

RESEARCH ARTICLE

BlockCRN-IoCV: Secure Spectrum Access and Beamforming for Defense Against Attacks in mmWave Massive MIMO CRN in 6G Internet of Connected Vehicles

P. DEEPANRAMKUMAR¹ AND N. JAISANKAR¹

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India

Corresponding author: N. Jaisankar (njaisankar@vit.ac.in)

ABSTRACT Cognitive Radio (CR) is a wireless communication system that is used for intelligent vehicles to solve spectrum scarcity and improve the utilization of the spectrum. However, spectrum sensing and data sharing are difficult due to the presence of malicious nodes which degrades the performance. To overcome these issues, we proposed the BlockCRN-IoCV method which includes authentication, density aware clustering, dual agent based spectrum access and secure beamforming. Here, authentication is performed for both Primary Users (PUs) and Secondary Users (SUs) using the Hybrid Advanced Encryption Standard and Hyper-elliptic Curve Cryptography (AES-HCC) algorithm by considering ID, PUF and location which ensures the legitimacy of the users. To address the mobility of the vehicle we perform density aware clustering using Density aware Dynamic Radius Clustering (DADRC) by considering location, distance and direction for increasing throughput. After completing clustering, we perform efficient spectrum access by using the Dual Agent based Twin Delayed (DA-TD3) algorithm which includes two agents, the first agent performs spectrum sensing by considering SNR, noise level and trust, and the second agent performs spectrum allocation by considering Channel State Information (CSI), in which the CSI is predicted by Quasi-Newton Iterative Unscented Kalman Filter (QNIUKF) algorithm for effective data transmission. Finally, secure beamforming is performed using Bi-Gated Recurrent Neural Network (BiGRU-CapsNet) by considering CSI, beam score, array factor, and direction of angle. The simulation is carried out by OMNET++ and SUMO simulation tools and the performance of this work is evaluated by throughput, packet delivery ratio, SNR, detection accuracy, BER, and delay. The simulation result shows that the proposed work achieves superior performance compared to existing work for secure spectrum sensing and beamforming.

INDEX TERMS

Cognitive radio network (CRN), 6G, Internet of Connected Vehicles (IoCV), spectrum sensing, secure beamforming, BiGRU-CapsNet, Quasi-Newton iterative unscented Kalman filter (QNIUKF).

I. INTRODUCTION

Cognitive Radio (CR) is a type of wireless communication that can intelligently detect the communication channel that is used or not [1]. A cognitive radio network (CRN) is aware of two primary environmental objectives, such as the efficient usage of the radio spectrum and highly reliable

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Jiang¹.

communication when needed [2]. The next generation wireless network with various technologies, such as beyond fifth generation (B5G) and sixth generation (6G), are estimated to provide a connection for the internet of vehicles (IoV) with high reliability and low latency using artificial intelligence (AI) [3]. The interconnection of vehicles is performed by vehicles that are equipped with WLAN using the internet. This is referred to as the internet of connected vehicles, and it is used for many applications, such as smart roads and

traffic management. To avoid and prevent accidents caused by errors of human driving systems, an automated driving system is developed by integrating various technologies, such as tracking, decision making and surrounding sensing. Machine learning (ML) and Deep Learning (DL) algorithms are used for detecting past and future predictions from large-scale datasets [4], [5].

CR devices track all the spectra located in the area to identify different spectrum holes and primary users. To mitigate the bandwidth shortage in CRs, two types of users are introduced: primary users (PUs) and secondary users (SUs) [6]. The licensed user can access the spectrum that has high priority, and the other user is known as an unlicensed user who can access the spectrum opportunistically [7]. In CR spectrum sharing, the SUs can exist with the primary transmitter and PUs below the condition that the interference affected by the cognitive base station (CBS) is acceptable to PUs. CR has a spectrum scarcity issue in which spectrum access is a main function for preventing concurrent spectrum access by SUs and PUs. The unused spectrum of PUs can be accessed by SUs. Hence, this type of access requires extra spectrum sensing by SUs for detecting the idle spectrum of PUs, and SUs are permitted to transmit at the highest power [8]. To solve these issues, a dynamic spectrum sharing and allocation method is developed in CR technology to enhance the efficiency of the spectrum [9], [10]. Then, the SUs select an idle channel for occupying the spectrum and collect the sensing report by the sensing module of the SUs. Reinforcement learning (RL) algorithms are used for selecting optimal channels, which are known as spectrum decisions in CR and control the overall throughput and false alarm probability [11]. Recently, the number of smart devices has increased, which leads to an increasingly high cost of upgrading and operating radio access networks. Massive multiple input and multiple outputs (MIMO) is proposed for handling high mobile traffic demands. A large number of antennas in radio frequency are needed for efficient communication. The massive MIMO improves spectral efficiency and reduces energy consumption [12]. The centralized MIMO leads to high diversity gains by beamforming, which provides the greatest performance and flexibility [13]. It can adapt the antenna array radiation pattern in massive MIMO. Efficient beamforming is used to suppress the problems of interference with high data rates. Three types of beamforming techniques are available in MIMO, such as digital, analog and hybrid beamforming [14], [15] [16]. Massive MIMO is implemented in beamforming for multiple SUs to provide efficient transmission and high spectrum efficiency in an environment with high mobility. Beamforming is improved with high energy efficiency, strong security, and enhanced spectral efficiency by implementing 6G mm waves in massive MIMO.

Various bandwidth availability and security issues are present in the evolution of technologies such as data bandwidth support, spectrum range and availability of spectrum. Currently, information or data security is mainly focused on wired and wireless communication because of the large

amount of data transmission, which suspects eavesdropping. Blockchain is used to improve data security by performing secure spectrum sensing and beamforming [17], [18]. Hence, more attention is given to physical layer security, which prevents the network from attackers such as eavesdropping, jamming and primary user emulation (PUE), spectrum sensing data falsification (SSDF), and attacks such as Byzantine, to handle spectrum scarcity for increasing QoS [19], [20]. However, effective spectrum access and beamforming in a secure manner is still a demand of state-of-the-art.

A. MOTIVATION & OBJECTIVES

The main aim of this research is to design an autonomous driving system using 6G and cognitive radio technology. This research also addresses the problems of spectrum scarcity, high mobility, security, network traffic control, and poor scalability in a 6G mmWave Massive MIMO cognitive radio network based IoCV environment. We are motivated by several problems which are shown as follows,

- **High Mobility:** The Internet of connected vehicles (IoCV) has high mobility due to its moving nature; however static mobility degrades the performance of the network. It increases high data loss and low throughput due to weak RSSI which reduces the communication between PUs and SUs and leads to unreliable communication.

- **High network traffic:** The IoCV environment has high network traffic due to sharing an enormous amount of data at a particular time, which increases high latency and reduces the performance of data sharing. The routing process is used to increase the packet delivery rate. Not considering the transmission direction leads to transmission delay.

- **Lack of security/privacy:** Lack of security leads to high data threats in the IoCV environment. The IoCV vehicle needs high security because it transmits information through the internet in a public way that can easily be compromised by attackers. This type of hacking leads to not only the loss of private information but also the loss of vehicles by theft.

- **Spectrum scarcity and Allocation:** Most of the available spectrum allocation leads to spectrum scarcity issues. Many types of research focus on solving these issues, but it still does not have an accurate solution. To reduce the utilization of the spectrum by SUs, proper spectrum allocation policies are necessary to solve this issue.

The motivation issues of this research are illustrated in fig 1. The main objective of this research is formulated by considering these issues to design an autonomous driving system with high security, low traffic, efficient spectrum allocation, and high scalability. The other objectives of this research are listed as follows:

- To increase the security level of the CRN network by performing blockchain-based authentication for both primary users and secondary users that perform against external attackers.

- To address the dynamic mobility of autonomous vehicles by performing density-aware clustering and handover of vehicles in an IoCV environment.

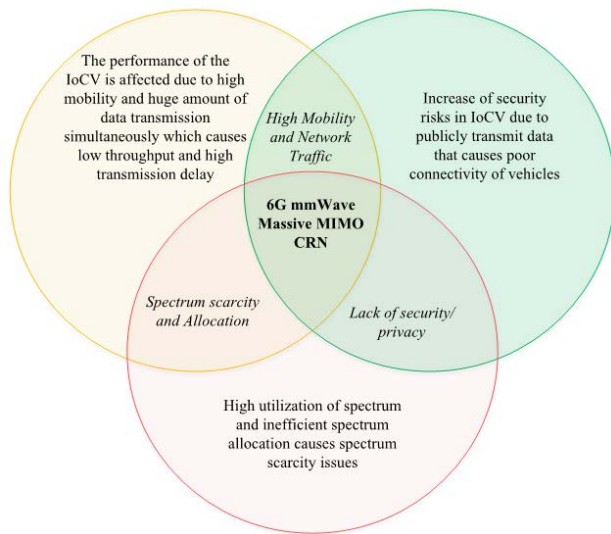


FIGURE 1. Research motivation.

- To address spectrum scarcity by performing dual agent-based spectrum access, which provides efficient spectrum access. By encrypting the spectrum sensing report, this research mitigates SSDF attacks in the network.
- To enhance the quality of the signal by performing secure beamforming, which enhances the transmitting speed in the network, and verifying the CSI using blockchain provides secure beamforming.

B. RESEARCH CONTRIBUTIONS

This approach is focused on designing an autonomous driving system by utilizing spectrum effectively using 6G and CRN. The AI in the IoCV environment is adopted to intelligently communicate with the environment (RSU and other vehicles) to reduce the risk during driving. 6G communication is utilized to reduce the latency and communication overhead and provide high transmission reliability during communication. Blockchain technology is used to ensure the security and privacy of the individual vehicle and RSU in the environment. Furthermore, clustering technology is adopted to reduce the energy consumption among the vehicles and mobility issues in the IoCV environment. The combination of these technologies in the IoCV environment supports energy efficient, highly secure, and robust contributions. The major contributions of this research are listed as follows:

- For enhancing the security of the IoCV environment, we perform authentication for both PUs and SUs using blockchain by a hybrid AES-HCC algorithm.
- For addressing dynamic mobility we perform density aware clustering using density aware dynamic radius clustering (DADRC) by considering location, distance, and direction with efficient handover.
- For efficient spectrum sensing and allocation, we perform dual agent based spectrum access using the DA-TD3 algorithm which properly senses the spectrum. Based on

that fusion center generate and encrypt the spectrum sensing report which prevents eavesdropping and SSDF attacks.

- Quasi-Newton Iterative Unscented Kalman Filter (QNIUKF) is used to evaluate the CSI which improves the efficacy of spectrum allocation and the data transmission process.
- To improve security and signal quality, we perform secure beamforming using the Bi-Gated Recurrent Unit-Capsule Network (Bi GRU-CapsNet) algorithm, in which the parameters are retrieved from the blockchain to provide secure beams that increase the security of the IoCV environment.

Finally, the performance of this research is evaluated in terms of throughput, packet delivery ratio, delay, SNR, detection accuracy, SINR, total transmit power, sensing delay and spectral efficiency.

C. PAPER ORGANIZATION

The remainder of this paper is structured as follows; Section II explains the survey of the existing works, which includes the research gaps. Section III presents the major problem statement of the existing approaches. Section IV provides the research methodology of the proposed BlockCRN-IoCV model with pseudocode, proper diagrams and mathematical representations. Section V explains the experimental results and provides comparisons of the proposed and existing approaches. Section VI presents the conclusion and future directions of the proposed work.

II. LITERATURE SURVEY

In this section, various existing works related to secure spectrum access and beamforming based on ML and DL techniques are classified into three categories, which are summarized as follows. This section additionally consists of the research gaps of these previous works.

A. SCHEMES FOR SECURITY ATTACKS IN CRN

In [21], the authors proposed resource allocation in the cognitive radio enabled internet of vehicles. The proposed system network is divided into multiple cognitive cells. The proposed SNO-CRAVANET model includes three subsections: the vehicular cluster mobility model, PU activity, and packet arrival process. First, the CRV-SU cluster is formed with minimum time, which manages the mobility using speed. Second, the PU (licensed user) transmits the packet from both the cluster head and cluster members. Finally, a queue is maintained with Q packets that are used at every CRV-SU CM to other buffer packets. Here, SINR is considered for estimating channel quality, which is not enough for measuring channel quality because CSI and environmental factors also affect the channel quality; hence, this work selects fewer quality channels that degrade the performance. The authors proposed a two-tier EI-empowered autonomous vehicle driving approach in [22]. The simulation result shows that the proposed model achieves high efficiency and finally provides open research topics. The proposed work expresses the

binary offloading decision-making process and resource allocation for mixed integer nonlinear programming problems (MINLP). To solve this problem, a multitask learning (MTL) framework is proposed that provides high efficiency and accuracy. An autonomous driving system includes three modes: the local inference mode, joint inference mode and edge inference mode. The inference performance depends on the vehicle's computational capability. A deep neural network (DNN) is used for dividing the edge vehicle joint inference. Here, the performance of inference depends on the vehicle's current available computation capability; however, it increases complexity in 6G environments, thus degrading the performance.

Authors proposed detecting PUEA and SSSF attacks using proactive learning method based MAC protocol in cognitive radio network [23]. The proposed PROLEM method is used for channel allocation due to the efficient learning and feedback method. The proposed model predicts the transmission state, such as idle or busy, for every PU channel. It includes three modules: the set point calculation module, error correction and target calculation module and control calculation module. The simulation result shows that the proposed PROLEM method achieves better performance in terms of channel utilization, backoff rate, and sensing delay when compared to existing methods. Here, all the processes (ex. transmission state prediction, feedback collection) are transmitted and stored in a public manner, which can easily be misuse by the attacker, leading to poor security. Ensemble learning based detection of the presence of malicious secondary users in a cognitive network was proposed in [24]. The degradation in the performance of sensing caused by malicious users in the network was addressed in this approach. The performance of the multimodel based detection technique was found to be higher than that of a single model-based detection technique. The multiple models utilized in this approach were SVM and TCRNN. The tuning of hyperparameters was performed based on the Bayesian optimization algorithm. The reputation based weighted majority learning method (RWMV) was used to determine the weights of the users based on their reputation. The probability based determination of the final threshold was performed to detect the malicious nodes. The secondary users in the network were determined to be trusted users and malicious users based on the current trust report, but the lack of consideration of the historical trust of the nodes degraded the efficiency of detection.

A probabilistic approach-based detection of malicious secondary users in the cognitive radio network was proposed in [25]. The detection of attacks in the network was carried out without any prior knowledge of the attack pattern. The fluctuation in the trust values was addressed by utilizing the sigmoid log function approach. The sliding window concept was leveraged to update the trust values of the nodes based on the decision taken over the sensing report. The static threshold was computed to differentiate the trusted secondary users and malicious secondary users in the network. Based

on the current threshold value and the past trust of the node, malicious nodes in the network were detected. The detection of malicious users was performed based on the static threshold computed on the difference between the sensing reports. However, the lack of generation of dynamic threshold values reduces the accuracy of the detection approach.

The authors in [26] proposed an approach to perform spectrum handoff in CRN with high security. Initially, the handoff mechanism was performed by computing the trust value of every user in the CRN, which increases the security by mitigating CUEA attacks. The trust value (i.e., the legitimacy or malicious characteristics) of the CU was evaluated using CCU, which computes TV to record all the DDR of CUs. The security of the handoff mechanism was implemented in two various types of cases in which the first case detects the NU as PU and the second case identifies the NU as HCU or CU.

