International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

AI-Enhanced Secure Communication using Blockchain Decentralized Zero Trust Authentication Mechanism with Quantum Bio-Inspired Approach for CRNs

T. Sundar[1]; Dr. A. Senthilkumar[2]

[1]Ph.D. - Research Scholar, Department of Computer Science,
Periyar University, Salem, Tamil Nadu, India – 636011
[2]Assistant professor, Department of Computer Science,
Thiruvalluvar Government Arts College, Rasipuram, Tamil Nadu, India – 637401
[1] admin.sundar@gmail.com; [2] senthilkumarmca76@gmail.com

DOI: https://doi.org/10.47760/ijcsmc.2026.v15i07.004

Abstract: Cognitive Radio Networks (CRNs) are a new era of wireless communication systems that enable secondary users to access spectrum bands opportunistically when primary users are not using them. Although a CRN can provide high-quality service and enhance spectrum utilization, there are still some important urgent problems to be solved, such as insecure communication, malicious nodes participating in the network, and unreliable routing performance. However, none of the existing security and communication schemes can achieve trusted entity validation, shortest-path optimization, and communication reliability simultaneously in CRNs. To address these challenges, this paper presents the AI assisted Blockchain Decentralized Zero Trust Authentication (BDZTA) approach for secure communication in CRN. Initially, the proposed Trust-Energy Aware Transmission Node Assessment (TEATNA) method is employed to identify the reliable transmission nodes. Then, the Adaptive Graph Neural Network (AGNN) model is used to classify the optimal shortest communication path by capturing the dynamic topological structure among cognitive radio nodes. After optimal route selection, Quantum-Inspired Whale Optimization with Elliptic Curve Cryptography (QIWO-ECC) approach is utilised for key generation and lightweight data encryption. Subsequently, the BDZTA approach is used to enable secure, decentralized communication through continuous identity verification. Finally, the Proof of Authority Verification (PoAV) scheme is used to validate authorized communication entities and ensure secure participation in transactions. The integrated framework significantly improves secure communication, trusted routing, Packet Delivery Ratio (PDR), energy efficiency, end-to-end delay, and energy consumption. The results of the experimental analysis show that the proposed approach achieves the best performance among existing schemes, thereby providing strong, reliable, and intelligent communication in CRNs.

Keywords: AI, CRNs, secure communication, authorized, Blockchain, verification, data encryption, truest nodes

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

I. INTRODUCTION

Cognitive Radio Networks (CRN) are intelligent wireless communication networks facilitating secondary users to opportunistically exploit underutilized spectrum bands without impacting the primary users, leading to efficient spectrum utilization, adaptive communication and improved transmission efficiency in dynamic wireless scenarios. CRN is extensively adopted in Wireless Sensor Network (WSN) applications, due to its flexibility in providing intelligent spectrum sensing and connectivity mechanisms. Existing methods like blockchain-based trust management [1], blockchain-based secure communication framework, blockchain-based traffic analysis [3], blockchain-based attack-resilient and blockchain-based secure multi-sensor network [3] models, blockchain-based secure spectrum sensing approaches, etc. . However, these methods suffer from several drawbacks in the connectivity and communication process in CRN-based WSN systems [4]. A majority of the existing methods still suffer from communication delay, high computational complexity, unstable routing performance, malicious node participation, wasted packets, dynamic topological changes and increased energy consumption [5]. vehicular blockchain communication systems [6], energy-aware secure transmission techniques [7], deep blockchain-based trusted routing schemes [8], reputation and trust management schemes, trust-based routing techniques, blockchain-based zero-trust routing techniques and so on have been proposed to provide reliable and secure connectivity in CRN [9]. Several approaches fail to provide continuous authentication and maintain connectivity security during the frequent spectrum switching and communication process of large numbers of nodes. Moreover, existing routing and trust management approaches suffer from low scalability, inefficient shortest path optimization and lack lightweight encryption for real-time communication [10].

To address the above limitations, the proposed method presents a secure communication framework for CRN-based WSN environments. Firstly, a reliable transmission node selection is performed by evaluating the trust, energy and communication stability of the nodes. Second, the best shortest communication path is found by an intelligent routing mechanism. Third, secure data transmission is achieved by applying lightweight encryption and optimized key generation. Fourth, the secure participation of communication entities is ensured by decentralized continuous authentication and authority-based validation. The proposed method achieves secure communication, trusted routing, communication reliability, connectivity stability, decentralized authentication, authority-based validation and energy-efficient secure data transmission in the CRN-based WSN environment.

The motivation of this research is to achieve secure and reliable communication in the CRN-based WSN environment. While CRNs promote efficient spectrum utilization and adaptive communication, they still suffer from malicious nodes' participation, insecure routing, packet loss, communication delay and excessive energy consumption. Blockchain-based security and trust management methods achieve secure communication but have heavy computational complexity, unstable connectivity and insufficient continuous authentication in the dynamic wireless environment. Thus, an intelligent secure communication framework is proposed for the CRN-based WSN environment, which is expected to achieve trusted routing, decentralized authentication, communication reliability, connectivity stability and energy-efficient secure data transmission.

A. Main Contribution of the work,

- Trusted node assessment enhances secure communication by discovering reliable cognitive radio nodes using trust, energy and transmission stability analysis.
- Intelligent routing mechanism decides best shortest communication path for minimization of delay and enhancement of connectivity stability in CRN based environment.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

- Lightweight encryption mechanism enables secure transmission of data by optimizing key generation having less computational complexity and energy usage.
- The decentralized authentication mechanism continuously authenticates communication nodes for avoiding unauthorized authentication and achieving effective secure connectivity performance.
- The authority-based verification process authenticates trusted network participants for enabling secure communications transaction in decentralized distributed wireless environment.
- The proposed framework enhances improvement of communication security, routing reliability, energy efficiency, stable trusted connectivity and scalable secure data transmission performance.

The proposed secure communication framework for CRN based WSN environment aims at improving trust routing, secure connectivity, decentralized authentication and reliable communication performance. The framework discovers trusted transmission node by assessing trust and energy, followed by intellectual routing for shortest path for stable communication. Light weight encryption mechanisms enable secure transmission of data with minimum energy usage and computational complexity. Continuous authentication and authority-based verification mechanisms help in avoiding unauthorized authentication and malicious communication among participants during communication. The overall system provides improvement in routing reliability, packet delivery performance, communication security, stable connectivity and scalable secure data transmission performance in dynamic CRN based wireless environment.

II. LITERATURE SURVEY

Automatic Dependent Surveillance-Broadcast (ADS-B) is an air-to-air and air-to-ground data link broadcast system that broadcasts aviation aircraft position data at specific intervals [11]. The access to the broadcast channel does not have a security authentication mechanism, and no information integrity protection measures are provided in the transmission protocol, due to the open nature of the ADS-B channel. Secure Trust-based Dijikstra's Method with many criteria to secure data transmission.

In [12] proposed a Bi-Directional GRU for Deep Packet Analysis. A blocking mechanism blocks intrusions (or malware) identified by deep packet inspection. The combination of algorithms resulted in more efficient Packet Delivery Ratio, productivity, time analysis, detection accuracy and security level for the suggested method.

The characteristics of cognitive radio (CR) technology, and other factors, routing is a problem in CRNs [13]. Firstly, the CR's frequency band is considered a dynamic spectrum. Therefore, since the routing algorithms used in other types of networks rely on a fixed frequency band, they cannot be directly used in CRNs. Secondly, with the dynamic spectrum access made possible by CR technology, the network performance is negatively impacted.

Propose a blockchain and artificial intelligence (Ai) empowered trust-information- centric network architecture for B5G [14]. Firstly, a trust evaluation and circulation mechanism for B5G node is designed as a blockchain-based, termed as TrustCoin, which can evaluate the trust of B5G node in a dynamic and fine-grained way, and manage the trust-coin circulation and trust-quota of B5G node. Second, to obtain the content credibility.

