International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/221888 Volume 10, Issue 3, May – June (2023)

RESEARCH ARTICLE

Blockchain Assisted Chaotic Chameleon Swarm Optimization Based Clustering Technique in Vehicular Ad Hoc Networks

R. Mohan
Department of Computer Science and Engineering, Annamalai University Annamalai Nagar, Chidambaram, Tamil Nadu, India.
rkmmails@gmail.com

G. Prabakaran
Department of Computer Science and Engineering, Annamalai University Annamalai Nagar, Chidambaram, Tamil Nadu, India.
gpaucse@yahoo.com

T. Priyaradhikadevi
Department of Computer Science and Engineering, Mailam Engineering College, Mailam, Villupuram Tamil Nadu, India.
hodcse@mailamengg.com

Received: 06 April 2023 / Revised: 18 May 2023 / Accepted: 26 May 2023 / Published: 30 June 2023

Abstract – Vehicular Ad Hoc network (VANET) has group of stationary or moving vehicles linked via wireless networks. Clustering in VANET is used to enhance network efficiency, scalability, and performance. By aggregating vehicles into clusters, communication overhead was decreased, and the network was managed with a greater count of vehicles. Moreover, clustering supports minimizing inter-cluster communication and decreasing congestion, therefore enhancing network reliability. The cluster head (CH) has the responsibility to manage communication in the cluster and forward communications to other clusters. In recent times, Blockchain (BC) technology has been executed to VANETs for enhancing privacy and security. A BC-based scheme is utilized for recording transactions like the change of data amongst vehicles from the secure and tamper-proof method. This makes sure that data cannot be falsified or altered and that the authenticity of data is verified. Therefore, this study develops a Blockchain Assisted Chaotic Chameleon Swarm Optimization based Energy Aware Clustering (BCCSO-EAC) technique in VANET. The presented BCCSO-EAC technique constructs clusters and selects CHs using a fitness function comprising residual energy (RE), node degree (ND), and intra-cluster distance parameters. The BCCSO-EAC technique selects CHs in such that the load among the nodes gets distributed properly. Moreover, BC technology was carried out to enable secure inter-cluster and intra-cluster VANET communication. The experimental result analysis of the BCCSO-EAC method is tested under various measures. The outcomes stated the improved results of the BCCSO-EAC technique over other recent approaches in terms of different evaluation metrics.

Index Terms – Vehicular Ad Hoc Networks, Chameleon Swarm Algorithm, Blockchain, Clustering, Fitness Function, Energy Efficiency, Multi-Hop Communication.

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are now seeing rapid advancement, and almost all industries are begun to make considerable efforts to compete in this domain [1]. The VANET can be referred to as mobile vehicles driving in an urban environment or on a highway while connected wirelessly. They use an ongoing data exchange between them or with roadside units (RSUs) for updating any data [2], driving assistance and guiding infrastructure-less driving. In VANET, vehicles on roads are formed into groups for facilitating transmission. Clustering stabilizes the connection between nodes by hierarchizing the architecture of the network, and all clusters are classified into three they are gateway (GW), cluster head (CH), and cluster member (CM) [3]. CM transmit the message to its CH while CM should make communication with other nodes. This CH can interact with other CHs [4]. The GW will be helpful to relay between CH and CH in case the intermediate CH is out of transmission coverage. If the data packets reach the final CH, the CH transmit message to the desired CM [5].

Above all, the clustering protocols are capable of enhancing the network stability by opting for the CH and making the clustering that can interact with various CHs [6]. Hence, the route connectivity was found to be more stable than the network without clustering only when the cluster is presented in the network. As the centralized node is absent in the VANETs, e.g., base station and access point, it is prone to attacks [7]. Some examples are wormhole attacks, denial of service (DOS) attacks, sinkhole attacks, etc. Thus, Blockchain (BC) technology is used in VANET clustering for many purposes [8]. BC technology is used to share data securely between vehicles in a cluster and also between diverse clusters. It is broadly leveraged for establishing trust between vehicles and to make sure the data sent is not corrupted or altered [9]. It is also used to constitute decentralized routing techniques, which allows the vehicles to make better decisions on how to route data by not depending on a central authority [10]. BC technology is widely used to protect the privacy of vehicles and data, along with that to certify that sensitive data is not revealed to unauthorized persons.

1.1. Problem Statement

VANETs face many problems containing effectual data management, secure networks, and effectual clustering of vehicles. Furthermore, the combination of BC technology with VANETs offers either promising solutions or unique obstacles. This problem at hand is to progress a robust clustering method integrated with BC technology for enhancing the effectiveness and security of VANETs. Designing a clustering technique which efficiently groups vehicles dependent upon its proximity and mobility patterns for enabling effectual data sharing and resource allocation. The clustering process can assume the dynamic nature of vehicular networks and adjust to altering network conditions. Besides, ensure secure networks among vehicles in the clusters and keep malicious attacks, identity spoofing, and data tampering. The BC technology offers an immutable and transparent ledger for secure transaction verification and recording. To address these problems, paving the way for an effectual and secure VANET ecosystem, allowing vehicles to exchange data, create intelligent decisions, and enhance overall traffic management and road safety.

1.2. Paper Contributions

This study develops a Blockchain Assisted Chaotic Chameleon Swarm Optimization based Energy Aware Clustering (BCCSO-EAC) technique in VANET. The presented BCCSO-EAC technique constructs clusters and selects CHs using a fitness function comprising residual energy (RE), node degree (ND), and intra-cluster distance parameters. The BCCSO-EAC technique selects CHs in such that the load among the nodes gets distributed properly. Moreover, BC technology is adopted to enable secure inter-cluster and intra-cluster VANET communication. The experimental result analysis of the BCCSO-EAC technique is tested under different measures.

1.3. Paper Organization

The rest of the paper is organized as follows. Section 2 presents the related works, and section 3 offer the proposed model. Next, section 4 provides the result analysis, and section 5 concludes the paper.

2. RELATED WORKS

The authors [11], using the red deer optimization method algorithm-related clustering with BC technology (RDOAC-BT), developed a potential privacy-preserving data transmission infrastructure in cluster-related VANET. This particular method includes the model of an RDOA-based clustering approach for opting CHs and building clusters. Apart from this, BC can be used for secured transmission in VANET. Also, BC is responsible for carrying out inter-cluster and intra-cluster communication processes. Liu et al. [12] devised a security algorithm related to BC technology, in which dual kinds of BC have been built depending on Certificate Authorities (CAs) and roadside units (RSUs). This security scheme involves many end-goals to find forged messages and identify malicious nodes related to multiple factors, like distance effectiveness of messages, reputation of sender node, and time. Besides, an incentive system was presented on the RSU-BC to boost RSU to implement active behaviours.

Chaudhary and Singh [13] grant a decentralized infrastructure of VANET containing BC technology. This BC-based method for VANET operates in 4 phases: pseudonym upload, BC network initialization, BC maintenance and vehicle registration. This has been a solution for the emerging issues in centralized structures and trusts problems between the entities. Zhang et al. [14] developed V-Lattice, which is a lightweight BC structure with the use of a DAG-lattice structure for VANET. In V-Lattice, all nodes (roadside units or vehicles) have its account chain. The transactions which are made might be included in the BC parallel and asynchronously, and resource-limited automobiles would save the pruned BC and effectuate BC-based functions normally. Simultaneously, a reputation-oriented incentive mechanism was presented in V-Lattice to inspire more nodes to join the BC. Folsom et al. [15] designed an innovative Novel Routing and Hybrid based Clustering Scheme (NRHCS) for VANET. The vehicles displacement and vehicle link counts were used in many concepts like cluster head election, cluster formation, addition and deletion of cluster, and re-clustering are effectuated.

Zhang et al. [16] present a dual BC-oriented conditional privacy-preserving authentication structure and protocol for VANET. The privacy-preservation and identity authentication of vehicle from VANET are understood without depending upon a centralized trusted 3rd party. The presented method is permitted for the conditional tracking of unauthorized vehicle.

