electronics

Article

Privacy-Preserving Mobility Model and Optimization-Based Advanced Cluster Head Selection (P2O-ACH) for Vehicular Ad Hoc Networks

Nejood Faisal Abdulsattar [1], Dheyaa Abdulameer Mohammed [1], Ahmed Alkhayyat [2,3], Shemaha Z. Hamed [4], Hussein Muhi Hariz [5], Ali S. Abosinnee [6], Ali Hashim Abbas [1,*], Mustafa Hamid Hassan [1], Mohammed Ahmed Jubair [1], Fatima Hashim Abbas [7], Abeer D. Algarni [8], Naglaa F. Soliman [8,9] and Walid El-Shafai [10,11]

1 College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna 66002, Iraq
2 College of Technical Engineering, The Islamic University, Najaf 54001, Iraq
3 Department of Medical Instruments Engineering Techniques, Al-Turath University College, Baghdad 10021, Iraq
4 Department of Medical Instruments Engineering Techniques, Al-Farahidi University, Baghdad 10011, Iraq
5 Computer Engineering Department, Mazaya University College, Nasiriya 64001, Iraq
6 Altoosi University College, Najaf 54001, Iraq
7 Medical Laboratories Techniques Department, Al-Mustaqbal University College, Hillah 51001, Iraq
8 Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
9 Department of Electronics and Communications, Faculty of Engineering, Zagazig University, Zagazig 44519, Egypt
10 Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia
11 Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
* Correspondence: alsalamy1987@gmail.com

check for updates

Citation: Abdulsattar, N.F.; Mohammed, D.A.; Alkhayyat, A.; Hamed, S.Z.; Hariz, H.M.; Abosinnee, A.S.; Abbas, A.H.; Hassan, M.H.; Jubair, M.A.; Abbas, F.H.; et al. Privacy-Preserving Mobility Model and Optimization-Based Advanced Cluster Head Selection (P2O-ACH) for Vehicular Ad Hoc Networks. *Electronics* **2022**, *11*, 4163. https://doi.org/10.3390/electronics11244163

Academic Editors: Joseph Bamidele Awotunde, Ali Ahmed and Tarek Gaber

Received: 8 October 2022
Accepted: 25 November 2022
Published: 13 December 2022

Abstract: In vehicular ad hoc networks (VANETs), due to the fast-moving mobile nodes, the topology changes frequently. This dynamically changing topology produces congestion and instability. To overcome this issue, privacy-preserving optimization-based cluster head selection (P2O-ACH) is proposed. One of the major drawbacks analyzed in the earlier cluster-based VANETs is that it creates a maximum number of clusters for communication that leads to an increase in energy consumption which reflects in a degradation of the performance. In this paper, enhanced rider optimization algorithm (ROA)-based CH selection is performed and that optimally selects the CH so that effective clusters are created. By analyzing this, the behavior of the bypass rider's CH is chosen, and this forms the optimized clusters, and during the process of transmission, privacy-preserving mobility patterns are used to secure the network from all kinds of malfunctions which are performed by the new vehicle blending and migration process. The proposed P2O-ACH is simulated using NS-2, and for performance analysis, two scenarios are taken, which contain a varying number of vehicles and varying speeds. For a varying number of vehicles and speeds, the considered parameters are energy efficiency, energy consumption, network lifetime, packet delivery ratio, packet loss, network latency, network throughput, and routing overhead. From the results, it is understood that the proposed method performed better when compared with earlier work, such as GWO-CH, ACO-SCRS, and QMM-VANET.

Keywords: ROA optimization; CH selection; privacy-preserving; VANETs security; mobility model

1. Introduction

Vehicular ad hoc networks (VANETs) are a type of mobile ad hoc network (MANETs), and their main motivation is to control accidents and obtain better road safety. VANETs consist of intelligent vehicles to monitor and control the traffic of intelligent transportation systems, and they concentrate on issues such as accident control, congestion control, traffic patterns, and energy [1]. Here, for connectivity purposes, vehicles are equipped with the onboard unit (OBU). The types of communication in VANETs are vehicle-to-vehicle, vehicle-to-Internet, and vehicle-to-infrastructure [2]. VANETs' intelligent vehicles are highly talented at accessing new services to provide road safety [3]. Now, the Internet of Energy (IoE) is newly introduced to compete for the industrial application to satisfy the utilization of energy and demand [4]. For effective communication, delay, and scalability, the dangerous issues this creates cause most of the damage in the network. In this situation, intelligent clustering approaches were introduced into a process that plays a significant role in the vehicular communication system. Clustering represents a grouping of the network based on the similarity according to certain parameters, such as node distance, bandwidth, etc. A cluster is a group of members that selects one among the nodes as the cluster head (CH) and all other nodes are cluster members (CM) [5,6]. In a vehicular network, cooperative communication is a preferable choice. It examines the V2V links based on VANETs in depth; particularly because the vehicle-to-vehicle (V2V) connections have more difficult mobility contexts than vehicle-to-infrastructure (V2I). Dynamic nature is a crucial property of VANETs; dynamic topology commonly happens and that leads to unreliable communications. Clustering, in reality, makes network structures and communication more reliable, and an adaptable manner and stable power control (RPC) technique could produce higher outcomes even when the mobile channel fluctuates. The joint clustering and RPC techniques are critically based on these findings [7].

VANET categorization is recognized as a critical strategy for improving the network efficiency. It is linked to several different aspects. Stable clustering, for instance, has been evident through strong MAC scheduler efficiency, efficient routing, and, as a consequence, a durable and secure system [8]. There are many different types and classes of clustering in VANET. Both single-hop networks and multi-hop networks are differentiated based on their architecture [9]. In regard to systems, there are centered as well as distributed forms of the present network; there are highway vs. urban models; based on volume, there are dense vs. sparse concepts; and based on capability, there are high vs. slow speed concepts. Morphology statistics, such as the kind of vehicle, driver's goal of moving from one place to another, and so on, and movement knowledge, including direction, velocity, and acceleration, can all be utilized to cluster VANETs [10].

Clustering is scalable and stable network structures provide an easy way for effective communication. Vehicles inside the clusters are CH, CM, and gateway. CH acts as an access point to manage the traffic pattern of the cluster. All of the CM nodes will communicate with the CH, and then inter-cluster communication is initiated to reach the destination. Cluster-based routing improves the network capacity, which leads to efficient data delivery and utilization of bandwidth [11]. In certain protocols, parameter-based CH is initiated, which is based on distance, direction, and speed. Such processes increased the network overhead. Some clustering protocols concentrate on reducing malfunctions and vulnerabilities in the network [12–14]. Infrastructure-less vehicular communication and group communication is essential in providing effective communication. To improve the security of the network, new methods need to be introduced in VANETs [15–17]. However, due to the huge dynamic mobility of vehicles, these protocols become inefficient for VANETs. To overcome these drawbacks in this research, privacy-preserving optimization-based advanced CH selection (P2O-ACH) is proposed, which helps to reduce network congestion and instability. The two main sections of the protocol are enhanced rider optimization algorithm-based CH selection and privacy-preserving mobility patterns. By using these methods, the network stability is increased, which leads to effective communication in VANETs.

Contribution of the Research

- The purpose of the development of the proposed P20-ACH method is to improve the privacy and energy efficiency of the VANETs network by reducing energy consumption, delay, and routing overhead.
- Effective cluster heads are chosen using the advanced ROA-based CH selection process that results in improving network connectivity and stability that reflects in the reduction of energy consumption and delay in the network.
- To protect the vehicles from malicious activities in this paper, the privacy-preserving mobility model is introduced so that the vehicle behavior is monitored, which reflects in the increase of the trustworthiness of the network.
- Through this effective CH selection and privacy-preserving mobility model, the effectiveness of the network is highly increased, which reflects in the increase of the network lifetime.

The rest of the paper is organized into the following sections. The related works are discussed in Section 2. The system model with network model assumptions is elaborated on in Section 3. The proposed P20-ACH method is detailed in Section 4. The simulation results are evaluated in Section 5. Finally, in Section 6, the conclusion as well as the possible future directions are given.

2. Related Works

2.1. Clustering Associated Research

Clustering is utilized in a variety of communication networks [18] and VANET cluster analysis [19]. The clustering of VANETs is the emphasis of this research study. Some additional method uses density as the major parameter for several VANET clustering techniques. A strategy for clustering depending on density measure is presented in [20].

In [21], the idea is proposed of presenting two CHs in a single cluster, which are the main CH and secondary CH. The maximum weight is given to the main CH (PCH), which is calculated using parameters such as the average rate of speed between vehicles. To enhance cluster stability, the secondary CH will act as the backup to the PCH and assumes responsibilities when the PCH leaves the cluster. Presented in [22] is the double-head clustering (DHC) approach, which used new measures for channel access to improve cluster stability and efficiency. It analyzes the signal strength and the connection expiry time, in addition to the vehicle's velocity, orientation, and location (LET).

Presented in [23] is a clustering algorithm to reduce power consumption. To enhance the lifetime of the network cluster, head and load balancing are concentrated. Elective CH election with CH rotation is done. This method improves the throughput and lifetime of the network, but fails to achieve a high packet delivery ratio; hence, this is not suitable for a network with dynamically varying topology.

In [24], the author recommended a destination-aware context-based routing scheme to increase the packet delivery ratio and reduce network delay. This structure includes cluster formation, motor location, and speed of the vehicles. The cluster creation and CH selection are done with the help of the motor mobility and connection details, but this method fails to achieve high throughput.

In [25], the author suggests a novel clustering method to improve the throughput and packet delivery ratio of the VANETs. The proposed method combines the modified k-means algorithm and the maximum stable set problem. Effective cluster formation and CH selection are done through this method. However, this method produces more overhead and delays during the process of transmission.

Presented in [26] is a two-fold model for a stable CH election process, which consists of one or many kinds of communication with the hyper-graph spectral clustering method and cluster maintenance. This method greatly helps to increase the lifetime of the network and achieves moderate improvement in the throughput and delivery ratio. Furthermore, this produces high routing overhead and delay.

Suggested in [27] is a fuzzy logic-based cluster selection to improve the stability of the network. This method greatly improves the lifetime and efficiency of the network, but fails to achieve high throughput and packet delivery ratio.

Presented in [28] is a cluster-based routing protocol to improve the path length and data delivery ratio, as well as to reduce the average end-to-end delay. Here, a named data network technique is used in a hybrid communication model for dedicated short-range communication. However, this method produces more overhead and fails to achieve high throughput.

Introduced in [29] is a multi-channel clustering-based congestion control algorithm to significantly improve the network performance by minimizing the energy consumption in VANETs. It is one of the proactive infrastructure-based clustering approaches. Though this method's energy efficiency has increased, this type of approach is not suitable for a network with a huge dynamic mobility model.

2.2. Optimization-Associated Research

Suggested in [30] is a novel approach to improve the packet delivery ratio of the network called reliability aware multi-objective optimization using the enhanced Gaussian mutation harmony searching method. The core process of this method is Gaussian mutation, objective decomposition, and a harmony memory extraction algorithm. This method improves the packet delivery ratio and reduced the delay. However, the routing overhead is high.

Promoted in [31] is a two-hop routing algorithm to improve the throughput, delay, packet delivery ratio, packet loss rate, and communication overhead of the VANETs. This algorithm is based on multi-objective Harris Hawks optimization. Though this method achieves a better overall performance, this type of approach is not suitable for a network with a huge dynamic mobility model.

In [32], the author described the federated learning and blockchain to improve the trust and integrity of the network. This paper shows the current research challenges of the VANETs in terms of security and privacy perspectives.

Introduced in [33] is a method to improve the convergence speed of the network called the Hybrid Genetic Firefly Algorithm-based Routing Protocol. The essential feature of GA is combined with the Firefly Algorithm and it is applied in both the lightly populated and heavily populated areas. The performance is better in both scenarios, but it fails to achieve higher throughput.

Suggested in [34] is a reactive routing protocol called AODV with ant colony optimization (ACO) to improve the data transmission in VANETs during the process of communication. The multicasting approach is used for path establishment. Due to this method, the system achieves high throughput, low packet loss, and low end-to-end delay, but it produces more routing overhead during transmission.

Developed in [35] is a method to improve the packet delivery ratio and throughput of unmanned aerial vehicles (UAVs). Here, the particle swarm optimization algorithm is utilized for finding the optimal deployment of UAVs, which is based on vehicle density, heading direction, and previous coverage information. This method produces high routing overhead.

In [36], the instability is reduced, which is created by random topology in VANETs after the author introduced a grey wolf optimization-based clustering algorithm. In this concept, the cluster head is chosen according to the social behavior and hunting mechanism of grey wolves. This method produced a high packet delivery ratio with reduced energy consumption, but the network throughput is very low. The efficiency of the network is reduced with the increase of the throughput in the network.

Proposed in [37] is a street-centric routing scheme (SCRS) for the process of optimal path selection in the VANET network. Concepts such as multipath routing and ant colony optimization (ACO)-based clustering play a major role in improving the performance of the network. This method greatly reduces the computational cost and end-to-end delay, and produced more packet delivery ratio. However, the routing overhead is high and throughput is moderate.

In [38], the author proposed the concept called QMM-VANET, which is the quality of service (QoS)-based mobility management; it is the reliable and stable CH selection method with the trustier vehicle. Additionally, it concentrates on retransmitting the packets using gateways and gateway recovery algorithms. This method achieves a high packet delivery ratio and network stability. However, throughput is moderate. Table 1 shows the summary of previous related works.