In low altitude networks, the Unmanned Aerial Vehicles (UAVs) can be equipped with various capabilities such as logistics, intelligence surveillance and environmental monitoring which can be supported by Base Stations (BSs) with significant computational power [15] But BSs have to cope with malicious UAVs

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

which may consume all the resources of the BS or may provide denial of service attacks. To formulate a blockchain-enabled access control model, which uses the UAV identities (IDs) and trajectories, positive and negative interactions with the BS to evaluate the reputations of UAVs.

TABLE 1: ANALYSIS OF SECURE COMMUNICATION FRAMEWORKS IN COGNITIVE RADIO AND IOT NETWORKS

S. No	Author et al.	Year	Proposed Method	Key Contribution	Limitations
16	Jia et al.	2026	Software Defined Networking–Blockchain Secure Routing for Zero-Trust UAV Networks (SDN-BSR)	Provides secure routing for UAV networks using SDN and blockchain integration.	Increases computational and communication overhead.
17	Yan et al.	2023	Information Chain Reputation-Based Blockchain System (Info-Chain)	Enhances secure information sharing in 6G intelligent transportation systems.	Reputation management complexity affects scalability.
18	Zhao et al.	2023	Blockchain-Based Trust Management Model for Vehicular Ad Hoc Networks (BBTM-VANET)	Improves trust management and secure communication in VANETs.	Blockchain latency may reduce real-time efficiency.
19	Wijesekara et al.	2025	Blockchain-Based Routing in Communication Networks Survey (BBRCN)	Reviews blockchain routing techniques and security mechanisms in communication networks.	Lacks practical implementation and performance validation.
20	Mehmood et al.	2020	Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS)	Enhances reliable and energy-efficient communication in wireless body area networks.	Energy optimization may reduce communication speed.
21	Vedachalam and Raj et al.	2024	ATSNRNN-Enabled Fuzzy Privacy-Preserved Data Encryption System (FPPDES)	Improves secure cooperative spectrum sensing using machine learning and privacy preservation.	High computational complexity during encryption and learning processes.
22	Samriya et al.	2023	Blockchain and Reinforcement Neural Network Trusted IoT Framework (BRNN-TIoT)	Integrates blockchain and reinforcement neural networks for trusted cloud-enabled IoT communication.	Requires high storage and processing resources.
23	Kholidy et al.	2022	Blockchain-Based Decentralized Trusted Computing Platform (BDTCP)	Secures spectrum and resource sharing in 5G networks using decentralized blockchain computing.	Blockchain consensus mechanisms increase delay.
24	Aslam et al.	2021	Sixth Generation Cognitive Radio Network Security Framework (6G-CRN)	Discusses applications, security issues, and challenges of 6G cognitive radio networks.	Mainly theoretical without experimental validation.
25	Deepanramkumar and Sharmila	2024	AI-Enhanced Quantum-Secured IoT Communication Framework (AI-QSICF)	Combines AI and quantum security for secure IoT communication in 6G cognitive radio networks.	Quantum security implementation requires high computational cost.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Table 1 shows a comparative analysis of the recently developed secure communication framework for advanced wireless, IoT, UAV and cognitive radio networks based on blockchain and AI. The methods under review concentrate on secure routing, trust management, privacy security, spectrum sharing, as well as energy efficient communication with respect to blockchain, machine learning, reinforcement learning and quantum security. These solutions greatly improve the reliability, decentralized protection, and intelligent communication of the network in 5G and 6G networks. But they have some problems like high resource consumption, blockchain latency, scalability problems, and computational complexity, which put a restriction on their practical use in large scale.

Blockchain technology-based solutions for Dynamic Spectrum Access (DSA) appear to be efficient and strong, in particular because of the intrinsic properties of blockchain technology, including decentralization, immutability, and transparency [26]. Furthermore, spectrum violations (i.e. unauthorized use of the spectrum) were not extensively discussed in most of the DSA systems found in the literature that are based on blockchain. It introducing a novel consensus protocol specially designed to perform DSA and find spectrum violations, which is also energy efficient, called the Distributed-Proof-of-Sense (DPoS).

In recent years, Blockchain Radio Access Network (B-RAN) has emerged as a promising paradigm for the sixth generation (6G) wireless communications to facilitate cooperative trust-building, pooling of wireless resources, and task scheduling for supporting inter- and intra-network tasks between independent network entities [27]. It is an open platform on a blockchain that will enable a range of wireless services and applications, including radio access, Internet of Things (IoT) and mobile-edge computing, using trusted interactions with improved security and efficiency.

The Q-learning mechanism reduces route flapping and encourages learning and adaptation. At the same time, blockchain and digital signatures create a decentralised trust layer that verifies devices and can be used to thwart attacks such as blackhole and Sybil [28]. Q-Routing has a longer network lifetime than Open Shortest Path First (OSPF), Deep Reinforcement Learning-Based Control Framework for Traffic Engineering (DRL-TE) and intelligent Edge Network Routing (ENIR).

TABLE 2: ANALYSIS OF SECURE ROUTING AND DATA TRANSMISSION TECHNIQUES IN WIRELESS NETWORKS

S. No	Author et al.	Year	Type of Dataset	Secure Efficiency	Data Transmission Short Path Rate
29	Kumar et al.	2023	Flying Ad-Hoc Network (FANET) routing dataset	High trust-based communication security	Improves multi-hop routing with optimized path selection
30	Swamynathan et al.	2024	VANET traffic and blockchain communication dataset	Enhances security using deep learning and blockchain	Achieves reliable and secure trusted routing paths
31	Jabeen et al.	2023	Healthcare wireless sensor network dataset	Provides secure healthcare monitoring communication	Supports efficient cognitive radio data transmission
32	Priya et al.	2025	Wireless Sensor Network (WSN) dataset	Improves trust-aware and blockchain-based security	Enhances energy-efficient adaptive routing paths
33	Porkodi and Kesavaraja	2020	IoT blockchain recommender dataset	Ensures trusted IoT communication security	Supports secure cognitive-based data transmission routing

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

The table 2 presents a comparison of recent secure routing and data transmission techniques developed for wireless networks like FANET, VANET, WSN and IoT environment. These techniques involve trust management, blockchain, deep learning, and cognitive radio technologies to enhance communication security, reliability, and efficiency. However, problems of computational burden, energy usage and scale are still large hurdles in the deployment of large-scale wireless network.

This article proposes deep learning (DL) framework constructed using deep autoencoder (DAE) to detect the malicious nodes in an Internet of Things (IoT) network assisted by the cognitive radio (CR) technology [34]. The era of IoT has a lot of nodes being attached to the network to gather and share data. Due to its efficient use of the available spectrum, CR technology is applicable to IoT applications.

An efficient reactive routing protocol considering the mobility and the reliability of a node in Cognitive Radio Sensor Networks (CRSNs) [35]. The proposed protocol is designed to handle the dynamic spectrum availability and chooses a stable transmission path from a source node to the destination. Outlined as a weighted graph problem, the proposed protocol measures the weight for an edge the measuring the mobility patterns of the nodes and channel availability.

