sustainability

MDPI

Article

Blockchain with Quantum Mayfly Optimization-Based Clustering Scheme for Secure and Smart Transport Systems

Hayam Alamro [1], Hamed Alqahtani [2], Fahad F. Alruwaili [3], Sumayh S. Aljameel [4] and Mohammed Rizwanullah [5,*]

[1] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2] Department of Information Systems, College of Computer Science, Center of Artificial Intelligence, Unit of Cybersecurity, King Khalid University, Abha 61421, Saudi Arabia
[3] Department of Computer Science, College of Computing and Information Technology, Shaqra University, Sharqa P.O. Box 11911, Saudi Arabia
[4] SAUDI ARAMCO Cybersecurity Chair, Computer Science Department, College of Computer Science and Information Technology, Imam Abdulrahman bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
[5] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
* Correspondence: r.mohammed@psau.edu.sa

Abstract: Blockchain (BC) with a clustering scheme can be used to build secure and smart Vehicular Ad-Hoc Networks (VANETs), which provide improved data integrity, enhanced security, efficient resource allocation, and streamlined processes. This technology has revolutionized the transport industry by enabling safer, more efficient, and transparent transportation networks. Therefore, this paper concentrates on the design of a new Blockchain with a Quantum Mayfly Optimization-based Clustering Scheme for Secure and Smart Transport Systems (BQMFO-CSSTS) technique. The objective of the presented BQMFO-CSSTS technique is to build a secure VANET via a BC-based technology and clustering process. Moreover, the BQMFO-CSSTS technique initially uses a Quantum Mayfly Optimization (QMFO) system with a fitness function for the selection of cluster heads (CHs) and the cluster construction process. In addition, BC technology is used as trust infrastructure to provide trustworthy services to the user and protect the privacy of the CHs and cluster members (CMs). The proposed scheme leverages the decentralized and immutable nature of BC to establish trust and ensure the integrity of cluster formation in VANETs. Finally, the BQMFO-CSSTS technique uses trajectory similarity metrics to protect the integrity of the CMs against attacks. The simulation results of the BQMFO-CSSTS technique are validated using a series of measures. The comprehensive results reported the superior outcomes of the BQMFO-CSSTS method over other recent approaches, with the maximum throughput being 1644.52 kbps. Therefore, integration of BC technology provides a transparent and secure framework through which to manage cluster membership, data sharing, and trust establishment among vehicles.

Keywords: transportation system; sustainability; blockchain; security; vehicular networks; clustering

Citation: Alamro, H.; Alqahtani, H.; Alruwaili, F.F.; Aljameel, S.S.; Rizwanullah, M. Blockchain with Quantum Mayfly Optimization-Based Clustering Scheme for Secure and Smart Transport Systems. *Sustainability* **2023**, *15*, 11782. https://doi.org/10.3390/su151511782

Academic Editor: Xu Li

Received: 11 June 2023
Revised: 19 July 2023
Accepted: 26 July 2023
Published: 31 July 2023

1. Introduction

Smart public transport systems (such as community scooters, buses, subways, and taxis) are a vital part of the growth of the dependable smart cities initiative, since they contribute to enhanced mobility and diminished carbon footprints [1]. For instance, the Internet of Vehicles (IoV) refers to a dispersed network of nodes in automobiles that allow automobiles to exchange data and link and interact with one another over the Internet [2,3]. The IoV aids in the understanding of smart transportation systems, since it enables automobiles fortified with computing nodes, sensors, and software to communicate

and interact with one another [4]. Different networks used in the maintenance of the smart public transport mechanisms are indispensably significant in terms of guaranteeing reliable operation without disturbance by illegal attacks [5,6]. These networks' susceptibility to cyber-attacks that could alter critical and urgent maintenance data or halt fundamental transport structures can lead to catastrophic consequences. An intelligent transportation system (ITS) has three processes: data uploading, data collection, and data processing [7]. User utility, efficiency, and safety are three significant metrics, as their participation in ITS allows systems to focus on delivering Quality of Service (QoS), utilities, and data safety concurrently.

Additionally, Artificial Intelligence (AI) is a vital technical innovation that can enable smart cities' applications [8]. Currently, along with AI and Internet of Things (IoT), Blockchain (BC) technology is recognized as an invention with the potential to enable integrated application processes, improve modern smart city applications, and generate new designs and methods [9,10]. BC can enhance the safety, transparency, security, trust, and privacy of different processes by presenting a shared and decentralized distributed ledger [11]. To this end, the BC evolution stages (1.0 to 4.0) were developed to create a range of properties, including strengths, functionality, challenges, security problems, and characteristics [12]. The BC method refers to the distributed ledger and has tamper-resistant, decentralized, anonymous, and trust-based features that can be combined with ITS to guarantee the safety of participants' data [13]. Although few researchers have inspected the integration of ITS and BC, they have focused on trust management, data sharing, BC-enabled crowdsensing, energy delivery, and BC network structure [14]. However, to the best of our knowledge, existing studies have ignored BC safety.

This paper concentrates on the design of a new BQMFO-CSSTS technique. The BQMFO-CSSTS technique initially uses the QMFO method, with a fitness function used for the selection of Cluster Heads (CHs) and the cluster construction process. In addition, BC technology is used as a trust infrastructure to provide trustworthy services to the user and protect the privacy of the CHs and Cluster Members (CMs). Finally, the BQMFO-CSSTS technique uses trajectory similarity metrics to protect CMs against attacks. The simulation results of the BQMFO-CSSTS technique are validated using varied measures.

2. Related Works

Fernandes et al. [15] described a decentralized reputation mechanism that depends on a consortium BC and an intellectual contract. This structure examines the dependability of data produced by vehicles, contributes to decision-making processes, and identifies malicious behaviours. The evaluation metrics, which are the comprehensive functional structure of the mechanism, describe the methods, message formats, and communication protocols that can be applied. In [16], the authors modelled an adaptation of BC that securely saves data in vehicular networks. The method can store externally sourced data, like information about a user's reputation and traffic events. The presented solution has two interconnected elements: the reputation system and the ITS-BC. The study presented a synthetic test that authenticates the usage case of the solution, i.e., the user-reporting speed and alerts, which ensures that the author recognizes a fair reputation mechanism that penalizes the false users. Zia [17] presented B-DRIVE, which is a BC-related distributed IoT network for smart urban transportation. This network can to link a large fleet of IoT gadgets, as it uses nodes installed on roadside structures and different vehicles, which can be sent to data storage centres, known as Full-Nodes, to disseminate and log sensor-generated datasets.

Das et al. [18] devised an identity generation and management approach that utilizes BC to solve present difficulties in ITS applications related to the security of identity management and validation of vehicles. In [19], the authors presented the BC-related decentralized trust score structure that uses participating nodes to find and blacklist internal aggressors in VANETs. The authors devised a two-level recognition mechanism, in which at the primary level, neighbouring nodes separately computed trust. At the secondary level, a consortium BC-based system included certified Road Side Units (RSU) as validators, which created total trust scores for vehicular nodes. Next, depending on trust scores created by the neighbouring nodes, the blacklist node table was dynamically modified. Wang et al. [20] introduced a BC-related special vehicle priority access guarantee method (BSV-PAGS). The authors utilized a Machine Learning (ML) approach to train and design special vehicle detectors to enhance the accuracy of detection methods used to identify special vehicles.