Table 1. Summary of the Literature.

Ref. No	Method	Advantage	Disadvantage
[24]	Destination aware context-based routing scheme	Packet delivery ratio is high and network delay is low	Throughput is low
[25]	Modified *k*-means algorithm and maximum stable set problem	Packet delivery ratio is high and throughput is high	Overhead and delay is high
[26]	Hyper graph clustering model	Efficiency, throughput, and packet delivery ratio is high	Delay and routing overhead is high
[27]	Fuzzy and game theory-based clustering	Lifetime and efficiency are high	Throughput and packet delivery ratio is low
[28]	Cluster-based routing protocol	Packet delivery ratio is high and network delay is low	Overhead is more and throughput is low
[29]	Multi-channel clustering-based congestion control algorithm	Energy consumption is low and energy efficiency is high	Throughput is low
[30]	Reliability aware multi-objective optimization	Packet delivery ratio is high	Routing overhead is high
[31]	Multi-objective Harris Hawks optimization	Packet delivery ratio is high, throughput is high, and network delay is low	Not suitable for a network with huge dynamic mobility model
[32]	Cuckoo search optimization	Packet delivery ratio is high	Overhead is more and throughput is low
[33]	Hybrid Genetic Firefly Algorithm-based Routing Protocol	Convergence speed of the network is high	Throughput is low
[34]	AODV with ant colony optimization	Throughput is high, packet loss is low	Routing overhead is high
[35]	Particle swarm optimization algorithm	Packet delivery ratio is high and throughput is high	Overhead is more
[36]	A grey wolf optimization-based clustering algorithm	Throughput is high	Efficiency is low
[37]	Ant colony optimization (ACO)-based clustering	Computational cost and end-to-end delay are low	Routing overhead is high, throughput is moderate
[38]	Quality of service (QoS)-based mobility management	Packet delivery ratio and network stability is high	Throughput is moderate

After analyzing the earlier study, the major limitations which are present in the earlier research are improper mobility management in dynamic communication range, improper inter-vehicular link reliability, ineffective cluster formation, and lack of security. Due to these drawbacks, the effectiveness of VANETs' communication is highly affected, which leads to a reduction in the performance of the network.

So, there is a need to develop a new model which fulfills these criteria. Therefore, in our proposed work, the privacy-preserving mobility mode and optimization-based advanced cluster head selection are performed. ROA-based CH selection is done to improve efficiency and reduce the congestion and overhead in the network. The privacy-preserving mobility model is used to improve the accuracy of the network by enhancing security. A detailed elaboration of the proposed method is given below.

3. System Model

Due to the increase in population in urban areas, the enhancement of infrastructures with appropriate facilities becomes essential. Hence, IoT-based smart cities are introduced to meet the requirements of the city inhabitants. The required system model with a WSN embedded IoT network is constructed. At the initial stage, clusters are generated and it is improvised in Section 4. Generally, the network is subdivided into N clusters. Each cluster consists of one cluster head (CH) and N number of cluster members (CM). The sink node S_{node} is used to collect the data packets from the CHs from each cluster and then transmit that to the required end user. The core objectives, which are used for the selection of CH are residual energy, coverage area, latency, and network traffic. Thus, the CH node is only able to communicate with the S_{node} and the other nodes in the network. Hence, the selection of CH becomes a more complex process in an IoT network; we are using multiple objectives for the selection of CH in our proposed work. In Table 2 the symbols and descriptions used for the entire proposed work are given.

Table 2. Communication Model.

Symbols	Descriptions
CH	Cluster Head
NR_{energy}	Normalized Residual Energy
$OF^{velocity}$	Objective Function for Velocity
OF^{LC}	Objective Function for Coverage Area
$OF^{latency}$	Objective Function for Latency
RE	Residual Energy
IE	Initial Energy
A_{speed}	Average Speed
T_o	Transmission Time
S_{node}	Sink Node
AR	Anchor Node
E	Event
δ_{th}	Threshold Value of the Event
K	Probability Factor
BR	Bypass Rider
F	Follower
O	Overtaker
AT	Attacker

3.1. Network Model Assumptions

The nodes are static in nature as well as homogeneous. The residual energy allocated to each CM node is 0.5 Joules. The structure of the S_{node} is centralized. At the initial stage, all the nodes are localized randomly. Then, groups are divided and CH is chosen, which helps transfer the data packets to the S_{node} using a single or multi-hop communication model. The node with maximum residual energy is chosen as a CH for better performance. Mobility model selection is given in Table 3.

Table 3. Communication Model.

Communication Type	Communication Items	Model Type
Short-Distance Communication	Between CM and CH	Free Space Mobility Model
Long-Distance Communication	Between CH and S_{node}	Multi-Path Fading Model

3.2. Initial CH Selection

The major objective functions used for the selection process of the CH and CM are velocity, link capacity, latency, and residual energy of the node. The expression for the calculation of

$$RE_{CH-CM}^{energy} = \frac{\sum_{i=1}^{n} OF_{CH}^{energy}(rem) - OF_{CH}^{energy}(initial)}{\sum_{i=1}^{n} OF_{CM}^{energy}(rem) - OF_{CM}^{energy}(initial)} \tag{1}$$

where, $OF_{CH}^{energy}(rem)$ represents residual energy of the CH, $OF_{CH}^{energy}(initial)$ represents initial energy of CH, $OF_{CM}^{energy}(rem)$ represents remaining energy of the CM, $OF_{CM}^{energy}(initial)$ represents initial energy of CM.

$$OF_{CH}^{energy}(rem) - OF_{CH}^{energy}(initial) = \sum_{i=1}^{N} RE(CH_j) - \sum_{i=1}^{N} IE(CH_j) \tag{2}$$

$$OF_{CM}^{energy}(rem) - OF_{CM}^{energy}(initial) = \sum_{i=1}^{N} RE(CM_j) - \sum_{i=1}^{N} IE(CM_j) \tag{3}$$

where, N is the number of nodes inside the cluster, $RE(CH_j)$ represents the remaining energy of the CH inside the cluster, $IE(CH_j)$ represents the initial energy of the CH inside the cluster, $RE(CM_j)$ represents the remaining energy of the CMs inside the cluster, $IE(CM_j)$ represents the initial energy of the CMs inside the cluster,

Velocity calculation of the network is calculated according to the average speed of the network. For example, a vehicle moves at the speed of 72 km/h and 100 km/h. Hence, the average speed (A_{speed}) for the assumption is given below [38].

$$OF^{velocity} = A_{speed} = \frac{2 \times 72 \times 100}{(72 + 100)} = 66.27 \text{ (Km/h)} \tag{4}$$

In Equation (4) the numerical values 72 and 100 denote the varying speed of the vehicle. The link capacity is defined as the maximum throughput produced for each transmission. The mathematical expression for link capacity is given below.

$$OF^{LC} = \frac{S_{packets}}{(P_{ready} - P_{received})T_o} \tag{5}$$

where, $S_{packets}$ represents the packet size, P_{ready} represents the calculation of packets ready to transfer, $P_{received}$ represents the calculation of packets received, and T_o represents the time taken for the transmission.

Latency Calculation: The latency calculation of the nodes is calculated using Equation (6) by the ratio of the number of CH nodes in the network with the number of nodes in the network. The math expression for the calculation of latency is given below.

$$OF^{latency} = \frac{\sum_{i=1}^{M} L_{CH-CM}}{M} \tag{6}$$

where, M represents the transmission count among the CH and CM, L_{CH-CM} represents the latency produced during the process of communication between the CH and CM.

Using these parameters in weight, the node to become CH is measured. The expression for the calculation of a node to become CH is described.

$$WC_{N-CH} = \left(W_1 \times RE_{CH-CM}^{energy}\right) + \left(W_2 \times OF^{velocity}\right) + \left(W_3 \times OF^{LC}\right) + \left(W_4 \times OF^{latency}\right) \tag{7}$$

In Equation (7) the terms $W_1, W_2, W_3,$ and W_4 are the experimental constants. Using Equation (7), initially CH is chosen and the optimal CH is selected using the ROA-based CH selection process, which is elaborated on in the upcoming section.

4. Privacy-Preserving Optimization Based on Advanced CH Selection (P2O-ACH)

The privacy-preserving optimization-based advanced CH selection (P2O-ACH) method is designed to improve the overall performance of the network. The major category which affects the network performance is lack of security and increased energy utilization due to the usage of a huge number of devices in the network. The proposed P2O-ACH method is mainly designed to overcome these issues, such as security and energy utility. The proposed method is subdivided into two sections, namely ROA-based CH selection and the privacy-preserving mobility model. ROA is a rider optimization-based algorithm used for the optimization-based CH selection approach, which concentrates both the energy consumption reduction and reducing the congestion in the network. The privacy-preserving mobility model is used to provide security to the network mainly during the process of new member blending and leaving the cluster in the network. The diagrammatical representation of the proposed P2O-ACH method is given below in Figure 1.

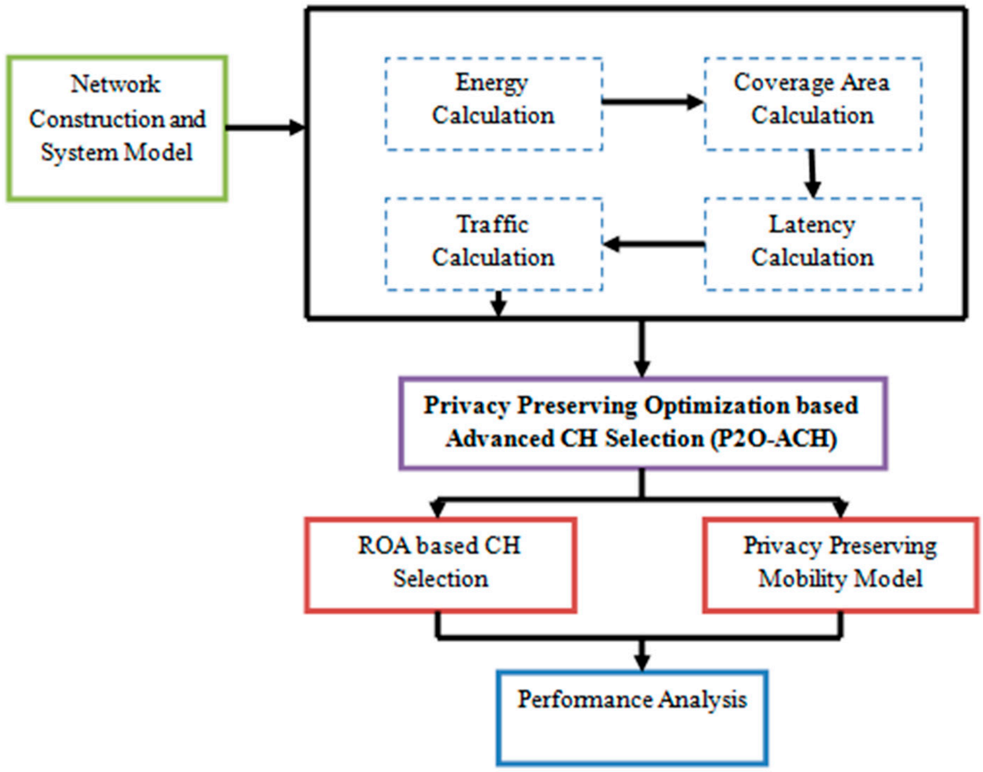

Figure 1. Architecture of the Proposed P2O-ACH Method.

The proposed P2O-ACH methods concentrated on improving both the energy efficiency and privacy of VANETs. For the purpose, the enhanced ROA-based CH selection and privacy-preserving mobility model are introduced. In the enhanced ROA algorithm, optimization issues are solved, and with the help of the principle of ROA the process of CH is performed so that the CH is highly optimal, which reflects in the reduction of energy consumption, delay, and overhead during communication. On the other hand, the privacy-preserving mobility model is employed, which provides security during the process of node joining and migration process. This is the proposed methodology which is done in this research.

4.1. Data Routing in Clustering

At the initial stage, the network is subdivided into several clusters that are headed by the CH. CH will collect the data packets from the CM nodes and transfer that to the SINK S_{node}. To reduce the delay and energy consumption, the data are fused and the volume is reduced. The core concept of clustering is data routing and data collection, and then forwarding that to that S_{node}. For the process of data routing, we are using a model called anchor-based routing. N number of anchors γ can be used for experimentation. In our research simulation, we used γ = 3. In the first segment, the S_{node} chooses the nearest node as an anchor and that is represented as AR_1, Then, S_{node} transmits the *DiscoverNearestNode* message to all the nodes in its coverage area. The nodes which are in that coverage area will receive the message and transmit an acknowledgement message with its ID and the residual energy at each instance of time. According to the signal strength, the best node is chosen by the S_{node}. The S_{node} transmits the *SINKRequest* message ($S_{node}, AR_1, E, \delta_{th}$); here, E is represented as the event and the δ_{th} is represented as the threshold value of the event.