RESEARCH ARTICLE

In [17], the authors plan BC-related mutual authentication and session key agreement protocol for inter- and intra-vehicular conditions by executing ECC and hash function. The presented approach approves security from every suitable attack in security study. In [18], the authors reveal the allocation manner for either network or computing resources as joint optimizer problems. The authors utilize a local DRL with prioritized experience replay model on edge node and utilize the BC to share better learning outcomes for optimizing the entire resource allocation problems. Feng et al. [19] examine an effectual BC-based authentication method for secure communication from VANET (EBAS). In EBAS, the regional trusted authority (RTA) obtains traffic communications uploaded by vehicle, composed of communications created by the unspent transaction output (UTXO) technique. Malik et al. [20] introduce a BC-related Security and Privacy-aware (BSPA) Protocol that offers reliability of model, and real identities are just exposed to certified vehicles. Roy and Madria [21] examine a BC-oriented Misbehavior Detection and Event Validation (BLAME) architecture which efficiently identifies valid traffic incident and malicious vehicle in ROI by exploiting neighbor data and incident recorded by separate vehicle, although it can be popular.

Though several clustering approaches are available in the literature, there is still needed to design energy-efficient clustering performance in the VANET. Most of the existing works do not focus on the security issue in the clustered VANET. At the same time, the clustering techniques need to consider multiple input parameters to cluster the node in the VANET to accomplish energy efficiency.

3. THE PROPOSED MODEL

In this study, a new BCCSO-EAC method was developed for energy-efficient clustering of the VANET. The presented BCCSO-EAC technique selects CHs in such that the load among the nodes gets distributed properly. Moreover, BC technology can be adopted to enable secure inter-cluster and intra-cluster VANET communication. Figure 1 represents the overall process of BCCSO-EAC approach.

3.1. Energy Model

As soon as the sensor node (SN) interacts with CH or CH interacts with other CHs, if interaction takes place between two models or in order to reach sink, energy model expresses how much energy it consumes [22]. The energy utilization of every SN relies on the size of the data packet and the distance from source to destination node.

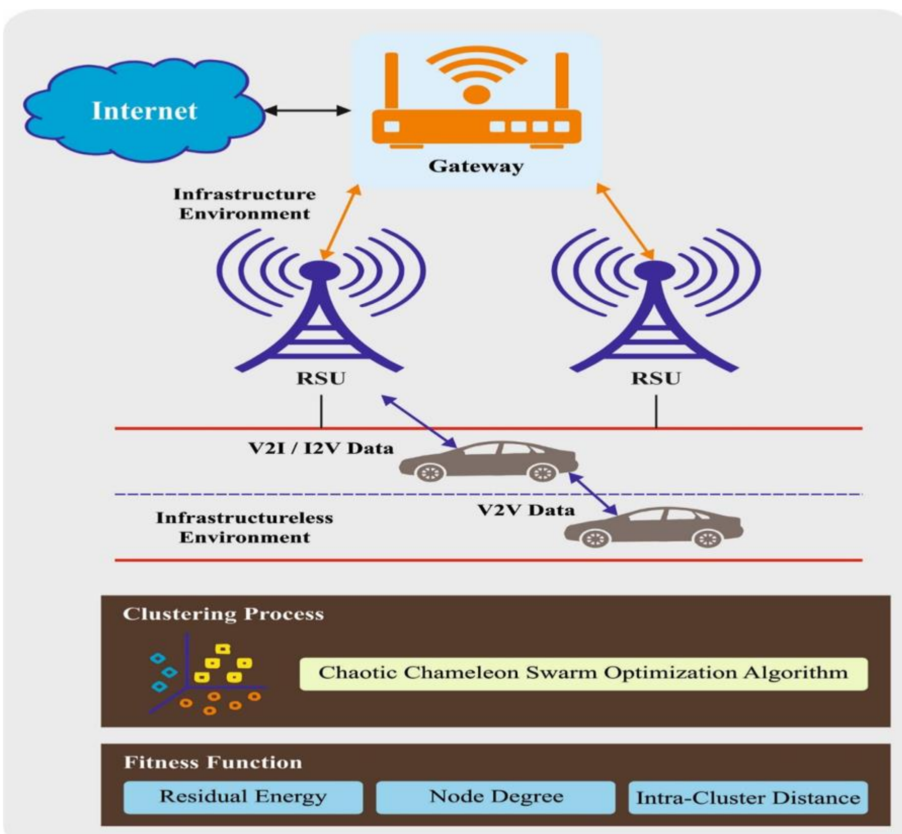

Figure 1 Overall Process of BCCSO-EAC System

RESEARCH ARTICLE

The energy utilization of the receiver and the transmitter nodes are measured by the subsequent equations (1) and (2):

$$Etx(l,d) = \begin{cases} l \times e + l \times efs \times d^2, d < d0 \\ l \times e + l \times emp \times d^4, d \geq d0. \end{cases} \quad (1)$$

$$Erx = l \times e \quad (2)$$

From the expression, e indicates the energy dissipation for every data during the implementation of distance secluded transmitter or receiver, $d0$ indicates the communication of threshold distance indicated $\frac{efs}{emp}$. The notation efs and emp show the transmitter amplifier and method of multipath correspondingly. Recently, information or Load imbalance amongst the SN has been a main challenge. The presented technique is capable of solving routing and load imbalance problems, and also it decreases delay in data transmission amongst the nodes, gives the best packet delivery ratio, increases amount of alive nodes in the network, and lowers energy consumption.

3.2. Design of CCSO Algorithm

In CSO algorithm, the chameleon behavior can be idealized into three stages: hunting prey, searching for prey, and eye rotation, and repeating the steps to obtain a better solution [23]. For CSO, variable dimension and population size are correspondingly set to d and N. In the t-th iteration, the location of chameleon i is represented as $y_i^t = [y_{i,1}^t, y_{i,2}^t, \ldots, y_{i,d}^t]$, $y_{i,j}^t$ signifies the location of the i-th chameleon at j-th dimension, whereas $i = 1,2,\cdots,N, j = 1,2,\cdots,d$.

Initially, a random population is produced, and it is evaluated using equation (3):

$$y_{i,j} = u_j + r \times (u_j - l_j) \quad (3)$$

In Eq. (3), u_j and l_j denote the upper and lower boundaries at j-th dimension, correspondingly. r is a randomly generated value within [0,1].

Chameleon finds prey by wandering constantly in trees and deserts. Due to movement, the chameleon location continuously changes during the search, as given in equation (4):

$$y_{i,j}^{t+1} = \begin{cases} y_{i.j}^t + p_1(P_{i.j}^t - G_j^t)r_2 + p_2(G_j^t - y_{i.j}^t)r_1 r_t \geq Pp \\ y_{i,j}^t + \mu((u_j - l_j)r_3 + l_j)sgn(rand - 0.5)r_i < Pp \end{cases} \quad (4)$$

Where $P_{i,j}^t$ and G_j^t represent the better position of chameleon i and the global optimum location. p_1 and p_2 are positive numbers controlling exploration capability of CSO. The probability that chameleon identifies prey can be represented as $Pp.r1, r2, r3$, and riindicate the uniformly generated random number within [0,1]. $sgn(rand - O.5)$ can be 1 or -l, which affected direction of exploitation and exploration. μ denotes a variable that reduces with increasing iteration, as given in equation (5):

$$\mu = \gamma e^{(\frac{-bt}{T})\beta} \quad (5)$$

Where t and T represent the existing, and the maximal amount of iterations, correspondingly, constants γ, b and β are correspondingly set to 1.0, 3.5, and 3.0.

Two eyes can independently rotate 180∘ that is a exclusive skill of a chameleon. Chameleon locates the prey with their eyes and moves the location based on the prey's position. The position updating equation can be given in equation (6):

$$y_i^{t+1} = yr_i^t + \overline{y}_i^t \quad (6)$$

Where $\overline{y}_i^t$ denotes the existing location of the chameleon i beforehand rotation, yr_i^t signifies rotating centered coordinate in search space that is given in equation (7):

$$yr_i^t = m \times yc_i^t \quad (7)$$

In Eq. (7), yc_i^t and m denoted center coordinate at t iteration and rotation matrix, correspondingly.