In [21], the authors devised a new method that integrated BC technology and a Deep Learning (DL) approach to better protect smart public transport mechanisms. As a hybrid DL-related approach that Integrated Multilayer Perceptron (MLP) and Auto Encoder (AE), this method could identify Distributed Denial Of Service (DDoS) attacks that try to block or halt the urgent and serious exchange in transport maintenance data between stakeholders. Akhter et al. [22] introduced a multilevel BC-related privacy-preserving validation system. The study explained the process of forming of key generation tasks, validation centres, and vehicle registration. Though several models are available in the literature, there is still a need to improve their performance.

Chaudhary and Singh [23] examined a decentralized VANET design that contained BC technology. The presented BC-based method for VANET mechanisms had 4 steps: vehicle registration, BC maintenance, BC network initialization, and pseudonym upload. It could effectively resolve the issues that developed in centralized structures and solved trust problems that affected the entities. Gazdar et al. [24] solved these problems by presenting a decentralized BC-based Trust Management Framework (BC-TMF) that calculated trust metrics for vehicles. These trust metrics depended on the messages' authenticity. Alharthi et al. [25] examined a Biometrics BC (BBC) structure used to secure data distribution between vehicles in VANETs and maintain statuary data using conventional and trusted methods. Using the presented system, the author presented benefits of using biometric data to keep a record of the genuine identities of the message senders, thus maintaining secrecy. Thus, the presented BBC technique ensured trust and security between vehicles connected via VANETs and had the capacity to trace identities when needed.

3. The Proposed Model

In this paper, a BQMFO-CSSTS technique is developed via the use of clustering and BC in VANETs. The presented BQMFO-CSSTS technique aims to enable secure VANETs using BC-based technology and clustering processes. It involves a series of processes, namely clustering, BC-based privacy-preserving, and security mechanisms. Figure 1 establishes the overall flow of the BQMFO-CSSTS approach.

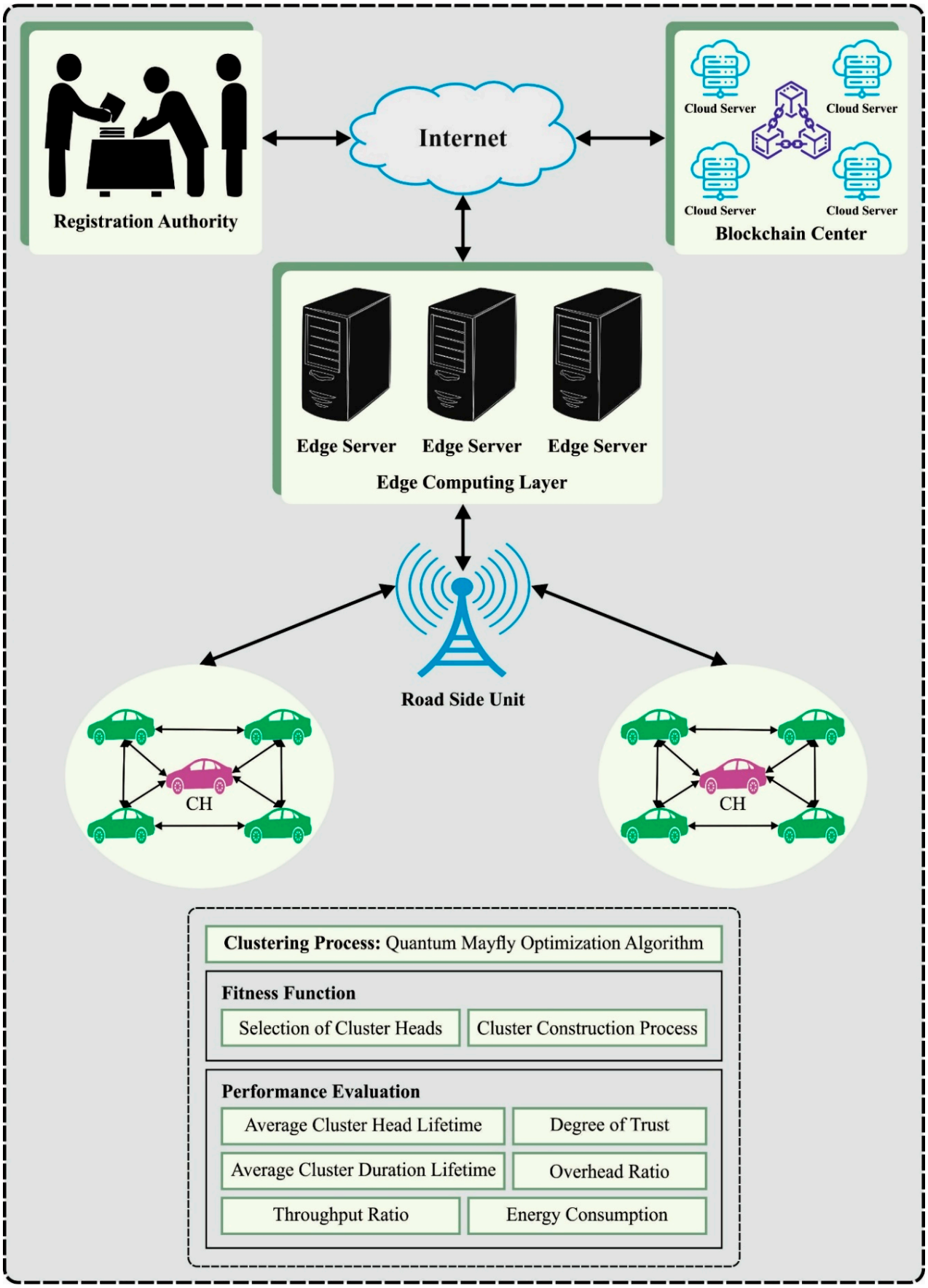

Figure 1. The overall flow of the BQMFO-CSSTS approach.

3.1. Design of QMFO-Based Clustering Process

In this study, the BQMFO-CSSTS technique initially uses the QMFO model and a fitness function for the selection of CHs and cluster construction processes. The MFO can be referred to as a bionics system, as it inspired by the social behaviours of the Mayfly (MF) [26]. The optimum and suboptimum individuals in all the populations, as well as the movement mode and reproduction processes of female and male individuals, are carefully chosen. In the meantime, via mating between the optimum female and male individuals, the optimum offspring generation and suboptimum offspring generation can be attained. The movement direction of all mayflies was impacted by the collective optimum position and dynamics of individual female and male MF targets when moving towards the location.

The flight mode of male MF is the same as the movement mode of the birds in a Particle Swarm Optimization (PSO) algorithm, and the distances and directions travelled by male MFs were changed based on their own flight experience using Equation (1):

$$x_i^{n+1} = x_i^n + v_i^{n+1} \tag{1}$$

where x_i^n and v_i^n denotes the present location and speed, respectively, of male MF i on the n^{th} search, as given in Equation (2):

$$v_{ij}^{n+1} = v_{ij}^n + \alpha_1 e^{-\beta l_p^2}\left(p_{best_i^j} - X_{ij}^n\right) + \alpha_2 e^{-\beta l_g^2}\left(g_{best_i^j} - X_{ij}^n\right) \tag{2}$$

Since male MFs dance on the water surface to attract females, the locations of the male MFs continuously vary. v_{ij}^n is the speed of n-th search of MF i-th at j-th dimension, and x_{ij}^n denotes the location at that time. α_1 and α_2 are assessed based on the positive attraction coefficient of social interaction, and β denotes the visibility coefficients of the MF.

In the meantime, the optimum locations of the individual and collective MFs are denoted as $p_{best_i^j}$ and $g_{best_i^j}$, respectively. Furthermore, the distances from an existing location to $p_{best_i^j}$ and $g_{best_i^j}$ are represented as l_p and l_g, respectively, and evaluated via Equation (3):

$$\left\|x_j - X_i\right\| = \sqrt[2]{\sum_{j=1}^{n}(x_{ij} - X_{ij})^2} \tag{3}$$

A fixed dance pattern should be used to better represents MFs within the population. In the meantime, a random component was presented to ensure that the speed changed continuously, as defined in Equation (4):

$$v_{ij}^{n+1} = v_{ij}^n + d \times r \tag{4}$$

In Equation (4), d denotes the dance coefficient, and r indicates the random number.

