.55	23.55
40	11	16.15	21.25
45	10.15	15.35	20.55
50	12	17	23.25

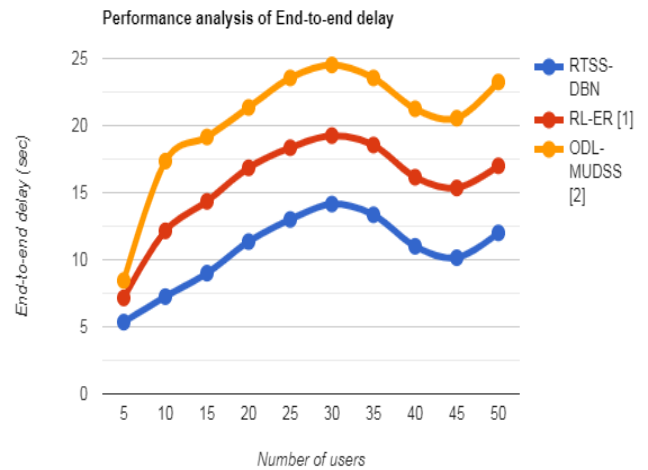


Fig. 5. Performance measurement based on end-to-end delay

In figure 5, represent the end-to-end delay in our proposed RTSS-DBN method and two existing methods, RL-ER [1] and ODL-MUDSS [2]. It is described that relationship between E2E and number of users in CRN is neither a contrary relation nor way relation. In other words, as the number of users improves, the E2E neither improve nor reduce in all three different methods. But, in our proposed RTSS-DBN method minimizes more than [1] and [2]. Consequently, our proposed secure data routing algorithm better than [1] and [2]. The end-to-end delay is improved by up to 9% and 15% upon comparison to [1], [2]. This is because of the end-to-end delay minimizes is having more SUs or users improves the chance of having more routes, hence, the data packets will be securely re-routed if one route is hidden. Also, by applying the Poisson Regressive Trust-based Authentication model in the first hidden layer, only the trusted classified nodes are sent to the second hidden layer for further processing. In this way by only sending the trusted classified nodes for further processing reduces the E2E in a significant manner.

5.4 Analysis of Packet delivery ratio

Ratio between packet delivery to the destination node and the packets generated by the source node is referred to as the packet delivery ratio. It is formulated as,

$$PDR = \frac{DP_{recvd}}{DP_{sent}} * 100$$

From equation (20), the 'PDR' is denotes the packet delivery ratio based on percentage ratio of packet sent 'DP_{sent}' to the packet received 'DP_{recvd}'. PDR is measured in percentage (%). From below Table 4, provides a comparison of the packet delivery ratio between the RTSS-DBN and existing methods, [1] and

[2]. The data clearly indicates that RTSS-DBN method consistently outperforms RL-ER [1] and ODL-MUDSS [2], not only in data confidentiality rate but also in packet delivery ratio also.

Table 4 Comparative analysis of proposed RTSS-DBN method based on packet delivery ratio

Data packets	Packet delivery ratio (%)		
	RTSS-DBN	RL-ER [1]	ODL-MUDSS [2]
50	90	80	76
100	87	78	70
150	83	76	68
200	82	75	67
250	80	73	65
300	80	73	65
350	82	75	67
400	84	79	71
450	85	80	72
500	88	81	73

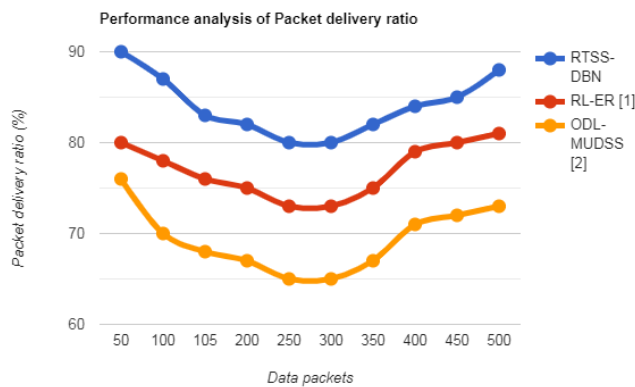


Fig. 6. Performance measurement based on packet delivery ratio

Figure 6 compares the packet delivery ratio (PDR) of the proposed RTSS-DBN method with two existing methods, RL-ER [1] and ODL-MUDSS [2]. The relationship between PDR and the number of data packets in the network is non-linear. Specifically, the PDR decreases as the number of data packets increases from 50 to 250, but it improves when the number of packets increases further from 300 to 500, due to the availability of multiple routing paths. Overall, the RTSS-DBN method achieves a higher packet delivery ratio compared to the other methods. It can reach up to 90% using RTSS-DBN method whereas reaches to 80% using [1] and 76% using [2] respectively. From this result the packet delivery ratio proved to be better using RTSS-DBN than [1] and [2]. The reason would be contributed to be application of Schnorr Signature Cryptography-based Secure Data Routing algorithm. By applying this algorithm only upon successful authenticity among the sender and