AR_1 transmits the *EVENTRequest* message ($AR_1, E, \delta_{th}, H = 0$) in a flooding manner. The node which receives the transmitted message is represented as N_j for the first time and then the hop count is incremented by 1. That node that transmits the message is denoted as the parent node P. Then, currently the packet format of the *EVENTRequest* message becomes (N_j, E, δ_{th}, H). Finally, the flow of the process becomes: the CM node transmits the event report to CH, from CH to AR_1 along with P and AR_1 to the S_{node} only in case the S_{node} is in the coverage area of the AR_1. If the S_{node} is not in the coverage area, then the new anchor node AR_2 is selected. Then, the new anchor request message will be transmitted by the S_{node} *LatestAnchorRequest* (S_{node}, AR_1). The node that receives the message becomes N_j, and transmits the latest message to the next hop called (S_{node}, AR_1, N_j). If this process is successful, then the node N_j becomes the next anchor with the reply message *LatestAnchorAck* (S_{node}, AR_1, N_j). Finally, the flow of the path becomes ($node \to CH \to AR_1 \to AR_2 \to S_{node}$). The same process will be continued to AR_3, if required.

4.2. Conventional ROA

Generally, rider optimization algorithm (ROA) is developed based on the concept of the riders being grouped to achieve the target. Here, bypass rider, follower, overtaker, and attacker are considered groups of riders. All the riders are arranged and then divided into groups according to this order. Each group produces their performance separately to achieve their goal. This algorithm pursues a sequential process in a step-by-step manner. At the initial stage, parameter initialization of riders and groups take place. In the ROA method, the determined groups are together represented as T and it randomly takes their position. Hence, the mathematical expression for the process of their group initialization is given below.

$$G^t = \{G^t(S_a, S_b)\}; 1 \leq S_a \leq NR_t; 1 \leq S_b \leq DI_t \tag{8}$$

In Equation (8), NR_t denotes the number of riders present in the race concerning time, DI_t denotes represents the dimension concerning time t. The position of the riders is denoted as $G^t(S_a, S_b)$. The notation represents the total number of riders such as bypass rider, follower, overtaker, as well as attacker are BR, F, O, and AT, where (T = BR + F + O + AT). The parameters that are considered are steering angle, acceleration, gear, as well as the brake, and they are installed in each group of riders. The mathematical expression for the calculation of steering angle (SA^t) is given below.

$$SA^t = \left\{SA^t_{S_a,S_b}\right\}; 1 \leq S_a \leq NR_t; 1 \leq S_b \leq DI_t \tag{9}$$

In Equation (9), the steering angle of the current rider is denoted as $SA^t_{S_a,S_b}$ and the beginning stage of the steering angle is shown in Equation (10).

$$SA^{t=0}_{S_a,S_b} = \begin{cases} \theta_a; & if\ S_b = 1 \\ SA^{t=0}_{S_a,S_b} = 1 + \alpha & if\ S_b \neq 1 \\ 0; & Otherwise \end{cases} \tag{10}$$

The angle of the current rider is represented as θ_a and the term α is the current rider position. To measure the success rate, the group leader is created. The leaders are centralized in nature and use the idea of an arbitrary search in all directions that reflects in the improvement of the success rate. The major parameter which is considered for the measure of the success rate is distance. The mathematical expression for the calculation of distance (CR_{dis}) is given below.

$$CR_{dis} = \frac{S_a + D_v}{S_a - D_v} \tag{11}$$

In Equation (11), S_a denoted the location of the current rider and D_v denotes the location of the destination. To increase the success, the rate of the process of leader identification is preceded. The major principle behind the process of leader selection is that the leader that is chosen has the minimum distance (high success rate) from the destination and the leaders are dynamic in nature, varying according to speed, position, and time. Now, the position update takes place according to the groups of riders. At the initial stage, the position update of the bypass rider is mathematically expressed below.

$$G_{t+1}^{BR_j}(S_a, S_b) = \gamma\big[G^t(\eta, S_b) \times \mu(S_b) + G^t(\epsilon, S_b) \times [1 - \mu(S_b)]\big] \tag{12}$$

In Equation (12), γ denotes an arbitrary number which lies between 0 and 1, η denotes a random value which ranges from 1 to T, ϵ a random value which ranges from 1 to T, μ represents an arbitrary value ranging between 0 and 1 of size $1 \times$ D. Secondly, the position update of the follower rider is mathematically expressed below.

$$G_{t+1}^{F}(S_a, S_b) = G^{L_{index}}(L_{index}, c) + \left[\cos\left(SA_{S_a,S_b}^{t=0}\right) \times G^{L_{index}}(L_{index}, c) \times d_{S_a}^t\right] \tag{13}$$

In Equation (13), $G^{L_{index}}$ denoted the leader location, L_{index} denoted the leader index, $SA_{S_a,S_b}^{t=0}$ denotes the current rider steering angle, and $d_{S_a}^t$ denotes the additional distance needed to cover the current rider. Thirdly, the position update of the overtaker rider is mathematically expressed below.

$$G_{t+1}^{O}(S_a, S_c) = G_t(S_a, S_c) + [Y_t^I(S_a) * G^{L_{index}}(L_{index}, S_c) \tag{14}$$

In Equation (14), $G_t(S_a, S_c)$ denotes the current rider location, and $Y_t^I(S_a)$ denotes the current rider direction. Finally, the position update of the attacker rider is mathematically expressed below.

$$G_{t+1}^{AT}(S_a, S_c) = G^{L_{index}}(L_{index}, S_b) + \left[\cos\left(SA_{S_a,S_b}^{t=0}\right) \times G^{L_{index}}(L_{index}, S_b)\right] + d_{S_a}^t \tag{15}$$

In Equation (15), $G^{L_{index}}(L_{index}, S_b)$ denotes the leader position, and $SA_{S_a,S_b}^{t=0}$ denoted the steering angle of the current rider. After the calculation of the group updates, the success rates are estimated among the riders. Based on those measurements, the newer positions and the leaders are chosen. To obtain improved performance, it is essential to update the steering angle and gear values. The process of leader selection is repeated according to the allocated time.

4.3. Enhanced ROA-Based CH Selection

In general, the ROA algorithm is used to solve complicated optimization issues. So, it is essential to improve the algorithm when it is applied to the dynamically varying VANETs. To improve the performance further, a trusted ROA is introduced. In general, ROA consist of four patterns, such as bypass, follower, overtaker, and attacker, which are chosen randomly to obtain the solution. Here, the pattern consists of an order to obtain better performance. Simultaneously, to protect the network from route request flooding, the selected patterns have to be encoded properly. Now, the patterns are processed in the order that is represented as $CH_{by}, CH_{fr}, CH_{ot}, CH_{at}$. Only this sequence will be repeated again and again. If any order changes occur, then we can identify if route request flooding happens.

So, detection and prevention of route request flooding are essential to finding the shortest path. To protect the network from this, an express trust model is initiated. The parameter which is considered for the express trust model is the rate of packet delivered, rate of packet loss, average latency, average energy, and integrity. The calculation of these parameters is given below.

Rate of packet delivered: Delivered packet rate is defined as the ratio of the total number of packets transmitted from the sender $TP_s(t)$ to the total number of packets accepted by the receiver $AP_r(t)$. The computation of delivered packets is given below.

$$DP_{rate}(t) = \frac{TP_s(t)}{AP_r(t)} \times 100 \tag{16}$$

Rate of packet loss: Loss of packet rate is defined as the ratio of the total number of packets accepted by the receiver to the total number of packets transmitted by the sender. The computation of packet loss is given below.

$$LP_{rate}(t) = \frac{AP_s(t)}{TP_r(t)} \times 100 \tag{17}$$

Average latency: Average latency is defined as the delay in time taken during the process of communication from the sender to the target. The latency can occur during route finding and request flooding. The computation of average latency is given below.

$$L_{average} = \frac{\sum_{i=1}^{N}(PT_i(time) - PA_i(time))}{TP_s(t)} \tag{18}$$

where, $PT_i(time)$ represents the packets transmitted time to the receiver and $PA_i(time)$ represents the packets allocated time by the sender to reach the receiver.

Average energy: The average energy remaining in the CH after the process of energy indulgence is computed below.

$$E_{average} = \frac{\sum_{j=1}^{CH^*} RE_j^{CH} - CE_j^{CH}}{IE_j^{CH}} \tag{19}$$

where, RE_j^{CH} represents the residual energy of CH_j and CE_j^{CH} represents the consumed energy of CH_j.

Integrity calculation: It is the final trust measure to improve trustworthiness. The trust values of CH and the CM are determined using the history that considers the normal joining, abnormal joining, normal leaving, and abnormal leaving of the neighbors, as well as the multiple distributions. Integrity is calculated according to the successful and unsuccessful transmission.

$$I_{CH-CM}(t) = \frac{1}{r}\,\frac{S_{CH-CM}(t)}{S_{CH-CM}(t) + US_{CH-CM}(t)} \tag{20}$$

where, r represents the node's overall neighbors, $S_{CH-CM}(t)$ represents the successful transmission, and $US_{CH-CM}(t)$ represents the unsuccessful transmission. These are the parameters calculated to protect the network from the route request flooding attack using an express trust-based ROA optimization approach. The process of ROA-based CH selection is described in a pseudo code in Algorithm 1.

Pseudo code for ROA-based CH selection:

Algorithm 1. ROA-based CH selection

Inputs—Rider inputs
Output—Optimal CH selection
Start
Step 1—For CH selection

- ROA rider's initialization—bypass rider, follower, overtaker, and attacker;
- ROA group initialization—$G^t = \{G^t(S_a, S_b)\}; 1 \le S_a \le NR_t; 1 \le S_b \le DI_t$;
- ROA steering angle of riders—$SA^t = \left\{SA^t_{S_a,S_b}\right\}; 1 \le S_a \le NR_t; 1 \le S_b \le DI_t$;
- Distance calculation for the current rider to reach the destination—$CR_{dis} = \frac{S_a + D_v}{S_a - D_v}$;

Step 2—Update the rider's positions

- Bypass rider position update—$G^{BR_j}_{t+1}(S_a, S_b) = \gamma\left[G^t(\eta, S_b) \times \mu(S_b) + G^t(\epsilon, S_b) \times [1 - \mu(S_b)]\right]$;
- Follower rider position update—$G^F_{t+1}(S_a, S_b) = G^{L_{index}}(L_{index}, c) + \left[\cos\left(SA^{t=0}_{S_a,S_b}\right) \times G^{L_{index}}(L_{index}, c) \times d^t_{S_a}\right]$;
- Overtaker rider position update—$G^O_{t+1}(S_a, S_c) = G_t(S_a, S_c) + [Y^I_t(S_a) \times G^{L_{index}}(L_{index}, S_c)$;
- Attacker rider position update—$G^{AT}_{t+1}(S_a, S_c) = G^{L_{index}}(L_{index}, S_b) + \left[\cos\left(SA^{t=0}_{S_a,S_b}\right) \times G^{L_{index}}(L_{index}, S_b)\right] + d^t_{S_a}$;

Step 3—Enhanced ROA-based CH selection—riders' pattern bypass, follower, overtaker, and attacker CH is chosen;

- CH pattern—$CH_{by}, CH_{fr}, CH_{ot}, CH_{at}$;

Step 4—Attack prevention—trust model initialization—packets delivered, rate of packets loss, average latency, average energy, and integrity;

- Calculation for packets delivered—$DP_{rate}(t) = \frac{TP_s\ (t)}{AP_r(t)} \times 100$;
- Calculation for rate of packet loss—$LP_{rate}(t) = \frac{AP_s\ (t)}{TP_r(t)} \times 100$;
- Calculation for average latency—$L_{average} = \frac{\sum_{i=1}^{N}(PT_i(time) - PA_i(time))}{TP_s\ (t)}$;
- Calculation for average energy—$E_{average} = \frac{\sum_{j=1}^{CH^*} RE^{CH}_j - CE^{CH}_j}{IE^{CH}_j}$;
- Calculation for integrity for a node to become CH—$I_{CH-CM}(t) = \frac{1}{r}\ \frac{S_{CH-CM}(t)}{S_{CH-CM}(t) + US_{CH-CM}(t)}$;

Step 5—Process is repeated until finding the best CH;
Step 6—Return
End.

4.4. Privacy-Preserving Mobility Model

A privacy-preserving mobility model is introduced here to secure the devices in the network. The major steps involved in this model are new node fusion and migration process. The process of new node fusion is defined as the frequent action taken to improve the computation and memory so as to reduce the transmission overhead of the network. The process of migration process is defined as for the active mobile node to endow with security during the process of joining the new code and migrating the node. The process of cluster creation and CH selection is done using a rider optimization-based CH selection approach. For the privacy-preserving mobility model, we concentrate on new node fusion and node migration.

4.4.1. New Node Fusion

Every node in the network is constructed with a chaotic map-based hash pin PIN_{hash} which helps to compute the secure key among the CH and the CM. In case the node N_j is interested in joining a cluster of CH_j, the joining process is described below. At the initial condition, the S_{node} is ready to transmit the PIN_{hash} into a new node to compute the hash key among the CH_j and the node N_j. Next, the N_j transmit the joining request message to the CH_j with its identification ID_{N_j}, time stamp TS_{N_j} with the PIN_{hash} code. After receiving the joining request message, the CH_j completely checks the message and then the network maintains its blocked node list. The CH_j checks whether the current ID is present in the blocked node list or not, then the CH_j asks the S_{node} to transmit the PIN_{hash} code. The PIN code request message $PINCode_{REQ}$ is encrypted with the help of the symmetric of the S_{node} as well as the CH_j. The encrypted message consists of the ID_{N_j} details and PIN_{hash} is retransmitted to the CH_j from the S_{node}. In this process, the CH_j computes the PIN'_{hash} and then checks that this pin is equal to the PIN_{hash} or not. The cluster head CH_j also transmits the key creation request message $KeyCreat_{REQ}$ to the node N_j. This request message maintains ID_j and n_{CH_j}.