III. PROPOSED METHODOLOGY

The architecture of our proposed AI-based secure communication scheme for CRN is depicted in Figure 1. The proposed system combines trusted-node evaluation, intelligent shortest-path selection, lightweight encryption, decentralized blockchain authentication, and authority-based verification to maintain secure and efficient communication in CRN. The framework contains 5 Phases, which are: TEATNA, AGNN-based shortest-path selection, QIWO-ECC, BDZTA, and PoAV. In the beginning, the CRN consists of primary users (PUs), secondary users (SUs) Trusted nodes, and malicious nodes. The dynamic spectrum access and the participation of malicious users make secure communication a nontrivial challenge in CRNs. Hence, the TEATNA approach is applied to find dependable communication nodes utilizing residual energy and trust values. This procedure eliminates malicious nodes and the trusted nodes are selected to take part in secure routing. Once the trusted node selections are completed, the AGNN model is applied to find the best shortest communication path from source to destination node. The proposed AGNN framework captures the dynamic topological relations among cognitive radio nodes and the efficient routing path with minimized communication delay and maximized routing performance is selected.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

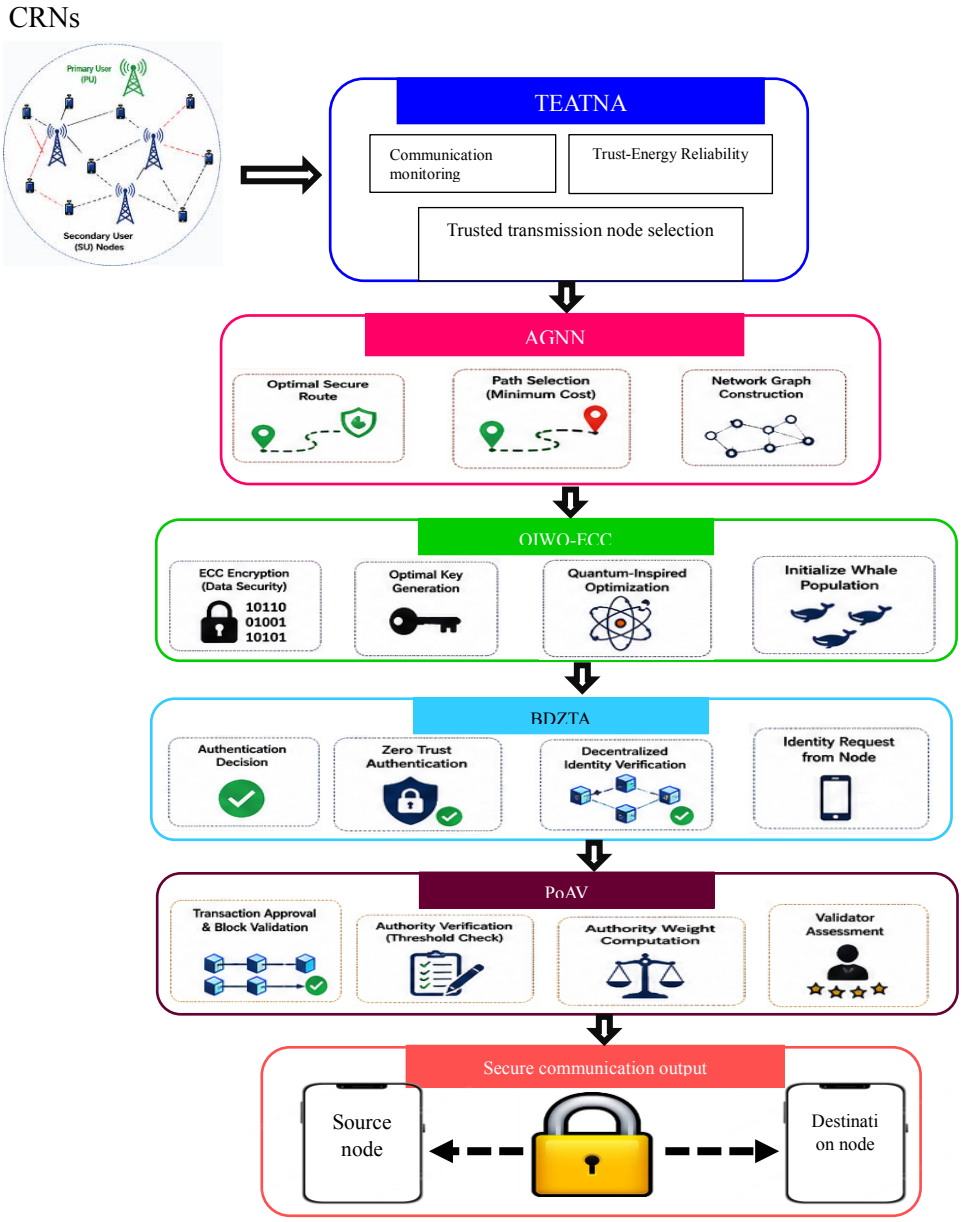

Fig.1 Architecture diagram

Then, the QIWO-ECC technique is applied for the optimal key generation and lightweight data encryption. Here, an optimal cryptographic key is generated using the Quantum Inspired Whale Optimization algorithm and the communication data is secured with low computational complexity and high confidentiality by ECC. Following encryption, the BDZTA system forms safe decentralized communication via dynamic

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

identities and trust-aware authentication. The communication records and authentication information are securely stored in the blockchain network to prevent any unauthorized access and malicious communication behaviors. Finally, PoAV authenticates the communication entities in an authorized domain before the secure data exchanging. After a successful authentication, the encrypted data packets are securely sent from the source node to the destination node along the authenticated routing path.

A. Trust-Energy Aware Transmission Node Assessment (TEATNA)

The input of the approach consists of cognitive radio node information, and communication parameters consisting of trust value, residual energy, packet delivery, transmission rate, connectivity strength and node behavior. Initially, node information collection and communication monitoring processes are performed to analyze the activities of all participants in the CRN-based WSN environment. The intermediate output consisting of communication profile with node trust value, energy level and transmission information is generated during this stage. Subsequently, trust evaluation and energy assessment processes identify trusted communication nodes by analyzing the packet forwarding behavior, communication consistency, residual power and connectivity stability. The intermediate output at this stage consists of trusted node feature maps and malicious node detection information. The following process is the transmission reliability analysis to analyze the routing stability, packet loss and communication delay among neighboring nodes. Finally, the evaluated parameters are integrated to determine trusted and energy-efficient transmission nodes. The final output of the approach is the reliable node set, which enables secure communication and stable network connectivity.

1) Cognitive Radio Node Communication Profile Generation

The TEATNA process captures communication-related parameters from the cognitive radio nodes in the CRN-based WSN environment. The presented equation 1 captured parameters are integrated to generate node communication profiles for trust and reliability analysis.

$$CRNP_i = \{T_i^{val}, E_i^{res}, R_i^{tx}, P_i^{dr}, C_i^{str}, B_i^{node}\} \quad (1)$$

where $CRNP_i$ represents the communication profile of node i. T_i^{val}, E_i^{res}, R_i^{tx}, P_i^{dr}, C_i^{str}, and B_i^{node} detenote trust validation, residual energy, transmission rate, packet delivery ratio, connectivity strength and node behavioural stability respectively.

2) Communication monitoring and connectivity analysis

Packet delivery efficiency, connectivity strength and transmission rate between neighbouring cognitive radio nodes are analysed in communication monitoring and connectivity analysis stage. Node stable connectivity is equation 2 determined based on weighted communication metric.

$$CMCA_i = \frac{\alpha P_i^{dr} + \beta C_i^{str} + \gamma R_i^{tx}}{\alpha + \beta + \gamma} \quad (2)$$

where $CMCA_i$ represents the communication monitoring and connectivity analysis score. In P_i^{dr}, C_i^{str}, and R_i^{tx} denote packet delivery ratio, connectivity strength and transmission rate respectively.

3) Trust-Energy Reliability Evaluation

The trust-energy reliability evaluation stage is used to identify reliable communication nodes using trust validation in equation 3, residual energy and node behavioural stability metrics. This stage discards malicious and unstable nodes from CRN based WSN environment.

$$TERE_i = \frac{\mu T_i^{val} + \lambda E_i^{res} + \delta B_i^{node}}{\mu + \lambda + \delta} \quad (3)$$

where $TERE_i$ represents the trust-energy reliability evaluation score, in T_i^{val}, E_i^{res}, and B_i^{node} denote trust validation, residual energy level and node behavioural stability respectively.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

4) Transmission reliability and stability computation

Transmission reliability and routing stability are equation 4 computed by combining communication monitoring and trust-energy reliability metric. To improve stable routing performance and secure data transmission, communication delay is also considered.

$$TRSC_i = \frac{\theta CMCA_i + \rho TERE_i - \sigma D_i^{comm}}{\theta + \rho + \sigma} \quad (4)$$

where $TRSC_i$ represents transmission reliability and stability computation, in $CMCA_i$, $TERE_i$, and D_i^{comm} denote communication monitoring score, trust-energy reliability score and communication delay factor respectively.