B. SCHEMES FOR BEAMFORMING

Authors in [27], addressed the problem of traditional beamforming energy allocation and power control by proposing SWIFT enable edge computing in cognitive radio. Here, SU and ET are prepared with a single antenna for harvesting radio frequency energy, creating mobile computing to enable wireless communications. The idle users are used to harvest the energy, which is known as energy receivers. The probabilistic CSI model is used to identify the channel vector errors. The proposed work includes an AN-aided communication methodology for a cognitive base station to effectively forward the information to users with artificial noise. The edge nodes are used to solve the energy problems in this research. SWIPT enables CR to be extended with unlimited scaling capability. Here, the cognitive base station transmits the information with artificial noise to the end users, which does not provide high security that can easily be compromised by the attackers, thus leading to poor security. The authors proposed antenna muting and beamforming optimization using a deep learning algorithm in distributed massive MIMO [28]. Here, a Deep Neural Network (DNN) is proposed for solving the muting and beamforming optimization problem. It includes an input layer, hidden layer, fully connected layer and output layer, which are the beamforming matrix, antenna state, and optimal transmission power, respectively. Then, the data generation process is explained in this paper, which includes the training and testing phases. A stochastic gradient algorithm is implemented for solving optimization. The simulation result shows that the proposed model achieves better performance in terms of accuracy and less computation time compared to the traditional algorithm. Here, beamforming only considers the beamforming matrix, optimal transmission power and antenna states, which are not sufficient for secure beamforming, thus degrading the performance of this work.

Authors in [29], proposed a beamforming verification method for data sharing in fifth generation (5G) VANET. The main aim of this research is to use multiple data resources with the aid of RSU for verifying the vehicle. The proposed

system includes two verification systems: the client server model and the local detector. First, the local detector verifies the target vehicle using a signal-based verification system. Next, the information is collected from V2X signal-based localization using the DCS-SOMPS/SAGE algorithm. The target trajectory is extracted by cooperative awareness messages (CAM). The Dempster-Shafer method is used for fused local and global detectors to make final decisions. The simulation result shows that the proposed work achieves better performance in terms of response time and detection accuracy compared to existing work. Here, all the data are shared and stored over the internet in a public manner, which can easily be hacked by attackers, resulting in eavesdropping of channels and thus leading to poor security. In [30], machine learning-based beamforming was proposed using selfish and altruistic strategies in an ultradense network. A reinforcement learning algorithm is proposed in machine learning for obtaining the best action of beamforming. A deep Q network is deployed to beamforming agents for calculating vectors of beamforming. The performance of the proposed work is evaluated in the Multiple Input and Multiple Output (MIMO) configuration. The simulation result shows that the proposed model achieves better performance using Q learning, which consists of both small- and large-scale fading and beamforming. Here, beamforming is performed by considering only the balancing coefficient, which is not sufficient for optimal beamforming and degrades the quality of the signal. The balancing coefficient is calculated and shared in a public manner without any verification, which leads to insecure beamforming.

The authors proposed a beamforming approach for secure data transmission in a 5G cognitive radio network [31]. The proposed beamforming approach includes two users: the primary user (PU) and the secondary user (SU). Every cluster includes multiple antennas and users. First, the licensed PU shared their data with the same frequency and time. The data leakage is addressed by the proposed technique in the base station. The CSI is calculated based on the receiver's response using a feedback channel. The secrecy outage possibility of both PU and SU was analyzed by the power allocation policy of CRN. Finally, the simulation result shows that the proposed work achieves better performance compared to existing works. During beamforming, CSI is evaluated by considering the receiver response, which is not enough for calculating CSI, thus increasing interference. The CSI is not verified before beamforming, which leads to insecure beamforming, thus reducing the performance of the proposed work.

The authors in [32] proposed an approach to perform dual stage beamforming using a neural network and bidirectional long short-term memory (Bi-LSTM) to reject the signal interferences. Initially, a neural beamformer was implemented to evaluate the original signal with interferences and noise using a convolutional neural network (CNN). The interference vectors estimation from the antennas by performing training with autocorrelation matrix using CNN algorithm. Sampling estimation for the desired signal was performed

using Bi-LSTM. All significant features were learned using individual memory cells of Bi-LSTM. Evaluation of this method was performed in terms of the SINR value.

In [33], the authors proposed an approach to perform hybrid beamforming in mmWave-based MIMO network communication with secured multicells. Initially, MU-MIMO-based mmWave communication was performed at legitimate users, BSs, and eavesdroppers by implementing hybrid beamforming. The eavesdropper attack was mitigated by using the mmWave-based 3D channel model to transmit the signal for every node. In the 3D channel model, AN beamforming was used to reduce eavesdropping by jamming it during the transmission. Finally, a beamforming design was performed by considering SLNR for the CoMP case. For the case of Non-CoMP, ZF, RB, and MRT were considered and evaluated in terms of computational complexity and secrecy rate.

C. SCHEMES FOR SPECTRUM SENSING AND ACCESS

The authors proposed a power domain-based dynamic spectrum access approach to control transmission power for building small cells in [34]. 28 GHz spectrum is allocated to the mobile network operator (MNO), which is known as the primary MNO. The transmission power threshold is generated by the primary MNO. In the proposed work, the secondary MNO is used to detect the user equipment of every primary MNO to update the access mode of the spectrum. For that, this research used both reactive and proactive sensing techniques. To satisfy the minimum CCI, this research proposed spectrum reuse techniques such as dynamic spectrum access (DSA) techniques. Three-dimensional small cell clusters are formed within a building to satisfy a lower CCI between small cell base stations (SBS). Here, a dynamic spectrum access technique is proposed for spectrum sensing; however, CSI calculation is a significant feature for spectrum sensing and access; otherwise, it leads to poor spectrum access. The allocation of the spectrum using a deep reinforcement approach was proposed in [35]. The integration of both backhaul and access networks was carried out, and allocation of the spectrum for both the backhaul links and access links was performed. The objective of the spectrum allocation approach was to maximize the cumulative log rate of the users in the network. The advantages of reinforcement learning approaches in solving dynamic problems were analyzed, and an actor critic-based resource allocation approach was introduced. The channel state information was not considered for the allocation of resources, which thereby reduced the complexity involved in allocating resources. The QoS requirements for each user were also considered for the resource allocation process. The actor critic model was utilized to achieve an effective solution in the allocation of the spectrum to the user nodes.

Authors proposed dynamic spectrum access and allocation method based on trading for cognitive Internet of Things network in [36]. The proposed work architecture includes four layers: the information sensing layer, network connection layer, cognitive layer and service layer. The IoT users need

TABLE 1. Summary of existing works.

Process	References	Objectives	Algorithms or Methods Used	Drawbacks
Security Attacks in CRN	[21]	Resource allocation in CR-IoV	Clustering, PU activity and packet arrival	Low channel quality
	[22]	Binary offloading decision and resource allocation for MINLP	MTL framework and DNN algorithm	High computation complexity
	[23]	Detection of PUEA and SSDF attacks	PROLEM method	Poor Security
	[24]	Detection of malicious SUs	SVM, TCRNN, and Bayesian optimization algorithms	Low detection efficiency
	[25]	Detection of malicious nodes	Sigmoid log function and Sliding window concept	Low detection accuracy
	[26]	Spectrum Handoff	Secure Handoff mechanism	High Interference
Beamforming	[27]	Secure Beamforming	Probabilistic CSI model and SWIFT based edge computing	Poor security
	[28]	Optimization of beamforming and antenna muting	DNN and Stochastic gradient algorithm	Insufficient security
	[29]	Verification of beamforming	SAGE algorithm and Dempster-Shafer method	Low Security
	[30]	Beamforming in ultra-dense network	Reinforcement learning algorithm	Insecure beamforming
	[31]	Secure Beamforming	Power allocation policy	Insufficient beamforming security
	[32]	Interference less Beamforming	Bi-LSTM	Inaccurate CSI
	[33]	Multiuser Beamforming	Deep Neural Network	High Attack Threats
Spectrum Sensing and Access	[34]	Dynamic spectrum access	Proactive and reactive techniques	Poor spectrum access
	[35]	Spectrum allocation	Deep reinforcement algorithm	High spectrum allocation latency
	[36]	Dynamic spectrum access and allocation	QAM modulation and Lagrange method	Low performance of spectrum allocation
	[37]	QoS aware spectrum access	ANN algorithm	Poor spectrum access efficiency
	[38]	Detection of false sensing	Dempster-Shafer theory	Partially overcome the malicious SUs

a spectrum from an authorized source. If the user receives an idle spectrum, then it is divided into multiple channel bands. The IoT users used QAM modulation to enhance the quality of the communication. The Lagrange method is proposed to solve the optimization problems (optimal spectrum allocation) of cognitive IoT users. The experimental results show that the proposed model achieves better performance for spectrum optimization. Here, spectrum allocation is performed by calculating the utility function; however, it does not have CSI information and previous interference, thus reducing the performance of the spectrum allocation in a cognitive IoT environment.

Authors in [37], proposed a QoS aware sensing access technique using a machine learning algorithm for the cognitive radio network. The main aim of this research is to reduce the sensing delay and be conscious of unlicensed user requirements. The proposed system includes 4 RATs near the SU for data transmission and provides coverage for the SU, which searches the available frequency band. The coverage considers the distance of the SU from its present location. The spectrum sensing process considered the selected RAT bandwidth. Sensing latency is used to calculate the delay by unsuccessful sensing, which is increased to many failures. An ANN is proposed for predicting the future traffic load for every RAT using historical data. Here, ANN is used for predicting future traffic load; however, the processing time of ANN is unknown, which increases high latency and does not provide optimum results, thus reducing the efficiency of the work.

The detection of false sensing reports generated in the cooperative sensing of the spectrum was proposed in [38]. The advantages of performing cooperative spectrum sensing

to mitigate several sensing problems were considered, and the effect of SSDF attacks in the cooperative sensing model was addressed in this approach. The credibility-based validation of the legitimacy was performed. Evidence theory was adopted to determine the probability assignment function for each node, and the weighted sum of these probabilities was computed to provide the global decision. The probability-based detection of malicious users was found to resist the influence of illegitimate users but cannot fully overcome the effects of these illegitimate secondary users. Table 1 shows the summary of the previous works.

III. PROBLEM STATEMENT

The major problem statement in spectrum access and beamforming is to minimize the sensing delay and maximize spectrum utilization and security. This is expressed in this section along with problems faced by existing works in spectrum access and beamforming in the 6G mmWave Massive MIMO cognitive radio-based IoCV environment. Let the number of SUs in the network be denoted as $SU_i = \{su_1, su_2, \dots, su_i\}$ and the number of PUs be denoted as $PU_i = \{pu_1, pu_2, \dots, pu_i\}$. The objective of this research is to minimize the sensing delay and maximize the spectrum utilization, security, throughput, and packet delivery rate in the proposed environment. Every SU takes t_i amount of time to sense the available spectrum, which is formulated as follows:

$$\text{Min} \sum_{i \in R} SL_{i,t(i)} \tag{1}$$

$$SL = \frac{N_f}{SU_P} \tag{2}$$

where SL represents sensing delay $t(i)$ represents the sensing time of i SUs, N_f represents a total count of channels sensed and SU_P represents the total count of transmitted SU packets. To reduce spectrum scarcity issues, we need to utilize the spectrum efficiently. For that purpose, we need to improve the spectrum utilization by SUs, which is defined as follows,

$$\text{Max} \sum_{i \in R} \tilde{a}_{i,a(i)} \quad (3)$$

where \tilde{a} represents the spectrum utilization and $a(i)$ represents the number of SUs utilized in the available spectrum in the environment. The other problems presented in the existing work are explained as follows. Blockchain-based security in the cognitive radio-assisted internet of connected vehicles environment was proposed in this paper [39]. The degradation in the performance of connected vehicles due to the presence of malicious nodes in the network was considered, and an effective security approach was executed during the sensing of the spectrum and transmission of information. The major problems of this research are listed as follows:

- The trust value of the vehicles in the network was computed by the fusion center by incorporating the TOPSIS method; however, it faced difficulties in maintaining the consistency of the decision.
- The CRT-BIoV approach improved the security and transparency of communication in the network, but security threats such as random SSDF attacks were not mitigated, which affected the security of the network.
- The data transmitted in the network are stored in the blockchain, which cannot be tampered with, but during the communication between the vehicles or to the infrastructure, the attackers can initiate eavesdropping due to lack of encryption of the data.

The deep reinforcement learning-based cooperative sensing of a spectrum in multiple user environments was proposed in this paper. The dueling deep Q network was implemented for the dynamic sensing of the spectrum to allocate the unoccupied spectrum to the users [40]. The two-level securities were provided for the users during spectrum sensing in cognitive radio networks [41]. The genetic algorithm (GA) based filtration of false sensing reports was proposed in this paper [42]. The major problem of this research is defined as follows:

- The security attacks such as PUE, jamming, eavesdropping, and SSDF carried out in the cognitive network during the spectrum sensing process were not mitigated which leads to increased interference and waste of resources in the network.

- However, the SSDF attacks launched by malicious secondary users during spectrum sensing were mitigated by this approach, but the other attacks such as jamming, PUE, and eavesdropping, during spectrum sensing were not mitigated affecting the robustness of this approach.

- The reputation of the nodes in the network was determined by the neighboring nodes based on the difference in the report but this increases the confusion in determining the

accurate reputation of a node as the malicious nodes provided the bad reputation to the legitimate users.

Secure beamforming framework for cognitive radio (CR) and Non-orthogonal Multiple Access (NOMA) networks was proposed in [43]. This research examines the physical layer security for the CR-NOMA network.

- The secure beamforming was carried out based on the CSI value but the lack of consideration of significant factors such as array factors and Direction of Angle (DoA) affects effective beamforming.
- Here, the secrecy rate is based on the QoS at the PU and transmitter power of the ST, which is not enough for calculating the secrecy rate of the SU, thus degrading the robustness of the process.
- The formation of a beam for the effective transmission of data was inefficiently performed due to the exception of the beam score, which leads to further scattering of the beam.

IV. BlockCRN-IoCV MODEL

The proposed work focuses on increased efficiency in the transmission of data through secure sensing and allocation of resources in the 6G mmWave Massive MIMO cognitive radio network-based IoCV environment. 6G communication is adopted to achieve increased throughput in the transmission of data between autonomous vehicles. Blockchain technology is used to ensure the security and privacy of the overall network. The implementation of various entities, methods, and technologies is performed in this work, which is described as follows:

(i) **6G Core-** This technology provides high bandwidth and communication speed, which is mainly implemented to perform effective communication between PUs to SUs and SUs to FCs in terms of high reliability and ultralow latency with sufficient network coverage.

(ii) **Beamforming-** The beamforming technique is used to enhance the signal quality by creating high-quality beams that also improve the spectral efficiency of the overall IoCV environment.

(iii) **Blockchain-** This technology is deployed to increase the security in the network. The trusted authority verifies all the requests of SUs by authenticating the SUs and stored in the blockchain to provide security during data transmission based on SU legitimacy.

(iv) **Spectrum Sensing-** Spectrum sensing is performed to analyze the available spectrum for allocating resources. FC performs decision making to ensure security by evaluating trust.