The female MF movement relies on the attraction of male MFs, and the location renewal relies on the rise of speed that is formulated via Equation (5):

$$y_i^{n+1} = y_i^n + v_i^{n+1} \tag{5}$$

Speed updating is a specific procedure that guarantees the offspring quality; thus, the superior female should be attracted to the superior male. It is represented in Equation (6):

$$v_{ij}^{n+1} = \begin{cases} v_{ij}^n + \alpha_2 e^{-\beta l_f^2}\left(x_{ij}^n - y_{ij}^n\right) \\ v_{ij}^n + g \times r \end{cases} \tag{6}$$

where y_{ij}^n denotes the location of the female MF, g indicates the random walking coefficient of the female MF, and l_f shows the distance between male and female MFs.

During mating, the optimum and suboptimum individuals in the female and male groups must be chosen for reproduction based on the fitness function. The outcomes of interbreeding that generate the optimum and suboptimum offspring are evaluated using Equation (7):

$$\begin{cases} offspring1 = L \times m + (1 - L) \times f_m \\ offspring2 = L \times f_m + (1 - L) \times m \end{cases} \quad (7)$$

In Equation (7), m and f_m represent the male and female in the parent group, respectively, and L denotes the random integer within a specific range.

The conventional MFO algorithm could precisely search for the optimum value in a single-peak function using the features used in MF reproduction. However, due to the complicated process of assessing a large population, the convergence is not fine, and the search speed is slower, as it is easier to become trapped in local optima while handling multi-peak functions. Thus, the quantum concept was proposed using the classical MFO algorithm, thus forming the QMFO algorithm. Meanwhile, the location and velocity of MF could not be defined in quantum space; thus, wave function was utilized to characterize the MF location, and the Monte Carlo algorithm was employed to resolve the problems using Equation (8).

$$\begin{cases} m_{best^n} = \frac{1}{N}\Sigma_{i=1}^{a} P_{best_i^n}(i = 1 \ldots n) \\ P_i^t = \gamma \times P_{best_i^n} + (1 - \gamma) \times g_{best}^n \\ X_i^{n+1} = P_i^n \pm \varepsilon \left| m_{best^n} - x_i^n \right| \log \frac{1}{a} \end{cases} \quad (8)$$

In Equation (8), r and a are uniformly distributed random values in the range 0–1, and c shows the last random motion parameter. N and n denote the numbers of individuals and iterations, respectively. m_{besi^n} denotes the average past optimum location of the male MF, and P_i^n denotes the modified location of the i^{th} male MF at n-th iterations.

The implementation steps of the QMFO algorithm are shown below:

Step 1: initialize the position of female and male MFs in the space.

Step 2: compute the average optimum position m_{best} of male MFs based on Equation (8).

Step 3: Compute the fitness value and compare it to the prior iteration value. When the present function value is lesser than the prior iteration, the existing MF location is modified based on the individual optimum location; otherwise, it retains the prior iteration. Thus, the optimum male individual position p_{besi} and collective position g_{besi} are attained.

Step 4: estimate the new locations of both MFs based on Equations (5) and (8), respectively, and mate in sequence.

Step 5: evaluate the fitness function and update p_{besi} and g_{besi}.

Step 6: repeat Steps 2 to 5 until the stopping criteria are satisfied.

The QMFO algorithm derives a fitness function for the optimum cluster creation procedure [27]. The fitness function used in the BQMFO-CSSTS is introduced as a multi-objective fitness function, as given in Equation (9).

$$Fit_{Fn} = w_1 \times fn_{(1)} + w_2 \times fn_{(2)} \quad (9)$$

In Equation (9), $fn_{(1)}$ and $fn_{(2)}$ functions characterize the sum of distances between all of the CMs and CHs of each cluster in the network and the differences between clusters in terms of route length. Based on Equation (10), the function $fn_{(1)}$ is computed.

$$Fit_{Fn}(Dist_{Sum}) = \sum_{i=1}^{N_C}\left(\sum_{q}^{CH_D}(EU_{Dist}(CM_{q,c}, CH_{q.c}))\right) \quad (10)$$

where $EU_{Dist}(CM_{q,c}, CH_{q.c})$ shows the Euclidean distance evaluated for the total number of clusters. The distances between every $CM_{q,c}$ vehicular network and the CHs $CH_{q.c}$ are

related to all of the clusters based on the overall number of clusters. At the same time, function $fn_{(2)}$ represents the absolute degree, as equated in Equation (11).

$$Fit_{Fn}(AB_{Degree}) = \sum_{i=1}^{N_C} AB_{Fn}(Deg_C - |CM_{q,c}|) \quad (11)$$

where $|CM_{q,c}|$ signifies the overall number of CM nodes based on route length, with the degree Deg_C emphasizing the constant value of cluster density. We note that lesser density can be recognized as the lowest value.

3.2. BC Technology for Privacy Preserving

The BQMFO-CSSTS architecture uses BC as a trust infrastructure to provide trustworthy services to the user and protect their privacy [4]. Two kinds of BC nodes are available based on the locations and capabilities of the entity in the ITS framework, vehicle gateways, servers, and RSUs that are set to these types and integrated with other functions. One example is a full BC node. The node works as a miner, as it synchronizes and maintains a full copy of the blocks. Meanwhile, this node could see every transaction that takes place in the BC; only the authorized node with high ability could be used as one of this type of node, which includes servers, gateways, and RSUs in the core network. Another example is a lightweight BC node. These types of nodes are analogous to the Simplified Payment-Verified (SPV) nodes used in Ethereum. The set of nodes could not authenticate transactions via mining; on the other hand, they could identify a transaction based on the network. It should be noted that based on the needs and positions of the ITS operator, the network entities, including RSUs, gateways, servers, routers, etc., are set as lightweight and full BC nodes. In particular, vehicles were set to lightweight and full BC nodes, allowing them to be deeply included in the ITS (i.e., included in the BC network to secure additional benefits) or utilize the secured services with data protection.

3.3. Security Mechanism

A new security mechanism can be developed to find malicious nodes to further improve the security and availability of VANETs [28]. In cluster networks, the security and availability of CHs are very important. CHs help the server to transmit to and collect data via CMs. If the attacker wants to access the private information of other vehicles, they must act as the CHs. The vehicles controlled by a malicious attacker provide various identities (i.e.,vehicles) during the Sybil attack, and each vehicle has an analogous position, direction, maximal acceleration, and speed. Henceforth, this vehicle should have a high probability of being chosen as the CH and high relative mobility metrics.

A S_t trajectory similarity metric is defined to protect network attacks for the CMs' privacy. The similarity metric is formulated in Equation (12):

$$S_{tc} = \frac{1}{N-1} \sum_{i=1}^{N-1} \left(\frac{\Delta t_i}{lifetime_i}\right), \quad (12)$$

In Equation (12), $lifetime_i$ shows the lifetime of the i node, and Δt_i denotes the duration of c and node i that belongs to a similar cluster. The server evaluates the trajectory similarity metric used whenever a CH is selected. If a single CH has high trajectory similarity metrics, the server checks every node in the cluster to identify malicious attackers.