5) Trusted transmission node selection

Trusted communication nodes are judged by equations 5 calculating the transmission reliability and stability score, and the nodes whose score is higher than the predefined threshold value are considered to be reliable communication nodes to achieve safe communication and routing.

$$TTN_i = \begin{cases} 1, & \text{if } TRSC_i \geq \tau_{th} \\ 0, & \text{if } TRSC_i < \tau_{th} \end{cases} \quad (5)$$

where TTN_i represents the trusted transmission node selection result, in $TRSC_i$denotes transmission reliability and stability score, and τ_{th} indicates the secure communication threshold.

B. Adaptive Graph Neural Network (AGNN)

After TEATNA, the trusted cognitive radio nodes were used for AGNN based Shortest Path Routing to calculate the optimal communication route in CRN based WSN environment. First, the trusted node information and communication parameters, including node connectivity, transmission delay, link stability, neighboring node distance, packet delivery ratio and routing cost, are loaded. Second, the dynamic communication graph is first constructed by taking cognitive radio nodes as graph vertices and communication links as graph edges. Third, the graph feature extraction is carried out to explore node relationship, connectivity and communication dependency among neighboring nodes. Fourth, the constructed communication graph is input into the AGNN model, in which the adaptive message passing and neighbourhoods aggregation mechanisms are adopted to learn the spatial communication relationships and dynamic routing behavior of the whole network. At this step, the intermediate outputs of the model were node embedding vector, connectivity feature map, routing probability scores and optimized communication path. Fifth, the shortest path is optimized, including the minimum delay, stable connectivity and maximum communication reliability routes. Finally, the optimal shortest communication path is outputted by the AGNN model for secure and efficient data transmission in the CRN based WSN environment.

1) Trusted node input initialization

The input of the trusted cognitive radio node Information generated equation 6 from the TEATNA stage is loaded in the AGNN-Based shortest path routing process, and the node connectivity, link stability, packet delivery ratio, communication delay, and the routing cost are used for the routing analysis.

$$TNI_i = \{N_i, C_i, L_i, P_i^{dr}, D_i^{link}, R_i^{cost}\} \quad (6)$$

where TNI_i represents trusted node input initialization of node i. N_i, C_i, L_i, P_i^{dr}, D_i^{link}, and R_i^{cost} costdenote trusted node information, connectivity strength, link stability, packet delivery ratio, communication delay, and routing cost respectively.

2) Dynamic communication graph construction

The dynamic communication graph construction analyses the equation 7 connectivity of neighboring nodes and the stable communication link of the CRN-based WSN, and constructs the graph-based communication relationship based on weighted connectivity.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

$$DCG_i = \frac{\alpha N_i + \beta C_i + \gamma L_i}{\alpha + \beta + \gamma} \quad (7)$$

where DCG_i represents dynamic communication graph construction score. N_i, C_i, and $L_i$denote trusted node connectivity, communication strength, and link stability respectively.

3) Graph connectivity feature extraction

The graph connectivity feature extraction analyses the equation 8 communication dependence and the stable interaction of the neighboring node to optimize the routing, and the communication consistency and the routing performance of the cognitive radio nodes are improved.

$$GCF_i = \frac{\mu C_i + \lambda L_i + \delta P_i^{dr}}{\mu + \lambda + \delta} \quad (8)$$

where GCF_i represents graph connectivity feature extraction score, C_i, L_i, and P_i^{dr} denote connectivity strength, link stability, and packet delivery ratio respectively.

4) AGNN node embedding computation

The AGNN model calculates equation 9 node embedding based on the aggregation of neighboring node information and communication relationships, thus learning the dynamic routing behavior and spatial communication.

$$NE_i^{(k+1)} = \sigma\left(\sum_{j \in \mathcal{N}(i)} W^{(k)} NE_j^{(k)} + B^{(k)}\right) \quad (9)$$

where $NE_i^{(k+1)}$ denotes updated embedding of node i. $W^{(k)}$, $NE_j^{(k)}$, and $B^{(k)}$ correspond to adaptive weight matrix, neighboring node embedding, and bias parameter.

5) Shortest path routing optimization

Shortest path routing optimization calculates equation 10 optimal communication path by utilizing communication delay, routing cost, and link stability parameters and chooses stable routing path with shortest transmission delay.

$$SPRO_i = \min(D_i^{link} + R_i^{cost} - L_i) \quad (10)$$

where $SPRO_i$ represents shortest path routing optimization score, D_i^{link}, R_i^{cost}, and L_i denote communication delay, routing cost, and link stability respectively.

6) Optimal route selection

The AGNN framework then equation 11 chooses optimal communication path with the minimum routing optimization score. The optimal communications route is eligible for secure communication data transmission in CRN-based WSNs.

$$OR_i = \begin{cases} 1, & \text{if } SPRO_i = \min(SPRO) \\ 0, & \text{if } SPRO_i \neq \min(SPRO) \end{cases} \quad (11)$$

where OR_i represents optimal route selection result, $SPRO_i$denotes shortest path routing optimization score for secure communication path selection.

C. Quantum-Inspired Whale Optimization with Elliptic Curve Cryptography (QIWO-ECC)

After the AGNN based Shortest Path Routing, the optimal communication path selected is forwarded to the QIWO-ECC stage for secure key generation and encrypted communication data transmission, which first load the optimized routing information along with the communication parameters such as node identity, communication packets, keys for transmission, routing cost and security attributes from trusted cognitive radio nodes. First, Quantum-Inspired Whale Optimization algorithm conducts search-space exploration and population initialization to search for the optimal cryptographic parameters for secure communication, then quantum-based position updating and whale optimization mechanisms are used to accelerate the convergence speed, optimize the accuracy, and secure key selection of communication. Second, elliptic curve cryptography

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

(ECC) processes the optimized parameters, and public and private cryptographic keys are generated by elliptic curve point operations for lightweight encryption and decryption, in this stage, the intermediate output is the optimized security parameters, encrypted packet representation, secured key feature sets, and communication security metrics. Third, ECC-based encryption is performed to encrypt the communication packets and secure the malicious attack of data transmission. Fourth, QIWO-ECC framework generates the optimized cryptographic keys, and secure encrypted communication data to achieve the reliable, lightweight and secure communication transmission in CRN based WSN network.

1) Optimal routing input initialization

After AGNN-based routing, the QIWO-ECC process starts to load the optimal path information and security related parameters from the selected communication route in equation 12. These parameters include the node identity, routing cost, packet information, key requirement for transmission, security attributes, hash values and link reliability factors for secure optimization.

$$ORI_i = \{P_i^{opt}, N_i^{id}, K_i^{comm}, T_i^{pkt}, R_i^{cost}, S_i^{attr}, H_i^{sec}, L_i^{link}\} \quad (12)$$

where ORI_i represents optimal routing input initialization of node i. P_i^{opt}, N_i^{id}, K_i^{comm}, T_i^{pkt}, R_i^{cost}, S_i^{attr}, H_i^{sec}, and L_i^{link} linkdenote optimal path, node identity, communication key, packet data, routing cost, security attributes, security hash, and link reliability respectively.

2) Quantum whale population initialization

The quantum whale population initialization generates equation 13 set of candidate solutions using routing, link security attributes, and cryptographic parameters of secure keys obtained from the AGNN output. This increases the exploration of secure key space and optimal routing-security combination.

$$QWP_i = \frac{\alpha P_i^{opt} + \beta S_i^{attr} + \gamma K_i^{comm} + \delta H_i^{sec}}{\alpha + \beta + \gamma + \delta} \quad (13)$$

where QWP_irepresents quantum whale population initialization score. P_i^{opt}, S_i^{attr}, K_i^{comm}, and H_i^{sec}denote optimal path, security attributes, communication key information, and security hash respectively.