The increased spectral efficiency is achieved by integrating the Massive MIMO technology in the cognitive radio network. The research methodologies of this approach are explained by the following subsections,

A. NETWORK MODEL

The proposed 6G mmWave Massive MIMO cognitive radio-based IoCV environment includes primary users (PUs) that are also known as licensed users and several vehicles that

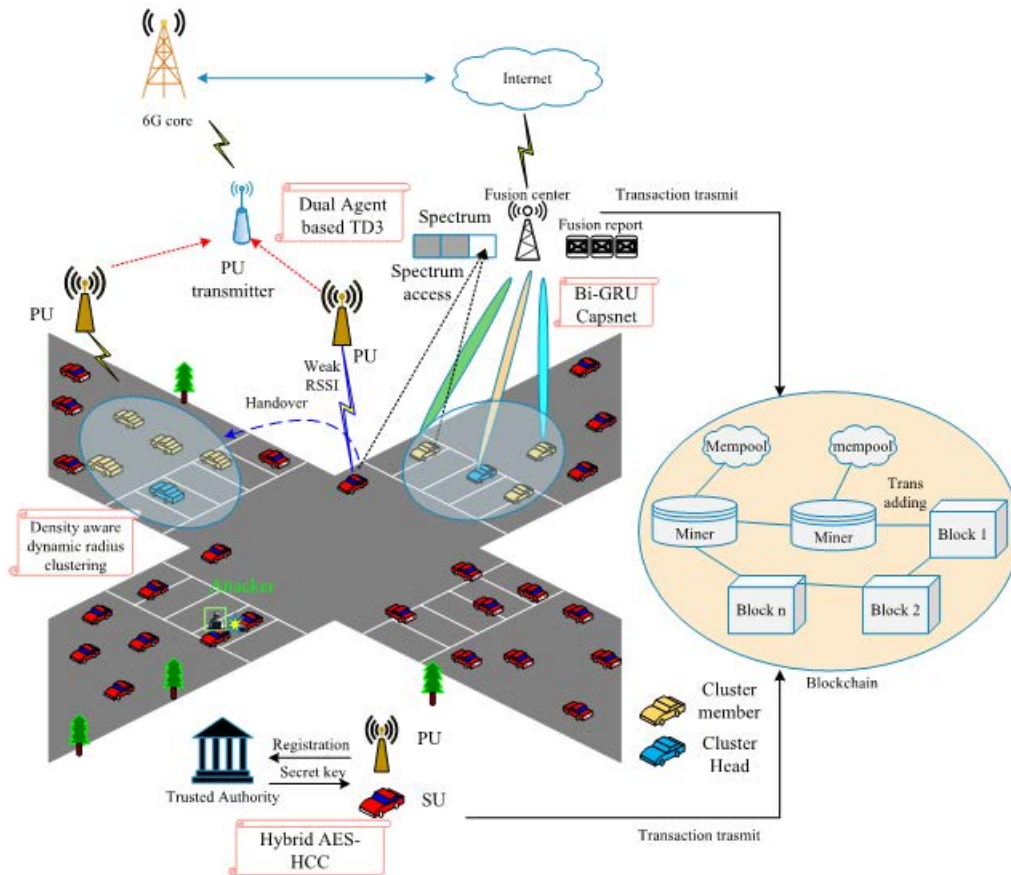


FIGURE 2. Architecture of BlockCRN-IoCV.

are known as secondary users (SUs) that are also called unlicensed users, which are illustrated in fig 2. The SUs can sense the environment to utilize the licensed spectrum if any of the licensed PU spectra is idle. All the SUs send the sensed spectrum report to the Fusion Center (FC), which is also called the Cognitive Base Station (CBS). Both CBS and FC have the same meaning in this research and are deployed with a mmWave Massive MIMO antenna. Here, the Trusted Authority (TA) is used to ensure the legitimacy of SUs and PUs because it provides the secret key to every PU and SU for validation. These private transactions are stored in the blockchain to provide high security. In this way, we mitigate the attacks in the environment and perform secure spectrum and beamforming. Table 2 represents the goals of the proposed work.

B. AUTHENTICATION

The authentication of both primary and secondary users is carried out to achieve increased security in the IoCV environment. For this purpose, both the primary users (PUs) and secondary users (SUs) in the CRN are authenticated by the blockchain-based trusted authority. In our proposed approach, the primary users are the road side units (RSUs), and the secondary users are the autonomous vehicles present

in the environment. Initially, credentials such as ID, Physically Unclonable Function (PUF), and location of both the PUs and SUs are registered to the blockchain-based trusted authority in which the credentials are stored in a hashed manner. The blocks are chained together, thereby providing an untampered nature. The secret key is generated by incorporating the hybrid AES-HCC algorithm. The execution of authentication mitigates the security threats caused by malicious secondary users.

The number of PUs is represented as $PU_i = \{1, 2, \dots, N\}$, and the number of SUs is denoted as $SU_i = \{1, 2, \dots, N\}$. The credentials of PUs and SUs, such as ID , PUF , and L are registered to TA, which is expressed as follows,

$$TA \leftarrow Reg(PU_{ID})(PU_{PUF})(PU_L) \quad (4)$$

$$TA \leftarrow Reg(SU_{ID})(SU_{PUF})(SU_L) \quad (5)$$

The credentials of PUs and SUs are hashed and stored in the blockchain after successful registration to the TA for authentication by hybrid encryption using the AES-HCC algorithm.

The Advanced Encryption Standard (AES) supports a 128-bit data block with keys of 128, 192 and 256 bits. Input data are arranged in 4×4 bytes with two-dimensional arrays

TABLE 2. Goals of proposed blockcrn-IoCV model.

Process	Algorithms	Goals
Authentication	Hybrid AES-HCC	<ul style="list-style-type: none"> • Increase security • Reduce external attackers
Density aware Clustering	DADRC	<ul style="list-style-type: none"> • Address mobility • Reliable communication • Increased performance
Dual Agent-based Spectrum Access	DA-TD3 QNIUKF	<ul style="list-style-type: none"> • Secure spectrum access • Improved spectrum utilization
Secure Beamforming	Bi GRU-CapsNet	<ul style="list-style-type: none"> • Secure beamforming • Improved spectral efficiency

Algorithm 1 Authentication

```

1: Begin
2: Initialize  $PU_i$  and  $SU_i$  where  $i=1,2,3,\dots,N$ 
3: for all  $PU_i$  and  $SU_i$  do
4:   Credential registration Phase ();
5:   Register  $C_i$  ();
6:    $C_i = \{PU_{ID}, PU_{PUF}, PU_L, SU_{ID}, SU_{PUF}, SU_L\}$ 
7:   Store Hashed Credentials in Blockchain;
8:   Initialize Authentication Phase ();
9:   Initialize AES phase ();
10:  AddRoundKey (state, &w[00])
11:  for  $i=1$  step 1 to 4 do
12:    SubBytes (state)
13:    ShiftRows (state)
14:    MixColumns (state)
15:    AddRoundKey (state, &w[j*4])
16:  end for
17:  Initialize HCC phase();
18:  Encrypt AES key using Public Key of HCC;
19:  Compress the ciphertext;
20:  Generate secret key for PUs and SUs;
21:  Verification of credentials;
22:  If (secret key == true) then
23:    Authentication Successful;
24:  Else
25:    Authentication Failed;
26:  End if
27: end for
28: End

```

known as the state, which has 16 bytes. It consists of three major steps, which are described as follows,

SubBytes is a first step, which is also a substitution step with nonlinear bytes that performs independently by a substitution table on State's every byte. Based on two transformations, the substitution table is derived and is invertible. Calculate multiplicative inverse in Galios Field, i.e., $GF(2^8)$ for the elements being mapped, and an affine transform is applied over $GF(2)$.

The second step is the ShiftRows step, which is also known as the transposition step that shifts the AES last three rows cyclicly toward the left with few bytes.

MixColumns is a final step and it is also called a permutation step that performs on each column present in the state. Every column of the state is assumed as four term polynomial with $GF(2^8)$ and $y^4 + 1$ multiplied modulo with $k(y) = \{03\}y^3 + \{01\}y^2 + \{01\}y + \{02\}$ fixed polynomial. The multiplication results in replacing four bytes in a single column which is expressed as follows,

$$\hat{a}_{0,k} = (\{02\} \cdot a_{0,k}) \oplus (\{03\} \cdot a_{1,k}) \oplus a_{2,k} \oplus a_{3,k} \quad (6)$$

$$\hat{a}_{1,k} = a_{0,k} \oplus (\{02\} \cdot a_{1,k}) \oplus (\{03\} \cdot a_{2,k}) \oplus a_{3,k} \quad (7)$$

$$\hat{a}_{2,k} = a_{0,k} \oplus a_{1,k} \oplus (\{02\} \cdot a_{2,k}) \oplus (\{03\} \cdot a_{3,k}) \quad (8)$$

$$\hat{a}_{3,k} = (\{03\} \cdot a_{0,k}) \oplus a_{1,k} \oplus a_{2,k} \oplus (\{02\} \cdot a_{3,k}) \quad (9)$$

In this step, each byte $a_{i,k}$ is multiplied by several constants, i.e., 01, 02, and 03 during encryption.

AddRoundKeys is the last step in which the addition of RoundKey with state and key scheduler is used to derive each RoundKey from the cipher key.

Hyper Elliptic Curved Cryptography (HCC) is used to encrypt the AES Key (k_{AES}) using the public encryption key of HCC $EN(k_{AES})$.

The transaction consisting of $(K_{pb}), (K_{pr}), EN(k_{ra}),$ key lifetime (k_L), current timestamp are submitted to the blockchain. The plaintext credentials are grouped to 1M packet and encrypt packet by the key generated by AES and public key of HCC respectively. Compressing the ciphertext of both AES and HCC to obtain overall ciphertext, this is expressed as follows,

$$\begin{aligned} \mathcal{R}_1 &= \sum_{c=1}^h \left\{ \mathcal{C} \left[\hat{E}n(T_{c \bmod 2 \equiv 1})_{k_{AES}} \right] \parallel \left[\hat{E}n(T_{c \bmod 2 \equiv 0})_{k_{HCCpub}} \right] \right\} \end{aligned} \quad (10)$$

where \mathcal{C} represents compression and $\hat{E}n$ denotes encryption.

$$\mathcal{R}_2 = \hat{E}n(k_{AES})_{k_{HCCpub}} \quad (11)$$

Encrypt the AES key by the HCC public key which is expressed as follows,

Where, k_{AES} represents the AES key and k_{HCCpub} represents the public key of HCC.

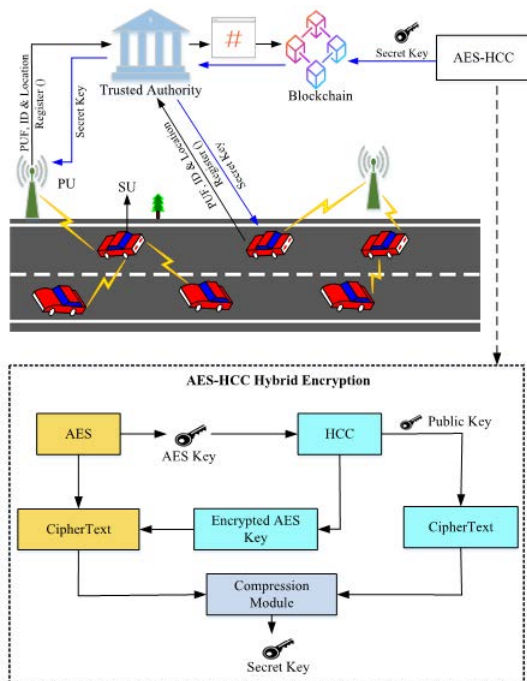


FIGURE 3. Authentication of PUs and SUs.

Connect \mathcal{R}_1 and \mathcal{R}_2 compress to obtain the overall ciphertext \mathcal{R} , which is expressed as follows,

$$\mathcal{R} = \mathcal{C}(\mathcal{R}_1 \parallel \mathcal{R}_2) \quad (12)$$

Initially, the SUs request the execution of the transaction in the network. Depending upon the request of SUs, a new block is created for transaction. The blockchain then verifies the newly created block by using the consensus mechanism. If consensus is achieved and the transaction is verified, the new block is mined, and the credentials of SUs are recorded in the blockchain. By doing so, the legitimacy of the SUs is verified before taking part in transmission. Only authenticated SUs can transmit through the fusion center; otherwise, malicious SUs are mitigated. Fig 3 illustrates the authentication of PUs and SUs.

C. DENSITY AWARE CLUSTERING

The mobility of vehicles in the environment is a crucial factor to be considered to address practical scenarios. For this purpose, the clustering of SUs is carried out in which the dynamic topology of the vehicles is considered. Density Aware Dynamic Radius Clustering (DADRC) is implemented based on significant parameters such as distance and direction. Only the same direction SUs are considered neighbor nodes. The radius of the cluster depends upon the density of the vehicles in a region at a particular time. Let $N = \{n_1, n_2, \dots, n_i\}$, $n_i \in P^d$ be the set of nodes, and $n_0 \in P^d$ be a given node and γ represent the positive integer of arbitrary. A set $S \subseteq N$ is known as γ radius neighbor of n_0 .

$$S = \{n_i \in N : d(n_i, n_0) \leq \gamma\} \quad (13)$$

Algorithm 2 Density Aware Clustering

```

1: Begin
2: Initialize  $c_1^{new} = \emptyset, i = 1$ 
3: for all nodes (n) do
4:   If (direction==1) then
5:     Select the nodes for clustering
6:   Else
7:     Get values of  $u_1, u_2, u_3$  using (16), (17) and (18)
8:   If (Values == True) then
9:     Compute  $c_1^{new} = \{u_1, u_2, u_3\}$ 
10:  Else
11:     $c_1^{new} = \{u_1\}$ 
12:  End if
13: End if
14: Develop  $c_1^{new}$  using  $\gamma$  radius based on (23) and (24)
15: If ( $c_1^{new} == \rho_i$ ) then
16:   Go to step 9
17: Else
18:    $c_i = c_1^{new}, i := i + 1, data := data \setminus c_1^{new}$ 
19: End if
20: Calculate the adaptive radius and centroid until met stopping condition
21: If ( $data == \emptyset$ ) then
22:   Stop cluster construction
23: Else
24:   Go to step 7
25: End if
26: // CH Selection
27: Initiate CH selection
28: If ( $n == \text{Max}(RSSI) \ \&\& \ \text{Max}(T)$ ) then
29:   Select the current  $n$  as CH
30: End if
31: end for
32: //Handover
33: Initialize parameters  $SINR, RSSI, d', LOS$ 
34: Compute  $F_p = \{SINR + RSSI + d' + LOS\}$ 
35: If ( $SU > Th$ ) then  $Th = -\sum_{j=1}^m P(F_p) \log P(F_p)$ 
36: Perform Handover
37: End if
38: End