Hunting prey was the last stage in chameleon hunting behavior. The chameleon tongue attack speed is mathematically formulated as given in equation (8):

$$v_j^t = \omega v_{i,j}^t + c_1(G_j^t - y_{i,j}^t)r_1 + c_2(P_{i,j}^t - y_{i,j}^t)r_2 \quad (8)$$

In Eq. (8), $C1$ and $C2$ denote the two positive numbers that control influence of $P_{i_j}^t$. And G_j^t on attack speed of chameleon tongue, $r1$ and $r2$ indicates two random values within [0,1]. ω shows the inertia weight as given in equation (9):

$$\omega = (1 - \frac{t}{T})^{\left(\rho\sqrt{\frac{t}{T}}\right)} \quad (9)$$

In Eq. (9), ρ indicates the constant that controls exploitation. The novel location is evaluated as provided in equation (10):

$$y_{i,j}^{t+1} = y_{i,j}^t + ((v_{i,j}^t)^2 - (v_{i,j}^{t-1})^2)/(2a) \quad (10)$$

In equation (11), a signifies the speed of chameleon tongue projection, and the rate gradually increased with iteration and lastly attained 2590 meters for every second squared.

$$a = 2590 \times (1 - e^{-\log(t)}) \quad (11)$$

Chaotic maps demonstrate a pseudo-random deterministic procedure which is non-converging bounded. It defines an initial convergence from evolutionary algorithms with avoiding local minimums. It must be various chaotic maps. Next, 1D maps are utilized as primary position patterns from CSO technique for developing the CCSO technique. The pseudocode of CSO algorithm is given in Algorithm 1.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/221888 Volume 10, Issue 3, May – June (2023)

Input: d, N, T

Output: The global optimum

Randomly initialize the position of N chameleons and the velocity of dropping chameleons' tongues

Calculate the fitness values of each chameleon's position

while (t <*iterMax*) do

for $j = 1{:}N$ do

$$y_{i,j}^{t+1} = \begin{cases} y_{i.j}^{t} + p_1\left(P_{i.j}^{t} - G_j^{t}\right)r_2 + p_2\left(G_j^{t} - y_{i.j}^{t}\right)r_1 r_t \geq Pp \\ y_{i,j}^{t} + \mu\left(\left(u_j - l_j\right)r_3 + l_j\right) sgn(rand - 0.5) r_i < Pp \end{cases}$$

end for

for $j = 1{:}N$ do

$$yr_i^t = m \times yc_i^t$$

$$y_i^{t+1} = yr_i^t + \overline{y}_i^t$$

end for

for $j = 1{:}N$ do

$$v_{i,j}^{t+1} = \omega v_{i,j}^t + c_1(G_j^t - y_{i,j}^t)r_1 + c_2(P_{i,j}^t - y_{i,j}^t)r_2$$

$$y_{i,j}^{t+1} = y_{i,j}^t + ((v_{i,j}^f)^2 - (v_{i,j}^{t-1})^2)/(2a)$$

end for

Calculate the fitness values of each chameleon's position

$$t = t + 1$$

end while

Algorithm 1 Chameleon Swarm Algorithm

3.3. Process Involved in BCCSO-EAC Technique

The presented BCCSO-EAC technique constructed optimal clusters and chose the CHs using a fitness function comprising RE, ND, and intra-cluster distance parameters. A multi-fitness function was designed by taking intra-cluster distance, RE, and ND. This function is used for selecting CHs and balances the load amongst the cluster effectively, as defined in equation (12). Next, the constraints are given in equations (13) and (14).

$$Minimize\ F = we_1 \times Residual\_node_{energy} + we_2 \times Sensor\_node_{degree} + we_3 \times Distance_{intra\_cluster} \quad (12)$$

Subjected to

$$Residual\_node_{energy} > E_{THR} \quad (13)$$

$$Sensor\_node_{degree} \leq nDistance_{THR} \quad (14)$$

$$Distance\_intra\_cluster < Tra_{\max x}$$

Now, $we_1 + we_2 + we_3 = 1$ and $we_1, we_2, we_3 \in [0,1]$. The $nDistance_{THR}$ is represented as the threshold significance of the sensor node, E_{THR} indicates the threshold dataset of the SN energy, and $Tra_{\max x}$ represent maximum data transmission range of a node. RE of the SN can be given in equation (15):

$$Minimize\ \left(Residual_{node_{energy}}\right) = \sum_{i=1}^{p} \frac{1}{EE_{CH_i}} \quad (15)$$

Where EE_{CH_i} denotes the RE of $i^{th} CH$, p denotes the overall amount of CHs. ND can be represented as the number of accessible nodes from the CHs. Also, this is useful for load balancing in an SN, which can be accomplished by maintaining load on CH of the network.

$$Minimize\ (Sensor\_node_{degree}) = \sum_{i=1}^{p} |\, CCM_i| \quad (16)$$

In equation (16), $|CCM_i|$ indicates the amount of cluster members (CMs) of $i^{th} CH$, and the CCM_j can be described by the amount of cluster members at $j^{th} CH$. The objective for distance is given in equation (17):

$$Minimize\ (Distance_{intra}\text{-}\ cluster) = \sum_{i=1}^{p} \left[\frac{\sum_{i=1}^{CCM_j} d\left(CH_j, CCM_i\right)}{CCM_j} \right] \quad (17)$$

The intra-cluster distance can be used for maximizing the quality of network connection amongst the $CMs,$ and CH, $d(CH_j, CCM_i)$ indicates Euclidean distance between the $j^{th} CH$ and $i^{th} CM$. The system can be able to discover shortest path amongst nodes and from node to CH through giraffe kicking optimized C-means model and is used for load balancing in the area of wireless sensor network.

3.4. BC Enabled Secure Transmission

In this work, BC technology can be adopted to enable secure inter-cluster and intra-cluster VANET communication. The BC has the potential to share detail of ledgers in a secure way [24]. Decentralized storage refers to source in a BC, and maximal information is transmitted and recorded from the present block to the prior block using smart contract codes. In Swarm, various factors are used for the decentralized databases, namely MoneroDB, SiacoinDB, LitecoinDB, BigchainDB, and Interplanetary File System (IPFS). It must be regarded that vehicles interact with each other via V2X and V2V transmission, and they are effectively connected to the Internet. Also, consider that each vehicle can be crucial as GPS, OBUs, and sensors. Further, many legal RSUs are higher than suspicious RSU. For these purposes, a novel kind of BC is needed, as standard BCs could not be used. A classical BC used is cryptocurrency, while a BC is developed that handles secure event messages without exploting crypto coins. It is a single BC that can be supervised and balanced autonomously for recording the transportation details. Figure 2 represents the infrastructure of BC.