receiver based on separate logarithm function secure data routing was ensured. The packet delivery ratio using proposed RTSS-DBN method is improved by 9% and 21% compared to [1] and [2].

5.5 Routing overhead

It is a ratio of the amount of routing packets to the total amount of packets transmitted through the network. In other words, routing overhead is a performance metric to evaluate significantly a routing protocol utilizes control traffic proportionate to data traffic. It's brought about by the requirement to send additional control packets with the objective to ensure that data packets are delivered successfully.

$$RO = \frac{DP_{RC}}{DP}$$

From (21), the RO formulate for measuring routing overhead in CRN is the total number of routing control packets ' DP_{RC} ' to total number of data packets ' DP '. Finally, table 5 given below lists the routing overhead incurred during the process of secure data routing in CRN.

Table 5 Comparative analysis of proposed RTSS-DBN method based on routing overhead

Number of available channels	Routing overhead (%)		
	RTSS-DBN	RL-ER [1]	ODL-MUDSS [2]
1	0.65	0.75	0.83
2	0.63	0.72	0.8
3	0.62	0.71	0.79
4	0.61	0.7	0.78
5	0.69	0.78	0.86
6	0.59	0.68	0.76
7	0.56	0.65	0.74
8	0.51	0.6	0.68
9	0.46	0.55	0.63
10	0.43	0.52	0.6

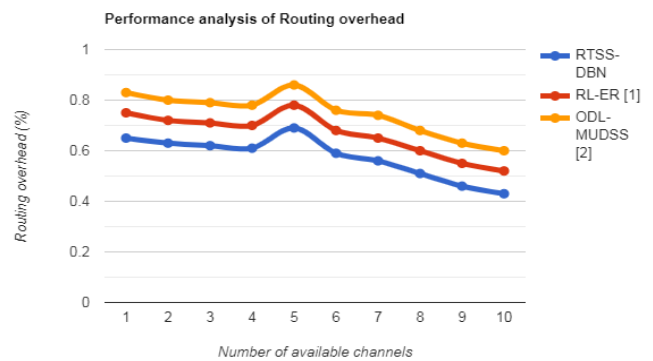


Fig. 7. Performance measurement based on routing overhead

Figure 7 illustrates the routing overhead of the proposed RTSS-DBN method compared with RL-ER [1] and ODL-MUDSS [2]. Routing overhead is measured as the ratio of routing packets to the total number of available channels in the network. As cognitive users gain access to more channels for sending data routing requests, the routing overhead decreases. Although the routing overhead generally reduces with an increasing number of available channels, the proposed RTSS-DBN method consistently maintains a lower overhead compared to RL-ER [1] and ODL-MUDSS [2], demonstrating its efficiency in managing network resources. The reason would be contributed to the application of Schnorr Signature Cryptography mechanism. By applying this mechanism in the second hidden layer of deep belief network the packet for each classified trusted user were routed via a network while safeguarding it from attacks by only ensuring authenticity of replies. The RTSS-DBN method using reduced routing overhead by 14% and 23% compared to [1] and [2]

6. CONCLUSION

A proposed secure data routing method in cognitive radio network using deep learning called, Deep Belief Neural Network (RTSS-DBN) is proposed in such a way that the data confidentiality rate and packet delivery ratio are enhanced with lesser end-to-end delay and routing overhead. First, Local spectrum sensing (LSS) phase and Energy-efficient scheduling (EES) phase were carried out and provided as input in the input layer. Next, an authentication mechanism employing Poisson Regressive Analysis was carried out and according to the trustworthiness of node, trusted users were sent for further processing whereas the malicious users were discarded. Finally, with the classified trusted users data routing process were initiated and then validated employing Schnorr Signature Cryptographic technique wherein classified trusted user were routed via a network while safeguarding it from attacks and only upon successful authenticity of replies ensured routing. It is delegated in simulation outcomes to maximum probability of data confidentiality rate and minimum routing overhead with optimal minimal end-to-end delay is achieved by proposed method.