```

where $d(n_i, n_o)$ represents the Euclidean distance between n_i and n_o . Here, the cluster is expanded based on the value of radius γ . The maximum extension of the cluster is calculated as follows,

$$\gamma = \max D = m + 2s_d \quad (14)$$

where m and s_d represent the mean and standard deviation of the past and current clusters, respectively. The largest value of the mean extension is calculated as follows,

$$\gamma = m + \frac{1.96s_d}{\sqrt{i}} \quad (15)$$

Then, initialize $c_1^o = \emptyset, c_1^n = \emptyset,$ and $Cen_{new} = \emptyset,$ where c_1^o and c_1^n represent before and after the update of the

current cluster, respectively. The three values of the cluster are defined as follows,

$$u_1 = \text{Arg} \min_{n_i \in N} \sum_{j=1}^k d(n_i, n_j) \quad (16)$$

$$u_2 = \text{Arg} \min_{n_i \in N/u_1} \sum_{j=1}^n d(n_i, u_1) \quad (17)$$

$$u_3 = \text{Arg} \min_{n_i \in N/u_1, u_2} \sum_{j=1}^n d(n_i, u_1) \quad (18)$$

where u_1 is the value of the cluster centroid and u_2 represent the nearest neighbor of u_1 and u_3 are the nearest neighbors of u_1 .

$$d(u_2, u_1) \leq d(u_3, u_1) < \left(\frac{2}{n}\right)^{-1} \sum_{i \neq j} d(n_i, n_j) \quad (19)$$

Update,

$$c_1^{old} = (u_1, u_2, u_3); c_1^{new} = \{u_1, u_2, u_3\} \quad (20)$$

If u_2 and u_3 are the two nearest neighbors of u_1 , however, the difference of distance is larger than the current dataset distances, then u_1 is considered as a single cluster and stops the cluster extension process. The distances are calculated based on the following formula,

$$d(n, m) = \sqrt{\sum_{i=1}^d (n_i - m_i)^2} \quad (21)$$

where m and n represents the data points and d represent the distance between the two data points. After calculating the distance the data are normalized into the interval $[0, 1]$ to equalize the data. The calculation of normalization is defined as follows,

$$Z_{ij} = \frac{n_{ij} - \text{Min}_i(n_{ij})}{\text{Max}_i(n_{ij}) - \text{Min}_i(n_{ij})} \quad (22)$$

where n_{ij} represents the variable value and Z_{ij} represents the normalized value of the variables. $\text{Max}_i(n_{ij})$ and $\text{Min}_i(n_{ij})$ represent the maximum and minimum values of the variables. For every $u_i \in c_1^{new}$ calculate the adaptive γ radius and update c_1^{new} and Cen_{new} based on the following formula,

$$c_1^{new} := c_1^{new} \cup \rho_i \quad (23)$$

$$Cen_{new} := \frac{Cen_{new}}{u_i} \quad (24)$$

where ρ_i represents the radius of neighbor nodes and Cen_{new} represents the value of the new centroid. If $c_1^{new}/c_1^{old} \neq \emptyset$, then $c_1^{old} := c_1^{new}$ and $c_1^{new} := Cen_{new} \cup c_1^{new}/c_1^{old}$. Again calculate adaptive radius and centroid until $Cen_{new} = \emptyset$, and then stop clustering. The above processes are repeated until all the nodes are assigned to the cluster. After cluster construction is completed, cluster head (CH) selection is initiated. Here, CH is selected by considering the maximum RSSI value and trust value. CH acts as an intermediate between the

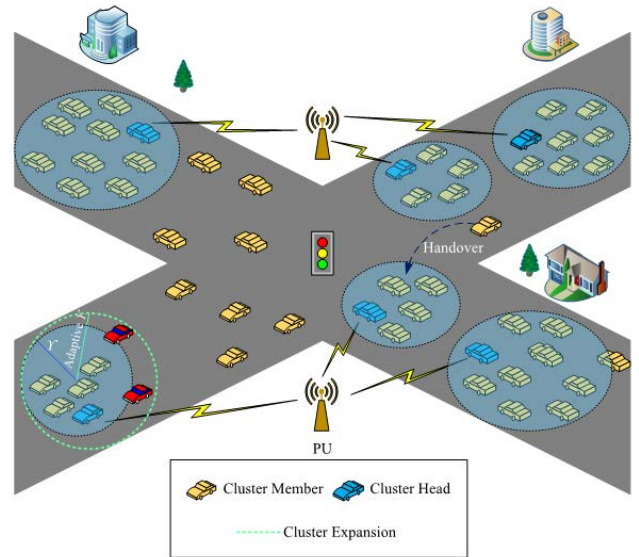


FIGURE 4. Dynamic clustering of SUs.

cluster member and the Fusion Centre (FC). The cluster head ID is generated to the CH by the trusted authority and broadcast to the cluster members to facilitate secure transmission. The clusters are formed in such a way that every vehicle in the cluster possesses one-hop communication with the CH. Handover of the vehicle is necessary for the high mobility environment. It is performed by PU between interclusters to increase the efficiency of coverage by considering coverage parameters such as SINR, direction, RSSI, distance, and elevation angle to address the dynamic mobility of the vehicles that are present in the network. Fig 4 represents the dynamic clustering of SUs.

(i) **SINR**- It is defined as the ratio between signal power and the sum of noise and interference power. It is also known as the signal-to-interference and noise ratio. The calculation of SINR is expressed as follows,

$$SINR = \frac{\check{s}_p}{N_p + \sum_{i=0}^I P_i} \quad (25)$$

where, \check{s}_p represents the signal power and P_i denotes the i^{th} channel's interference. N_p indicates the noise power.

(ii) **RSSI**- It is defined as the amount of received signal power which is measured by the ratio of the transmitted power to the received power and is expressed as follows,

$$RSSI = \frac{\hat{T}x_p}{\hat{R}x_p} \quad (26)$$

(iii) **Distance (d')**- The distance is calculated between two SUs in which the formulation for calculating distance can be represented as,

$$d'(\hat{r}, \hat{u}) = \sqrt{\sum_{j=1}^k (\hat{u}_j - \hat{r}_j)^2} \quad (27)$$

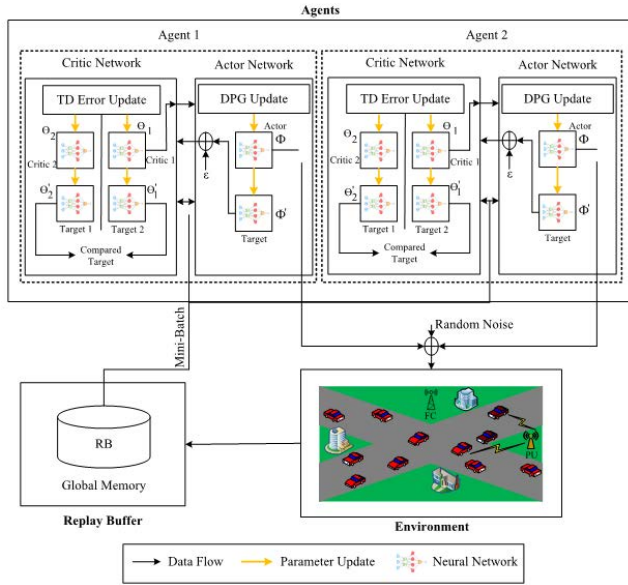


FIGURE 5. Dual agent-based spectrum access.

where, \hat{r} , \hat{u} represents the SUs and \hat{u}_j , \hat{r}_j represents the directions of the SUs.

(iv) **Elevation Angle (LOS)**- It is defined as the angle between the PUs horizontal line of sight and line of sight of SUs. The measurement of the elevation angle is represented as,

$$LOS = \frac{1}{1 + e^{-v(\frac{180}{\pi}\theta - y)}} \quad (28)$$

where v and y are constant values based on the environment and θ represents the elevation angle.

D. DUAL AGENT-BASED SPECTRUM ACCESS

The process of determining the availability of the unoccupied spectrum in the network is called spectrum sensing. Every SU in the network performs spectrum sensing and shares the sensing report with the FC to determine the global decision and to allocate the resources according to it. The Dual Agent-based Twin Delayed Deep Deterministic Policy Gradient (DA-TD3) algorithm is performed for spectrum access, in which the first agent focuses on spectrum sensing and the second agent focuses on the allocation of resources. The sensing of the spectrum is carried out based on factors such as SNR, noise level, and trust factor for each time interval. Fig 5 illustrates the spectrum access using the DA-TD3 algorithm. The trust factor is considered to mitigate the security attacks caused by the compromised SU. During sensing of the presence of PU, the PUE attack is mitigated by comparing the past nature of the signal with the current signal. The SUs in the network sense the spectrum by discovering the PU signal presence, which is formulated as follows,

$$R_n = \begin{cases} y(n), & T_0 = PU \text{ Absent} \\ C_g * S(n) + y(n), & T_1 = PU \text{ Absent} \end{cases} \quad (29)$$

TABLE 3. Attributes of DA-TD3 algorithm.

Attributes	Description
State (\mathcal{A})	SNR, noise level, and trust factor
Action (\mathcal{S})	Spectrum sensing
Reward (\mathcal{R})	Maximize $\bar{\delta}$, P_d, hv and minimize S_d

where $n = 1, \dots, N$ and N represent the count of samples and $R(n)$ represent the received signals of the SU and $S(n)$ represent the signal of PU and $y(n)$ represent the additive noise with zero mean and variance and T represent the sensing channel gain. This spectrum sensing is performed by the first agent of DA-TD3. The spectrum sensing is constructed as a Markov decision process with Action (\mathcal{S}), State (\mathcal{A}), and Reward (\mathcal{R}). The proposed DA-TD3 algorithm performs spectrum sensing and allocation. The attributes of DA-TD3 are illustrated in Table 3. Every agent includes actor network (π^i) and two critic networks ($C_{\pi 1}$, $C_{\pi 2}$) and the target network. This type of joint environment is used to observe the current status of the environment to perform an action. At time t , the action (\mathcal{S}_t^i) performed by the agents based on the current observation (O_t^i) in i , which represents the agent index. The combined reward (\mathcal{R}_t) is produced for the agent-based on \mathcal{S}_t^i . The two agents learn the policy $\pi^i(O^i | \mathcal{S}^i)$ to maximize the reward. The new state $\mathcal{A}_t^i(\mathcal{A}_{t+1}^i)$ is generated to perform the corresponding action in this state.

The value of the gradient is calculated based on the continuous policy with parameters θ^i which is defined as follows,

$$\nabla_{\theta^i} J(\pi_i) = E_{\mathcal{A}, \mathcal{S} \sim D} \left[\nabla_{\theta^i} \pi^i(\mathcal{S}^i | O^i) \nabla_{\mathcal{S}^i} Q_{\pi^i}(\mathcal{A}, \mathcal{S}^1, \dots, \mathcal{S}^n) \Big|_{\mathcal{S}^i = \pi^i(O^i)} \right] \quad (30)$$

One of the main reasons for using DA-TD3 is the over-valuation of Q values, which is mitigated using three main methods: developing clipped double Q learning, updating the policy using the delayed method, and target policy smoothing. Using the clipped double Q learning, the network selects a minimum Q value through the minimization function. That value is sent to the policy network, which is defined as follows,

$$x = \mathcal{R} + \sigma (1 - D) \text{Min} Q_{\pi}^i(\tilde{O}, \bar{\mathcal{S}}^1, \dots, \bar{\mathcal{S}}^n) \quad (31)$$

Target policy smoothing is performed to make it problematic for the policy to make use of the errors in the Q function, which is defined as follows,

$$\bar{\mathcal{S}} = \text{clip}(\tilde{\pi}^i(\tilde{O}^i) + \tilde{N}(0, \text{Err}), \mathcal{S}_l, \mathcal{S}_u) \quad (32)$$

where $N(0, \text{Err})$ represent the Gaussian error with zero mean and variance Err , respectively. The error value is added to the target actions when executing the critic updating. \mathcal{S}_l denotes the lower bound of the smoothed action, and \mathcal{S}_u denotes the upper bound of the smoothed action. With π_{θ^i} the policy of agents, the sample sequences $[O^1, O^2, \dots, O^n, \mathcal{S}^1, \dots, \mathcal{S}^n, \mathcal{R}, \tilde{O}^1, \tilde{O}^2, \dots, \tilde{O}^n]$ are obtained from the

buffer D to update the action function, which is defined as follows,

$$x = \mathfrak{R} + \text{Min}Q_{\tilde{\pi}^{1,2}} \times \left(\left(\tilde{O}^1, \tilde{\mathfrak{S}}^1, \dots, \left(\tilde{O}^n, \tilde{\mathfrak{S}}^n \right) \right) \Big|_{\tilde{\mathfrak{S}}^i = \tilde{\pi}^i(\tilde{O}^i) + \tilde{N}(0, \text{Err})} \right) \quad (33)$$

$$\phi^{1,2} \leftarrow \text{ArgMin}_{\phi^{1,2}} \sum \left(Q_{\pi^{1,2}} \left(\left(O^1, \mathfrak{S}^1 \right), \dots, \left(O^n, \mathfrak{S}^n \right) \right) - x \right)^2 \quad (34)$$

The policy delayed updating is performed to create the critic network for converging the priory, hence updating the actor network with an appropriate gradient, which is formulated as follows,

$$\nabla_{\theta^i} J(\pi_i) = E_{\mathfrak{A}, \mathfrak{S} \sim D} \times \left(\nabla_{\mathfrak{S}^i} Q_{\pi} \left(\left(O^1, \mathfrak{S}^1 \right), \dots, \left(O^n, \mathfrak{S}^n \right) \right) \Big|_{\mathfrak{S}^i = \pi^i(O^i)} \right) \quad (35)$$

In this way, the network learning rate is increased gradually without disturbing the stability. By using DA-TD3, all the SUs sensed the spectrum, and the sensing report was forwarded to the CH, whose responsibility was to generate the reputation for the cluster members based on the aggregated sensing report. The sensing report along with the reputation value is transmitted to the FC through a control channel that determines the final decision. The FC performs the weighted average of the report and provides the decision. The FC computes the trust value of the nodes in that particular time interval and generates a dynamic threshold for the trust value, which is expressed as follows,

$$Tn_i = \frac{Tn_{i,j}, SU_i | T_{i,j} \geq \text{Max}}{Tn_i, j | T_{i,j} \geq \text{Max}} \quad (36)$$

where Tn_i represents the threshold of the trust value between SU_i and SU_j in the network. Based on the trust value, the legitimacy of the nodes is evaluated. If the node has a maximum level of threshold trust, then it will know as a legitimate node; otherwise, it is considered a malicious node. Based on the computed trust value and historic trust values achieved in past time intervals, the FC determines a node to be the malicious node. By doing so, the SSDF attacks in the network can be mitigated.