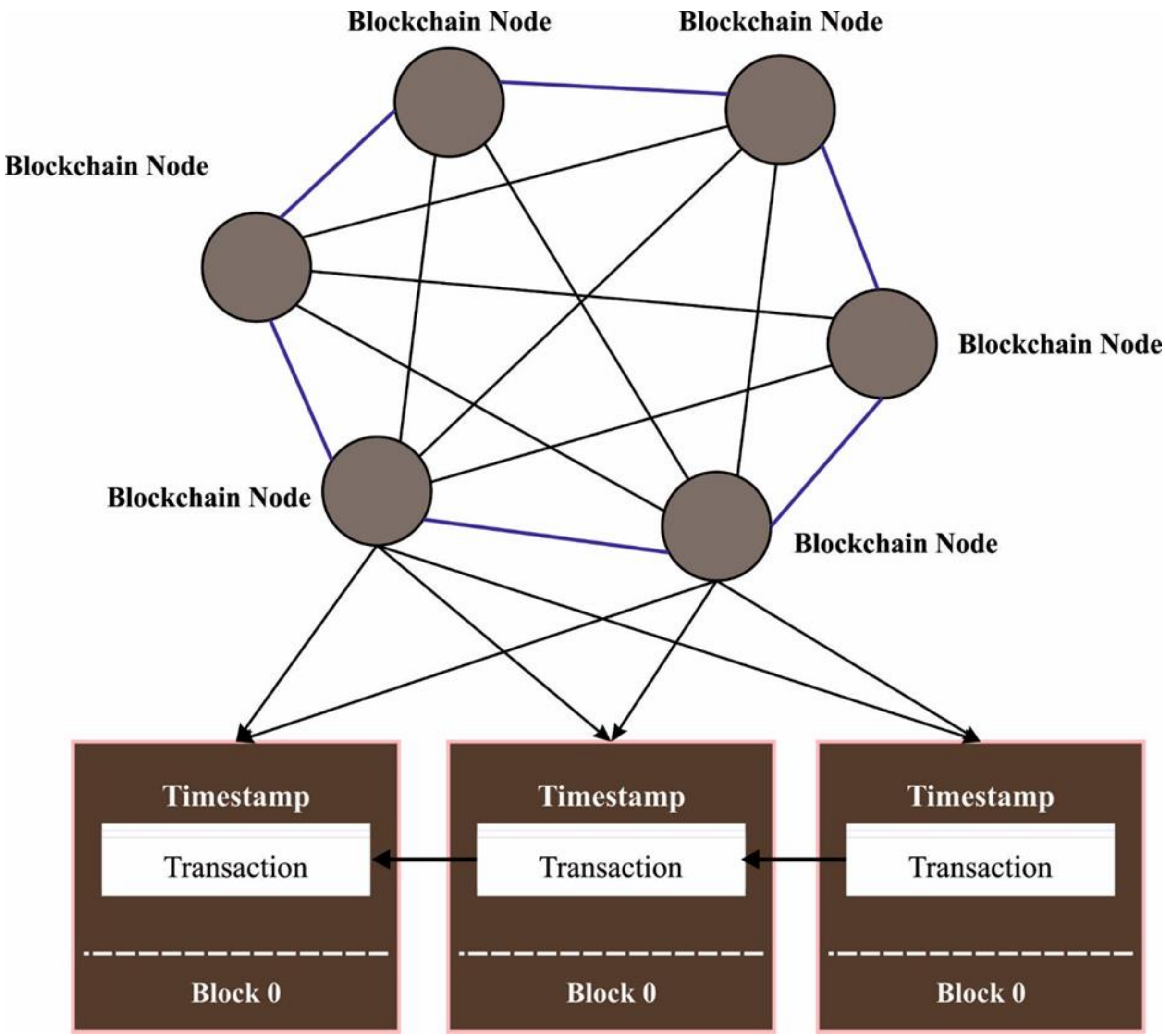

Figure 2 Structure of Blockchain

Each vehicle telecasts the position with a beacon message. Location certificate (LC) can be utilized as digital proof that characterizes vehicles within the period and at a specified distance. Each vehicle requires an LC to simultaneously approve the location. An LC is provided by the legal RSU. It performs as a proof of location (PoL) for vehicle that assists to ascertain the event message in the geographical region. In the traditional BC, the recently minted block can be transmitted globally. Nevertheless, the VANET message doesn't cross the boundary of certain location because accident and traffic details of locations are not known to vehicle found in another location. Thus, novel BC technology was needed. In that regard, each miner mines fresh block depends on the event message and transmits the recently minted block to local BC. Next, they can query its safety level, if necessary, through the BC. The new block is transmitted when the generation is completed, and vehicle in the network upgrade and validate the BC.

4. RESULT ANALYSIS

In this section, the experimental results of the BCCSO-EAC model are studied under different aspects. The experimental

RESEARCH ARTICLE

analysis are executed utilizing the Network Simulator-2 (NS-2) version 2.35 includes mobility of vehicles made by the simulation of urban mobility (SUMO). The parameter settings of the proposed technique are shown in Table 1.

Table 1 Parameter Settings

Parameter	Value
Number of Nodes	100
Maximum Vehicle Speed	33 m/s
Maximum Acceleration	2.6 m/s^2
Maximum Deceleration	4.5 m/s^2
Number of RSUs	10
RSU Coverage	1km

Table 2 represents the comparative number of clusters (NOC) obtained by the BCCSO-EAC model with existing models on the 100mx100m grid [25]. The results imply that the BCCSO-EAC model reaches optimal NOC values under all transmission ranges (TR). For example, with TR of 10, the BCCSO-EAC methodology attains lower NOC of 24 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B models obtain higher NOC of 30, 29, 27, and 25, respectively. In addition, with TR of 60, the BCCSO-EAC method attains lower NOC of 3 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B approaches acquire higher NOC of 10, 7, 6, and 4 correspondingly.

Table 3 demonstrates the brief NOC acquired by the BCCSO-EAC method with existing techniques on the 100mx100m grid. The experimental values implies that the BCCSO-EAC method reaches optimal NOC values under all TR. For example, with TR of 10, the BCCSO-EAC approach attains lower NOC of 29 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B methods obtain higher NOC of 38, 33, 32, and 31, correspondingly. As well, with TR of 60, the BCCSO-EAC approach attains a lower NOC of 3 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B techniques obtain higher NOC of 9, 7, 7, and 4 correspondingly.

Table 4 shows the comparative analysis of NOC found by the BCCSO-EAC approach with existing methods on the 100mx100m grid. The outcomes imply that the BCCSO-EAC model reaches optimal NOC values under all TR. For instance, with TR of 10, the BCCSO-EAC method reaches lower NOC of 40 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B approaches gain higher NOC of 49, 46, 44, and 42, respectively. Also, with TR of 60, the BCCSO-EAC method attains lower NOC of 6 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B models attain higher NOC of 12, 10, 8, and 7 correspondingly.

Table 2 Comparative NOC Analysis of BCCSO-EAC Model with 30 Nodes on 100 m × 100 m Grid

Number of Clusters; Nodes = 30					
Transmission Range	GWO-CNET Model	MO-PSO Model	CL-PSO Model	ROAC-B Model	BCCSO-EAC
10	30	29	27	25	24
15	28	26	24	23	20
20	23	22	20	18	16
25	21	19	19	16	13
30	20	17	15	13	11
35	19	15	14	12	10
40	17	15	13	11	8
45	16	11	9	6	5
50	14	9	8	6	4
55	12	8	7	5	4
60	10	7	6	4	3

RESEARCH ARTICLE

Table 3 Comparative NOC Analysis of BCCSO-EAC Model with 40 Nodes on 100 m × 100 m Grid

Number of Clusters; Nodes = 40					
Transmission Range	GWO-CNET Model	MO-PSO Model	CL-PSO Model	ROAC-B Model	BCCSO-EAC
10	38	33	32	31	29
15	33	32	31	27	25
20	32	30	26	23	21
25	28	25	22	19	17
30	24	22	20	17	15
35	20	19	17	14	12
40	17	16	15	12	10
45	15	13	11	9	8
50	13	11	8	6	4
55	11	8	7	5	3
60	9	7	7	4	3

Table 4 Comparative NOC Analysis of BCCSO-EAC Model with 50 Nodes on 100 m × 100 m Grid

Number of Clusters; Nodes = 50					
Transmission Range	GWO-CNET Model	MO-PSO Model	CL-PSO Model	ROAC-B Model	BCCSO-EAC
10	49	46	44	42	40
15	47	44	37	33	31
20	41	35	28	25	23
25	39	32	24	22	20
30	30	27	22	20	16
35	25	24	18	15	13
40	20	21	17	14	11
45	17	18	14	12	10
50	14	15	11	9	8
55	12	13	9	8	7
60	12	10	8	7	6

Table 5 displays the clear NOC gained by the BCCSO-EAC method with existing models on the 100mx100m grid. The outcomes imply that the BCCSO-EAC technique reaches optimal NOC values under all TR. For instance, with TR of 10, the BCCSO-EAC technique attains lower NOC of 42 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B models obtain higher NOC of 56, 49, 46, and 44 correspondingly. Also, with TR of 60, the BCCSO-EAC method accomplishes lower NOC of 6 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B approaches attain higher NOC of 9, 9, 8, and 7 correspondingly.

Figure 3 demonstrates the comparative NOC analysis of the BCCSO-EAC approach with existing methods under distinct nodes on 100mx100m grid.

RESEARCH ARTICLE

Table 6 signifies the comprehensive study of NOC obtained by the BCCSO-EAC method with existing methods on the 200mx200m grid. The results imply that the BCCSO-EAC system reaches optimal NOC values under all TR. For instance, with TR of 10, the BCCSO-EAC approach attains lower NOC of 21 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B models obtain higher NOC of 26, 33, 28, and 24 correspondingly. In addition, with TR of 60, the BCCSO-EAC approach gains lower NOC of 1 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B methods obtain higher NOC of 8, 7, 5, and 1 correspondingly.