After the process of this key creation, N_j transmits a reply message to CH_j, which is the encrypted acknowledgement including the newly created hash key and the new message contains $(ID_{N_j}$, nonce, $KeyCreat_{REP})$. If the nonce of the message is not a valid one, then the message is neglected and the node is block listed. Once the node N_j is added as a CM node of CH_j it transmits a join success encrypted data packet to the node N_j. After joining, the node N_j becomes the CM of the CH_j and then the CM node transmits the secure data to its destination through CH_j. By using the same method, the CH_j also transmits the data to the S_{node}.

4.4.2. Node Migration Process

As we know that the nodes used in our network are mobile in nature, during the process of communication they will migrate from one place to another. Due to this process at each instance of time anywhere in the network, new nodes joining and leaving the cluster will occur simultaneously. To secure this process of migration in the network, the concept of node migration is initiated. The core idea of this process is to provide both forward privacy as well as backward privacy in an effective way. In the above section, each node uses the authenticate key to join or leave a cluster and the presence and absence of the node in each cluster are periodically monitored by the CH_j with the help of transmitting the beacon signals. If any node is absent in the group, then automatically, CH_j neglects the node from its routing list. At the time of migration, the node N_j moves away from the coverage area of the CH_j as well as receives a request message from the neighbor CH. If the node in any cluster leaves the current cluster CH_j, then that node N_j tries to transmit a joining request message to any neighbor cluster CH_{new} with the transfer ID ID_j. Then, CH_{new} will accept the request of the node N_j. Then, the CH_{new} will check the neglect list. If the current node ID is not present in that list, then it will precede the process further. Otherwise, neglect the request. If the ID_j is not found, then the CH_{new} will send the key request message to the N_j. Continued on from that, the CH_{new} transmits the encrypted request message with the ID_j and time stamp. Then, the S_{node} sends the encrypted request message to the CH_{new}. Next, CH_{new} transmits the message to the N_j along with the encrypted key received from the S_{node}. Now, this message consists of the ID_j, nonce, as well as the transmitted request message.

Following this, the node N_j transmits the reply message to the CH_{new} in response to the transmitted request message. This reply also consists of the ID_j, nonce, and time stamp, and the message is encrypted. The time stamp and the worth of the nonce is checked by the CH_{new}. Once all the verification is done and after obtaining satisfaction, the CH_{new} node will accept the N_j node as its CM node. Finally, the CH_{new} node will update the finalized list to its S_{node}.

5. Results and Analysis

The major operations which are proposed in the P2O-ACH approach are ROA-based CH selection and the privacy-preserving mobility model. At the initial stage of simulation, the vehicles are distributed randomly. Then, CH selection parameters are measured using the Equations (1)–(7) and the optimal CH is chosen according to the process of the ROA algorithm from Equations (16)–(20). Following that, the mobility model is assigned according to the rekeying and mobility supervision process, which consists of vehicle blending and the vehicle migration process.

To calculate the performance of the network, we assess the parameters, which, concentrated in this research, are energy efficiency, energy consumption, network lifetime, packet delivery ratio, packet loss, network latency, network throughput, and routing overhead. For the process of performance comparison, our proposed P2O-ACH is compared with earlier works, such as GWO-CH [36], ACO-SCRS [37], and QMM-VANET [38]. The software used for the simulation experimentation is NS2.35 with frond-end OTCL and back-end C language on Ubuntu 16.04. OTCL is used for network construction, data transmission, and configuration. The initial energy allocated for the network is 1000 Joules, and the data transmission and reception energies are 0.005 Joules and 0.001 Joules, respectively. The network coverage area is 1500 $\times$ 1500 m. Eight clusters are deployed and the coverage area of each cluster is 500 m and the sensing range of the cluster head is 15 m. The network parameters [39–41] are listed in parameter Table 4.

Table 4. Simulation Parameters.

Parameters	Values
Simulator Version	NS-2.35
Simulation Time	200 ms
Simulation Coverage Area	1500 m $\times$ 1500 m
MAC Interface	MAC/802.11
Number of Vehicles	150 Vehicles
Cluster Radius	500 m
Transmission Range	150 m
Vehicle Speed Range	10 m/s to 35 m/s
Channel	Channel/Wireless
Radio Propagation Model	Two-Ray Propagation Model
Antenna Type	Omni-Directional Antenna
Queue Type	DropTail
Initial Power	1000 Joules
Transmission Power	0.005 Joules
Receiving Power	0.001 Joules
Data Packet Size	512 bytes
Agent Type	Transmission Control Protocol

5.1. Scenarios Details

For the performance analysis process, two scenarios are taken, which are according to the number of vehicles and speed of vehicles. The parameters, which are calculated according to the number of vehicles, are energy efficiency, energy consumption, network lifetime, packet delivery ratio, packet loss, network latency, network throughput, and routing overhead. The parameters, which are calculated according to the various speed of vehicles, are cluster head efficiency and cluster member efficiency. All the calculations are elaborated on below.

5.2. Performance Analysis Based on the Number of Vehicles

In Figure 2, the graphical representation of the energy efficiency calculation of the proposed P2O-ACH is given and it is compared with the earlier approaches. The major parameters, which are concentrated by the proposed P2O-ACH, are to reduce the energy consumption of the network using the enhanced ROA-based CH selection. During the simulation, it is greatly achieved and the energy efficiency of the proposed P2O-ACH is much better than others. Because of using the rider optimization-based CH selection process, an optimized stable CH is chosen that reduces the energy consumption of the network.

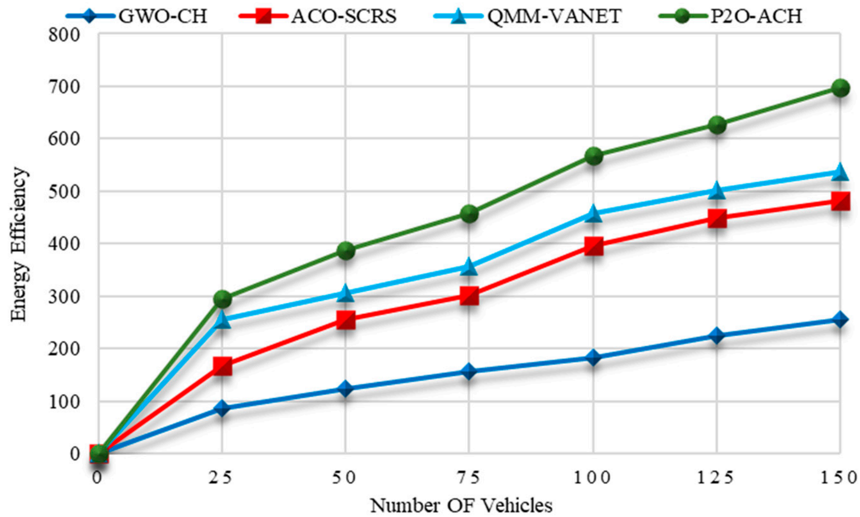

Figure 2. Energy Efficiency Calculation.

In Figure 3, the energy consumption of the network is shown. In Table 5 the simulation result values of energy efficiency and energy consumption are given.

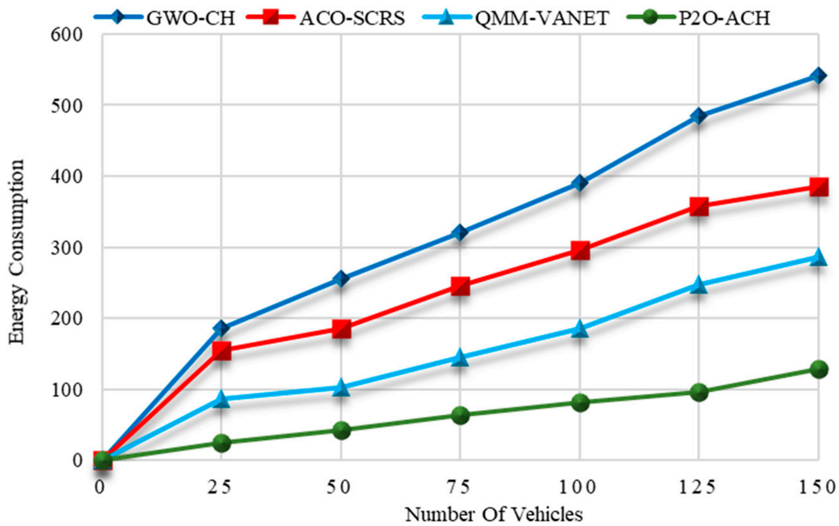

Figure 3. Energy Consumption Calculation.

Table 5. Performance Values of Energy Efficiency and Energy Consumption of the Network.

S. No	GWO-CH	ACO-SCRS	QMM-VANET	P2O-ACH
Energy Efficiency	357 Joules	598 Joules	657 Joules	864 Joules
Energy Consumption	658 Joules	486 Joules	358 Joules	157 Joules

The values stated in Table 5 prove that the efficiency achieved by the proposed P2O-ACH is better than earlier works where the efficiency of the P2O-ACH is 864 Joules and the efficiency of the GWO-CH, ACO-SCRS, and QMM-VANET is 357 Joules, 598 Joules, and 657 Joules, respectively. Then, the energy consumption of the proposed P2O-ACH is lower than earlier works where the consumption of the P2O-ACH is 157 Joules and the consumption of the GWO-CH, ACO-SCRS, and QMM-VANET is 658 Joules, 486 Joules, and 358 Joules, respectively. In the proposed P2O-ACH method, advanced CH selection is done using a rider optimization algorithm, especially to reduce the energy consumption of the network. The network becomes more stable with the help of this CH selection process.

In Figure 4, the pictorial representation of the calculation packet loss is shown where the performance of the proposed P2O-ACH is compared with the earlier approaches. With the use of the enhanced ROA method privacy-preserving mobility model, congestion of the network is reduced and security is improved, which leads to the reduction of the packet loss in the network. From the results, it is proven that the proposed P2O-ACH generates very low packet loss when compared with the others. In the proposed P2O-ACH method, the concept of a privacy-preserving mobility model is used that works on the fusion of nodes and the node migration process. In a maximum of the cases, the packet loss will occur during grouping and migration. This mobility pattern creates a stable grouping and migration; this leads to reducing the loss of packets in the network.

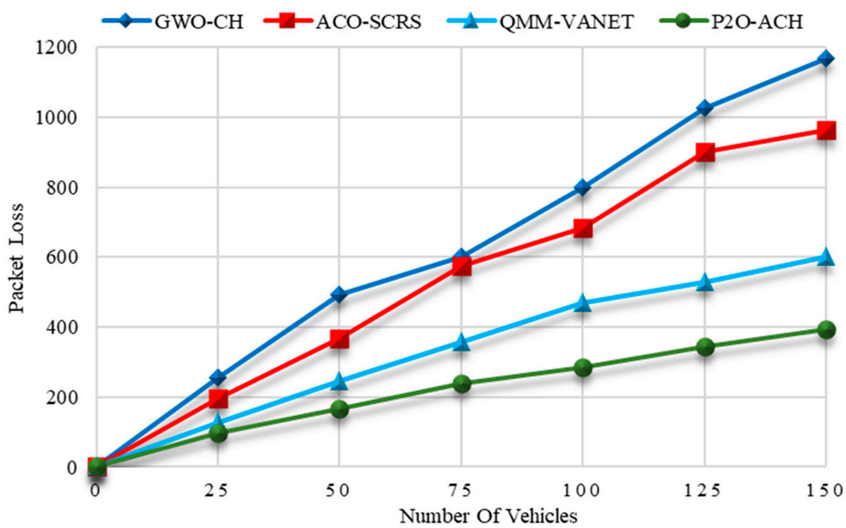

Figure 4. Packet Loss Calculation.

In Figure 5, the lifetime of the network is calculated. Hence, our method achieves high energy efficiency, which automatically reflects in the generation of a higher lifetime. This is achieved with the help of the stable and optimized cluster head selection process where energy consumption is reduced during the process of communication in the network, which increased efficiency and lifetime. In Table 6, the simulation result values of packet loss and network lifetime are given.

The values stated in Table 6 prove that the lifetime achieved by the proposed P2O-ACH is better than earlier works where the lifetime of the P2O-ACH is 97.46% and the lifetimes of the GWO-CH, ACO-SCRS, and QMM-VANET are 65.22%, 71.86%, and 85.47%, respectively. The proposed P2O-ACH method achieved around 10% to 30% more life time by using the rider optimization-based CH selection process. Hence, firmer and more effective CH is created, which helps communication with minimum utilization of energy. Then, the packet loss of the proposed P2O-ACH is lower than earlier works where the packet loss of the P2O-ACH is 458 packets and the packet losses of the GWO-CH, ACO-SCRS, and QMM-VANET are 1578 packets, 1248 packets, and 867 packets, respectively. The proposed method works with an effective mobility pattern where the grouping and migration of the vehicle are processed stably. This reduces the packet loss of the network, which amounts to 400 packets to 1000 packets lower than the earlier works.