The allocation of resources is carried out based on the decision of the FC, which is performed by the second agent. Here, the Channel State Information (CSI) of the communication link between the vehicles along with the interference is considered to perform the precise selection of transmit power and channel. The CSI is considered imperfect and estimated more accurately using the *Quasi-Newton Iterative Unscented Kalman Filter* (QNIUKF) [44] based on several signal factors, such as RSSI, spectral efficiency, SINR, and environmental factors, such as weather, temperature, and humidity. The proposed QNIUKF only needs to compute the first-order derivatives when compared to Newton's method. Hence, the second-order term has the importance of finding

Algorithm 3 Dual Agent-Based Spectrum Access

```

1: Begin
2: Initialize actor networks  $\pi^i$  with parameters  $\theta^i$ 
3: Initialize critic networks  $Q_{\pi^{1,2}}$  with parameters  $\phi^{1,2}$ 
4: Initialize target actor networks  $\tilde{\theta}^i \leftarrow \theta^i$ ,
5: Initialize target critic networks  $\tilde{\phi}^{1,2} \leftarrow \phi^{1,2}$ 
6: Initialize replay buffer D
7: Set  $i = 2$ 
8: for  $e < \text{Max } e$  do
9:   Random noise initialization
10:  Get both agent observations from  $\mathfrak{A}_0$  as,
11:    $[O_1^i, O_2^i, \dots, O_i^i] \triangleq \mathfrak{A}_0$ 
12:  for  $t=1$  to Max i length do
13:   for both agents do
14:    Select action using (32)
15:   end for
16:   Execute action and achieve  $\mathfrak{R}_t, \tilde{\mathfrak{A}}_t$ 
17:   Stock  $(\mathfrak{A}_t, \tilde{\mathfrak{A}}_t, \mathfrak{A}_t, \mathfrak{R}_t)$  in D and update  $\mathfrak{A}_{t+1} \leftarrow \tilde{\mathfrak{A}}_t$ 
18:  end for
19:  If not met the termination condition then
20:   Calculate Q value of critic using (33)
21:   Execute the updation of value function using (34)
22:  If  $t \text{ Mod } \text{delay}$  then
23:   Execute the update of policy parameter using (35)
24:   Update the parameters of the target network
25:    $\tilde{\theta}^i \leftarrow \mu\theta^i + (1 - \mu)\tilde{\theta}^i$ 
26:    $\tilde{\phi}^{1,2} \leftarrow \mu\phi^{1,2} + (1 - \mu)\tilde{\phi}^{1,2}$ 
27:  End if
28:  End if
29: end for
30: End

```

a better search direction when the initiating point is distant from the optimum or when it lacks a Jacobian. The second-order term matrix is calculated and added into the IUKF, which is formulated as follows,

$$y_{i+1} = \hat{y} + k_i^p (x - \hat{x}_i - h_i \hat{y}_i) - s_i^p T_i \hat{y}_i \quad (37)$$

$$s_i^p = (h_i^T r^{-1} h_i + p^{-1} + T_i)^{-1} \quad (38)$$

$$k_i^p = s_i^p h_i^T r^{-1} \quad (39)$$

where $\hat{y}_i = \hat{y} - y_i$ and add a parameter of step size to the result to (37), (38), (39) which is formulated as follows,

$$y_{i+1} = y_i + \alpha_i (\hat{y}_i + k_i^p (x - \hat{x}_i - h_i \hat{y}_i) - s_i^p T_i \hat{y}_i) \quad (40)$$

Then calculate the covariance by using the following formula,

$$R_{t|t} = (I - k_i h_i) R (I - k_i h_i)^T + k_i Q k_i^T \quad (41)$$

By doing so, the effective allocation of resources to the SUs for data transmission is carried out. The parameters of the CSI prediction are listed as follows:

(i) **Spectral Efficiency** (S_E) - The amount of information present in the transmitting signal through the channel is

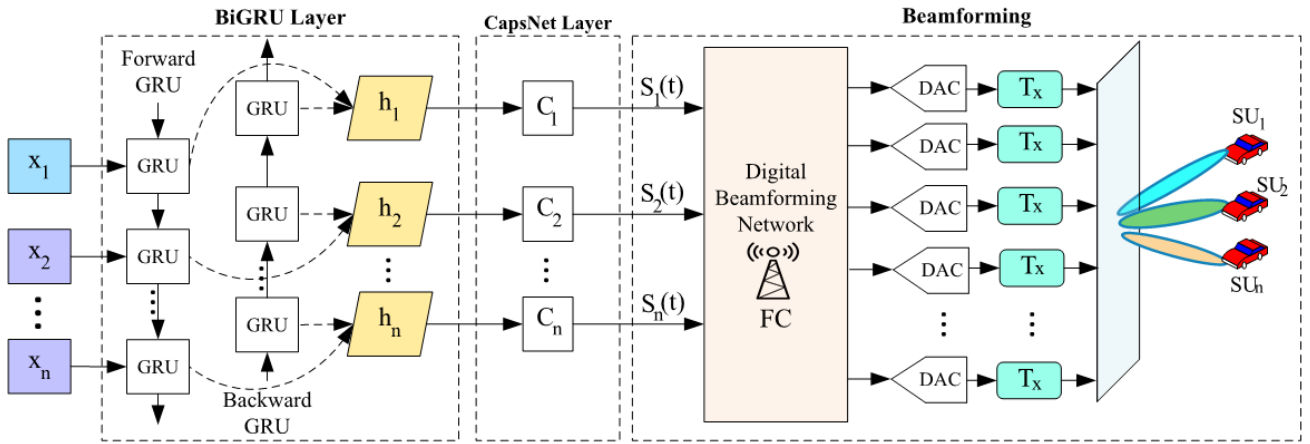


FIGURE 6. BiGRU-CapsNet based beamforming.

stated. It is measured based on the ratio of channel bandwidth (B_C) and information rate(R_I), which is formulated as follows,

$$S_E = \frac{R_I}{B_C} \quad (42)$$

(ii) **Temperature (\mathbb{T})** - The temperature affects the radio signal by initiating signal fading and scattering. Hence, the temperature is taken for accurate CSI prediction.

$$\mathbb{T} = \{t_1, t_1, \dots, t_i\} \quad (43)$$

where \mathbb{T} represents the overall temperature and t_i represents the temperature in j^{th} time.

(iii) **Humidity (h)** - The level of humidity also affects the signal transmission which causes signal scattering and fading. The formulation of gas present in the air is given as follows,

$$\varepsilon = \varepsilon_o + \varepsilon_w = 1820 \times 10^{-4} fr \check{N}fr \quad (44)$$

where ε represents the attenuation, which is computed in terms of db/km ; ε_o represents the attenuation in dry air; ε_w represents the attenuation in water molecules present in the air; fr represents the frequency; 1820 denotes the attenuation constant; and \check{N} represents the refractivity.

(iv) **Weather-** The changes in weather conditions also affect signal propagation. The attenuation produced due to rainfall is formulated as follows,

$$\varepsilon_r = P g^\beta \quad (45)$$

where ε_r represents the rate of attenuation, g represents the rainfall rate, and the parameters β and P are varied regarding other factors.

E. SECURE BEAMFORMING

Communication is carried out by the transmission of data between the nodes in the network. Beamforming is performed to enhance the quality of the signal, thereby improving the speed of the transfer of information. Here, beams

Algorithm 4 Secure Beamforming

- 1: **Begin**
- 2: Initialize parameters CSI, B_S, A_F, DOA
- 3: **for all** SUs **do**
- 4: Compute DOA using (49),(50)
- 5: Compute A_F using (52)
- 6: Compute B_S using (53)
- 7: Feed the input into both GRU_F and GRU_B
- 8: Compute the output of $F(H(t))$ using (54)
- 9: Compute the output of $B(H(t))$ using (55)
- 10: Concatenate the output of $F(H(t))$ and $B(H(t))$ using (56) to get the output of BiGRU
- 11: Feed the output of BiGRU to CapsNet for beamforming
- 12: Performing beamforming using (63)
- 13: **end for**
- 14: **End**

are generated between FC and multiple SUs because we used mmWave Massive MIMO for beamforming using 6G, which provides higher bandwidth and less congestion. Hence, we proposed the Bi Gated Recurrent Unit-Capsule Network (BiGRU-CapsNet) to perform effective beamforming. The BiGRU performs faster results and acquires limited memory than the existing models, such as BiLSTM and RNN. CapsNet gives concentration to features that are interpreted to be important. Fig 6 illustrates the secure beamforming using BiGRU-CapsNet. The parameters considered for beamforming are the CSI, beam score (B_S), array factor (A_F), and DOA. In most massive MIMO situations, the FC follows the channel state from the uplink transmitted signal from several terminals at t^{th} time ($T = 1, 2..t$); hence, the received signal at the FC can be defined as follows,

$$z_{i,v}(T) = \sqrt{Q_v} \sum_{k=1}^K h_{i,k}(T) S_k(T) + n_i(t) \quad (46)$$

where $h_{i,k}(T) \in C^{M \times 1}$ represents the channel vector of uplink transmission from k^{th} user in the FC, M represents the number of elements in the antenna array, S_k is a symbol transmitted through k^{th} user in the FC at T^{th} time slot, and $n_i(t) \in C^{m \times 1}$ represents the vector of additive noise received at time slot T . We used Massive MIMO with a set of array elements ($m \times n$). The antenna array of both the x-axis and y-axis is defined as follows,

$$X_f = \left[a_0, a_1 e^{i(\varnothing_1 + \mu_x)}, \dots, a_n e^{in(\varnothing_1 + \mu_x)}, \dots, a_{n-1} e^{i(N-1)(\varnothing_1 + \mu_x)} \right] \quad (47)$$

$$Y_f = \left[b_0, b_1 e^{i(\varnothing_2 + \mu_y)}, \dots, b_m e^{im(\varnothing_2 + \mu_y)}, \dots, a_{m-1} e^{i(M-1)(\varnothing_2 + \mu_y)} \right] \quad (48)$$

where a_n and b_m represent the weight values of the n^{th} and m^{th} antenna elements, and μ_x, μ_y represent the values of the direction of angle (DOA) at the location, and $\varnothing_1, \varnothing_2$ represent the intended SUs DOA. The mathematical representation of these parameters is defined as follows,

$$\varnothing_1 = v\delta_x \sin\theta \cos\vartheta \quad (49)$$

$$\varnothing_2 = v\delta_y \sin\theta \sin\vartheta \quad (50)$$

where $\delta = 2\pi/\omega$ and $\mu_x = -v\delta_x \sin\theta \cos\vartheta, \mu_y = -v\delta_y \sin\theta \sin\vartheta$. For efficient beamforming, we need to compute the values of array factor (A_F) by adding the overall elements present in the vector. To calculate the array factor, we consider μ_x or μ_y and the radiation factor, which is defined as follows,

$$\mu_{xy} = \mu_x^T \times \mu_y \quad (51)$$

Here, the calculation of (A_F) for the mmWave Massive MIMO antenna is defined as follows,

$$A_F = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \sigma_{nm} e^{j[\ln(\varnothing_1 + \mu_x) + m(\varnothing_2 + \mu_y)]} \quad (52)$$

where $\sigma_{nm} = a_n \times b_m$ represents the weight value of the antenna array. Based on A_F, CSI, DOA and B_S , beams are generated using Bi GRU-Caps Net. where B_S is evaluated as follows,

$$B_S = \sum_{i=0}^I n_b \times V_{CSI} \quad (53)$$

where n_b represents the number of baseband channels and V_{CSI} is the N-dimensional CSI vector of the antenna along with the historic information. These parameters are retrieved from the blockchain, thereby producing secure beamforming. Here, Bi-GRU-CapsNet generates the beams for SUs, which includes three layers: the input layer, BiGRU layer and Capsule layer. Initially, all the input parameters are fed into the backward and forward layers of the GRU concurrently. Then, the hidden layer adds the output of both forward $F(H(t))$ and

backward GRU $B(H(t))$ at time t , which are represented as follows,

$$F(H(t)) = GRU_F(F(H(t-1), I_t)) \quad (54)$$

$$B(H(t)) = GRU_B(B(H(t-1), I_t)) \quad (55)$$

$$H_t = Con[F(H(t)), B(H(t))] \quad (56)$$

The working of the GRU cell state is defined as follows,

$$y_t = \sigma(w_y \cdot [h_{t-1}, I_t] + a_y) \quad (57)$$

$$P_t = \sigma(w_P \cdot [h_{t-1}, I_t] + a_P) \quad (58)$$

$$\hat{H}(t) = \tanh(w_H \cdot [y_t * H(t-1), I_t] + a_H) \quad (59)$$

$$H(t) = (1 - P_t) * H(t-1) * \hat{H}(t) \quad (60)$$

where σ represents the sigmoid function, w_y, w_P, w_H represents the weight matrices, a_y, a_P, a_H represents the bias metrics, I_t represents the input, $H(t)$ is a hidden layer, P_t is an update gate that is used for controlling the previous and current hidden layer output, and P_t represents the reset gate. The output of BiGRU is fed into the capsule layer for beamforming. The process involved in the capsule layer is defined as follows,

$$V_{ij} = w_{ij} \cdot V_i \quad (61)$$

$$S_i = \sum_i d_{ij} V_{ij} \quad (62)$$

$$V_i = \frac{\|S_i\|^2 S_j}{1 + \|S_j\|^2 \|S_j\|} \quad (63)$$

$$c_{ij} = c_{ij} + V_{ij} \cdot V_i \quad (64)$$

where V_{ij} represents the output predictive vector of j^{th} primary capsule and i^{th} digit capsule, w_{ij} represents the weight matrix and c_{ij} is the logarithmic preceding probability of the capsules, which is normalized through the softmax layer to obtain d_{ij} . Then, squashing (S_i) is performed to obtain the output digit capsule. Finally, the weight values are updated using (64), and the process continues until convergence. In this way, BiGRU-CapsNet performs beamforming for SUs. Furthermore, the secure routing of data is facilitated by encrypting the messages using the proposed cryptographic algorithm and transmitting it through the most trusted path.

V. EXPERIMENTAL RESULTS

The performance of our proposed BlockCRN-IoCV method is evaluated in this section. The experimental results of the proposed method prove that this approach achieves high efficiency. This section is further divided into three subsections: simulation setup, comparative analysis, and research summary.

A. SIMULATION SETUP

The proposed BlockCRN-IoCV work is performed by combining the technology, i.e., mmWave massive MIMO with CRN-IoCV and blockchain. The proposed work is simulated by the Objective Modular Network tested in C++ (OMNET++) for network simulation and Simulation of

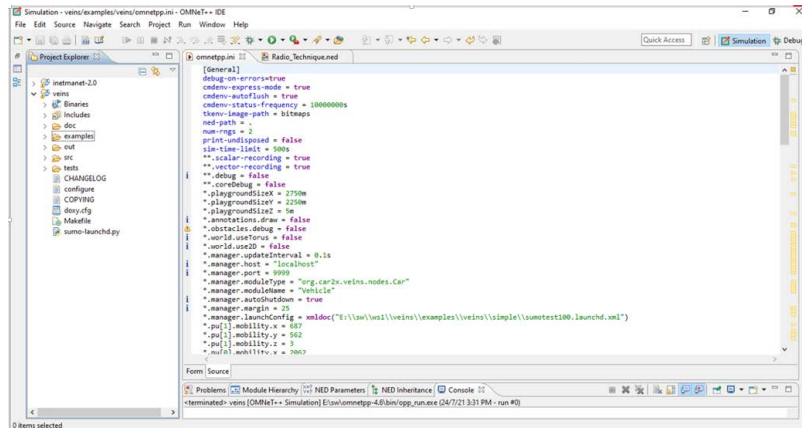


FIGURE 7. Simulation source coding.

Urban Mobility (SUMO) for traffic simulation. The execution of the simulation is performed using an Intel Core i7-11370H processor with 8 GB RAM. The operating system used for the simulation of the proposed work is Windows 10 pro 64 bits. The system parameters of the proposed method are illustrated in Table 4, and the simulation parameters are shown in Table 5. The source code of this simulation is illustrated in Fig. 7.