4. Performance Validation

In this section, the experimental validation of the BQMFO-CSSTS technique takes place, with consideration given to various aspects, such as the varying number of nodes n, transmission range r, and speed limit v. The proposed model was simulated using the NS3 tool. The existing models [29] used for comparative analysis were BC-Assisted Trusted Clustering Mechanism for IoT-Enabled Smart Transportation System (ATCM IOT-ESTS), Whale

Optimization Algorithm for Clustering in Vehicular Ad hoc Networks (WOACNET), Deep learning-based Dynamic Stable Cluster Head Selection (DL-SCHS), and StabTrust (ST).

In Table 1 and Figure 2, the average cluster head lifetime (ACHL) results of the BQMFO-CSSTS technique are compared to those of recent models with varying r and v values [29]. The results indicate that the BQMFO-CSSTS technique identifies improved values of ACHL that are superior to those of other models. For instance, with r and v values of 50 and 30, the BQMFO-CSSTS technique gains an increased ACHL of 493.38 s, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST models obtain decreased ACHLs of 467.49 s, 342.89 s, 249.03 s, and 459.40 s, respectively. Moreover, with r and v values of 250 and 90, the BQMFO-CSSTS method acquires an increased ACHL of 543.55 s, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST techniques gain decreased ACHLs of 519.27 s, 456.16 s, 480.44 s, and 517.65 s, respectively.

Table 1. ACHL analysis of BQMFO-CSSTS approach compared to other systems and with varying r and v values.

Average Cluster Head Lifetime	BQMFO-CSSTS	ATCM IOT-ESTS	WOACNET	DL-SCHS	Stab Trust
(r, v) (50, 30)	493.38	467.49	342.89	249.03	459.40
(r, v) (100, 40)	543.55	519.27	394.67	457.78	418.94
(r, v) (125, 50)	541.93	520.89	397.91	428.65	418.94
(r, v) (150, 60)	527.36	506.33	472.34	464.25	321.85
(r, v) (200, 70)	541.93	528.98	485.29	509.56	504.71
(r, v) (225, 80)	541.93	522.51	449.69	501.47	399.52
(r, v) (250, 90)	543.55	519.27	456.16	480.44	517.65

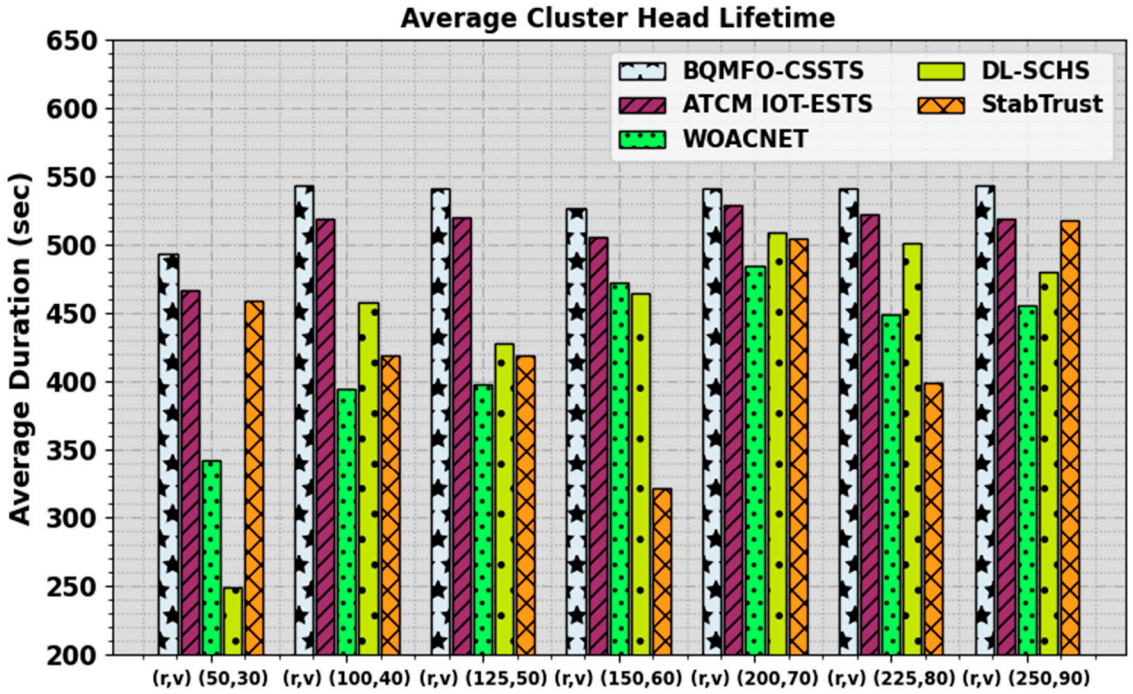

Figure 2. ACHL outcomes of BQMFO-CSSTS approach compared to other systems and with varying r and v values.

In Table 2 and Figure 3, the average cluster duration lifetime (ACDL) outcomes of the BQMFO-CSSTS method are compared to recent methods with varying n and r values. The figure specifies that the BQMFO-CSSTS algorithm achieves improved values of ACDL

superior to those of other models. For example, with n and r values of 20 and 50, the BQMFO-CSSTS method gains an increased ACDL of 502.45 s, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST methods attain decreased ACDLs of 479.45 s, 270.69 s, 484.76 s, and 491.83 s, respectively.

Table 2. ACDL outcome of BQMFO-CSSTS approach compared to other systems and with varying n and r values.

Average Cluster Duration Lifetime	BQMFO-CSSTS	ATCM IOT-ESTS	WOACNET	DL-SCHS	Stab Trust
(n, r) (20, 50)	502.45	479.45	270.69	484.76	491.83
(n, r) (40, 100)	539.60	521.91	290.15	511.29	507.76
(n, r) (60, 150)	594.45	573.22	304.30	523.68	571.45
(n, r) (80, 200)	592.68	583.83	472.37	578.52	482.99
(n, r) (100, 250)	597.98	590.91	518.37	589.14	589.14
(n, r) (120, 300)	599.75	589.14	555.52	564.37	566.14