From Figure 6, the graphical representation of the packet delivery ratio calculation of the proposed P2O-ACH is given and it is compared with the earlier approaches. The packet delivery ratio is one of the core parameters which decide the quality of the network.

The proposed P2O-ACH has a higher packet delivery ratio when compared with the earlier works. Lower packet loss reflects an increase in the packet delivery ratio of the network. In the proposed P2O-ACH method, the packet loss is very low using the mobility patterns that lead to improving the packet delivery ratio.

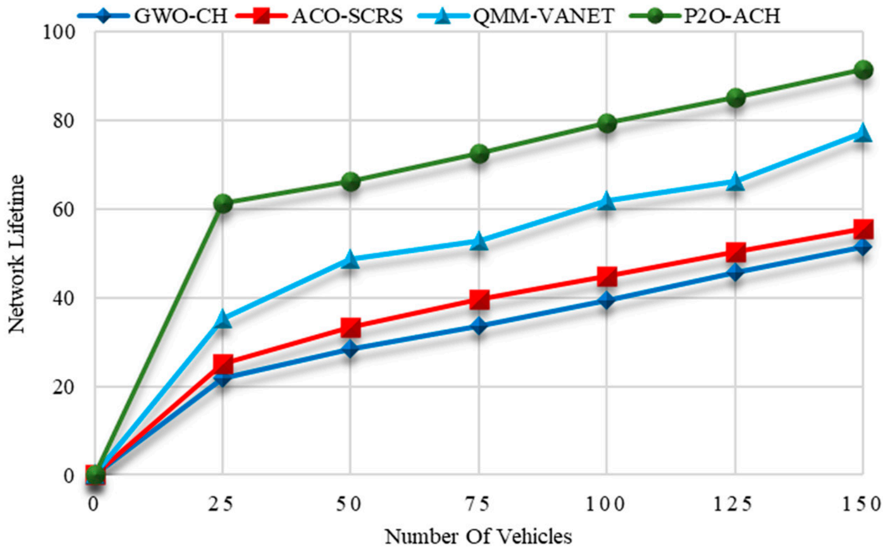

Figure 5. Network Lifetime Calculation.

Table 6. Performance Values of Packet Loss and Lifetime Calculation of the Network.

S. No	GWO-CH	ACO-SCRS	QMM-VANET	P2O-ACH
Packet Loss	1578 Packets	1248 Packets	867 Packets	458 Packets
Network Lifetime	65.22%	71.86%	85.47%	97.46%

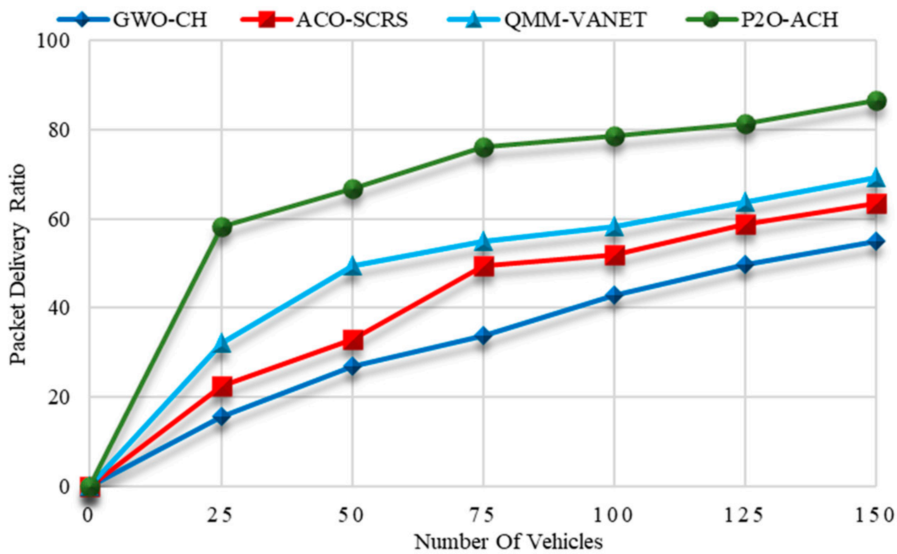

Figure 6. Packet Delivery Ratio Calculation.

In Figure 7, the latency is calculated, which is defined as the overall delay time of the network. In Table 7, the simulation result values of packet delivery ratio and latency are given.

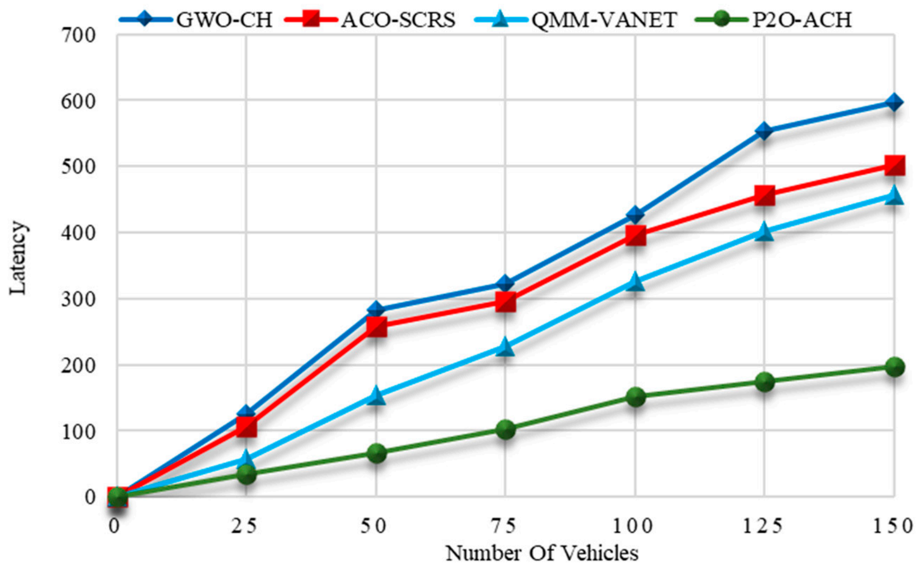

Figure 7. Latency Calculation.

Table 7. Performance Values of Packet Delivery Ratio and Latency Calculation of the Network.

S. No	GWO-CH	ACO-SCRS	QMM-VANET	P2O-ACH
Packet Delivery Ratio	75.12%	81.28%	89.46%	95.13%
Latency	681.92 ms	546.23 ms	502.48 ms	253.79 ms

The values stated in Table 7 prove that the packet delivery ratio achieved by the proposed P2O-ACH is better than earlier works where the packet delivery ratio of the P2O-ACH is 95.13% and the packet delivery ratios of the GWO-CH, ACO-SCRS, and QMM-VANET are 75.12%, 81.28%, and 89.46%, respectively. This is achieved because the privacy-preserving mobility pattern provides security during the process of vehicles joining and leaving the cluster, which reduces the loss of packets, and automatically increases the packet delivery ratio. Then, the latency of the proposed P2O-ACH is lower than earlier works where the latency of the P2O-ACH is 253.79 ms and the latencies of the GWO-CH, ACO-SCRS, and QMM-VANET are 681.92 ms, 546.23 ms, and 502.48 ms, respectively. The network is constructed stably so as to reduce the latency. Due to the advanced clustering method, the communication is highly standardized, which reduced the latency in the network. In Figure 8, the routing overhead is calculated and in the comparative graph the values of all the methods are shown. The main aim of the research is to reduce the energy consumption and overhead of the network. From the results, it is understood that the overhead produced by the proposed P2O-ACH is very much lower than that of the other works. This is because the privacy-preserving mobility pattern generation measures each action of the clusters, such as vehicle migration and fusion. Additionally, hash-based security is provided in it. So, the traffic pattern is secured and stable, which reflects in the overhead.

In Figure 9, network throughput is calculated and the throughput achieved by the proposed P2O-ACH is higher than the earlier works. The parameters, such as latency and overhead, are comparatively low in the proposed P2O-ACH method. That is the main reason to achieve high throughput in the network.

The values stated in Table 8 prove that the routing overhead achieved by the proposed P2O-ACH is low when compared with the earlier works where the overhead of the P2O-ACH is 2547 packets and the overheads of the GWO-CH, ACO-SCRS, and QMM-VANET are 7658 packets, 5967 packets, and 3467 packets, respectively. This performance is achieved mainly using the idea of CH selection that makes the network more reliable during the process of communication. Hence, VANETs are networks with huge mobility. The mobility pattern is properly scheduled so that the overhead should be low. Then, the throughput achieved by the proposed P2O-ACH is higher than earlier works where the throughput of the P2O-ACH is 1047.467 Kbps and the throughputs of the GWO-CH, ACO-SCRS, and QMM-VANET are 301.124 Kbps, 457.128 Kbps, and 857.845 Kbps, respectively. Lowering the network overhead increases the throughput of the network. In the proposed P2O-ACH method, around 1000 packets to 5000 packets are comparatively saved from overhead, which reflects in the increase of throughput from 200 Kbps to 500 Kbps.

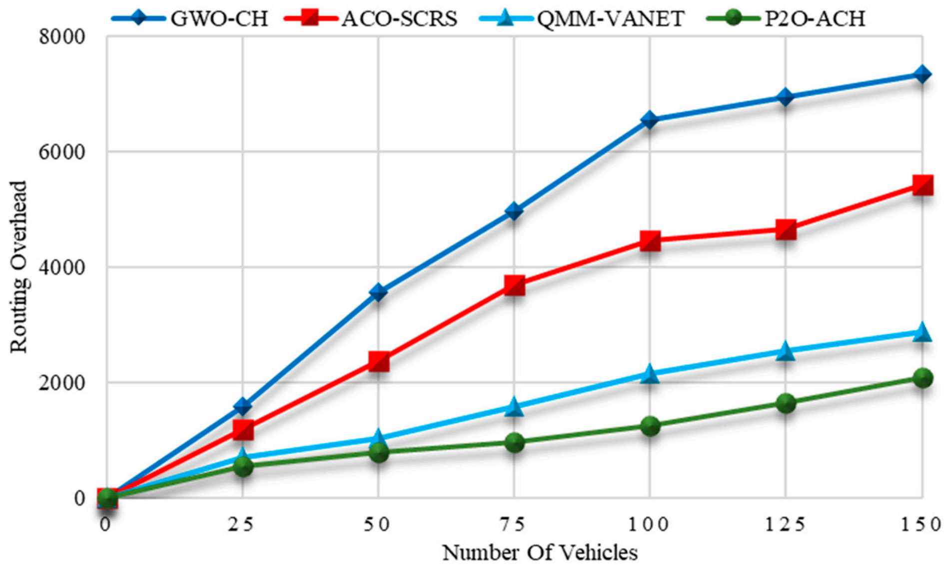

Figure 8. Routing Overhead Calculation.

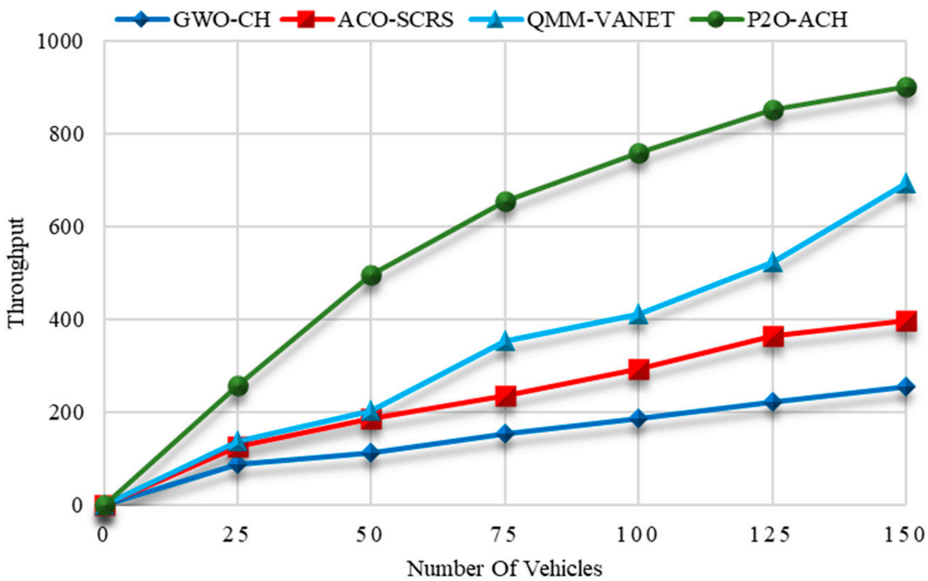

Figure 9. Network Throughput Calculation.

Table 8. Performance Values of Routing Overhead and Throughput Calculation of the Network.

S. No	GWO-CH	ACO-SCRS	QMM-VANET	P2O-ACH
Routing Overhead	7658 Packets	5967 Packets	3467 Packets	2547 Packets
Network Throughput	301.124 Kbps	457.128 Kbps	857.845 Kbps	1047.467 Kbps

Discussion Performance Analysis Based on the Number of Vehicles

The major conceptual concentration of the proposed P2O-ACH method is the creation of advanced CH selection with rider optimization algorithm and security-based privacy-preserving mobility pattern generation. Due to this, we can increase the efficiency, throughput, and packet delivery ratio, whilst likewise reducing the latency, overhead, and packet loss. Because the major drawbacks identified from the earlier works are, in the GWO-CH method, energy efficiency and the lifetime are moderate, in ACO-SCRS, the overhead is high and throughput is low, and in QMM-VANET the throughput is low. These are the major drawbacks of the earlier works.