B. USE-CASE SCENARIO (SELF-DRIVING Cars)

Currently, the technology of IoCV in CRNs and its applications are expanded, especially for self-driving cars that are connected to the internet. Fig 8 illustrates the use-case scenario of self-driving cars in the IoCV environment. Based on this application scenario, several processes are performed in this application of self-driving cars, such as data sharing (i.e., multimedia file sharing), emergency message dissemination, sharing of safety and traffic conditions, parking requests, etc. Various issues are present in the applications, such as high delay, spectrum scarcity, security issues, etc., which remain unsolved. Therefore, we proposed a BlockCRN-IoCV approach for the application of self-driving cars. Authentication of PUs and SUs is performed by hybrid encryption using the AES-HCC algorithm. The credentials of the PUs and SUs are stored in the blockchain in an as hashed manner to improve security by mitigating the malicious SUs before data transmission. For this application of self-driving cars, a huge amount of spectrum is needed for the reliable transmission of data. This is achieved by performing dynamic spectrum access and efficient allocation of resources using the DA-TD3 algorithm. Secure beamforming is performed by considering the beam score, array factor, direction of angle, and CSI to reduce spectrum scarcity for efficient data transmission. This also increases the speed of data transmission, which reduces the transmission delay. Various attacks, such as random SSDF attacks, PUE attacks, eavesdropping, and jamming, are detected and mitigated by comparing the nature of previous and current signals using the trust values generated by the FC and blockchain information.

TABLE 4. System parameters.

Hardware Specifications	Hard Disk	500 GB
	RAM	8 GB
Software Specifications	Network Simulator	OMNET++, SUMO
	OS	Windows 10 Pro
	Processor	Intel Core i7-11370H

TABLE 5. Simulation parameters.

	Parameter	Values
Network Parameters	Number of PUs	3
	Number of SUs	100
	Number of PU Transmitter	1
	Number of Fusion Center	1
	Simulation area	1000×1000
Packet Parameters	Packet Size	1024
	Number of generated packets	2048
	Packet interval	0.1s
Channel Parameters	Number of channels	22
	Channel Bandwidth	21 MHz
	Spectrum range	5 to 100 MHz
6G Parameters	Data rate	1 Tbps (Max)
	Spectral Efficiency	100 bps/Hz
	End-to-End Delay	0.1 ms
Simulation Time		100s

C. SECURITY ANALYSIS

This section explains the security analysis of the BlockCRN-IoCV environment. Spectrum/data sharing is a challenging task due to the presence of malicious users; hence, we need to provide security to the environment. In this research, we detected four attacks, which are listed as follows:

i) **SSDF**- In this type of attack, the attacker provides the wrong information about spectrum sensing to the FC. If the PU is available then the malicious users report the PU is occupied, based on this information SU broadcast the data. In order to mitigate and prevent this attack, we have encrypted the sensing report using a hybrid AES-HCC encryption

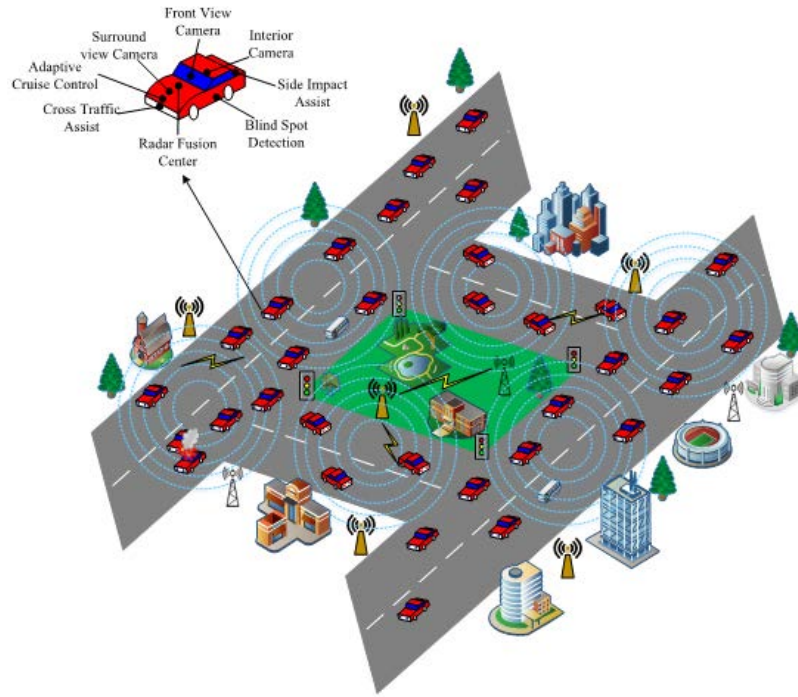


FIGURE 8. Scenario of IoCV self-driving cars.

algorithm and the ciphertext of the sensing report is then sent to the FC, which performs against SSDF.

ii) **PUE**- In this attack, the attacker emits the signals like a licensed primary transmitter. However, the malicious user provides the wrong information about the spectrum status to the SUs. To mitigate this attack, we perform secure spectrum sensing using DA-TD3. In addition, the trust factor is evaluated for every user in the environment which leads to high security and performance against PUE attacks.

iii) **Eavesdropping** - In this attack, the attacker discovers the information of the confidential communication and drops the corresponding information in terms of modifying. To overcome this issue, we have encrypted the spectrum report using a cryptography algorithm. In addition, we perform authentication using blockchain which allows the authenticated node to participate in the communication.

iv) **Jamming** - In this attack, the attacker compromises the sensing time of PU and data transmission of SU by decreasing the SINR. To detect the jamming attack, we evaluate the noise and SNR during spectrum sensing using blockchain which increases high security and performs against jamming attacks.

D. COMPARATIVE ANALYSIS

In this section, the proposed BlockCRN-IoCV method is compared with several previous methods, such as CRT-BIoV [39], DSS [40], SSS-CRN [41], SSGA-CR [42], and RSB-CRN [43], to analyze its performance. Various metrics are considered to evaluate the performance of these works,

such as throughput, packet delivery ratio, delay, bit error rate, detection accuracy, probability of detection, total transmit power, sensing delay, and spectral efficiency.

1) ANALYSIS OF THROUGHPUT

The sum of the delivered data for every SU present in the network is known as throughput. throughput calculates the efficient data delivery at the respective time slot over the network, which is represented as,

$$\mathcal{T} = \frac{D_s}{Tx_t} \tag{65}$$

where D_s denotes the size of the data and Tx_t represents the time required for transmission. The throughput is generally computed as bits/second. The maximum throughput achieved by any beamformer can be formulated as,

$$\mathcal{T}_w(\partial_\theta) = 0.5E\{(W - W_w^{bw}) \log_2(1 + \beth_w)\} \tag{66}$$

where the channel bandwidth is denoted as W , the allocated bandwidth is denoted as W_w^{bw} , and the concave function is denoted as \log_2 . However, the concave function hampers the analytical analysis; therefore, the upper bound can be formulated as,

$$\mathcal{T}_w^{ubound} = 0.5E\{(W - W_w^{bw}) \log_2(1 + \beth_w)\} \tag{67}$$

where,

$$\mathcal{T}_w(\partial_\theta) \rightarrow \mathcal{T}_w^{ubound} \tag{68}$$

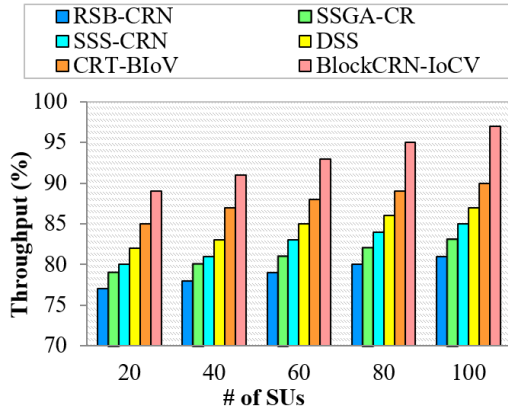


FIGURE 9. Throughput vs. # of SUs.

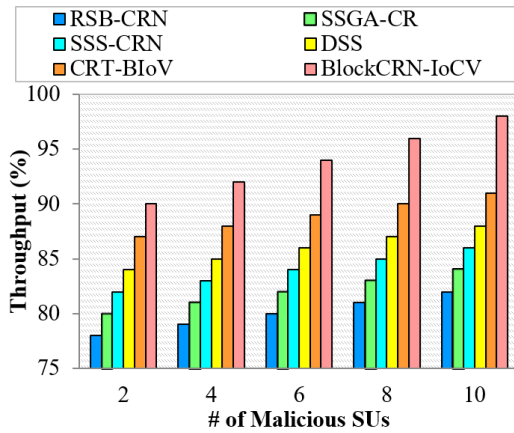


FIGURE 10. Throughput vs. # of malicious SUs.

The above equation denotes that both cases are the same; therefore, $\mathcal{T}_w(\partial_\theta)$ can be altered as,

$$\mathcal{T}_w(\partial_\theta) = 0.5\{(R_r - R_w^{bw}) \log_2(1 + \mathcal{I}_w)\} \quad (69)$$

where R_r and R_w^{bw} denote the bit rates of transmission and overhead, respectively. The overall throughput gain can be formulated as,

$$G\mathcal{T}_w(\partial_\theta) = \frac{\mathcal{T}_w(\partial_\theta) - \mathcal{T}_w^{ubound}}{\mathcal{T}_w^{ubound}} \quad (70)$$

Fig. 9 represents the comparison of throughput to the number of SUs between the proposed BlockCRN-IoCV method and various existing methods. If the number of SUs increases, it increases the throughput simultaneously. The CRT-BIoV and DSS methods have high-security threats by various attacks, such as random SSDF attacks and PUE attacks. The CR-BIoV method computes only trust values by TOPSIS for every user; however, the sensing report remains insecure, which leads to SSDF attacks. This affects the throughput of these works. The proposed work achieves better throughput than CRT-BIoV by performing detection and mitigation of random SSDF attacks and PUE attacks by sending the encrypted sensing report to the fusion center and calculating

the trust factor for every SU in the environment. Poor detection of malicious nodes is performed in the SSS-CRN and SSGA-CR methods, which increases the time complexity and decreases the throughput when compared with the proposed work.

Dynamic clustering by the DADRC algorithm and node reputation computed by CH decreases the time complexity and increases the throughput. Secure beamforming is performed in the proposed method to increase the throughput, whereas scattering of the beam occurs in the RSB-CRN method, which provides less throughput when compared with the proposed work. The BlockCRN-IoCV method achieves an average throughput of 93% while the existing works RSB-CRN, SSGA-CR, SSS-CRN, DSS, and CRT-BIoV achieve average throughput of 79%, 81%, 82.6%, 84.6%, and 87.8% which is 8-13% greater than the existing methods. Similarly, Fig.10 shows the throughput for malicious SUs, which is approximately the same as the throughput of legitimate SUs. Efficient authentication, dynamic clustering, and secure beamforming performed in the proposed BlockCRN-IoCV method increases the throughput when compared with various existing approaches. The average throughput of the proposed BlockCRN-IoCV is 94% while the existing works RSB-CRN, SSGA-CR, SSS-CRN, DSS, and CRT-BIoV achieve an average throughput of 80%, 82%, 84%, 86%, and 89% which is 5-14% greater than the existing works.

2) ANALYSIS OF PACKET DELIVERY RATIO (PDR)

Packet delivery ratio is defined as the ratio of a total number of successfully received packets to the total number of packets transmitted without any loss from source to destination. The formulation of the packet delivery ratio is represented as,

$$P = \frac{R_p}{T_x_p} \quad (71)$$

where R_p represents the received packets and T_x_p denotes the total transmitted packets. For an efficient packet delivery ratio, low packet loss is needed.

Fig 11 represents the comparison of the packet delivery ratio to the number of SUs between the proposed and existing works. An increase in SUs increases the packet delivery ratio. The proposed work achieves a high packet loss ratio by the detection and mitigation of attacks such as SSDF, PUE, and eavesdropping that are performed in the BlockCRN-IoCV method by the AES-HCC and DA-TD3 algorithms, which decreases the loss of packets. While the existing work CRT-BIoV limits with less packet loss ratio as the packets are manipulated by the attackers by performing various attacks during communication between vehicles and fusion center. Secure spectrum sensing is performed in both the SSS-CRN method and SSGA-CR method by analyzing the reputation of the SUs and selecting optimal sensing reports; however, poor attack detection and mitigation during spectrum sensing increases the packet loss due to various attacks that affect the packet delivery ratio. Secure spectrum

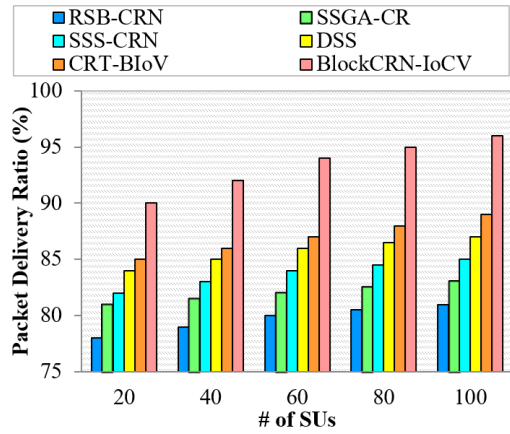


FIGURE 11. Packet delivery ratio vs. # of SUs.

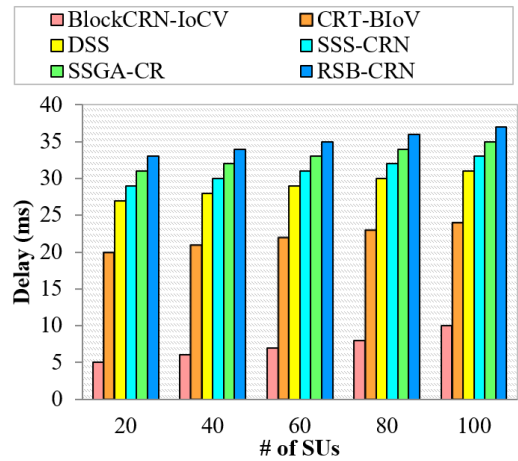


FIGURE 13. Delay vs. # of SUs.

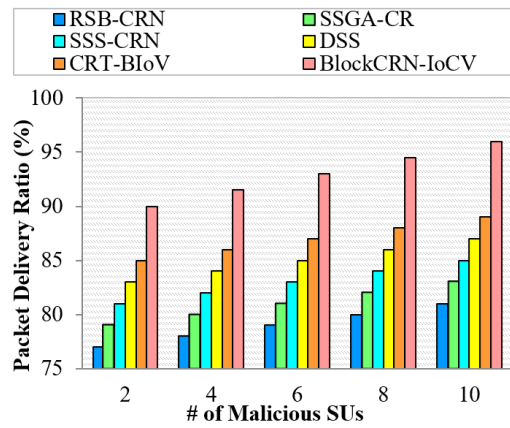


FIGURE 12. Packet delivery ratio vs. # of malicious SUs.