Table 7 denotes the complete analysis of NOC gained by the BCCSO-EAC model with existing methods on the 200mx200m grid. The results imply that the BCCSO-EAC algorithm reaches optimal NOC values under all TR. For instance, with TR of 10, the BCCSO-EAC system attains lower NOC of 27 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B methods gain higher NOC of 40, 36, 35, and 35, respectively. In addition, with TR of 60, the BCCSO-EAC method achieves lower NOC of 1 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B models reach higher NOC of 7, 9, 8, and 1 correspondingly.

Table 8 characterizes the comparative NOC found by the BCCSO-EAC method with existing models on the 200mx200m grid. The outcomes imply that the BCCSO-EAC model reaches optimal NOC values under all TR. For instance, with TR of 10, the BCCSO-EAC method attains lower NOC of 43 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B techniques obtain higher NOC of 53, 46, 44, and 43 correspondingly. Furthermore, with TR of 60, the BCCSO-EAC method attains lower NOC of 2 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B approaches obtain higher NOC of 8, 7, 7, and 6 correspondingly.

Table 9 exhibits the brief NOC obtained by the BCCSO-EAC model with existing methods on the 200mx200m grid. The results imply that the BCCSO-EAC method reaches optimal NOC values under all TR. For instance, with TR of 10, the BCCSO-EAC technique attains lower NOC of 39 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B approaches obtain higher NOC of 57, 49, 44, and 41 correspondingly. As well, with TR of 60, the BCCSO-EAC model attains lower NOC of 2 while the GWO-CNET, MO-PSO, CL-PSO, and ROAC-B methods obtain higher NOC of 10, 12, 9, and 3 correspondingly.

Figure 4 demonstrates the comparative NOC analysis of the BCCSO-EAC approach with existing methods under distinct nodes on 200mx200m grid.

The ETED assessment of the BCCSO-EAC model is tested with existing methods in Table 10 and Figure 5. The experimental outcomes demonstrate that the BCCSO-EAC technique results in decreased ETED values over other models. For examples , with 20 nodes, the BCCSO-EAC method reaches reducing ETED of 0.0931s. Meanwhile, with 40 nodes, the BCCSO-EAC approach reaches reducing ETED of 0.1400s. Moreover, with 60 nodes, the BCCSO-EAC technique reaches reducing ETED of 0.1628s. Finally, with 100 nodes, the BCCSO-EAC model reaches reducing ETED of 0.2348s.

Table 5 Comparative NOC Analysis of BCCSO-EAC Model with 60 Nodes on 100 m × 100 m Grid

Number of Clusters; Nodes = 60					
Transmission Range	GWO-CNET Model	MO-PSO Model	CL-PSO Model	ROAC-B Model	BCCSO-EAC
10	56	49	46	44	42
15	49	42	38	38	36
20	35	35	32	28	26
25	31	27	24	24	22
30	28	25	21	21	18
35	22	19	17	15	14
40	17	16	15	14	12
45	16	15	15	13	10
50	13	12	11	9	8
55	11	10	10	9	7
60	9	9	8	7	6

RESEARCH ARTICLE

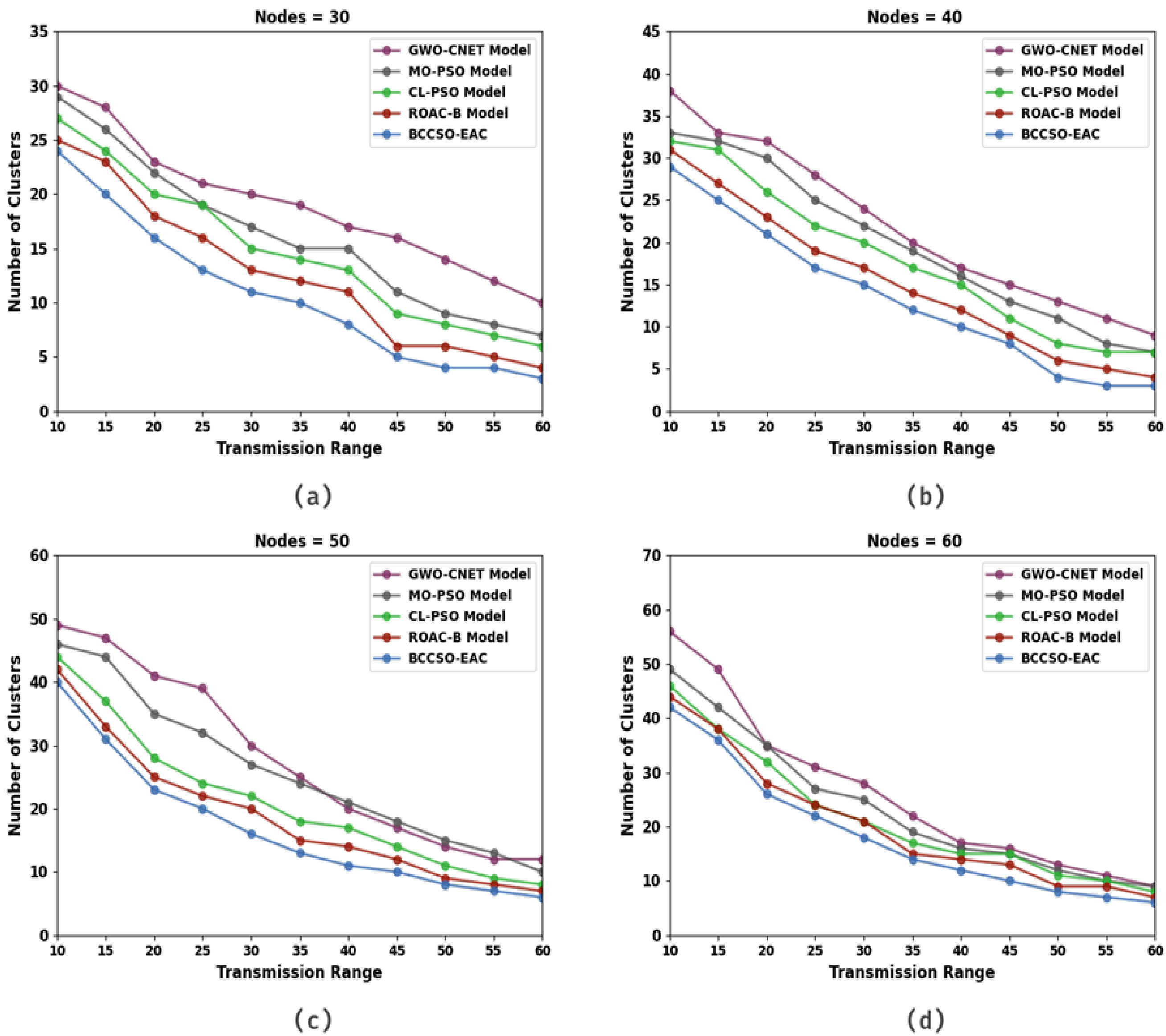

Figure 3 NOC Analysis of BCCSO-EAC Approach on 100mx100m Grid (a) 30 Nodes, (b) 40 Nodes, (c) 50 Nodes, and (d) 60 Nodes

Table 6 Comparative NOC Analysis of BCCSO-EAC Model with 30 Nodes on 200 m × 200 m Grid

Number of Clusters; Nodes = 30					
Transmission Range	GWO-CNET Model	MO-PSO Model	CL-PSO Model	ROAC-B Model	BCCSO-EAC
10	26	33	28	24	21
15	24	28	25	24	20
20	23	21	18	20	15
25	23	20	17	19	13
30	22	18	17	16	12

RESEARCH ARTICLE

35	20	14	14	15	8
40	18	14	14	11	6
45	15	13	11	10	6
50	14	12	10	9	3
55	13	9	5	4	1
60	8	7	5	1	1

Table 7 Comparative NOC Analysis of BCCSO-EAC Model with 40 Nodes on 200 m × 200 m Grid

Number of Clusters; Nodes = 40					
Transmission Range	GWO-CNET Model	MO-PSO Model	CL-PSO Model	ROAC-B Model	BCCSO-EAC
10	40	36	35	35	27
15	35	34	29	28	25
20	35	29	28	24	21
25	29	25	22	20	19
30	28	18	19	18	12
35	17	15	19	14	12
40	15	14	15	13	9
45	14	14	11	8	6
50	13	12	11	7	4
55	12	10	9	5	2
60	7	9	8	1	1

Table 8 Comparative NOC Analysis of BCCSO-EAC Model with 50 Nodes on 200 m × 200 m Grid