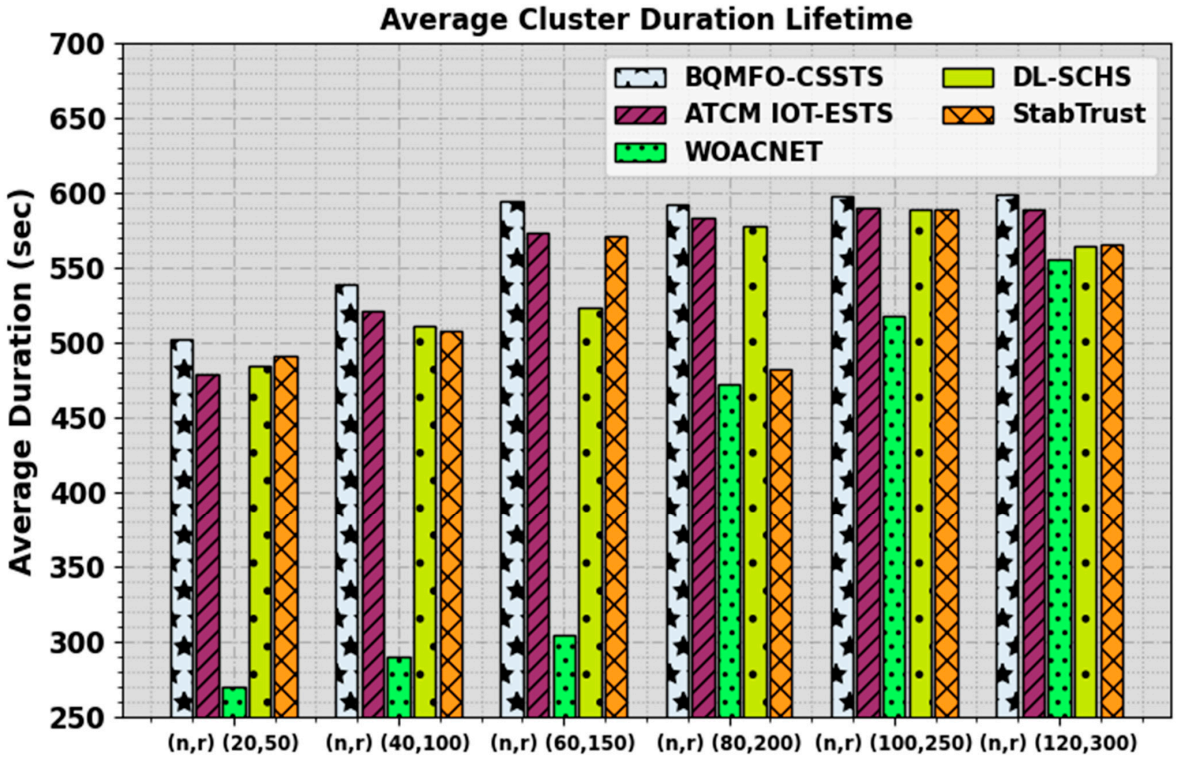

Figure 3. ACDL outcome of BQMFO-CSSTS method with varying n and r values.

Furthermore, with the values n and r values of 120 and 300, the BQMFO-CSSTS method gains an increased ACDL of 599.75 s, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST methods gain decreased ACDLs of 589.14 s, 555.52 s, 564.37 s, and 566.14 s, respectively.

In Table 3 and Figure 4, the ACDL results of the BQMFO-CSSTS method are compared to recent approaches with varying r and v values. The figure specifies that the BQMFO-CSSTS method achieves improved values of ACDL superior to those of other approaches. For example, with r and v values of 50 and 30, the BQMFO-CSSTS algorithm gains an increased ACDL of 474.21 s, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST approaches gain decreased ACDLs of 464.53 s, 338.72 s, 253.24 s, and 456.47 s, respectively.

Also, with r and v values of 250 and 90, the BQMFO-CSSTS method gains an increased ACDL of 543.57 s, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST approaches gain decreased ACDLs of 520.99 s, 464.53 s, 485.50 s, and 509.69 s, respectively.

Table 3. ACDL outcome of BQMFO-CSSTS approach compared to other systems and with varying r and v values.

Average Cluster Durational Lifetime	BQMFO-CSSTS	ATCM IOT-ESTS	WOACNET	DL-SCHS	Stab Trust
(r, v) (50, 30)	474.21	464.53	338.72	253.24	456.47
(r, v) (100, 40)	532.28	516.15	382.27	461.31	429.05
(r, v) (125, 50)	540.34	524.21	400.01	416.14	409.69
(r, v) (150, 60)	537.11	503.24	467.76	464.53	324.21
(r, v) (200, 70)	541.95	520.99	480.66	498.40	501.63
(r, v) (225, 80)	535.50	520.99	450.02	506.47	408.08
(r, v) (250, 90)	543.57	520.99	464.53	485.50	509.69

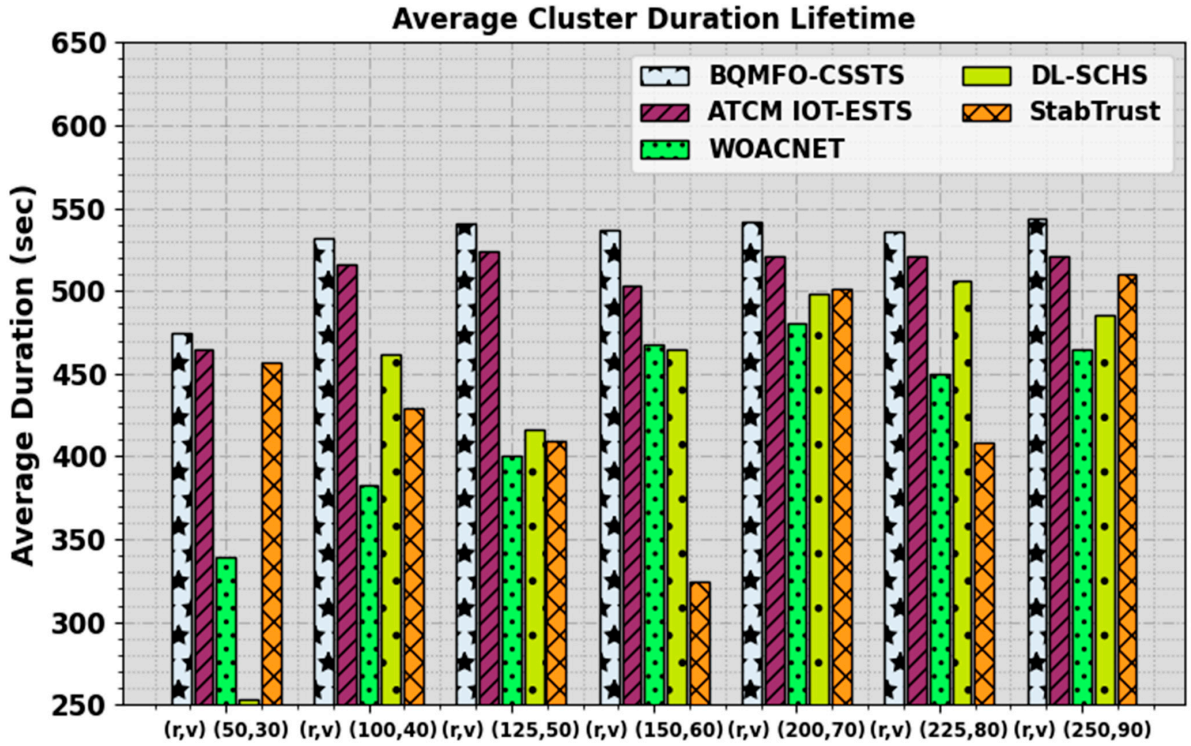

Figure 4. ACDL outcome of BQMFO-CSSTS approach with varying r and v values.

Table 4 and Figure 5 represents the Overhead Ratio (OHR) results of the BQMFO-CSSTS technique compared to other recent methods and at varying points in time. The figure shows that the BQMFO-CSSTS method results in the lowest OHR values over all time intervals. At 50 min, the BQMFO-CSSTS technique gains a lower OHR of 4.94, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST models accomplish higher OHRs of 9.46, 13.97, 14.42, and 27.97, respectively. On the other hand, at 900 min, the BQMFO-CSSTS method gains a lower OHR of 43.2, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST approaches accomplish higher OHRs of 54.16, 107.89, 77.19, and 117.83, respectively.

Table 4. OHR outcome of BQMFO-CSSTS approach compared to other systems and at varying points in time.