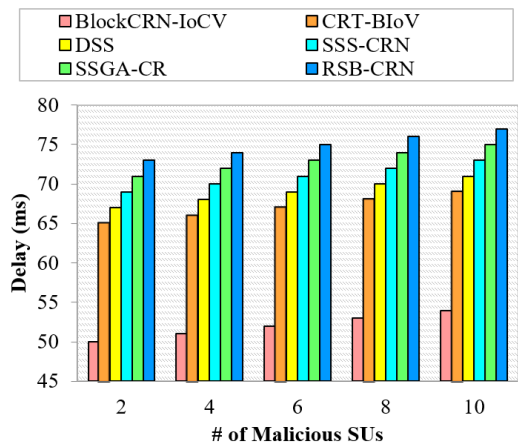


FIGURE 14. Delay vs. # of malicious SUs.

sensing and beamforming are performed by the DA-TD3 and Bi-GRU-CapsNet algorithms, which reduces packet loss by mitigating attacks to increase the packet delivery ratio. The proposed BlockCRN-IoCV method has an average packet delivery ratio of 93.4% while the existing works RSB-CRN, SSGA-CR, SSS-CRN, DSS, and CRT-BIoV achieve average packet delivery ratios of 79.7%, 82%, 83.7%, 85.7%, and 87% which are 7.4-15% greater than the previous works. Fig. 12 illustrates the packet delivery ratio of malicious SUs, which is the same as the packet delivery ratio of legitimate SUs. The proposed BlockCRN-IoCV method has an average packet delivery ratio when the number of malicious users is increased of 93%, while the existing works RSB-CRN, SSGA-CR, SSS-CRN, DSS, and CRT-BIoV achieve average packet delivery ratios of 79%, 81%, 83%, 85%, and 87%, which is 7-14% greater than the previous works.

3) ANALYSIS OF DELAY

Delay is referred to as the amount of time required for the data transmitted from source to destination. The computation of delay consists of queuing (\mathcal{D}_Q), transmission time (\mathcal{D}_{Tx_t}) and propagation (\mathcal{D}_p). The formulation of calculating delay

can be represented as,

$$\mathcal{D} = [\mathcal{D}_Q + \mathcal{D}_{Tx_t} + \mathcal{D}_p] \quad (72)$$

Efficient spectrum sensing and beamforming reduce the time for transmission of data.

Fig. 13 represents the comparison of delay to the number of SUs between the proposed BlockCRN-IoCV method and various previous methods. In the DSS and SSGA-CR methods, spectrum sensing is performed for efficient data transmission, but high noise and low SINR values affect spectrum sensing, which leads to a scarcity of spectra. This condition increases the data transmission time, which increases the delay. In the SSGA-CR method, malicious SUs are detected by a genetic algorithm. However, this algorithm increases the time complexity, thereby decreasing the detection rate of malicious SUs, which reduces the data transmission rate. In the proposed BlockCRN-IoCV method, spectrum sensing is performed dynamically by using the DA-TD3 algorithm for efficient spectrum sensing and resource allocation. This increases the rate of data transmission, which decreases the delay when compared with the existing approaches. The

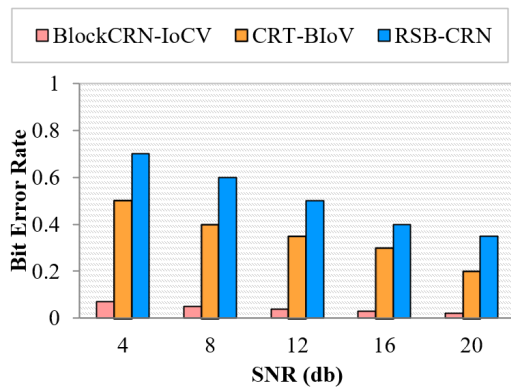


FIGURE 15. Bit error rate vs. SNR.

proposed BlockCRN-IoCV method achieves a low average delay of 7.2 ms for 100 SUs by a high data transmission rate, while the existing works have delays of 22 ms, 29 ms, 31 ms, 33 ms, and 35 ms, which are 15-22 ms greater than those of the proposed method. Fig. 14 shows the delay of malicious SUs, which is greater than the delay of legitimate SUs. The low average delay of malicious SUs in the environment is 52 ms, while the existing works achieve 67 ms, 69 ms, 71 ms, 73 ms, and 75 ms, which is 17-23 ms less than the previous approaches.

4) ANALYSIS OF BIT ERROR RATE (BER)

The bit error rate is defined as the ratio of the number of error bits (E_b) to the total number of transmitted bits (T_{x_b}). The computation of BER is represented as,

$$B = \frac{E_b}{T_{x_b}} \tag{73}$$

The BER is based on the characteristics of MIMO with noise, signal interference, and fading of channels.

Fig 15 illustrates the comparison of BER to the SNR range between the proposed BlockCRN-IoCV method and several existing methods, such as the CRT-BIoV and RSB-CRN methods. An increase in SNR decreases the bit error rate. In the CRT-BIoV method, the security of the network is improved, but the presence of noise increases the bit error rate, while the lack of consideration of channel noise improves the bit error rate. In the RSB-CRN method, beamforming is performed with a lack of beam score that increases the scattering of the beam, which results in a high bit error rate.

In the proposed BlockCRN-IoCV method, dynamic spectrum sensing is performed by considering the SNR, noise, and trust factor using the DA-TD3 algorithm, and secure beamforming is performed by considering parameters such as the beam score, CSI, array factor, and DOA with mmWave massive MIMO using 6G. This reduces the bit error rate up to 0.07 when the SNR is 4 db, which is approximately smaller than the 0.3-bit error rate of the CRT-BIoV method and the

TABLE 6. Numerical analysis of bit error rate.

Performance Metrics	RSB-CRN	CRT-BIoV	BlockCRN-IoCV
Bit error rate	0.51	0.35	0.042

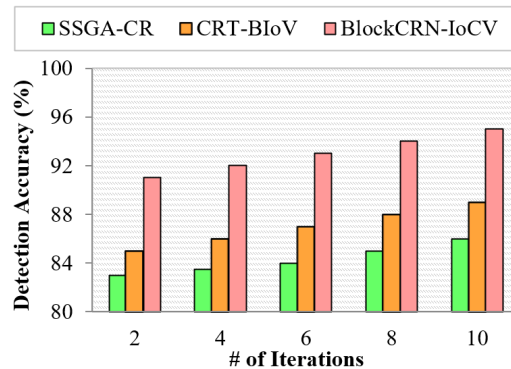


FIGURE 16. Detection accuracy vs. # of iterations.

0.47-bit error rate of RSB-CRN. Table 6 shows the numerical analysis of the bit error rate.

5) ANALYSIS OF DETECTION ACCURACY

The detection accuracy is defined as calculating the detection of attack preciseness in the proposed BlockCRN-IoCV. The detection accuracy is formulated by the total number of attacks detected from the overall SUs, which are represented as,

$$\hat{A} = \frac{T_p + \hat{F}_p}{T_p + T_n + \hat{F}_p + \hat{F}_n} \tag{74}$$

where T_p denotes true positive, \hat{F}_p represents false positive, T_n shows true negative and \hat{F}_n denotes false negative.

Fig 16 illustrates the comparison of detection accuracy to the number of iterations between the proposed BlockCRN-IoCV method and various existing methods, such as the CRT-BIoV method and the SSGA-CR method. The detection accuracy increases with an increasing number of iterations. The CRT-BIoV method improved network security by detecting random SSSF attacks. However, the method used for the computation of the trust value of the Sus attains decision difficulty, which affects the detection accuracy. In the SSGA-CR method, the detection of malicious Sus was performed by computing a static threshold, which reduces the detection accuracy. The proposed BlockCRN-IoCV method performs the computation of the true value based on the current time interval and historic trust value for an effective decision, and the dynamic threshold is computed for the detection of malicious Sus to increase the detection accuracy. The proposed works achieve high detection accuracy when compared with existing works. The average detection accuracy of the proposed BlockCRN-IoCV method is 93% while the existing works achieve average detection accuracy of 84.3% and 87%, which is 6% greater than the CRT-BIoV

TABLE 7. Numerical analysis of detection accuracy.

Performance Metrics	SSGA-CR	CRT-BIoV	BlockCRN-IoCV
Detection Accuracy (%)	84.3±0.3	87±0.2	93±0.1

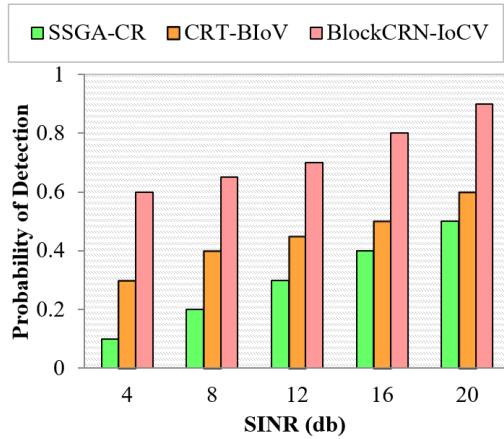


FIGURE 17. Probability of detection vs. SINR.

method and 9% greater than the SSGA-CR method. The numerical analysis of detection accuracy is represented in table 7.

6) ANALYSIS OF PROBABILITY OF DETECTION

This metric is used to calculate the performance of detection of attacks by FC for effective mitigation of attacks. The proposed work achieves a high probability of detection.

Fig. 17 represents the comparison of detection probability to the SINR value between the proposed BlockCRN-IoCV and several existing works, such as CRT-BIoV and SSGA-CR methods. An increase in SINR increases the detection probability. The proposed BlockCRN-IoCV method performs the computation of the trust value by performing average weights for providing decisions using FC, and it determines the malicious nodes accurately, which increases the detection probability when compared with the CRT-BIoV method. The CRT-BIoV method computes trust values with high decision difficulty. Based on the dynamic threshold, the detection of malicious SUs is performed in the proposed BlockCRN-IoCV method to improve the probability of detection, whereas the SSGA-CR method detects malicious SUs with a static threshold that decreases the detection probability when compared with the proposed BlockCRN-IoCV method. The average detection probability of the proposed BlockCRN-IoCV method is 0.73, while the existing work achieves average probabilities of 0.3 and 0.45, which are 0.3 higher than those of the CRT-BIoV method and 0.45 higher than those of the SSGA-CR method. Table 8 shows the numerical analysis of the probability of detection.

TABLE 8. Numerical analysis of probability of detection.

Performance Metrics	SSGA-CR	CRT-BIoV	BlockCRN-IoCV
Probability of Detection	0.3	0.45	0.73

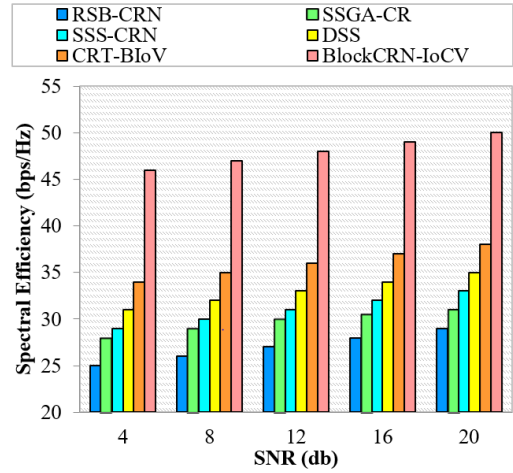


FIGURE 18. Spectral efficiency vs. SNR.

7) ANALYSIS OF SPECTRAL EFFICIENCY

This metric is used to analyze the spectrum sensing by the amount of information present in the transmitting signal and it is measured as the ratio of channel bandwidth and information rate. It is computed in terms of bits per second per hertz. The spectral efficiency of downlink scenario with K number of antennas and N number of vehicles can be represented as,

$$SE = \log_2 \left(1 + \frac{RKN^2\forall^2|\alpha\tau|^2\text{sinc}^2(\beta_\mu)\text{sinc}^2(\beta_N)}{KN^2\forall^2|\alpha\tau|^2\text{sinc}^2(\beta_N)\sigma^2 + \sigma^2} \right) \tag{75}$$

where \forall , σ , β_μ , and β_N are constants. Two cases determine the spectral efficiency,

Case 1: For an ideal system, SE will be reduced, which can be denoted as

$$SE_{ideal} = \log_2 \left(1 + \frac{R}{\sigma^2}KN^2|\alpha\tau|^2 \right) \tag{76}$$

Fig 18 illustrates the comparison of spectral efficiency to the SNR between the proposed BlockCRN-IoCV method and existing works. An increase in the SNR value increases the spectral efficiency. In the DSS method, spectrum sensing is performed without considering the noise and SINR value, and the presence of malicious SUs increases the signal interference and provides high resource wastage that leads to spectrum scattering, which affects the spectral efficiency. In the SSGA-CR method, several attacks, such as random SSDF and PUE, are not mitigated during spectrum sensing, which decreases the spectral efficiency.

In the proposed BlockCRN-IoCV method, dynamic spectrum sensing is performed by considering several parameters, such as SINR, noise, and trust factor, using the DA-TD3

TABLE 9. Numerical analysis of accuracy.

Performance Metrics	DNN	Bi-LSTM	DQN	BiGRU-CapsNet
Accuracy	74.3 ± 0.4	79.4 ± 0.3	85.2 ± 0.2	93.1 ± 0.1

TABLE 10. Numerical analysis of proposed vs. existing works.

Performance Metrics		RSB-CRN	SSGA-CR	SSS-CRN	DSS	CRT-BIoV	BlockCRN-IoCV
Throughput (%)	# of SUs	79±0.5	81±0.4	82.6±0.4	84.6±0.3	87.8±0.2	93±0.1
	# of Malicious SUs	80±0.4	82±0.5	84±0.3	86±0.4	89±0.2	94±0.1
Packet delivery Ratio (%)	# of SUs	79.7±0.4	82±0.5	83.7±0.3	85.7±0.3	87±0.2	93.4±0.1
	# of Malicious SUs	79±0.5	81±0.4	83±0.4	85±0.3	87±0.2	93±0.1
Delay (ms)	# of SUs	35±0.5	33±0.5	31±0.4	29±0.3	22±0.2	7.2±0.1
	# of Malicious SUs	75±0.5	73±0.5	71±0.4	69±0.4	67±0.2	52±0.1
Spectral Efficiency (bits)	SNR (db)	27±0.4	29.7±0.5	31±0.3	33±0.2	36±0.2	48±0.1

algorithm and the detection and mitigation of malicious SUs by computing the trust value based on the current interval of time and historic trust values at FC to improve the efficiency of spectrum sensing, which increases the spectral efficiency when compared with existing works. Additionally, the secure beamforming in the proposed work by BiGRU and CapsNet improves the spectral efficiency. The proposed BlockCRN-IoCV method has a high average spectral efficiency of 48 bps/Hz, while the existing works achieve average spectral efficiencies of 27 bps/Hz, 29.7 bps/Hz, 31 bps/Hz, 33 bps/Hz, and 36 bps/Hz, which are 8-13 bps/Hz greater than those of the existing methods.

8) ANALYSIS OF ACCURACY

This metric is used to analyze the accuracy for beamforming generation between the proposed BiGRU-CapsNet algorithm and other algorithms, which was proposed in several existing approaches, such as DNN [27], DQN [29], and Bi-LSTM [31]. It is computed in terms of percentage. Fig. 19 shows the comparison of accuracy between the proposed BlockCRN-IoCV and several previous works. The proposed BI-GRU-CapsNet performs efficient beamforming with high accuracy due to its forward and backward GRU units, such as the reset gate and update gate. This algorithm requires fewer memory and training parameters to train, which provides faster training and execution with high accuracy. CapsNet is combined with BiGRU to identify the entities regarding security for providing secure beamforming. However, other existing algorithms provide incomplete and indistinct information about the signals with low feature concentration, which reduces the accuracy when compared with the proposed BiGRU-CapsNet algorithm. From the figure, it is proven that the proposed BiGRU-CapsNet performs secure beamforming with high accuracy when compared with the state-of-the-art algorithms. The proposed algorithm achieves a high accuracy of approximately 93%, which is 8-19% greater than the previous methods' algorithms. Table 9 shows the analysis of accuracy.