The parameters that are used for performance analysis of the proposed research are energy efficiency, energy consumption, packet loss, network lifetime, packet delivery ratio, latency, routing overhead, and throughput. According to these parameters, the proposed P2O-ACH is compared with earlier works. Some of the common drawbacks which are identified in this earlier work are low throughput, low efficiency, high congestion, overhead, and delay. So to overcome these drawbacks in the proposed P2O-ACH, CH selection, optimization, and secured mobility models are constructed. Due to ROA optimization-based clustering in the proposed method, network efficiency reached up to 864 Joules, whereas the earlier work reached up to 650 Joules at maximum. The network energy consumption is reduced up to 157 Joules, whereas the earlier works range from 358 Joules to 658 Joules. By the use of ROA optimization, congestion is reduced, which reduced the packet loss and routing overhead of the network. The packet loss of the proposed P2O-ACH is 458 packets, whereas the earlier work ranged from 867 packets to 1578 packets. The routing overhead of the proposed P2O-ACH is 2547 packets, whereas the earlier work ranged from 3467 packets to 7658 packets. Similarly, by using the secured mobility model, the parameters which are improved are packet delivery ratio, throughput, and latency. The packet delivery ratio of the proposed P2O-ACH is 95.13%, whereas the earlier work ranges from 75.12% to 89.46%. The throughput achieved by the proposed P2O-ACH is 1047.467 Kbps, whereas the earlier work ranges from 301.124 Kbps to 857.845 Kbps. The latency produced by P2O-ACH is 253.79 ms, whereas the earlier work ranges from 502.48 ms to 681.92 ms. Finally, by analyzing all the parameters, it is understood that our proposed P2O-ACH outperforms the earlier methods in many cases.

5.3. Performance Analysis Based on Speed

In Figure 10, the graphical representation of energy efficiency calculation is performed. The results show that the proposed P2O-ACH outperforms when compared with the earlier works in terms of energy efficiency. It is achieved by using the optimization-based CH selection process.

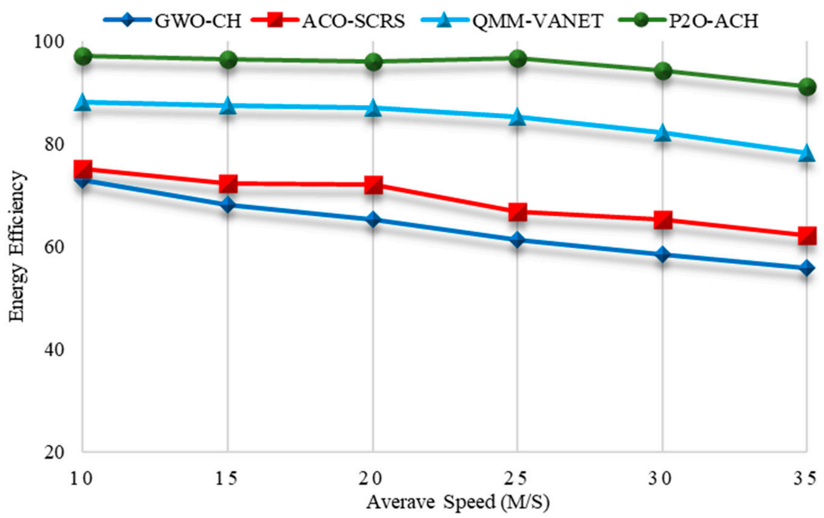

Figure 10. Energy Efficiency Calculation.

The consumption of energy is highly reduced using this method. This leads to an increase in the energy efficiency. The graphical representation for the calculation of energy consumption is shown in Figure 11, but according to speed variation, it is understood that an increase in speed reduces efficiency and increases the energy consumption of the network.

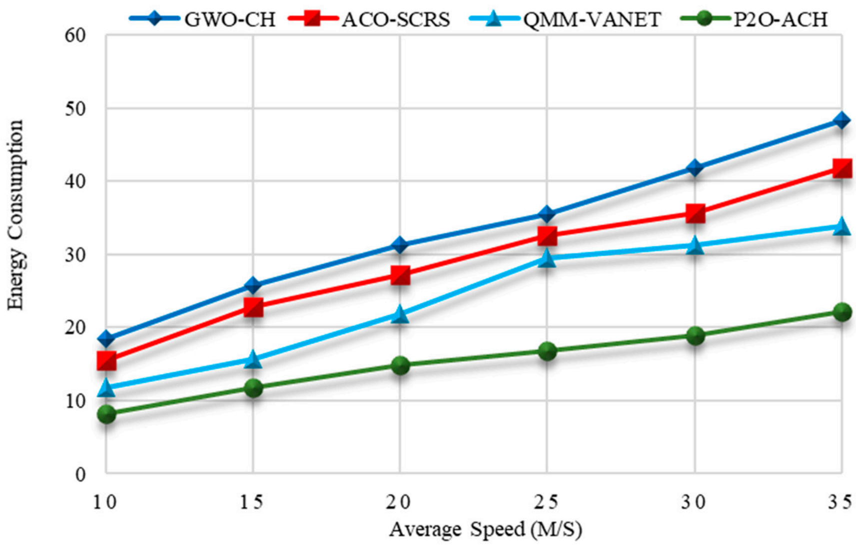

Figure 11. Energy Consumption Calculation.

In Figure 12, the packet loss is shown, where the performance of the proposed P2O-ACH is compared with the earlier approaches, such as GWO-CH, ACO-SCRS, and QMM-VANET. In the proposed P2O-ACH, congestion control is properly done, which helps to reduce packet loss compared to the earlier methods. Meanwhile, from the figure, it is understood that, according to the increase in speed, packet loss also increased.

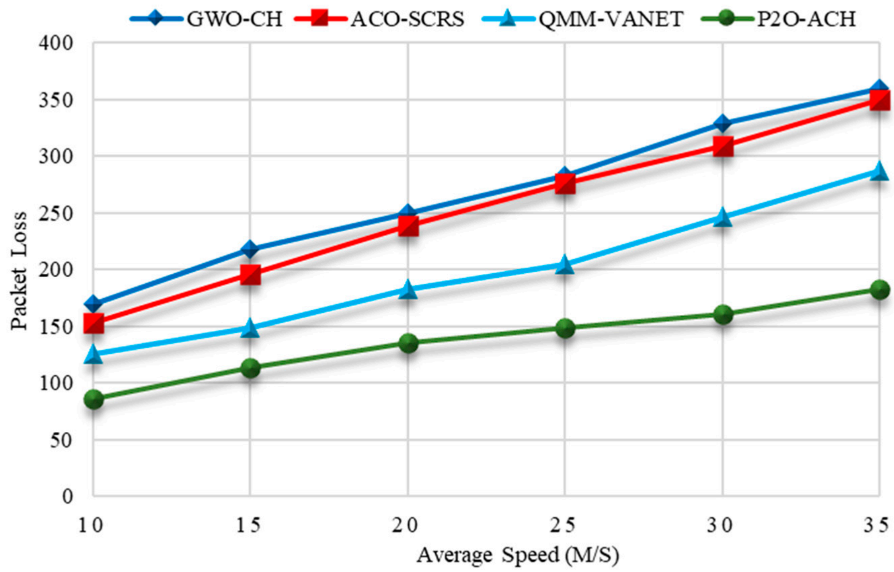

Figure 12. Packet Loss Calculation.

In Figure 13, the lifetime of the network is calculated. The network lifetime is high when compared with the earlier methods, such as GWO-CH, ACO-SCRS, and QMM-VANET; however, according to the increase in speed, the lifetime of the network is reduced.

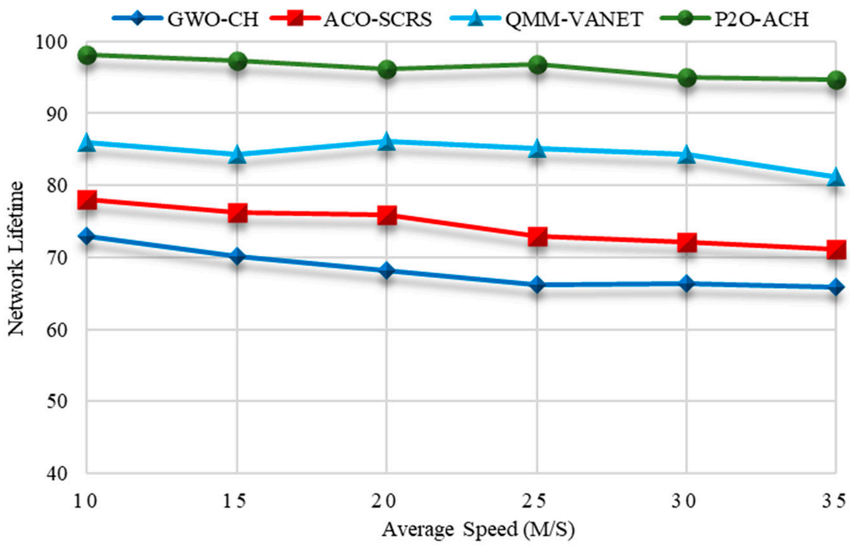

Figure 13. Network Lifetime Calculation.

In Figure 14, the graphical representation of the packet delivery ratio calculation of the proposed P2O-ACH is given and it is compared with the earlier approaches. The packet delivery ratio of the proposed P2O-ACH is high because, here, optimization-based CH selection is done and the privacy-preserving mobility pattern is initiated, which helps to increase the packet delivery ratio of the P2O-ACH compared to the earlier works, but due to the increase in speed, the packet delivery ratio is slightly reduced.

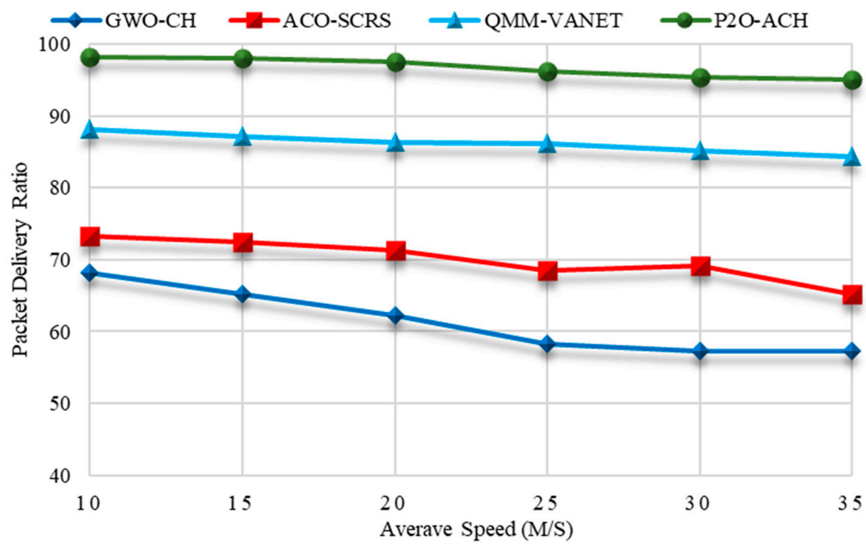

Figure 14. Packet Delivery Ratio Calculation.

In Figure 15, the latency of the proposed P2O-ACH is the calculation and it is compared with the earlier works. The proposed P2O-ACH is highly concerned with reducing the congestion in the network, which reflects in the reduction of latency when compared with the earlier works, but according to the increase of speed the latency is also increased.

In Figure 16, the routing overhead of the network is calculated. Hence, by using the enhanced ROA-based CH selection in the proposed P2O-ACH, energy consumption of the network is reduced, which reflects in the reduction of the routing overhead in the network. According to the varying speed, if the speed increases that will increase the overhead, comparatively.

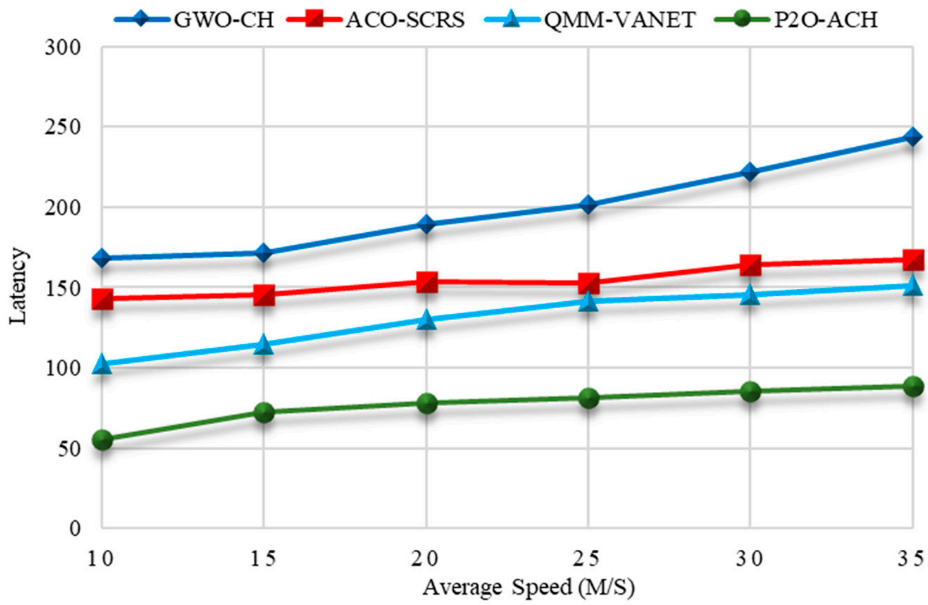

Figure 15. Latency Calculation.