Number of Clusters; Nodes = 50					
Transmission Range	GWO-CNET Model	MO-PSO Model	CL-PSO Model	ROAC-B Model	BCCSO-EAC
10	53	46	44	43	43
15	46	38	42	34	28
20	43	32	33	23	22
25	39	24	33	20	16
30	34	21	25	20	16
35	29	20	22	15	13
40	22	18	21	14	10
45	18	14	17	13	8
50	17	11	17	11	7
55	10	8	16	8	6
60	8	7	7	6	2

RESEARCH ARTICLE

Table 9 Comparative NOC Analysis of BCCSO-EAC Model with 60 Nodes on 200 m × 200 m Grid

Number of Clusters; Nodes = 60					
Transmission Range	GWO-CNET Model	MO-PSO Model	CL-PSO Model	ROAC-B Model	BCCSO-EAC
10	57	49	44	41	39
15	48	46	38	34	33
20	36	37	31	29	25
25	33	26	27	25	21
30	25	24	17	24	15
35	20	21	19	12	11
40	13	16	18	11	10
45	17	17	14	11	9
50	16	13	12	9	7
55	12	6	13	8	5
60	10	12	9	3	2

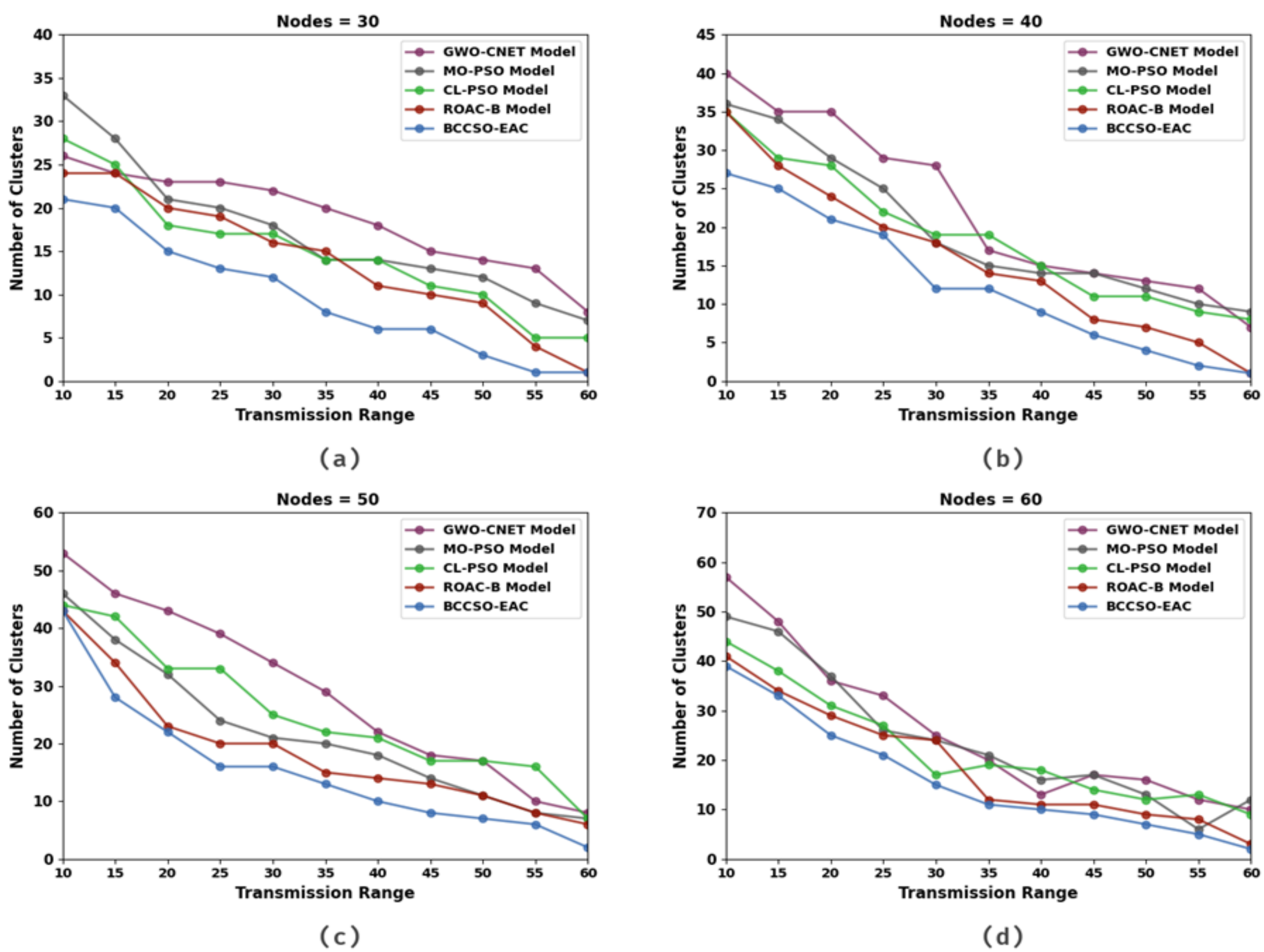

Figure 4 NOC Analysis of BCCSO-EAC Approach on 200mx200m Grid (a) 30 Nodes, (b) 40 Nodes, (c) 50 Nodes, and (d) 60 Nodes

RESEARCH ARTICLE

Table 10 ETED Analysis of BCCSO-EAC Approach with Other Systems under Distinct Nodes

End to End Delay (s)					
Number of Nodes	HEPPA	LAKAP	ASC	ROAC-B	BCCSO-EAC
20	0.2805	0.1206	0.1343	0.1034	0.0931
40	0.2908	0.1743	0.2108	0.1834	0.1400
60	0.3331	0.2748	0.2394	0.1926	0.1628
80	0.4279	0.3719	0.3251	0.2931	0.2508
100	0.4736	0.5228	0.3537	0.3011	0.2348