3) Quantum position update mechanism

The quantum whale position updates the equation 14 mechanism iteratively optimizes the candidate solutions using whale-like search behavior and quantum optimization technique. This increases the convergence speed, and optimization of secure key.

$$QPU_i^{(t+1)} = QPU_i^{(t)} + A(B_i^{best} - QPU_i^{(t)}) + C \cdot rand + \eta H_i^{sec} \quad (14)$$

where $QPU_i^{(t+1)}$ is the updated position at iteration $t+1$, B_i^{best} best is the best solution, A and C are the adaptive coefficients, rand is the random exploration factor, η is the quantum adjustment, ηH_i^{sec} the security hash

4) Fitness function evaluation

The fitness function calculates the equation 15 whale optimization fitness score for each candidate solution according to its security level, routing cost, link reliability, and communication delay. This selects the best solution that is secure and efficient.

$$WOF_i = \min(D_i^{sec} + R_i^{cost} - S_i^{level} + \omega L_i^{link}) \quad (15)$$

where WOF_i is the whale optimization fitness score, D_i^{sec} is the security delay, R_i^{cost} cost is the routing cost, S_i^{level} is the security level, L_i^{link}link is the link reliability.

5) Enhanced elliptic curve key generation

The ECC-based encryption of the transmission packets with the generated equation 16 cryptographic keys and the security hash and link reliability integration is for the confidentiality and integrity during the transmission of the data.

$$ECK_i = (K_i^{pr} \times G) \oplus H_i^{sec} \oplus ID_i^{node} \quad (16)$$

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

where ECK_irepresents elliptic curve cryptographic key. K_i^{pr}denotes private key, $G$is generator point, H_i^{sec}represents security hash, and ID_i^{node}denotes node identity.

6) ECC-based data encryption

The ECC-based encryption of the transmission packets with the generated equation 17 cryptographic keys and the security hash and link reliability integration is for the confidentiality and integrity during the transmission of the data.

$$ED_i = (T_i^{pkt} \oplus ECK_i) + H_i^{sec} + L_i^{link} \quad (17)$$

where ED_i represents encrypted data, K_i^{pr}denotes transmission packet, ECK_irepresents cryptographic key, H_i^{sec}indicates security hash, and L_i^{link}denotes link reliability factor.

7) Secure communication

The final stage of the evaluation of the equation 18 optimized fitness result and the selection of the secure communication output for the secure transmission result by the security threshold and link reliability conditions.

$$SCO_i = \begin{cases} 1, & \text{if } WOF_i \le \tau_{sec} \text{ and } L_i^{link} \ge \theta_{th} \\ 0, & \text{otherwise} \end{cases} \quad (18)$$

where SCO_i represents secure communication output generation result, in WOF_i denotes fitness score, $\tau_{sec}$is security threshold, θ_{th}indicates link reliability threshold.

D. Blockchain Decentralized Zero Trust Authentication (BDZTA)

Once the data is encrypted, the proposed BDZTA mechanism utilizes to facilitate secure, decentralized communication in Cognitive Radio Networks. Within the proposed framework, all the communicating entities are constantly authenticated before and during the data transmission to avoid unauthorized and potentially malicious participation. The BDZTA mechanism facilitates trust-aware, decentralized authentication by validating the communication identity, trustworthiness, communication integrity and transaction legitimacy in a blockchain-enabled fashion. Initially, each encrypted communication request generated from node Ni is authenticated using trust score, communication behavior and identity validation parameters. The proposed authentication score of the communication entity is calculated as:

$$A_i = \alpha T_i + \beta V_i + \gamma I_i \quad (19)$$

Here, A_i denotes the authentication score of node i, T_i is the trust evaluation value, V_i lies the communication, I_i is the integrity validation parameter and α, β and γ are the weighting coefficients($\alpha + \beta + \gamma = 1$) .

Trust evaluation factor computes communication reliability of the node considering its communication participation, route participation, and node participation in the routing behavior. It is mathematically expressed as:

$$T_i = \frac{S_t}{S_t + F_t} \quad (20)$$

Herein, S_t lies the successful transactions and F_t denotes the number failed or suspicious transactions.

The communication verification score confirms that the communication node continually meets the secure communication requirements. It is calculated as follows:

$$V_i = \frac{P_r + B_a}{2} \quad (21)$$

Assuming that, P_r is the packet reliability ratio, and B_a denotes the behavioural analysis score,

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

The validation parameter for integrity check determines if communication data is encrypted and its status is checked along with the transmission with blockchain hash verification:

$$I_i = H(E_d \,||\, H_p \,||\, T_s) \quad (22)$$

Assuming that, $H(.)$ denotes the cryptographic hash function, E_d denotes the encrypted data, H_p denotes the previous block hash, T_s is the timestamp.

After the computation of authentication score estimation during communication node is periodically validated in session. Node is deemed authenticated, as calculated in the following equation

$$A_i > A_{th} \quad (23)$$

Where, A_{th} refers to predefined authentication threshold.

When the authentication score is less than the threshold, the communication entity may be considered as an unauthenticated node and is not allowed to continue in the communication process. The condition for detection of an unauthorized access is expressed as follows:

$$U_a = \begin{cases} 1, & A_i < A_{th} \\ 0, & A_i \geq A_{th} \end{cases} \quad (24)$$

Assuming that, U_a =1 indicate the unauthorized access, U_a=0 defines the authorized communication. In order to maintain persistent zero-trust validation, the authentication score is refreshed during each communication interval by the BDZTA scheme on the proposed mechanism. The continuous validation feature is mathematically expressed as:

$$A_i^{t+1} = A_i^t + \Delta T_i + \Delta V_i + \Delta I_i \quad (25)$$

Where, $A_i^{t+1}$is a updated authentication score, A_i^t is the previous authentication score, ΔT_i denotes the trust variation, ΔV_i lies the communication behaviour variation, ΔI_i denotes the integrity variation.

This continual validation process ensures that each communication request is authenticated independently, without relying on any communication entity being intrinsically trustworthy. Subsequently, authenticated communication sessions are stored in distributed blockchain blocks. The blockchain block format can be seen as:

$$B_n = \{ID_n, E_d, H_{n-1}, A_i, T_s\} \quad (26)$$

Assuming that, B_n is the current blockchain block, ID_n denote the communication node identity, E_d lies the encrypted data, $H_{n-1}$is the previous block hash, A_i is the authentication score, and T_s lies the timestamp. Thus, the BDZTA scheme enhances the decentralized authentication, continuous trust evaluation, communication security, malicious node prevention, unauthorized access detection, and provides strong and resilient communication in CRNs.

E. Proof of Authority Verification (PoAV)

Following the decentralized zero-trust authentication, the proposed PoAV scheme goes through a final validator approval and transaction authorization within CRNs. Whether the communication entity has enough permission and validation power to be involved in secure FCI communication with the support of the blockchain is checked by the proposed PoAV protocol. Instead of trust-aware authentication, the PoAV protocol is based on the validator trustworthiness, ability of transaction approval and verification from the consensus blockchain, before allowing sending the packets in a secure way.

At the beginning, the reputation of communication validator node V_i is calculated in terms of authority, transaction approval, and participation in consensus. The weight of the authority verification of the validator node is calculated as follows:

$$A_w(i) = \frac{\lambda R_v(i) + \mu T_a(i) + \nu C_s(i)}{\lambda + \mu + \nu} \quad (27)$$

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Herein, $A_w(i)$ is the authority weight of validator node i, $R_v(i)$ is the validator reputation score, $T_a(i)$ lies the transaction approval capability, $C_s(i)$ denotes the consensus stability factor, λ, μ, ν= weighting parameters

The validator reputation score quantifies how well an entity has performed in the past in communicating securely and is denoted as:

$$R_v(i) = \frac{B_v(i)}{B_t(i)} \quad (28)$$

Where, $B_v(i)$ is the number of successfully verified blocks, and $B_t(i)$ refers to total participated blockchain transactions. Transaction approval ability assesses the validator node's ability to approve valid encrypted transactions and is quantified as:

$$T_a(i) = \frac{T_l(i)}{T_r(i)} \quad (29)$$

Here, $T_l(i)$ denotes the number of legitimate transactions, and $T_r(i)$ is the total received transactions.