REFERENCES

1. P. Deepanramkumar, A. Helen Sharmila, "AI-Enhanced Quantum-Secured IoT Communication Framework for 6G Cognitive Radio Networks", *IEEE Access*, Vol. 12, Oct 2024 [Reinforcement Learning-based Ensemble Regression (RL-ER)]
2. Latifah Almuqren, Mohammed Maray, Faiz Abdullah Alotaibi, Abdulrahman Alzahrani, Ahmed Mahmud, Mohammed Rizwanullah, "Optimal Deep Learning Empowered Malicious User Detection for Spectrum Sensing in Cognitive Radio Networks", *IEEE Access*, Vol. 12, Mar 2024 [Optimal Deep Learning Empowered
3. Malicious User Detection for Spectrum Sensing (ODL-MUDSS)
3. Yuan Zhao, Qi Lu, Zhisheng Ye and Kang Chen, "A communication failure and repair mechanism with adjustable transmission rates for PU packets in CRNs", *Heliyon*, Elsevier, Volume 9, 2023, Pages 1-13
4. Antoinette A and Buvanewari S, "Security and Energy Management in Cooperative Spectrum Sensing", *Procedia Computer Science*, Elsevier, Volume 230, 2023, Pages 716-724
5. Sharhabeel H. Alnabelsi, Haythem Bany Salameh, Ramzi R. Saifan and Khalid A. Darabkh, "A multi-layer hyper-graph routing with jamming-awareness for improved throughput in full-duplex cognitive radio networks", *Journal of King Saud University - Computer and Information Sciences*, Elsevier, Volume 34, Issue 8, Part A, September 2022, Pages 5318-5332
6. Saeed Sheikhzadeh, Mohsen Pourghasemian, Mohammad Reza Javan, Nader Mokari and Eduard A. Jorswieck, "AI-Based Secure NOMA and Cognitive Radio-Enabled Green Communications: Channel State Information and Battery Value Uncertainties", *IEEE Transactions on Green Communications and Networking*, Volume 6, Issue 2, June 2022, Pages 1037 - 1054
7. Nadine Abbas, Youssef Nasser, Karim El Ahmad, "Recent advances on artificial intelligence and learning techniques in cognitive radio networks", *EURASIP Journal on Wireless Communications and Networking*, Jun 2015
8. Nassmah Y. Al-Matari, Ammar T. Zahary, Asma A. Al-Sh, "A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks", *Scientific Reports*, Dec 2024
9. Matgorzata Wasilewska, Hanna Bogucka, and H. Vincent Poor, "Secure Federated Learning for Cognitive Radio Sensing", *IEEE Communications Magazine*, Vol. 61, Mar 2023
10. Senthil Kumar Jagatheesaperumal, Ijaz Ahmad, Marko Höyhty, Suleman Khan, Andrei Gurtov, "Deep learning frameworks for cognitive radio networks: Review and open research challenges", *Journal of Network and Computer Applications*, Elsevier, Vol. 233, Jan 2025
11. Mohd Yamani Idna Idrisa, Ismail Ahmedya, Tey Kok Soona, Muktar Yahuzaa, Abubakar Bello Tambuwald, Usman Alie, "Cognitive radio and machine learning modalities for enhancing the smart transportation system: A systematic literature review", *The Korean Institute of Communications and Information Sciences*, Vol. 10, Aug 2024
12. Van Nhan Vo, Viet-Hung Dang, Hung Tran, Dac-Binh Ha, Cong Le, Tu Dac Ho, Chakchai So-In, "Secondary Network Throughput Optimization of NOMA Cognitive Radio Networks Under Power and Secure Constraints", *IEEE Access*, Vol. 11, Apr 2023
13. Salma Benazzouza, Mohammed Ridouani, Fatima Salahdine, Aawatif Hayar, "Chaotic Compressive Spectrum Sensing Based on Chebyshev Map for Cognitive Radio Networks", *Symmetry*, MDPI, Mar 2021
14. Anushree Srivastava, Raghavendra Pal, Arun Prakash, Rajeev Tripathi, Nishu Gupta, Ahmed Alkhayat, "Optimal Channel Selection and Switching Using Q-Learning in Cognitive Radio Ad Hoc Networks", *IEEE Transactions on Consumer Electronics*, Vol. 70, No. 3, Aug 2024
15. Debabrata Dansana, Prafulla Kumar Behera, Abdulbasir A. Darem, Zubair Ashraf, Abu Taha Zamani, Mohammad