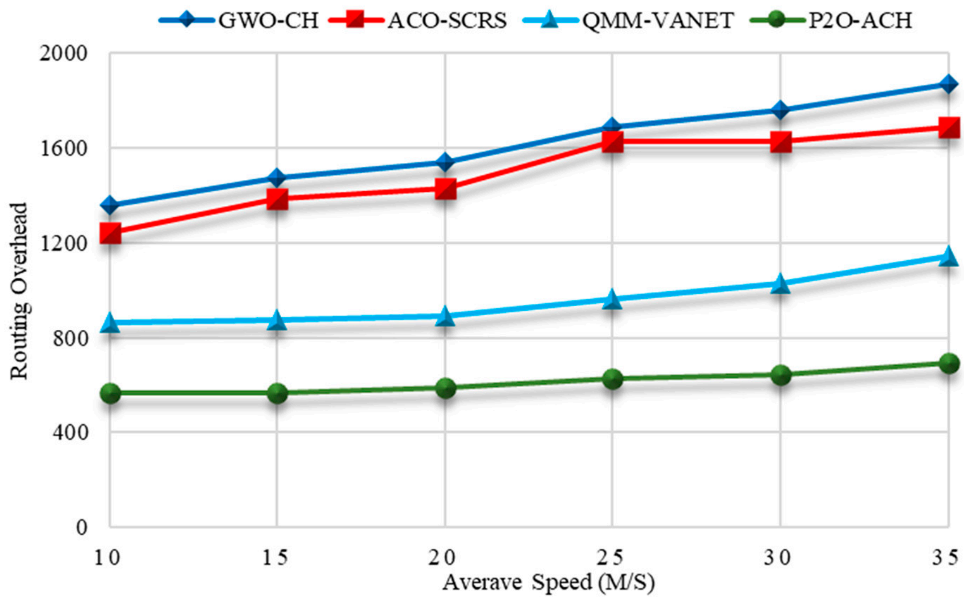

Figure 16. Routing Overhead Calculation.

In Figure 17, the throughput of the proposed P2O-ACH is calculated and then compared with the earlier works. The throughput performance of the proposed work is high when compared with the earlier works. According to the varying speed, the throughput of the proposed is maintained. That leads to an increase in the performance of the network.

Results Discussion

The parameters that are calculated according to the varying speed are energy efficiency, energy consumption, packet loss, network lifetime, packet delivery ratio, latency, routing overhead, and throughput. In Table 9, the performance analysis values of the parameters, such as energy efficiency, energy consumption, packet loss, and network lifetime, are given.

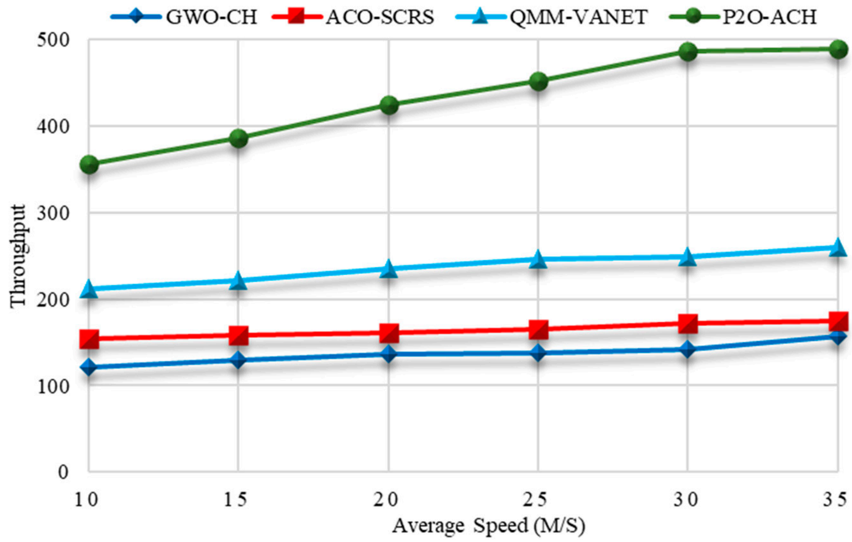

Figure 17. Network Throughput Calculation.

Table 9. Performance Analysis of Energy Efficiency, Energy Consumption, Packet Loss, and Network Lifetime in Terms of Varying Speed.

Parameters	Speed (m/s)	GWO-CH	ACO-SCRS	QMM-VANET	P2O-ACH
Energy Efficiency (%)	10	72.86	75.16	88.18	97.17
	15	68.17	72.18	87.35	96.35
	20	65.17	71.96	86.89	95.92
	25	61.23	66.86	85.27	96.75
	30	58.39	65.19	82.17	94.17
	35	55.84	62.11	78.16	91.17
Energy Consumption (%)	10	18.46	15.43	11.75	8.26
	15	25.79	22.76	15.63	11.76
	20	31.22	27.13	21.75	14.86
	25	35.46	32.49	29.43	16.78
	30	41.74	35.55	31.28	18.85
	35	48.32	41.76	33.86	22.17
Packet Loss (packets)	10	169	153	125	86
	15	218	196	149	113
	20	249	238	182	135
	25	283	276	205	148
	30	329	309	246	161
	35	359	350	287	182
Lifetime (%)	10	72.86	78.06	85.98	98.17
	15	70.17	76.18	84.31	97.25
	20	68.17	75.96	86.19	96.12
	25	66.23	72.86	85.07	96.85
	30	66.39	72.19	84.25	95.07
	35	65.84	71.11	81.25	94.65

The energy efficiency of the proposed P2O-ACH varies from 97% to 91%, whereas earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET, vary from 73% to 55%, 75% to 62%, and 88% to 78%, respectively. In terms of speed variation, the efficiency of the P2O-ACH is reduced by up to 6%, and the performance of the earlier work GWO-CH reduced by 18%; ACO-SCRS reduced by 13%; and QMM-VANET reduced by 10%. Finally, according to the analysis, it is understood that the overall energy efficiency performance of the proposed P2O-ACH is more improved than the others.

The energy consumption of the proposed P2O-ACH increases from 8% to 22%, whereas earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET, increase from 18% to 48%, 15% to 41%, and 11% to 33%, respectively. In terms of speed variation, the consumption of the P2O-ACH increased by up to 14%, and the performance of the earlier work GWO-CH increased by 30%; ACO-SCRS increased by 26%; and QMM-VANET increased by 20%. According to the analysis, it is understood that the overall energy consumption performance of the proposed P2O-ACH is reduced compared to the existing works.

The packet loss of the proposed P2O-ACH increases from 86 packets to 182 packets, whereas earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET, increase from 169 packets to 359 packets, 153 packets to 350 packets, and 125 packets to 287 packets, respectively. In terms of speed variation, the packet loss of the P2O-ACH is increased by up to 100 packets, and the performance of the earlier work GWO-CH increased by 250 packets; ACO-SCRS increased by 200 packets; and QMM-VANET increased by 150 packets. According to the analysis, it is understood that the overall packet loss performance of the proposed P2O-ACH is lesser than the other works.

The network lifetime of the proposed P2O-ACH varies from 98% to 94%, whereas earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET, vary from 72% to 65%, 78% to 71%, and 85% to 81%, respectively. In terms of speed variation, the lifetime of the P2O-ACH is reduced by up to 4%, and the performance of the earlier work GWO-CH is reduced by 7%; ACO-SCRS is reduced by 7%; and QMM-VANET is reduced by 5%. From the analysis, it is understood that the network lifetime of the proposed P2O-ACH is superior to the earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET. In Table 10, the performance analysis values of the parameters, such as packet delivery ratio, latency, routing overhead, and throughput, are given.

Table 10. Performance Analysis of Packet Delivery Ratio, Latency, Routing Overhead, and Throughput in Terms of Varying Speed.

Parameters	Speed (km/h)	GWO-CH	ACO-SCRS	QMM-VANET	P2O-ACH
Packet Delivery Ratio (%)	10	68.16	73.19	88.14	98.15
	15	65.17	72.45	87.16	98.01
	20	62.17	71.26	86.29	97.46
	25	58.29	68.46	86.11	96.17
	30	57.19	69.17	85.13	95.44
	35	57.24	65.24	84.25	95.02
Latency (ms)	10	168.2	142.7	102.41	55.13
	15	171.2	145.8	114.80	72.19
	20	189.2	153.2	129.76	78.14
	25	201.3	152.4	141.27	81.25
	30	221.5	164.2	145.76	85.76
	35	243.6	167.2	151.23	88.76
Overhead (packets)	10	1356	1243	865	568
	15	1475	1386	874	567
	20	1538	1427	892	586
	25	1689	1628	964	625
	30	1758	1625	1028	645
	35	1869	1689	1142	692
Throughput (Kbps)	10	121.3	153.4	212.45	356.2
	15	129.4	158.3	221.35	386.1
	20	136.2	161.2	235.27	425.1
	25	137.1	165.2	245.69	452.1
	30	141.8	171.4	249.38	486.2
	35	156.7	175.2	259.36	489.2

The packet delivery ratio of the proposed P2O-ACH is reduced from 98% to 95%, whereas earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET, are reduced from 68% to 57%, 73% to 65%, and 88% to 84%, respectively. In terms of speed variation, the packet delivery ratio of the P2O-ACH is reduced up to 3%, and the performance of the earlier work GWO-CH is reduced by 11%; ACO-SCRS is reduced by 8%; and QMM-VANET is reduced by 5%. From the analysis, it is stated that the packet delivery ratio performance of the proposed P2O-ACH is more improved than the others.

The latency of the proposed P2O-ACH increases from 55.13 ms to 88.76 ms, whereas earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET, increase from 168.24 ms to 243.68 ms, 142.71 ms to 167.28 ms, and 102.41 ms to 151.23 ms, respectively. In terms of speed variation, the latency of the P2O-ACH is increased up to 33 ms, and the performance of the earlier work GWO-CH is increased by 75 ms; ACO-SCRS is increased by 25 ms; and QMM-VANET is increased by 50 ms. According to the analysis, it is understood that the overall latency performance of the proposed P2O-ACH is lesser than the earlier works.

The routing overhead of the proposed P2O-ACH increases from 568 packets to 692 packets, whereas earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET, increase from 1356 packets to 1869 packets, 1243 packets to 1689 packets, and 865 packets to 1142 packets, respectively. In terms of speed variation, the routing overhead of the P2O-ACH is increased by up to 130 packets, and the performance of the earlier work GWO-CH is increased by 310 packets; ACO-SCRS is increased by 400 packets; and QMM-VANET is increased by 280 packets. From the analysis, it is proved that the routing overhead performance of the proposed P2O-ACH is lesser than the other works.

The throughput of the proposed P2O-ACH improved from 356 Kbps to 489 Kbps, whereas earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET, improved from 121 Kbps to 156 Kbps, 153 Kbps to 175 Kbps, and 212 Kbps to 259 Kbps, respectively. In terms of speed variation, the throughput of the P2O-ACH increased up to 150 Kbps, and the performance of the earlier work GWO-CH improved by 35 Kbps; ACO-SCRS improved by 30 Kbps; and QMM-VANET improved by 45 Kbps. From the analysis, it is stated that the throughput of the proposed P2O-ACH is more improved than the others. This detail's analysis in terms of both the number of vehicles and speed shows that the overall performance of the proposed P2O-ACH is better when compared with the earlier works, such as GWO-CH, ACO-SCRS, and QMM-VANET.

5.4. Algorithm Comparison

In the GWO-CH method [36], a grey wolf optimization algorithm-based clustering approach is proposed to solve the scalability issues in the VANETs. The social characteristics and hunting of the grey wolf are utilized to find the effective CHs in the network. Through this method, the energy consumption, delay, and routing overhead of the network fail to improve the packet delivery ratio and throughput of the network. Due to a lack of security, packet loss occurred in the network, which affects the effectiveness of the network. In the ACO-SCRS method [37], the ant colony optimization (ACO) algorithm is used to rely on the bus selection and effective clustering to improve the communication standard of VANETs. The model improves the energy efficiency of the network, but fails to reduce the data loss which happens due to the ground-level obstacles in the VANETs environment, which is reflected in the effective communication in the network. In the QMM-VANETs model [38], to improve the connectivity and network stability, an improved trust-based clustering algorithm is proposed so that trusted vehicles are introduced in the network, which leads to reduced packet loss, and the energy consumption is also reduced; however, this method consumes more energy when it reaches high speed with dynamic mobility. The major drawbacks, which are identified in the earlier approaches, are low density of vehicle, high packet loss due to ineffective security, and high delay and overhead. To solve these issues, in the proposed P2O-ACH approach, an efficient optimization with CH selection and the privacy-preserving mobility model is introduced, which concentrates on reducing the energy consumption and packet loss in an effective manner so that it directly improves the energy efficiency, packet delivery ratio, and network throughput.