The consensus stability factor measures how stable a validator node is during the blockchain's consensus process. It is calculated as follows:

$$C_s(i) = 1 - \frac{\sigma_i}{\sigma_{max}} \quad (30)$$

Where, σ_i denotes the communication deviation of validator node i, and σ_{max} explains the maximum allowable consensus deviation.

After estimating the weight of the authority, the blockchain validator node will be voted in only if the authority verification condition holds:

$$A_w(i) \geq A_{min} \quad (31)$$

Herein, A_{min} refers to minimum authority threshold.

If the authority's weight is below the threshold, the communication node is treated as an unauthoritative validator and prevented from joining the blockchain. The condition for the detection of an unauthorized validator is expressed as:

$$U_i = \begin{cases} 1, & A_w(i) < A_{min} \\ 0, & A_w(i) \geq A_{min} \end{cases} \quad (32)$$

Herein, U_i=1 is the unauthorized validator access, U_i=0 is the authorized validator approval.

Subsequently, the approved validator node performs secure blockchain transaction verification using encrypted transaction hashes. The block verification function is represented as:

$$B_h(i) = H(E_d \,||\, V_i \,||\, T_s \,||\, H_p) \quad (33)$$

Where, $B_h(i)$ verified blockchain hash, E_d denotes the encrypted communication data, $V_i$is the validator node identity, and $H_p$presents the previous block hash. Finally, the confirmed transaction block is safely added to the blockchain as:

$$B_n = \{V_i, E_d, B_h(i), T_s, A_w(i)\} \quad (34)$$

Where, B_n is the verified block, and $A_w(i)$ denotes the authority weight. Thus, the introduced PoAV scheme efficiently authenticates the legitimate communicating entities and accurately detects false validator, enhances the reliability of the transactions on the blockchain, and guarantees safe integrity of communications in CRNs.

IV. RESULT AND DISCUSSION

The proposed AI-based secure communication protocol based on BDZTA with Quantum Bio-Inspired optimization was simulated and analyzed in CRNs using a Python environment. The efficacy of the proposed method was compared with state-of-the-art methods such as BRNN, FPPDES, and BDTCP. The performance evaluation was conducted using different metrics, including Packet Delivery Ratio (PDR), Authentication, Energy Consumption, Data Confidentiality Rate, and Throughput.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

TABLE 1: SIMULATION PARAMETERS

Parameters	**Values**
Simulation Tool	Python
Network Area	1000X1000 m^2
Number of Cognitive Radio Nodes	50 – 500
Number of Primary Users	10
Number of Secondary Users	40 – 490
Communication Channel	Wireless Channel
Initial Energy	100 J
Packet Size	512 Bytes
Transmission Range	250 m
Simulation Time	100 sec
Spectrum Type	Dynamic Spectrum
Performance Metrics	PDR, Delay, Energy efficiency, Throughput, Authentication Accuracy

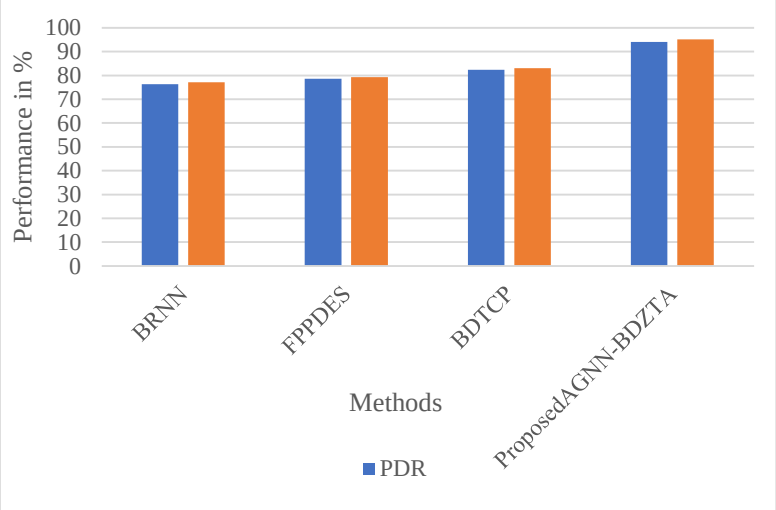

Fig.2 Comparison of PDR and throughput performance

Figure 2 shows the PDR and energy efficiency results of the AGNN-BDZTA scheme in comparison with BRNN, FPPDES, and BDTCP approaches over CRN. The BRNN method achieved 76.25% PDR and 77.16% energy efficiency, while FPPDES achieved 78.61% PDR and 79.3% energy efficiency. In the same way, the BDTCP protocol achieved 82.3% PDR and 83.04% energy efficiency using blockchain-supported communication. On the other hand, the PDR and energy efficiency of the proposed AGNN-BDZTA scheme attain the best values of 94.06% and 95.16%, respectively. The better result come from the TEATNA employed for trusted node selection, AGNN-based optimal shortest-path routing, HQIWO-ECC secure encryption, and

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

BDZTA-PoAV authentication, along with verification schemes. Hence, the proposed have higher PDR, more secure, and reliable communication with better packet transmission in CRNs.

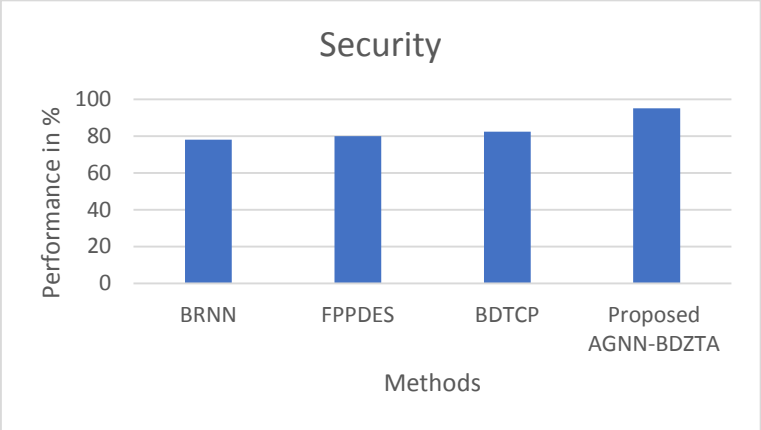

Figure 3: Comparison of security performance

Figure 3 compares the security rate of the proposed AGNN-BDZTA framework with traditional methods, BRNN, FPPDES, and BDTCP, in CRNs. The security performance of the BRNN method is 78.16%, followed by the FPPDES and BDTCP methods at 80.04% and 82.46%, respectively. Meanwhile, the highest security of 95.07% is achieved by the proposed AGNN-BDZTA framework. The remarkable enhancement is achieved through TEATNA-based trusted node evaluation, AGNN-based secure shortest-path selection, lightweight QIWO-ECC encryption, BDZTA decentralized zero-trust authentication, and PoAV-based authorized entity validation. These methods are for preventing malicious nodes from participating in or disrupting communication, while improving secure data transmission in CRNs.

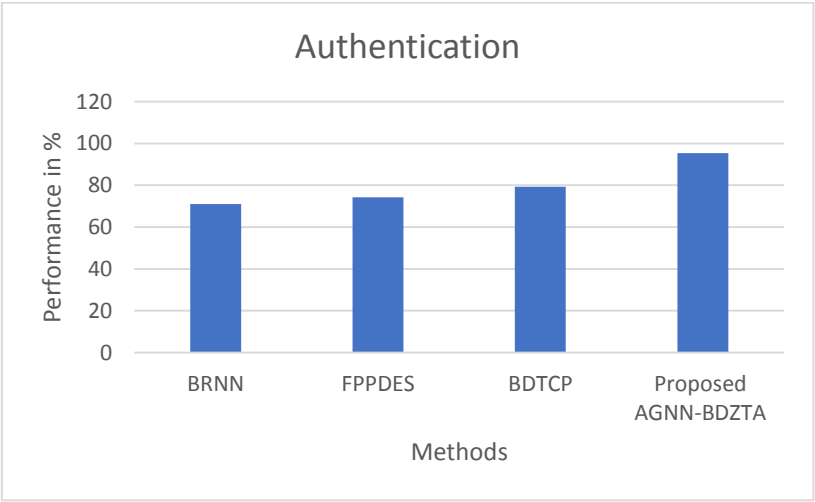

Figure 4: Comparison of authentication performance

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Fig. 4 compares the proposed AGNN-BDZTA framework with the conventional BRNN, FPPDES, and BDTCP schemes in terms of authentication performance in CRN. The BRNN-based method achieved an authentication performance of 71.08%; the FPPDES- and BDTCP-based authentication schemes achieved 74.19% and 79.3%, respectively. On the other hand, the proposed AGNN-BDZTA framework achieved the best authentication performance of 95.35%. This advancement is mainly attributed to the combination of BDZTA and PoAV, which continuously authenticate communication nodes and prevent malicious attacks. Meanwhile, the TEATNA protocol can also successfully distinguish between trusted/byzantine nodes, thereby improving authentication and communication reliability in CRNs.