- Nadeem Ahmed, GoplaKrishna Patro, Mohammad Shahmeem, "BDDTPA: Blockchain-Driven Deep Traffic PatternAnalysis for Enhanced Security in Cognitive RadioAd-Hoc Networks", IEEE Access, Vol. 11, Sep 2023
16. Sally Elghamrawy, Alshimaa H. Ismail, Aboul Ella Hassanien, "Energy consumption optimization in greencognitive radio networks based on collaborativespectrum sensing", EURASIP Journal on WirelessCommunications and Networking, Sep 2024
 17. K. Saravanan, K. B. Gurumorthy, Allwin Devaraj Stalin, Om Prakash Kumar, "Secure channel estimation model for cognitive radio network physical layer security using two-level shared key authentication", Scientific Reports, Jan 2025
 18. RiptySingla, Navneet Kaur, Deepika Kounda, Saima Anwar Lashari, Surbhi Bhatia, Mohammad Khalid Imam Rahmani, "Optimized Energy Efficient Secure RoutingProtocol for Wireless Body Area Network", IEEE Access, Vol. 9, Aug 2021
 19. Greeshma Arya, Ashish Bagwari, Durg Singh Chauhan, "Performance Analysis of Deep Learning-BasedRouting Protocol for an Efficient DataTransmission in 5G WSN Communication", IEEE Access, Vol. 10, Jan 2022
 20. Senthil Kumar Jagatheesaperumal, Ijaz Ahmad, Marko Höyhty, Suleman Khan, Andrei Gurtove, "Deep Learning Frameworks for Cognitive Radio Networks: Review andOpen Research Challenges", Journal of Network and Computer Applications, Vol. 233, Jan 2025
 21. Vinodkumar Mohanakurup, Vishwadeepak Singh Baghela, Sarvesh Kumar, Prabhat Kumar Srivastava, Nitika Vats Doohan, MukeshSoni, Halifa Awal, "5G Cognitive Radio Networks Using Reliable Hybrid DeepLearning Based on Spectrum Sensing", Wireless Communications and Mobile Computing, Wiley, Apr 2022
 22. Seghiri Naouel, Baba-Ahmed Mohammed Zakarya, Benmammam Badr, Houari Nadhir, Khellafi Mohammed Kamal, Abdelgherfi Mohammed Ayyou, "Data Security of a Cognitive Radio Network for Multicriteria Secondary Users", Journal of Electrical and Electronics Engineering, Vol. 15, Oct 2022
 23. Yuan Zhao, Qi Lu, Zhisheng Ye, Kang Chen, "A communication failure and repair mechanism with adjustable transmission rates for PU packets in CRNs", Heliyon, Vol. 9, Feb 2023
 24. Jihong Wang, Hao Ni, Yiyang Ge, Shuo Li, "Traffic-driven ions motion optimization-based clustering routing protocol for cognitive radiosensor networks", PLOS ONE, Sep 2022
 25. Sharhabeel H. Alnabelsi, Haythem Bany Salameh, Ramzi R. Saifan, Khalid A. Darabkh, "A multi-layer hyper-graph routing with jamming-awareness for improved throughput in full-duplex cognitive radio networks", Journal of King Saud University -Computer and Information Sciences, Elsevier, Vol. 34, Sep 2022
 26. Mahmoud Khasawneh, Ahmad Azab, Saed Alrabaee, Heba Sakkal, Hossameldein Hussein Bakhit, "Convergence of IoT and Cognitive Radio Networks: A Survey of Applications, Techniques, and Challenges", IEEE Access, Vol. 11, Jul 2023
 27. Chengxiao Chen, Xiaogang Qi, Ying Cai, Jiabin Zhang, "Regional autonomous security cooperative spectrum sensing method based on trust value", IET Communications, Wiley, May 2023
 28. Saraswathi M.I, Logashanmugam E., "Chicken swarm optimization modelling for cognitive radio networks using deep belief network-enabled spectrum sensing technique", PLOS ONE, Aug 2024
 29. Guanghua Zhang, Zhenguo Chen, Liqin Tian, Dongwen Zhang, "Using Trust to Establish a Secure Routing Model in Cognitive Radio Network", PLOS ONE, Sep 2015
 30. Jamal Elhachmi, "Distributed reinforcement learning for dynamic spectrum allocation in cognitive radio-based internet of things", IET Networks, Wiley, Jul 2022