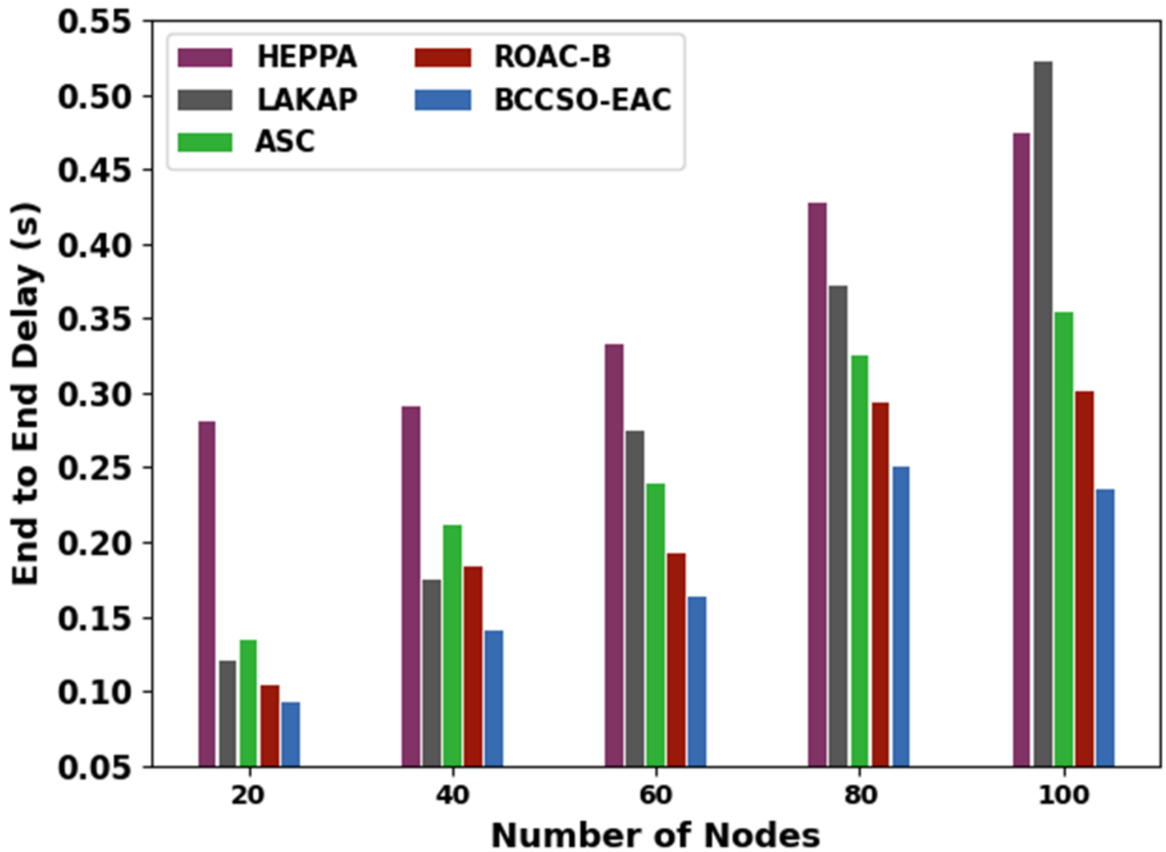

Figure 5 ETED Analysis of BCCSO-EAC Approach under Distinct Nodes

Next, a detailed PDR examination of the BCCSO-EAC model is performed with recent models in Table 11 and Figure 6. The experimental values demonstrate that the BCCSO-EAC model results in increased values of PDR over other models. With 20 nodes, the BCCSO-EAC model gains higher PDR of 96.26%. Moreover, with 40 nodes, the BCCSO-EAC model gains higher PDR of 70.04%. Concurrently, with 80 nodes, the BCCSO-EAC approach gains higher PDR of 53.90%. Finally, with 100 nodes, the BCCSO-EAC method gains higher PDR of 37.77%.

Next, a comprehensive THRO inspection of the BCCSO-EAC model is performed with recent models in Table 12 and Figure 7. The experimental values demonstrate that the BCCSO-EAC approach results in increased values of THRO over other methods. With 5s simulation time (ST), the BCCSO-EAC model gains higher THRO of 16.91%. Also,

RESEARCH ARTICLE

with 25s ST, the BCCSO-EAC model gains higher THRO of 40.87%. Concurrently, with 55s ST, the BCCSO-EAC approach has higher THRO of 70.53%. Lastly, with 70s ST, the BCCSO-EAC model gains higher THRO of 83.41%.

These outcomes highlighted the enhanced performance of the BCCSO-EAC model over other methods.

Table 11 PDR Analysis of BCCSO-EAC Approach with Other Systems under Distinct Nodes

Packet Delivery Ratio (%)					
Number of Nodes	HEPPA	LAKAP	ASC	ROAC-B	BCCSO-EAC
20	79.26	46.12	60.24	92.23	96.26
40	53.04	41.80	30.28	60.24	70.04
60	45.84	33.73	19.61	57.94	65.72
80	39.78	31.43	16.73	46.99	53.90
100	16.73	16.44	7.51	31.14	37.77

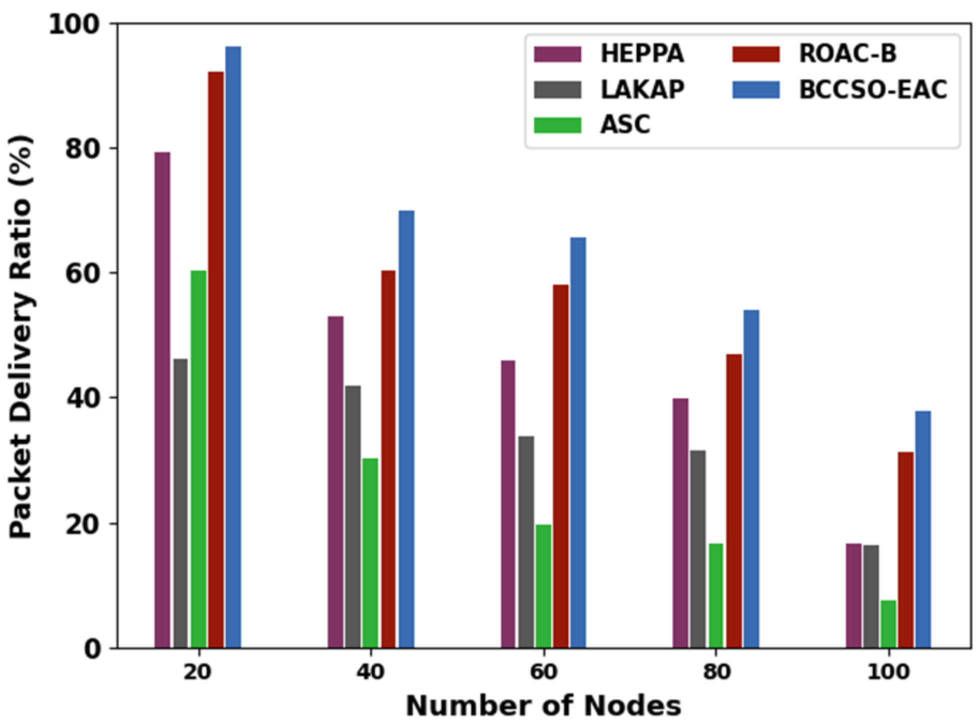

Figure 6 PDR Analysis of BCCSO-EAC Approach under Distinct Nodes

Table 12 THRO Analysis of BCCSO-EAC Approach with Other Systems under Distinct Simulation Times

Throughput (%)					
Simulation Time (sec)	HEPPA	LAKAP	ASC	ROAC-B	BCCSO-EAC
5	2.53	2.23	3.13	8.22	16.91
10	3.43	5.82	5.23	9.12	22.00

RESEARCH ARTICLE

15	7.02	5.52	10.92	13.61	27.99
20	7.92	4.93	10.92	15.41	34.28
25	11.52	12.41	14.81	18.11	40.87
30	18.11	25.90	19.30	23.20	46.86
35	21.70	28.59	34.28	40.57	52.86
40	27.39	29.49	48.36	54.35	60.05
45	31.29	29.19	51.36	56.75	64.54
50	33.98	35.18	53.75	60.65	69.03
55	38.78	40.87	55.85	60.35	70.53
60	43.57	45.67	59.15	63.94	73.83
65	48.06	50.46	60.94	64.54	75.32
70	55.25	60.65	65.74	68.43	83.41
75	60.94	67.54	71.43	75.02	85.81
80	64.54	72.03	75.92	79.82	87.31
85	69.33	73.23	78.02	82.81	89.40
90	72.33	75.62	81.61	84.61	93.00
95	74.72	78.32	85.51	87.61	93.90
100	79.22	84.01	92.10	93.90	94.20

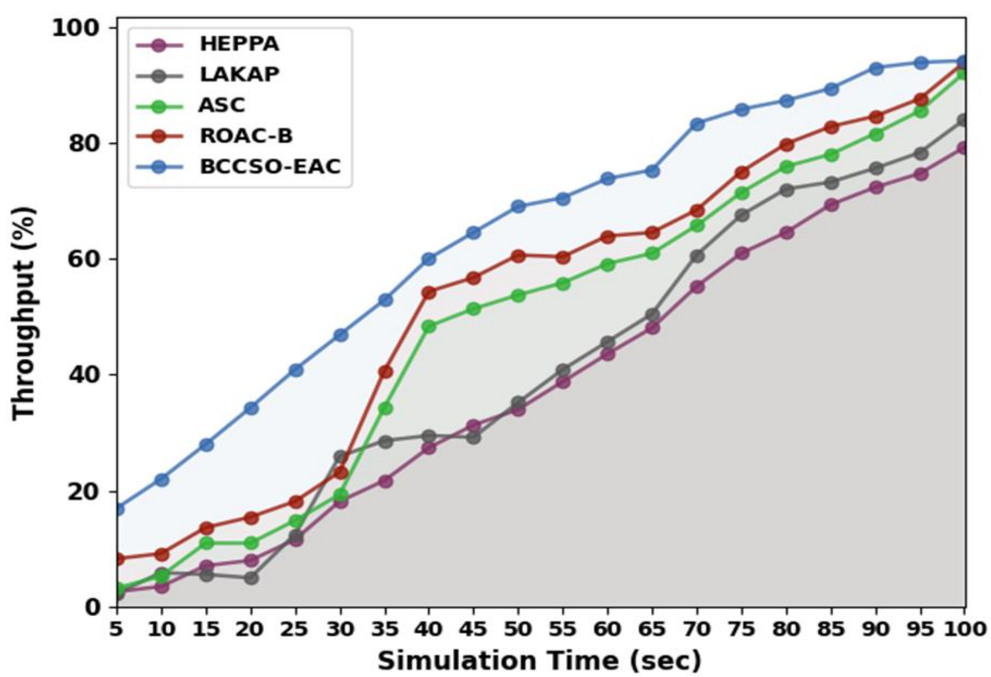

Figure 7 THRO Analysis of BCCSO-EAC Approach under Distinct Simulation Times

RESEARCH ARTICLE

5. CONCLUSION

In this study, a new BCCSO-EAC technique was introduced for energy-efficient clustering of the VANET. The presented BCCSO-EAC technique constructed optimal clusters and chose the CHs using a fitness function comprising RE, ND and intra-cluster distance parameters. In addition, the BCCSO-EAC technique selects CHs in such that the load among the nodes gets distributed properly. Moreover, BC technology is adopted to enable secure inter-cluster and intra-cluster VANET communication. The experimental result analysis of the BCCSO-EAC technique is tested under distinct measures. The results stated the improved results of the BCCSO-EAC approach over other recent methods in terms of different evaluation metrics. In future, the performance of the BCCSO-EAC method can be improvised by data aggregation protocols.