In terms of algorithm, when compared with the grey wolf optimization and the ant colony optimization, our enhanced ROA optimization shows better performance in the parameters such as delay, overhead, and energy consumption. When compared with other

CH selection processes, our method is highly effective in achieving high energy efficiency. The whole the overall performance of the proposed P2O-ACH is better when compared with the earlier approaches, namely GWO-CH, ACO-SCRS, and QMM-VANET.

6. Conclusions

In this research, the major drawbacks to concentrate on are reducing energy consumption and improving security during the process of communication in VANETs. For this purpose, an efficient privacy-preserving mobility model and enhanced ROA-based CH selection are implemented, and they greatly improve the overall performance of the network by reducing energy consumption and congestion as well as improving the security of the network. Advanced CH selection is performed, which becomes a great solution for security and energy utility issues. By using an optimization-based CH selection process, the congestion is reduced. The enhanced ROA model solves the complication in the high-speed VANET network, which reflects in the trustworthiness of the network. Through the privacy-preserving mobility model, each data transmission at each instant of time is protected, and the data are free from the malfunction that occurred in the eternal environment. Results of the proposed P2O-ACH are found effective when compared with the GWO-CH, ACO-SCRS, and QMM-VANET. By the use of an enhanced ROA-based CH selection method, the energy consumption is reduced, which leads to improving energy efficiency and the lifetime of the network. The privacy-preserving mobility model provides security, especially during the process when the nodes leave the cluster during the process of communication and when the nodes try to join in the other cluster. Then, the routing list of all the clusters is securely updated to the SINK. From the simulation analysis, according to the number of vehicles, it is proven that our proposed P2O-ACH produced around 200 Joules with higher efficiency, 200 joules lower energy consumption, around 800 packets lower loss, around 2000 packets lower overhead, around 10% higher packet delivery ratio, and around 400 Kbps high throughput when compared with the earlier approaches, such as GWO-CH, ACO-SCRS, and QMM-VANET. According to the speed variation, the differences achieved are very low and normal. Our proposed research is highly beneficial to the community because it is a highly-cost effective method, which can achieve high energy efficiency and high security as well. For vehicular communication, the proposed method can provide an effective experience in communication. In future work, many scenarios will be introduced and the performance of the network will be analyzed using the proposed P2O-ACH method.

Author Contributions: Investigation, N.F.A. and N.F.S.; resources, D.A.M.; writing—original draft preparation, A.A. and S.Z.H.; methodology, H.M.H.; software, A.S.A.; supervision and writing—review and editing, A.H.A.; visualization, M.H.H.; visualization, M.A.J.; project administration, F.H.A.; formal analysis and funding acquisition, N.F.A. and A.D.A. and funding acquisition W.E.-S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ullah, A.; Yao, X.; Shaheen, S.; Ning, H. Advances in position based routing towards ITS enabled FoG-oriented VANET-A survey. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 828–840. [CrossRef]
2. Al-Mayouf, Y.R.B.; Mahdi, O.A.; Taha, N.A.; Abdullah, N.F.; Khan, S.; Alam, M. Accident management system based on vehicular network for an intelligent transportation system in urban environments. *J. Adv. Transp.* **2018**, *2018*, 6168981. [CrossRef]
3. Abizar; Farman, H.; Jan, B.; Khan, Z.; Koubaa, A. A smart energy-based source location privacy preservation model for Internet of Things-based vehicular ad hoc networks. *Trans. Emerg. Telecommun. Technol.* **2020**, *33*, e3973. [CrossRef]

4. Wei, L.; Wu, J.; Long, C.; Lin, Y.-B. The Convergence of IoE and Blockchain: Security Challenges. *IT Prof.* **2019**, *21*, 26–32. [CrossRef]
5. Abbas, A.H.; Habelalmateen, M.I.; Audah, L.; Alduais, N. A Novel Intelligent Cluster-Head (ICH) to Mitigate the Handover Problem of Clustering in VANETs. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 0100627. [CrossRef]
6. Abbas, A.H.; Mansour, H.S.; Al-Fatlawi, A.H. Self-Adaptive Efficient Dynamic Multi-Hop Clustering (SA-EDMC) Approach for Improving VANET's Performance. *Int. J. Interact. Mob. Technol.* **2022**, *16*, 136–151. [CrossRef]
7. Wang, H.; Liu, R.P.; Ni, W.; Chen, W.; Collings, I.B. VANET modeling and clustering design under practical traffic, channel and mobility conditions. *IEEE Trans. Commun.* **2015**, *63*, 870–881.
8. Oubabas, S.; Aoudjit, R.; Rodrigues, J.J.P.C.; Talbi, S. Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme. *Veh. Commun.* **2018**, *13*, 128–138. [CrossRef]
9. Zhang, D.; Ge, H.; Zhang, T.; Cui, Y.-Y.; Liu, X.; Mao, G. New Multi-Hop Clustering Algorithm for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 1517–1530. [CrossRef]
10. Tseng, H.-W.; Wu, R.-Y.; Lo, C.-W. A stable clustering algorithm using the traffic regularity of buses in urban VANET scenarios. *Wirel. Networks* **2019**, *26*, 2665–2679. [CrossRef]
11. Bylykbashi, K.; Elmazi, D.; Matsuo, K.; Ikeda, M.; Barolli, L. Effect of security and trust- worthiness for a fuzzy cluster management system in VANETs'. *Cogn. Syst. Res.* **2019**, *55*, 153–163. [CrossRef]
12. Touil, A.; Ghadi, F. Efficient dissemination based on passive approach and dynamic clustering for VANET. *Procedia Comput. Sci.* **2018**, *127*, 369–378. [CrossRef]
13. Khan, A.A.; Abolhasan, M.; Ni, W. An evolutionary game theoretic approach for stable and optimized clustering in VANETs. *IEEE Trans. Veh. Technol.* **2018**, *67*, 4501–4513. [CrossRef]
14. Otrok, H.; Mourad, A.; Robert, J.M.; Moati, N.; Sanadiki, H. A cluster-based model for QoS-OLSR protocol for urban vehicular ad hoc networks. In Proceedings of the 2011 7th International Wireless Communications and Mobile Computing Conference, Istanbul, Turkey, 4–8 July 2011; pp. 1099–1104.
15. Tan, H.; Zheng, W.; Vijayakumar, P.; Sakurai, K.; Kumar, N. An Efficient Vehicle-Assisted Aggregate Authentication Scheme for Infrastructure-Less Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2022**, 1–11. [CrossRef]
16. Tan, H.; Kim, P.; Chung, I. Practical Homomorphic Authentication In Cloud-Assisted Vanets With Blockchain-Based Healthcare Monitoring For Pandemic Control. *Electronics* **2022**, *9*, 1683. [CrossRef]
17. Xue, K.; Luo, X.; Ma, Y.; Li, J.; Liu, J.; Wei, D.S.L. A Distributed Authentication Scheme Based on Smart Contract for Roaming Service in Mobile Vehicular Networks. *IEEE Trans. Veh. Technol.* **2022**, *71*, 5284–5297. [CrossRef]
18. Alami, E.H.; Najid, A. ECH: An Enhanced Clustering Hierarchy Approach to Maximize Lifetime of Wireless Sensor Networks. *IEEE Access* **2019**, *7*, 107142–107153. [CrossRef]
19. Awan, K.A.; Din, I.U.; Almogren, A.; Guizani, M.; Khan, S. StabTrust-A Stable and Centralized Trust-Based Clustering Mechanism for IoT Enabled Vehicular Ad-Hoc Networks. *IEEE Access* **2020**, *8*, 21159–21177. [CrossRef]
20. Du, M.; Ding, S.; Xue, Y.; Shi, Z. A novel density peaks clustering with sensitivity of local density and density-adaptive metric. *Knowl. Inf. Syst.* **2018**, *59*, 285–309. [CrossRef]
21. Tambawal, A.B.; Noor, R.; Salleh, R.; Chembe, C.; Oche, M. Enhanced weight-based clustering algorithm to provide reliable delivery for VANET safety applications. *PLoS ONE* **2019**, *14*, e0214664. [CrossRef]
22. Alsuhli, G.H.; Khattab, A.; Fahmy, Y.A. Double-Head Clustering for Resilient VANETs. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 2917238. [CrossRef]
23. Behera, T.M.; Mohapatra, S.K.; Samal, U.C.; Khan, M.S.; Daneshmand, M.; Gandomi, A.H. Residual Energy-Based Cluster-Head Selection in WSNs for IoT Application. *IEEE Internet Things J.* **2019**, *6*, 5132–5139. [CrossRef]
24. Elira, B.; Keerthana, K.P.; Balaji, K. Clustering scheme and destination aware context based routing protocol for VANET. *Int. J. Intell. Netw.* **2021**, *2*, 148–155. [CrossRef]
25. Kandali, K.; Bennis, L.; Bennis, H. A New Hybrid Routing Protocol Using a Modified K-Means Clustering Algorithm and Continuous Hopfield Network for VANET. *IEEE Access* **2021**, *9*, 47169–47183. [CrossRef]
26. Jabbar, M.K.; Trabelsi, H. A Novelty of Hypergraph Clustering Model (HGCM) for Urban Scenario in VANET. *IEEE Access* **2022**, *10*, 66672–66693. [CrossRef]
27. Alsarhan, A.; Kilani, Y.; Al-Dubai, A.; Zomaya, A.Y.; Hussain, A. Novel Fuzzy and Game Theory Based Clustering and Decision Making for VANETs. *IEEE Trans. Veh. Technol.* **2019**, *69*, 1568–1581. [CrossRef]
28. Ardakani, S.P.; Kwong, C.F.; Kar, P.; Liu, Q.; Li, L. CNN: A Cluster-Based Named Data Routing for Vehicular Networks. *IEEE Access* **2021**, *9*, 159036–159047. [CrossRef]
29. Sewalkar, P.; Seitz, J. MC-COCO4V2P: Multi-Channel Clustering-Based Congestion Control for Vehicle-to-Pedestrian Communication. *IEEE Trans. Intell. Veh.* **2020**, *6*, 523–532. [CrossRef]
30. Rashid, S.A.; Alhartomi, M.; Audah, L.; Hamdi, M.M. Reliability-Aware Multi-Objective Optimization-Based Routing Protocol for VANETs Using Enhanced Gaussian Mutation Harmony Searching. *IEEE Access* **2022**, *10*, 26613–26627. [CrossRef]
31. Hossain, M.A.; Noor, R.M.; Yau, K.-L.A.; Azzuhri, S.R.; Z'Abar, M.R.; Ahmedy, I.; Jabbarpour, M.R. Multi-Objective Harris Hawks Optimization Algorithm Based 2-Hop Routing Algorithm for CR-VANET. *IEEE Access* **2021**, *9*, 58230–58242. [CrossRef]
32. Javed, A.R.; Hassan, M.A.; Shahzad, F.; Ahmed, W.; Singh, S.; Baker, T.; Gadekallu, T.R. Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey. *Sensors* **2022**, *22*, 4394. [CrossRef] [PubMed]

33. Singh, G.D.; Prateek, M.; Kumar, S.; Verma, M.; Singh, D.; Lee, H.-N. Hybrid Genetic Firefly Algorithm-Based Routing Protocol for VANETs. *IEEE Access* **2022**, *10*, 9142–9151. [CrossRef]
34. Sindhwani, M.; Singh, R.; Sachdeva, A.; Singh, C. Improvisation of optimization technique and AODV routing protocol in VANET. *Mater. Today: Proc.* **2021**, *49*, 3457–3461. [CrossRef]
35. Islam, M.; Khan, M.T.R.; Saad, M.M.; Tariq, M.A.; Kim, D. Dynamic positioning of UAVs to improve network coverage in VANETs. *Veh. Commun.* **2022**, *36*, 100498. [CrossRef]
36. Fahad, M.; Aadil, F.; Rehman, Z.; Khan, S.; Shah, P.A.; Muhammad, K.; Lloret, J.; Wang, H.; Lee, J.W.; Mehmood, I. Grey wolf optimization based clustering algorithm for vehicular ad-hoc networks. *Comput. Electr. Eng.* **2018**, *70*, 853–870. [CrossRef]
37. Khan, Z.; Fang, S.; Koubaa, A.; Fan, P.; Abbas, F.; Farman, H. Street-centric routing scheme using ant colony optimization-based clustering for bus-based vehicular ad-hoc network. *Comput. Electr. Eng.* **2020**, *86*, 106736. [CrossRef]
38. Fatemidokht, H.; Rafsanjani, M.K. QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks. *J. Syst. Softw.* **2020**, *165*, 110561. [CrossRef]
39. Alazab, M.; Lakshmanna, K.; Reddy, T.; Pham, Q.-V.; Maddikunta, P.K.R. Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities. *Sustain. Energy Technol. Assess.* **2021**, *43*, 100973. [CrossRef]
40. Sharef, B.; Alsaqour, R.; Alawi, M.; Abdelhaq, M.; Sundararajan, E. Robust and trust dynamic mobile gateway selection in heterogeneous VANET-UMTS network. *Veh. Commun.* **2018**, *12*, 75–87. [CrossRef]
41. Abbas, A.H.; Ahmed, A.J.; Rashid, S.A. A Cross-Layer Approach MAC/NET with Updated-GA (MNUG-CLA)-Based Routing Protocol for VANET Network. *World Electr. Veh. J.* **2022**, *13*, 87. [CrossRef]