E. RESEARCH SUMMARY

The proposed work integrates technologies such as 6G communication, blockchain technology, and mmWave MIMO in

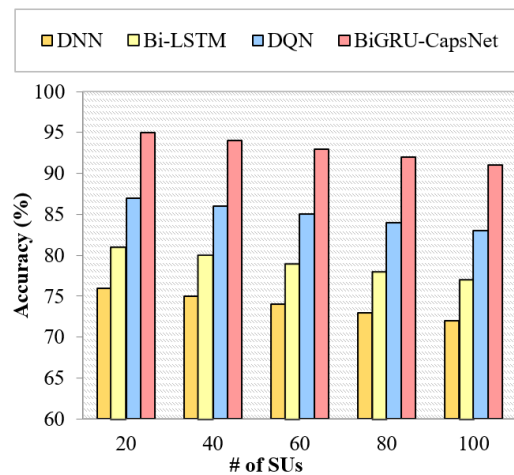


FIGURE 19. Accuracy vs. models.

the IoCV environment. The integration of these technologies impacts positive outcomes which result in,

- Low latency and high transmission reliability
- High communication efficiency
- Ensure security and privacy
- Energy efficiency and spectral efficiency
- Highly robust

The 6G communication in the proposed IoCV environment enables highly reliable communication without communication overhead, as there are many PUs and SUs in the environment. mmWave MIMO beamforming supports high-frequency communication. The process and method are used to enhance the performance of spectrum sensing in the BlockCRN-IoCV environment. Furthermore, the deployment of blockchain and FC improves the security and performance in terms of throughput with a packet delivery ratio of 94%, detection accuracy of 93%, spectral efficiency of 48 bits/s/Hz, BER of 0.042, and delay of 7.2 ms. Finally, the comparison study shows that the proposed approach achieves superior performance compared to existing approaches. Table 11 denotes the algorithm parameters of the proposed work. Table 12 represents the comparison of

TABLE 11. Hyperparameters of proposed algorithms.

Algorithms	Parameters	Values
Density Aware Dynamic Radius Clustering	γ	Max distance
	u	Cluster centroid
	Min points	0.09
	Time for samples (sec)	0.1s
DA-TD3	Output action numbers	5
	Replay memory	5×10^5
	Input states number	10
	Activation	[linear, Elu, Relu]
BiGRU-CapsNet	Loss	MSE
	Per layer nodes	[6,12,18,24]
	Hidden layers	[2,4,6,8]
	Dropout	[0.5,0,1]
	Optimizer	[RMS, Adam]
	Rate of learning	10^{-2}
	Primary Caps length	3
	Digi caps length	3
Capsule dimension	6	

TABLE 12. Comparison of existing beamforming algorithm with proposed.

Algorithm	Time for training step (ms)	Log-likelihood	Layers count	Parameters	WER%
BiGRU	16	0.226	256,512	850	14.44%
Bi-LSTM	24	0.19	256,512	1160	17.45%
Bi-RNN	62	-3.336	256,512	1172	27.11%

the proposed BiGRU algorithm with existing algorithms such as LSTM and RNN.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have proposed the BlockCRN-IoCV model to achieve better performance in spectrum sensing and beamforming. To achieve this objective, we integrate multiple technologies that provide us with a robust, energy-efficient, highly efficient, and secure environment. The proposed four processes, authentication, clustering, secure spectrum sensing, and beamforming, achieve security by verifying the entities to the blockchain. First, authentication is performed by using the AES-HCC algorithm, which provides security to the environment. In the second, clustering is performed to handle the mobility of the environment, which provides reliable communication. Third, we perform secure spectrum sensing using the DA-TD3 algorithm, which enhances spectrum utilization and reduces spectrum scarcity. Finally, we perform secure beamforming using BiGRU-CapsNet, which retrieves the input parameters from the blockchain to enhance security. The proposed work achieved better performance in terms of throughput, packet delivery ratio, BER, detection accuracy, and delay. In the future, we plan to perform hybrid beamforming to provide hardware efficiency, spectral efficiency, and computational efficiency.

REFERENCES

- [1] H. Khaled, I. Ahmad, D. Habibi, and Q. V. Phung, "A secure and energy-aware approach for cognitive radio communications," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 900–915, 2020.
- [2] R. Kulshrestha, "Channel allocation and ultra-reliable communication in CRNs with heterogeneous traffic and retries: A dependability theory-based analysis," *Comput. Commun.*, vol. 158, pp. 51–63, May 2020.
- [3] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020.
- [4] P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for internet of vehicles," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4991–4999, Mar. 2021.
- [5] D. Kwon, J. Kim, D. A. Mohaisen, and W. Lee, "Self-adaptive power control with deep reinforcement learning for millimeter-wave internet-of-vehicles video caching," *J. Commun. Netw.*, vol. 22, no. 4, pp. 326–337, Aug. 2020.
- [6] B. Soni, D. K. Patel, and M. López-Benítez, "Long short-term memory based spectrum sensing scheme for cognitive radio using primary activity statistics," *IEEE Access*, vol. 8, pp. 97437–97451, 2020.
- [7] K. Rapetswa and L. Cheng, "Convergence of mobile broadband and broadcast services: A cognitive radio sensing and sharing perspective," *Intell. Converged Netw.*, vol. 1, no. 1, pp. 99–114, Jun. 2020.
- [8] A. Gao, C. Du, S. X. Ng, and W. Liang, "A cooperative spectrum sensing with multi-agent reinforcement learning approach in cognitive radio networks," *IEEE Commun. Lett.*, vol. 25, no. 8, pp. 2604–2608, Aug. 2021.
- [9] W. S. H. M. W. Ahmad, N. A. M. Radzi, F. Samidi, A. Ismail, F. Abdullah, M. Z. Jamaludin, and M. Zakaria, "5G technology: Towards dynamic spectrum sharing using cognitive radio networks," *IEEE Access*, vol. 8, pp. 14460–14488, 2020.
- [10] M. Devi, N. Sarma, and S. K. Deka, "A double auction framework for multi-channel multi-winner heterogeneous spectrum allocation in cognitive radio networks," *IEEE Access*, vol. 9, pp. 72239–72258, 2021.
- [11] R. Rajaguru, K. V. Devi, and P. Marichamy, "A hybrid spectrum sensing approach to select suitable spectrum band for cognitive users," *Comput. Netw.*, vol. 180, Oct. 2020, Art. no. 107387.
- [12] M. Wenyang, Q. Chenhao, Z. Zhang, and J. Cheng, "Sparse channel estimation and hybrid precoding using deep learning for millimeter wave massive MIMO," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 2838–2849, Feb. 2020.
- [13] A. Chawla, R. K. Singh, A. Patel, A. K. Jagannatham, and L. Hanzo, "Distributed detection for centralized and decentralized millimeter wave massive MIMO sensor networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7665–7680, Aug. 2021.

- [14] K. Izadinasab, A. W. Shaban, and O. Damen, "Detection for hybrid beamforming millimeter wave massive MIMO systems," *IEEE Commun. Lett.*, vol. 25, no. 4, pp. 1168–1172, Apr. 2021.
- [15] C. M. Yetis, E. Björnson, and P. Giselsson, "Joint analog beam selection and digital beamforming in millimeter wave cell-free massive MIMO systems," 2021, *arXiv:2103.11199*.
- [16] Y. Zhang, J. Du, Y. Chen, X. Li, K. M. Rabie, and R. Kharel, "Near-optimal design for hybrid beamforming in mmWave massive multi-user MIMO systems," *IEEE Access*, vol. 8, pp. 129153–129168, 2020.
- [17] A. Sajid, B. Khalid, M. Ali, S. Mumtaz, U. Masud, and F. Qamar, "Securing cognitive radio networks using blockchains," *Future Gener. Comput. Syst.*, vol. 108, pp. 816–826, Jul. 2020.
- [18] A. Khanna, P. Rani, T. H. Sheikh, D. Gupta, V. Kansal, and J. J. P. C. Rodrigues, "Blockchain-based security enhancement and spectrum sensing in cognitive radio network," *Wireless Pers. Commun.*, pp. 1–23, Jul. 2021.
- [19] G. Rathee, N. Jaglan, and B. K. Kanaujia, "An attack resilient framework in cognitive radio network environment for inter-domain and intra-domain communication," *Wireless Pers. Commun.*, vol. 114, no. 4, pp. 3457–3475, Oct. 2020.
- [20] R. Sarmah, A. Taggu, and N. Marchang, "Detecting Byzantine attack in cognitive radio networks using machine learning," *Wireless Netw.*, vol. 26, no. 8, pp. 5939–5950, Nov. 2020.
- [21] J. Eze, S. Zhang, E. Liu, and E. Eze, "Design optimization of resource allocation in OFDMA-based cognitive radio-enabled internet of vehicles (IoVs)," *Sensors*, vol. 20, no. 21, p. 6402, Nov. 2020.
- [22] B. Yang, X. Cao, K. Xiong, C. Yuen, Y. L. Guan, S. Leng, L. Qian, and Z. Han, "Edge intelligence for autonomous driving in 6G wireless system: Design challenges and solutions," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 40–47, Apr. 2021.
- [23] M. Patnaik, V. Kamakoti, V. Matyas, and V. Rehak, "PROLEMus: A proactive learning-based MAC protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 2, pp. 400–412, Jun. 2019.
- [24] Y. Zhang, Q. Wu, and M. R. Shikh-Bahaei, "On ensemble learning-based secure fusion strategy for robust cooperative sensing in full-duplex cognitive radio networks," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6086–6100, Oct. 2020.
- [25] Y. Fu and Z. He, "Bayesian-inference-based sliding window trust model against probabilistic SSDF attack in cognitive radio networks," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1764–1775, Jun. 2020.
- [26] G. Rathee, N. Jaglan, S. Garg, B. J. Choi, and K.-K.-R. Choo, "A secure spectrum handoff mechanism in cognitive radio networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 3, pp. 959–969, Sep. 2020.
- [27] Z. Wang, T. Li, J. Ye, X. Yang, and K. Xiong, "AN-aided secure beamforming in SWIPT-aware mobile edge computing systems with cognitive radio," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–10, Nov. 2020.
- [28] Y. Chen, K. Zhao, J.-Y. Zhao, Q.-H. Zhu, and Y. Liu, "Deep learning based antenna muting and beamforming optimization in distributed massive MIMO systems," in *Proc. Int. Conf. 5G Future Wireless Netw.* Cham, Switzerland: Springer, 2019, pp. 18–30.
- [29] V. L. Nguyen, P.-C. Lin, and R.-H. Hwang, "A beamforming signal-based verification scheme for data sharing in 5G vehicular networks," *IEEE Access*, vol. 8, pp. 211723–211737, 2020.
- [30] C. Sun, Z. Shi, and F. Jiang, "A machine learning approach for beamforming in ultra dense network considering selfish and altruistic strategy," *IEEE Access*, vol. 8, pp. 6304–6315, 2020.
- [31] H. S. M. Antony and T. Lakshmanan, "Secure beamforming in 5G-based cognitive radio network," *Symmetry*, vol. 11, no. 10, p. 1260, Oct. 2019.
- [32] M.-R. Ramezanzpour and M.-R. Mosavi, "Two-stage beamforming for rejecting interferences using deep neural networks," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4439–4447, Sep. 2021.
- [33] B. Özbek, O. Erdoğan, S. A. Busari, and J. Gonzalez, "Hybrid beamforming strategies for secure multicell multiuser mmWave MIMO communications," *Phys. Commun.*, vol. 46, Jun. 2021, Art. no. 101319.
- [34] R. K. Saha, "Power-domain based dynamic millimeter-wave spectrum access techniques for in-building small cells in multioperator cognitive radio networks toward 6G," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, May 2021.
- [35] W. Lei, Y. Ye, and M. Xiao, "Deep reinforcement learning-based spectrum allocation in integrated access and backhaul networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 3, pp. 970–979, May 2020.
- [36] F. Li, K.-Y. Lam, L. Meng, H. Luo, and L. Wang, "Trading-based dynamic spectrum access and allocation in cognitive Internet of Things," *IEEE Access*, vol. 7, pp. 125952–125959, 2019.
- [37] M. Ozturk, M. Akram, S. Hussain, and M. A. Imran, "Novel QoS-aware proactive spectrum access techniques for cognitive radio using machine learning," *IEEE Access*, vol. 7, pp. 70811–70827, 2019.
- [38] D. Yao, S. Yuan, Z. Lv, D. Wan, and W. Mao, "An enhanced cooperative spectrum sensing scheme against SSDF attack based on Dempster-Shafer evidence theory for cognitive wireless sensor networks," *IEEE Access*, vol. 8, pp. 175881–175890, 2020.
- [39] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: A cognitive radio technique for blockchain-enabled internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4005–4015, Jul. 2021.
- [40] S. Liu, J. He, and J. Wu, "Dynamic cooperative spectrum sensing based on deep multi-user reinforcement learning," *Appl. Sci.*, vol. 11, no. 4, p. 1884, Feb. 2021.
- [41] M. Khasawneh, A. Azab, and A. Agarwal, "Towards securing routing based on nodes behavior during spectrum sensing in cognitive radio networks," *IEEE Access*, vol. 8, pp. 171512–171527, 2020.
- [42] N. Gul, M. S. Khan, J. Kim, and S. M. Kim, "Robust spectrum sensing via double-sided neighbor distance based on genetic algorithm in cognitive radio networks," *Mobile Inf. Syst.*, vol. 2020, pp. 1–10, Jul. 2020.
- [43] Q. Li and S. Zhao, "Robust secure beamforming design for cooperative cognitive radio nonorthogonal multiple access networks," *Secur. Commun. Netw.*, vol. 2021, pp. 1–9, Mar. 2021.
- [44] M. A. Skoglund, F. Gustafsson, and G. Hendeby, "On iterative unscented Kalman filter using optimization," in *Proc. 22th Int. Conf. Inf. Fusion (FUSION)*, Jul. 2019, pp. 1–8.



mobile ad hoc networks, AI, machine learning, and deep learning.



N. JAISANKAR received the B.E. degree in computer science and engineering from Bharathiar University, the M.E. degree in computer science and engineering from M. K. University, and the Ph.D. degree in computer science and engineering from the Vellore Institute of Technology (VIT University), Vellore, India. He was the Program Head for M.Tech. (CSE) Program and the Division Head of the Computer Network Division. He is a Professor with the School of Computer Science and Engineering, VIT University. He has over 20 years of experience in teaching and research. He received certification for CCNA Instructor and SUN certified Java Instructor. He has reviewed many books titled *Network Security*, *Data Mining*, *TCP/IP Protocol Suite*, and *Programming in Java*. He has participated as a Coach at the International Programming Contest held at IIT Kanpur, Kanpur, India. He has worked with Neusoft Institute, Guangdong, China. He has published many papers in international and national journals and conferences on networks security, computer networks, and data mining. His research interests include computer networks, networks security, cloud computing, and data mining. He has served in many peer reviewed international journals as an Editorial Board Member, a guest handling editor, an Advisory Board Member, and a reviewer. He has also served in many international conferences as the general chair, an International Advisory Board Member, a Technical Program Committee Member, the publication chair, an Organizing Committee Member, and a reviewer. He is a Life Member of the Indian Society for Technical Education, the Computer Society of India, the International Association of Computer Science and Information Technology, and the International Society for Research in Science and Technology; and a member of the International Association of Engineers.

...