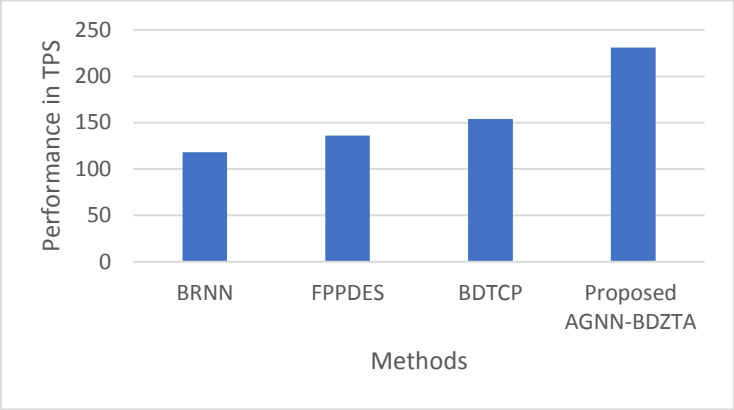

Figure 5: Comparison of Throughput performance

The throughput results, in terms of TPS, for our AGNN-BDZTA and other benchmark schemes, namely BRNN, FPPDES, and BDTCP, are shown in Fig. 5. The BRNN, FPPDES, and BDTCP methods yielded 118 TPS, 136 TPS, and 154 TPS, respectively. However, the AGNN-BDZTA framework reported a maximum throughput of 231 TPS. The enhancement is realized through AGNN-based optimal routing, lightweight QIWO-ECC encryption, distributed BDZTA authentication, and high-performance PoAV validation schemes to minimize transaction verification delay efficiently and securely, while maintaining it in CRNs.

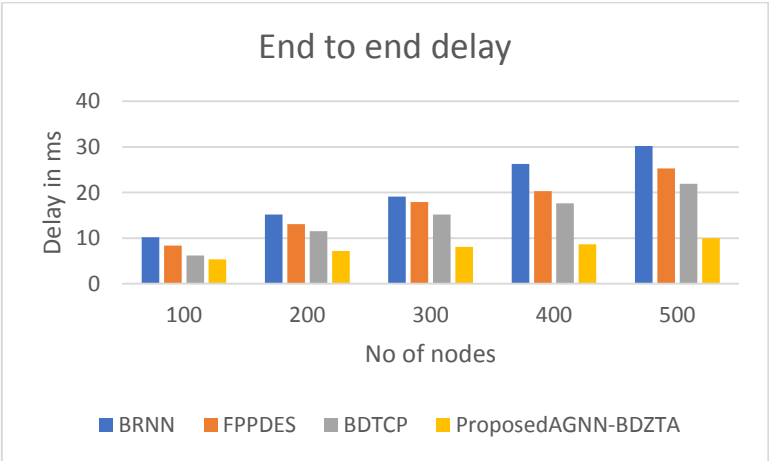

Figure 6: Comparison of End-to-end delay performance

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

Figure 6 presents the averaged results comparing the proposed AGNN-BDZTA scheme with the BRNN, FPPDES, and BDTCP methods in CRNs for 100–500 communication nodes. At 100 nodes, the proposed AGNN-BDZTA achieved the lowest delay of 5.36 ms, compared with BRNN (10.2 ms), FPPDES (8.37 ms), and BDTCP (6.19 ms). Likewise, at 500 nodes, our approach results in a delay of only 10.01 ms, while BRNN, FPPDES, and BDTCP result in 30.19 ms, 25.3 ms, and 21.9 ms, respectively. The delay reduction benefits from TEATNA-based trusted node selection, AGNN-based optimal shortest-path routing, lightweight QIWO-ECC encryption, and an effective BDZTA-PoAV authentication technique to provide swift and robust communication services in CRNs.

V. CONCLUSION

In this article, an AI-based secure communication framework for CRN using BDZTA with Quantum Bio-Inspired optimization was introduced. The TEATNA protocol first selects a trusted, energy-efficient communication node based on residual energy and trust values. Subsequently, the AGNN model finds the shortest communication path for reliable routing. After selecting the path, the QIWO-ECC technique generates optimal cryptographic keys and encrypts data securely and efficiently. Then, the BDZTA protocol continues authenticating communication parties using decentralized, blockchain-enabled zero-trust validation. Lastly, the PoAV mechanism certifies authorized validators and a secure blockchain. The simulation results indicated that the proposed AGNN-BDZTA framework surpassed the BRNN, FPPDES, and BDTCP approaches, achieving 94.06% PDR, 95.16% energy efficiency, 95.07% Security Performance, 95.35% Authentication, and throughput is 231TPS. Hence, the proposed scheme enhanced secure communication, trusted routing, authentication reliability, and blockchain transaction validation in CRNs.

REFERENCES

[1]. Mahvash, Mahsa, Neda Moghim, Mojtaba Mahdavi, Mahdieh Amiri, and Sachin Shetty. "Blockchain-inspired trust management in cognitive radio networks with cooperative spectrum sensing." *Pervasive and Mobile Computing* 106 (2025): 101999.

[2]. Sajid, Adnan, Bilal Khalid, Mudassar Ali, Shahid Mumtaz, Usman Masud, and Farhan Qamar. "Securing cognitive radio networks using blockchains." *Future Generation Computer Systems* 108 (2020): 816-826.

[3]. Dansana, Debabrata, Prafulla Kumar Behera, Abdulbasit A. Darem, Zubair Ashraf, Abu Taha Zamani, Mohammad Nadeem Ahmed, Gopal Krishna Patro, and Mohammad Shameem. "BDDTPA: Blockchain-driven deep traffic pattern analysis for enhanced security in cognitive radio ad-hoc networks." Ieee Access 11 (2023): 98202-98216.

[4]. Dansana, Debabrata, Prafulla Kumar Behera, S. Gopal Krishna Patro, Quadri Noorulhasan Naveed, Ayodele Lasisi, and Anteneh Wogasso Wodajo. "BSMACRN: Design of an efficient blockchain-based security model for improving attack-resilience of cognitive radio ad-hoc networks." *IEEE Access* 12 (2024): 10047-10058.

[5]. Khanna, Ashish, Poonam Rani, Tariq Hussain Sheikh, Deepak Gupta, Vineet Kansal, and Joel JPC Rodrigues. "Blockchain-based security enhancement and spectrum sensing in cognitive radio network." *Wireless Personal Communications* 127, no. 3 (2022): 1899-1921.

[6]. Asif, Fatima, Huma Ghafoor, and Insoo Koo. "Secure Cognitive Radio Vehicular Ad Hoc Networks Using Blockchain Technology in Smart Cities." *Applied sciences* 14, no. 18 (2024): 8146.

[7]. Ramalingam, Gomathi, and Palani Uthirapathy. "Optimizing Secure Data Transmission in Cognitive IoT-WSN: An Energy-Aware Approach With Hybrid POA-SCA and Block Chain Technology." *International Journal of Communication Systems* 38, no. 8 (2025): e70081.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

[8]. Abd El-moghith, Ibrahim A., and Saad M. Darwish. "Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach." *IEEE Access* 9 (2021): 103822-103834.