	Overhead Ratio				
Time (Min)	**BQMFO-CSSTS**	**ATCM IOT-ESTS**	**WOACNET**	**DL-SCHS**	**Stab Trust**
50	04.94	09.46	013.97	14.42	027.97
100	05.84	13.07	017.13	18.94	033.39
150	08.10	17.13	020.74	25.71	039.26
200	08.10	15.33	021.65	28.42	041.06
250	08.10	16.23	024.36	26.61	046.48
300	09.91	17.58	027.97	34.74	050.09
350	13.52	20.74	030.23	39.26	054.16
400	13.52	23.91	031.13	43.77	059.58
450	14.87	27.52	037.90	47.84	063.64
500	18.94	30.23	042.42	49.64	065.00
550	21.20	31.13	044.68	55.06	073.12
600	23.45	31.58	047.39	57.77	077.19
650	24.81	34.29	053.26	60.48	083.96
700	26.61	35.65	059.58	64.54	085.77
750	32.48	39.26	069.51	65.45	090.73
800	37.45	46.48	078.54	67.25	098.41
850	39.71	49.64	088.02	70.87	101.57
900	43.32	54.16	107.89	77.19	117.83

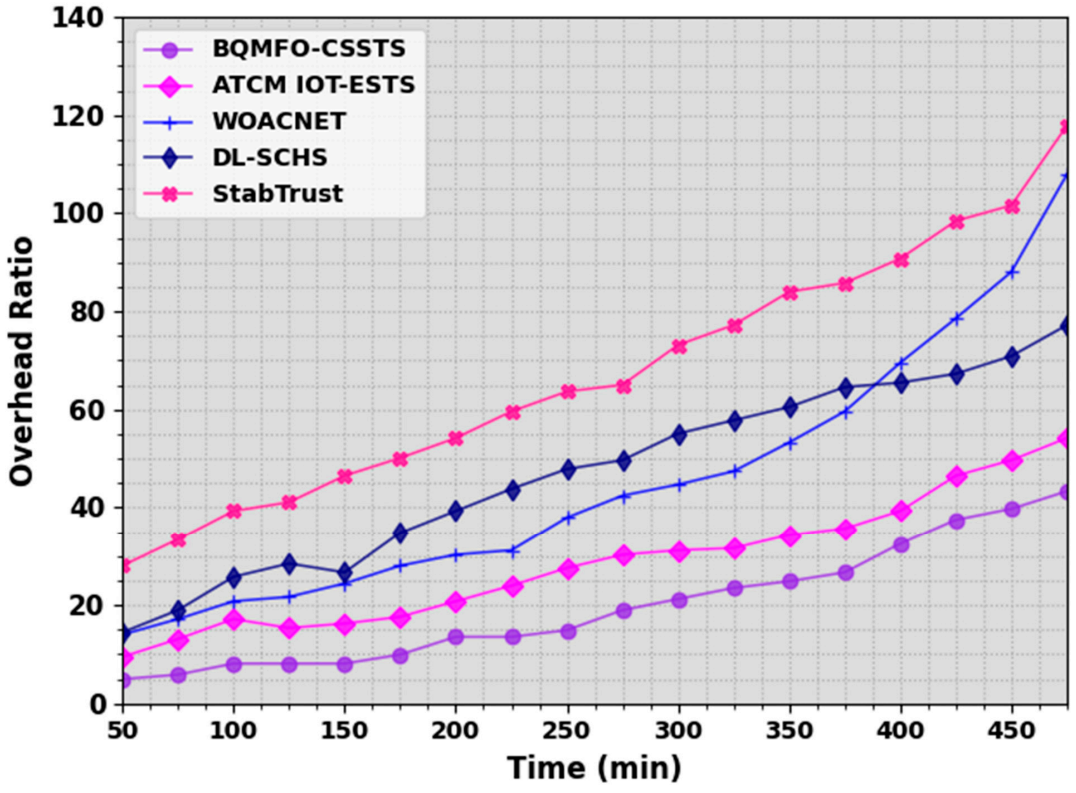

Figure 5. OHR outcome of BQMFO-CSSTS approach at varying points in time.

In Table 5 and Figure 6, the Throughput (THROT) outcome of the BQMFO-CSSTS technique is compared to other recent approaches at varying times intervals. The outcomes imply that the BQMFO-CSSTS technique gains enhanced values of THROT relative to other models. For instance, at 50 min, the BQMFO-CSSTS technique gains an increased THROT of 352.93 kbps, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST systems reach lesser THROTs of 209.42 kbps, 281.17 kbps, 154.22 kbps, and 110.06 kbps, respectively. Additionally, at 900 min, the BQMFO-CSSTS system gains a higher THROT of 1644.52 kbps, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST methods obtain lower THROTs of 1561.73 kbps, 1368.54 kbps, 1197.43 kbps, and 888.33 kbps, respectively.

Table 5. THROT outcome of BQMFO-CSSTS approach compared to other systems and at varying points in time.

	Throughput Ratio (kbps)				
Time (Min)	**BQMFO-CSSTS**	**ATCM IOT-ESTS**	**WOACNET**	**DL-SCHS**	**Stab Trust**
50	0352.93	0209.42	0281.17	0154.22	110.06
100	0490.92	0341.89	0281.17	0225.98	121.10
150	0529.56	0363.97	0347.41	0237.02	176.30
200	0579.23	0375.01	0397.08	0281.17	237.02
250	0612.35	0413.64	0485.40	0286.69	275.65
300	0689.62	0468.84	0595.79	0308.77	292.21
350	0816.58	0546.11	0684.10	0325.33	292.21
400	0866.25	0634.43	0728.26	0380.53	303.25
450	0949.05	0783.46	0728.26	0419.16	347.41
500	1015.28	0766.90	0800.02	0496.44	363.97
550	1120.16	0899.37	0822.10	0546.11	375.01
600	1213.99	0982.16	0882.81	0667.55	413.64
650	1225.03	1009.76	0965.61	0728.26	468.84
700	1307.82	1114.64	0971.13	0827.62	524.04
750	1401.66	1169.83	1098.08	0899.37	601.31
800	1489.97	1313.34	1208.47	0926.97	673.07
850	1556.21	1401.66	1263.67	1087.04	805.54
900	1644.52	1561.73	1368.54	1197.43	888.33

Table 6 and Figure 7 represent the Energy Consumption (ECON) results of the BQMFO-CSSTS method compared to other recent methods and using varying numbers of nodes. The results showed that the BQMFO-CSSTS technique resulted in the lowest number of ECON values over nodes. When using 50 nodes, the BQMFO-CSSTS technique gained a low ECON of 59.09 J, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST models accomplish higher ECONs of 93.41 J, 115.33 J, 153.45 J, and 186.81 J, respectively. On the other hand, when using 300 nodes, the BQMFO-CSSTS technique acquires a low ECON of 157.26 J, while the ATCM IOT-ESTS, WOACNET, DL-SCHS, and ST methods accomplish higher ECONs of 187.76 J, 322.15 J, 306.90 J, and 311.67 J, respectively. These results confirmed the enhanced performance of the BQMFO-CSSTS technique.