REFERENCES

[1] Mchergui, A., Moulahi, T. and Zeadally, S., 2022. Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs). Vehicular Communications, 34, p.100403.

[2] Nahar, A. and Das, D., 2023. MetaLearn: Optimizing routing heuristics with a hybrid meta-learning approach in vehicular ad-hoc networks. Ad Hoc Networks, 138, p.102996.

[3] Sun, R., Huang, Y. and Zhu, L., 2021. Communication by credence: trust communication in vehicular Ad Hoc networks. Mobile Networks and Applications, pp.1-13.

[4] Sharan, B., Chhabra, M. and Sagar, A.K., 2022, March. State-of-the-art: Data Dissemination Techniques in Vehicular Ad-hoc Networks. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 126-131). IEEE.

[5] Dwivedi, S.K., Amin, R., Das, A.K., Leung, M.T., Choo, K.K.R. and Vollala, S., 2022. Blockchain-based vehicular ad-hoc networks: A comprehensive survey. Ad Hoc Networks, p.102980.

[6] Akhter, A.S., Ahmed, M., Shah, A.S., Anwar, A. and Zengin, A., 2021. A secured privacy-preserving multi-level blockchain framework for cluster based VANET. Sustainability, 13(1), p.400.

[7] Alboqomi, O., Gazdar, T. and Munshi, A., 2020, November. A new blockchain-based trust management protocol for vehicular Ad Hoc networks. In The 4th International Conference on Future Networks and Distributed Systems (ICFNDS) (pp. 1-5).

[8] Sindhwani, M., Singh, C. and Singh, R., 2022. Blockchain Technology-based System in Vehicular Ad-hoc Network. Cross-Industry Blockchain Technology: Opportunities and Challenges in Industry 4.0, p.110.

[9] Saad, M., Khan, M.K. and Ahmad, M.B., 2022. Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review. Sustainability, 14(7), p.3919.

[10] Chaudhary, B. and Singh, K., 2021. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. Peer-to-Peer Networking and Applications, 14, pp.3198-3212.

[11] Vinoth Kumar, K. and Duraisamy, B., 2022. Efficient Privacy-Preserving Red Deer Optimization Algorithm with Blockchain Technology for Clustered VANET. Tehničkivjesnik, 29(3), pp.813-817.

[12] Liu, G., Fan, N., Wu, C.Q. and Zou, X., 2022. On a blockchain-based security scheme for defense against malicious nodes in vehicular ad-hoc networks. Sensors, 22(14), p.5361.

[13] Chaudhary, B. and Singh, K., 2021. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. Peer-to-Peer Networking and Applications, 14, pp.3198-3212.

[14] Zhang, X., Li, R., Hou, W. and Zhao, H., 2021. V-Lattice: a lightweight blockchain architecture based on DAG-lattice structure for vehicular Ad Hoc networks. Security and Communication Networks, 2021, pp.1-17.

[15] Folsom, R.D., Aravindhan, K. and Sikamani, K.T., 2021. A Novel Routing and Hybrid Based Clustering Scheme in vehicular Ad Hoc networks. International Journal of Intelligent Networks, 2, pp.103-114.

[16] Zhang, J., Jiang, Y., Cui, J., He, D., Bolodurina, I. and Zhong, H., 2022. DBCPA: Dual Blockchain-Assisted Conditional Privacy-Preserving Authentication Framework and Protocol for Vehicular Ad Hoc Networks. IEEE Transactions on Mobile Computing.

[17] Dwivedi, S.K., Amin, R., Vollala, S. and Khan, M.K., 2023. B-HAS: Blockchain-Assisted Efficient Handover Authentication and Secure Communication Protocol in VANETs. IEEE Transactions on Network Science and Engineering.

[18] Zhang, D., Shi, W. and Yang, R., 2023, February. A Blockchain-Based Distributed Machine Learning (BDML) Approach for Resource Allocation in Vehicular Ad-Hoc Networks. In Green, Pervasive, and Cloud Computing: 17th International Conference, GPC 2022, Chengdu, China, December 2–4, 2022, Proceedings (pp. 110-121). Cham: Springer International Publishing.

[19] Feng, X., Cui, K., Jiang, H. and Li, Z., 2022. EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network. Symmetry, 14(6), p.1230.

[20] Malik, M.W., Gul, Q. and Raja, G., 2022, August. Blockchain-based Security and Privacy-aware Protocol for Vehicular Ad Hoc Network. In 2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST) (pp. 279-284). IEEE.

[21] Roy, A. and Madria, S.K., 2021, June. BLAME: A Blockchain-assisted Misbehavior Detection and Event Validation in VANETs. In 2021 22nd IEEE International Conference on Mobile Data Management (MDM) (pp. 69-78). IEEE.

[22] Behura, A., Srinivas, M. and Kabat, M.R., 2022. Giraffe kicking optimization algorithm provides efficient routing mechanism in the field of vehicular Ad Hoc networks. Journal of Ambient Intelligence and Humanized Computing, 13(8), pp.3989-4008.

[23] Hu, G., Yang, R. and Wei, G., 2023. Hybrid chameleon swarm algorithm with multi-strategy: A case study of degree reduction for disk Wang–Ball curves. Mathematics and Computers in Simulation, 206, pp.709-769.

[24] Nguyen, G.N., Le Viet, N.H., Devaraj, A.F.S., Gobi, R. and Shankar, K., 2020. Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks. Sustainable Computing: Informatics and Systems, 28, p.100464.

[25] Joshi, G.P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T. and Ibrahim, A., 2020. Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks. Electronics, 9(9), p.1358.

Authors

R. Mohan Completed his Master of Technology in the field of Information Technology in Sathyabama University Chennai in the year 2012. He completed his Bachelor of Technology under Adhiparasakthi Engineering College, Melmaruvathur in the year 2007. He works as a Assistant Professor at Mailam Engineering College, Mailam, India from 2012 to till date. He is presently a part time Research Scholar in the Department of Computer Science and Engineering, Annamalai University, Chidambaram, India. His main thrust research areas are VANET Security.

RESEARCH ARTICLE

Dr. G. Prabakaran completed his Ph.D in the domain of image processing in Annamalai University Chidambaram in the year 2016. Under his guidance 6 members was awarded Ph.D degree. He participated and presented a paper count of 60 national/international conferences. He is working as a Associate Professor at Annamalai University, Chidambaram, India from 2001 to till date. His main thrust research areas are Image processing & computer graphics.

Dr. T. Priyaradhikadevi completed her Ph.D in Information and Communication Engineering in Anna University, Chennai in the year 2015. She Completed Master of Technology in the field of Information Technology in Bharath University, Chennai in the year 2005. She is working as a Professor at Mailam Engineering College, Mailam, India from 2004 to till date. Her main thrust research areas are Software Engineering.

How to cite this article:

R. Mohan, G. Prabakaran, T. Priyaradhikadevi, “Blockchain Assisted Chaotic Chameleon Swarm Optimization Based Clustering Technique in Vehicular Ad Hoc Networks”, International Journal of Computer Networks and Applications (IJCNA), 10(3), PP: 325-341, 2023, DOI: 10.22247/ijcna/2023/221888.