[9]. Raza, Abir, Elarbi Badidi, Mohammad Hayajneh, Ezedin Barka, and Omar El Harrouss. "Blockchain-based reputation and trust management for smart grids, healthcare, and transportation: a review." *IEEE Access* 12 (2024): 196887-196913.

[10]. Jia, Ziye, Sijie He, Ligang Yuan, Fuhui Zhou, Qihui Wu, Zhu Han, and Dusit Niyato. "Blockchain-Enabled Routing for Zero-Trust Low-Altitude Intelligent Networks." *IEEE Journal on Selected Areas in Communications* (2026).

[11]. Wu, Zhijun, Tong Shang, Meng Yue, and Liang Liu. "ADS-Bchain: a blockchain-based trusted service scheme for automatic dependent surveillance broadcast." *IEEE Transactions on Aerospace and Electronic Systems* 59, no. 6 (2023): 8535-8549.

[12]. Ilakkiya, N., and A. Rajaram. "A secured trusted routing using the structure of a novel directed acyclic graph-blockchain in mobile ad hoc network internet of things environment." *Multimedia tools and applications* 83, no. 40 (2024): 87903-87928.

[13]. Khasawneh, Mahmoud, Ahmad Azab, and Anjali Agarwal. "Towards securing routing based on nodes behavior during spectrum sensing in cognitive radio networks." *IEEE Access* 8 (2020): 171512-171527.

[14]. Pan, Qianqian, Jun Wu, Jianhua Li, Wu Yang, and Zhitao Guan. "Blockchain and AI empowered trust-information-centric network for beyond 5G." *IEEE network* 34, no. 6 (2020): 38-45.

[15]. Lu, Xiaozhen, Lixin Liu, Zhibo Liu, Qihui Wu, and Liang Xiao. "Blockchain-based intelligent trusted computational resource allocation for low-altitude networks." *IEEE Transactions on Mobile Computing* (2025).

[16]. Jia, Ziye, Yulu Han, Jingjing Zhao, Qiuming Zhu, Yao Wu, Qihui Wu, and Zhu Han. "SDN-Blockchain based Secure Routing for Zero-Trust UAV Networks." *IEEE Transactions on Cognitive Communications and Networking* (2026).

[17]. Yan, Kun, Wenping Ma, Qi Yang, Shaohui Sun, and Weiwei Wang. "Info-chain: Reputation-based blockchain for secure information sharing in 6G intelligent transportation systems." *IEEE Internet of Things Journal* 11, no. 5 (2023): 9198-9212.

[18]. Zhao, Junhui, Fanwei Huang, Longxia Liao, and Qingmiao Zhang. "Blockchain-based trust management model for vehicular ad hoc networks." *IEEE Internet of Things Journal* 11, no. 5 (2023): 8118-8132.

[19]. Wijesekara, Patikiri Arachchige DSN. "A Survey on Blockchain-Based Routing in Communication Networks." *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)* 13, no. 1 (2025): 196-225.

[20]. Mehmood, Gulzar, Muhammad Zahid Khan, Abdul Waheed, Mahdi Zareei, and Ehab Mahmoud Mohamed. "A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks." *IEEE Access* 8 (2020): 131397-131413.

[21]. Vedachalam, Saraswathi, and Dayana Raj. "Development of a privacy-preserved and secure cooperative spectrum sensing system in cognitive radio networks using ATSNRNN-enabled FPPDES with machine learning." *IEEE Access* 12 (2024): 155838-155850.

[22]. Samriya, Jitendra Kumar, Surendra Kumar, Mohit Kumar, Minxian Xu, Huaming Wu, and Sukhpal Singh Gill. "Blockchain and reinforcement neural network for trusted cloud-enabled IoT network." *IEEE Transactions on Consumer Electronics* 70, no. 1 (2023): 2311-2322.

[23]. Kholidy, Hisham A., Mohammad A. Rahman, Andrew Karam, and Zahid Akhtar. "Secure spectrum and resource sharing for 5G networks using a blockchain-based decentralized trusted computing platform." *arXiv preprint arXiv:2201.00484* (2022).

[24]. Aslam, Muhammad Muzamil, Liping Du, Xiaoyan Zhang, Yueyun Chen, Zahoor Ahmed, and Bushra Qureshi. "Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges." *Wireless Communications and Mobile Computing* 2021, no. 1 (2021): 1331428.

International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

T. Sundar *et al*, Volume 15, Issue 7, July 2026, pg. 46-65
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)
ISSN: 2320-088X
Impact Factor: 7.056

[25]. Deepanramkumar, P., and A. Helen Sharmila. "AI-enhanced quantum-secured IoT communication framework for 6G cognitive radio networks." *IEEE Access* 12 (2024): 144698-144709.

[26]. Fernando, Pramitha, Keshawa Dadallage, Tharindu Gamage, Chathura Seneviratne, An Braeken, Arjuna Madanayake, and Madhusanka Liyanage. "Distributed-proof-of-sense: Blockchain consensus mechanisms for detecting spectrum access violations of the radio spectrum." *IEEE Transactions on Cognitive Communications and Networking* 9, no. 5 (2023): 1110-1125.

[27]. Le, Yuwei, Xintong Ling, Jiaheng Wang, Ruiwei Guo, Yongming Huang, Cheng-Xiang Wang, and Xiaohu You. "Resource sharing and trading of blockchain radio access networks: Architecture and prototype design." *IEEE Internet of Things Journal* 10, no. 14 (2021): 12025-12043.

[28]. Mishra, Pranati, Nikola Ivković, Swati Lipsa, Ranjan Kumar Dash, and Korhan Cengiz. "QLB-IoT: Intelligent and Trust-Aware Routing for IoT-Edge Networks with Blockchain-Assisted Q-Learning." *IEEE Internet of Things Journal* (2025).

[29]. Kumar, Rakesh, Bhisham Sharma, and Senthil Athithan. "TBMR: trust based multi-hop routing for secure communication in flying ad-hoc networks." *Wireless Networks* (2023): 1-17.

[30]. Swamynathan, Cloudin, Revathy Shanmugam, Kanagasabapathy Pradeep Mohan Kumar, and Balasubramani Subbiyan. "Traffic Prevention and Security Enhancement in VANET Using Deep Learning With Trusted Routing Aided Blockchain Technology." *Transactions on Emerging Telecommunications Technologies* 35, no. 11 (2024): e70004.

[31]. Jabeen, Tallat, Ishrat Jabeen, Humaira Ashraf, Ata Ullah, N. Z. Jhanjhi, Rania M. Ghoniem, and Sayan Kumar Ray. "Smart wireless sensor technology for healthcare monitoring system using cognitive radio networks." *Sensors* 23, no. 13 (2023): 6104.

[32]. PRIYA, A. SANGEETHA, DR S. DEVARAJU, and DR ANTONY CYNTHIA. "DYNAMIC ADAPTIVE SELF-AWARE TRUST ENERGY-EFFICIENT ROUTING WITH BLOCKCHAIN FRAMEWORK FOR WIRELESS SENSOR NETWORK." *TPM–Testing, Psychometrics, Methodology in Applied Psychology* 32, no. S5 (2025): Posted 03 August (2025): 599-622.

[33]. Porkodi, S., and D. Kesavaraja. "A Trust-Based Recommender System Built on IoT Blockchain Network With Cognitive Framework." *Recommender system with machine learning and artificial intelligence: practical tools and applications in medical, agricultural and other industries* (2020): 291-311.

[34]. Abdalzaher, Mohamed S., Mohamed Elwekeil, Taotao Wang, and Shengli Zhang. "A deep autoencoder trust model for mitigating jamming attack in IoT assisted by cognitive radio." *IEEE Systems Journal* 16, no. 3 (2021): 3635-3645.

[35]. Akter, Sharmin, Mohammad Shahriar Rahman, and Nafees Mansoor. "An Efficient Routing Protocol for Secured Communication in Cognitive Radio Sensor Networks." In *2020 IEEE Region 10 Symposium (TENSYMP)*, pp. 1713-1716. IEEE, 2020.