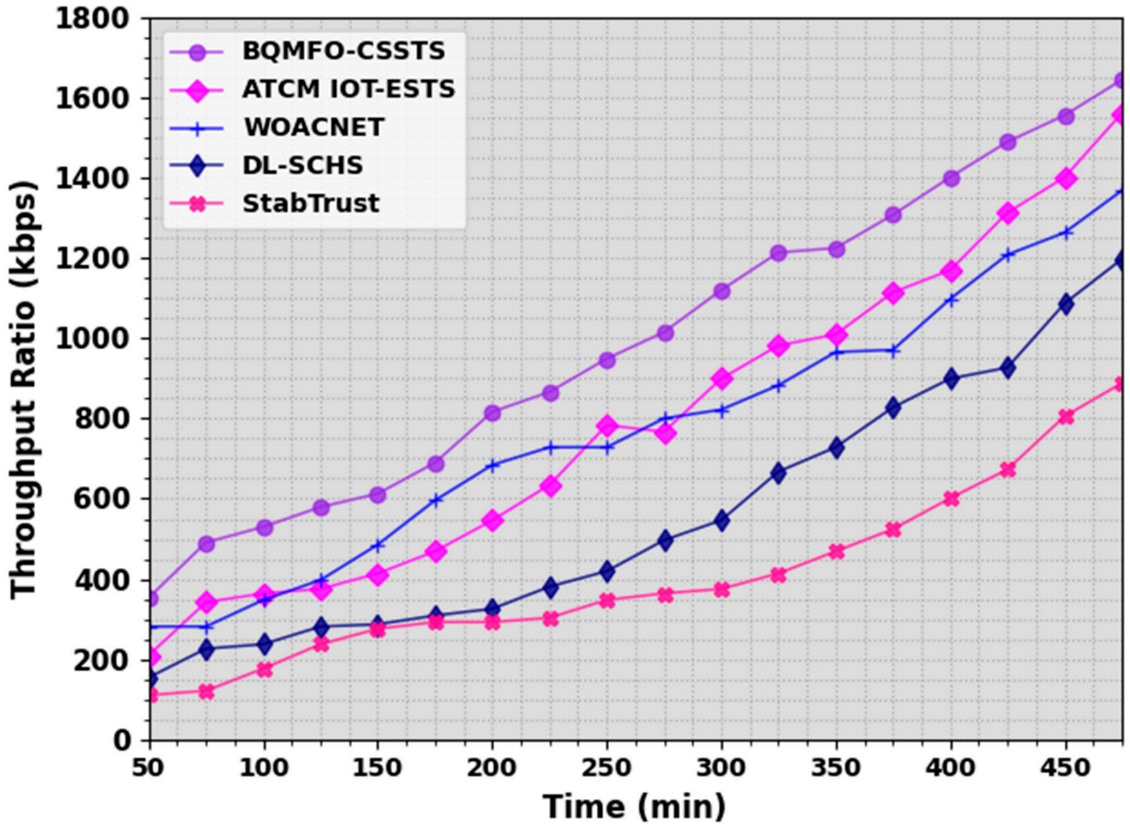

Figure 6. THROT outcome of BQMFO-CSSTS approach at varying points of time.

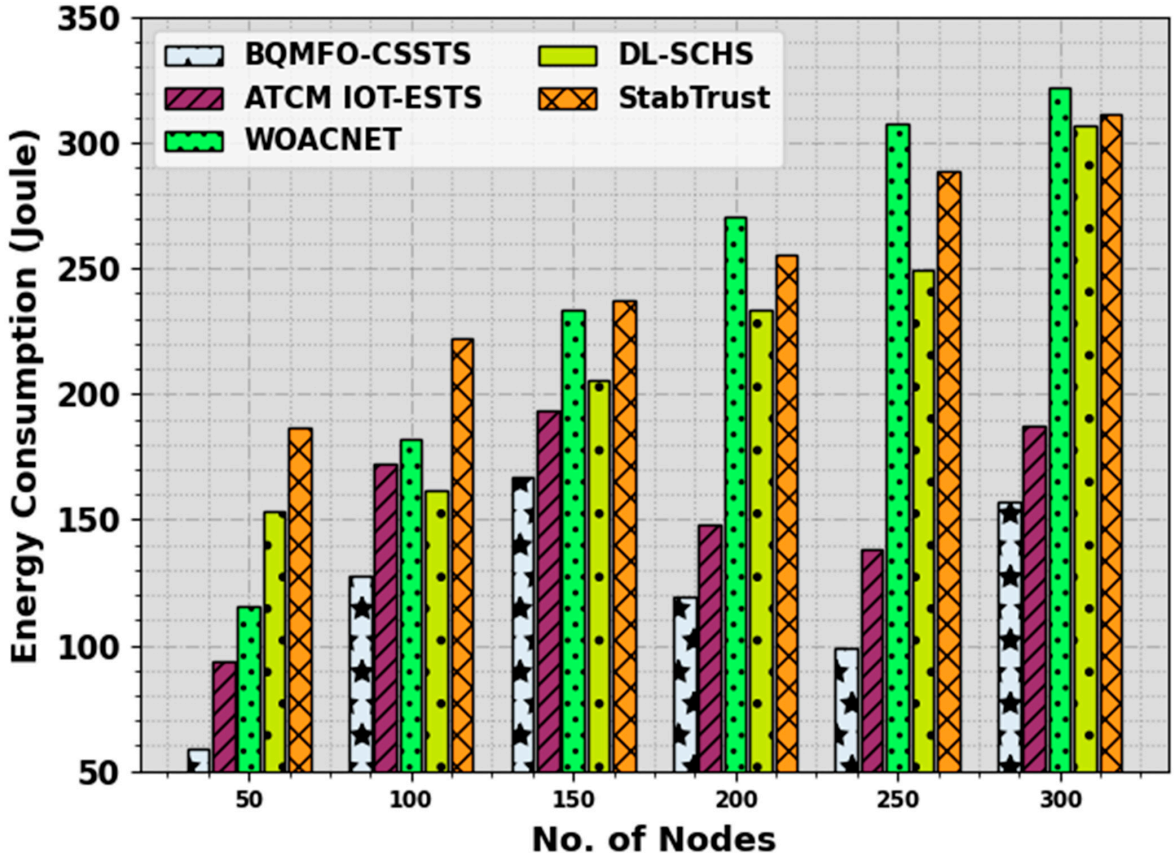

Figure 7. Comparative ECON outcome of BQMFO-CSSTS approach using varying numbers of nodes.

Table 6. ECON outcome of BQMFO-CSSTS approach compared to other systems and using varying numbers of nodes.

	Energy Consumption (Joule)				
No. of Nodes	**BQMFO-CSSTS**	**ATCM IOT-ESTS**	**WOACNET**	**DL-SCHS**	**Stab Trust**
50	059.09	093.41	115.33	153.45	186.81
100	127.72	172.51	182.04	162.03	222.08
150	166.79	193.48	233.51	205.87	237.32
200	119.14	147.73	270.68	233.51	255.43
250	099.12	138.20	307.86	249.72	288.79
300	157.26	187.76	322.15	306.90	311.67

5. Conclusions

In this paper, a privacy-preserving cluster scheme known as the BQMFO-CSSTS technique on VANET is developed. The presented BQMFO-CSSTS technique aims to accomplish secure VANET via BC technology and clustering process. It involves a series of processes, namely clustering, BC-based privacy-preserving, and security mechanisms. Moreover, the BQMFO-CSSTS technique initially uses the QMFO approach with a fitness function for the selection of CHs and the cluster construction process. In addition, BC technology is used as trust infrastructure to provide trustworthy services to the user and protect the privacy of the CHs and CMs. Finally, the BQMFO-CSSTS technique uses trajectory similarity metrics to protect the privacy of the CMs against attacks. The simulation results of the BQMFO-CSSTS technique are validated utilizing a series of measures. The comprehensive outcomes stated the superior performance of the BQMFO-CSSTS method over those of other recent algorithms. While the integration of BC technology provides the groundwork for enabling secure clustering in VANETs, future research can concentrate on improving the security aspects using privacy-preserving techniques, robust consensus mechanisms, and secure communication protocols to protect sensitive information and prevent malicious attacks from occurring within the clustering technique. In addition, the proposed clustering scheme should be implemented and tested in real-world VANET environments to validate its effectiveness and evaluate its performance under various realistic scenarios.

Author Contributions: Conceptualization, H.A. (Hayam Alamro); Methodology, H.A. (Hamed Alqahtani); Software, S.S.A.; Validation, F.F.A. and S.S.A.; Investigation, H.A. (Hayam Alamro); Data curation, S.S.A.; Writing—original draft, H.A. (Hayam Alamro), H.A. (Hamed Alqahtani), F.F.A. and M.R.; Writing—review & editing, H.A. (Hayam Alamro), H.A. (Hamed Alqahtani), F.F.A., S.S.A. and M.R.; Visualization, M.R.; Project administration, M.R.; Funding acquisition, H.A. (Hamed Alqahtani). All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a large group research project under grant number (RGP2/159/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R361), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. We would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: This article does not contain any studies in which human participants took part.

Data Availability Statement: Data sharing concerns do not apply to this article, as no datasets were generated during the current study.

Conflicts of Interest: The authors declare that they have no conflict of interest. The manuscript was written with the contribution of all authors. All authors have read and approved the final version of the manuscript.

References

1. Liu, J.; Zhang, L.; Li, C.; Bai, J.; Lv, H.; Lv, Z. Blockchain-based secure communication of intelligent transportation digital twins system. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 22630–22640. [CrossRef]
2. Ning, Z.; Sun, S.; Wang, X.; Guo, L.; Guo, S.; Hu, X.; Hu, B.; Kwok, R.Y. Blockchain-enabled intelligent transportation systems: A distributed crowdsensing framework. *IEEE Trans. Mob. Comput.* **2021**, *21*, 4201–4217. [CrossRef]
3. Finogeev, A.; Deev, M.; Parygin, D.; Finogeev, A. Intelligent SDN Architecture with Fuzzy Neural Network and Blockchain for Monitoring Critical Events. *Appl. Artif. Intell.* **2022**, *36*, 2145634. [CrossRef]
4. Li, Y.; Ouyang, K.; Li, N.; Rahmani, R.; Yang, H.; Pei, Y. A blockchain-assisted intelligent transportation system promoting data services with privacy protection. *Sensors* **2020**, *20*, 2483. [CrossRef]
5. Ali, M.; Karimipour, H.; Tariq, M. Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges. *Comput. Secur.* **2021**, *108*, 102355. [CrossRef]
6. Beenish, H.; Javid, T.; Fahad, M.; Siddiqui, A.A.; Ahmed, G.; Syed, H.J. A Novel Markov Model-Based Traffic Density Estimation Technique for Intelligent Transportation System. *Sensors* **2023**, *23*, 768. [CrossRef]
7. Chandio, A.A.; Tziritas, N.; Xu, C.Z. Big-data processing techniques and their challenges in transport domain. *ZTE Commun.* **2015**, *1*, 1–21.
8. Wang, Q.A.; Zhang, C.; Ma, Z.G.; Ni, Y.Q. Modelling and forecasting of SHM strain measurement for a large-scale suspension bridge during typhoon events using variational heteroscedastic Gaussian process. *Eng. Struct.* **2022**, *251*, 113554. [CrossRef]
9. Wang, Q.A.; Dai, Y.; Ma, Z.G.; Wang, J.F.; Lin, J.F.; Ni, Y.Q.; Ren, W.X.; Jiang, J.; Yang, X.; Yan, J.R. Towards high-precision data modeling of SHM measurements using an improved sparse Bayesian learning scheme with strong generalization ability. *Struct. Health Monit.* **2023**, 14759217231170316. [CrossRef]
10. Wang, Q.A.; Wang, C.B.; Ma, Z.G.; Chen, W.; Ni, Y.Q.; Wang, C.F.; Yan, B.G.; Guan, P.X. Bayesian dynamic linear model framework for structural health monitoring data forecasting and missing data imputation during typhoon events. *Struct. Health Monit.* **2022**, *21*, 2933–2950. [CrossRef]
11. Baker, T.; Asim, M.; Samwini, H.; Shamim, N.; Alani, M.M.; Buyya, R. A blockchain-based Fog-oriented lightweight framework for smart public vehicular transportation systems. *Comput. Netw.* **2022**, *203*, 108676. [CrossRef]
12. Medel, D.K.S.; Perez, B.A.M.; Alpaño, P.V.; Pedrasa, J.R. Mitigation of Data Integrity Attacks using Blockchain-based Intelligent Transportation System. In Proceedings of the 2021 26th IEEE Asia-Pacific Conference on Communications (APCC), Kuala Lumpur, Malaysia, 11–13 October 2021; pp. 13–18.
13. Maskey, S.R.; Badsha, S.; Sengupta, S.; Khalil, I. Bits: Blockchain-based intelligent transportation system with outlier detection for the smart city. In Proceedings of the 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Austin, TX, USA, 23–27 March 2020; pp. 1–6.
14. Das, D.; Banerjee, S.; Chatterjee, P.; Biswas, M.; Biswas, U.; Alnumay, W. Design and development of an intelligent transportation management system using blockchain and smart contracts. *Clust. Comput.* **2022**, *25*, 1899–1913. [CrossRef]
15. Fernandes, C.P.; Montez, C.; Adriano, D.D.; Boukerche, A.; Wangham, M.S. A blockchain-based reputation system for trusted VANET nodes. *Ad Hoc Netw.* **2023**, *140*, 103071. [CrossRef]
16. Cocîrlea, D.; Dobre, C.; Hîrţan, L.A.; Purnichescu-Purtan, R. Blockchain in intelligent transportation systems. *Electronics* **2020**, *9*, 1682. [CrossRef]
17. Zia, M. B-DRIVE: A blockchain-based distributed IoT network for smart urban transportation. *Blockchain Res. Appl.* **2021**, *2*, 100033. [CrossRef]
18. Das, D.; Dasgupta, K.; Biswas, U. A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems. *Comput. Electr. Eng.* **2023**, *105*, 108535. [CrossRef]
19. Kudva, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. A scalable blockchain-based trust management in VANET routing protocol. *J. Parallel Distrib. Comput.* **2021**, *152*, 144–156. [CrossRef]
20. Wang, Y.; Yu, J.; Yan, B.; Wang, G.; Shan, Z. BSV-PAGS: Blockchain-based special vehicles priority access guarantee scheme. *Comput. Commun.* **2020**, *161*, 28–40. [CrossRef]
21. Liu, T.; Sabrina, F.; Jang-Jaccard, J.; Xu, W.; Wei, Y. Artificial intelligence-enabled DDoS detection for blockchain-based smart transport systems. *Sensors* **2022**, *22*, 32. [CrossRef]
22. Akhter, A.S.; Ahmed, M.; Shah, A.S.; Anwar, A.; Zengin, A. A secured privacy-preserving multi-level blockchain framework for cluster-based VANET. *Sustainability* **2021**, *13*, 400. [CrossRef]
23. Chaudhary, B.; Singh, K. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3198–3212. [CrossRef]
24. Gazdar, T.; Alboqomi, O.; Munshi, A. A Decentralized Blockchain-Based Trust Management Framework for Vehicular Ad Hoc Networks. *Smart Cities* **2022**, *5*, 348–363. [CrossRef]
25. Alharthi, A.; Ni, Q.; Jiang, R. A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. *IEEE Access* **2021**, *9*, 87299–87309. [CrossRef]

26. Liu, X.; Zhao, M.; Wei, Z.; Lu, M. Economic Optimal Scheduling of Wind–Photovoltaic-Storage with Electric Vehicle Microgrid Based on Quantum Mayfly Algorithm. *Appl. Sci.* **2022**, *12*, 8778. [CrossRef]
27. Konduru, S.; Sathya, M. Remora optimization algorithm-based optimized node clustering technique for reliable data delivery in VANETs. *Int. J. Intell. Netw.* **2022**, *3*, 74–79. [CrossRef]
28. Cheng, X.; Huang, B. A center-based secure and stable clustering algorithm for VANETs on highways. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 8415234. [CrossRef]
29. Awan, K.A.; Din, I.U.; Almogren, A. A Blockchain-Assisted Trusted Clustering Mechanism for IoT-Enabled Smart Transportation System. *Sustainability* **2022**, *14*, 14889. [CrossRef]