IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 October 2022, accepted 13 November 2022, date of publication 24 November 2022, date of current version 2 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3224466

RESEARCH ARTICLE

A QoS Aware Cluster Head Selection and Hybrid Cryptography Routing Protocol for Enhancing Efficiency and Security of VANETs

MOHAMMED AHMED JUBAIR[1], SALAMA A. MOSTAFA[2], (Member, IEEE), DILOVAN ASAAD ZEBARI[3], HUSSEIN MUHEE HARIZ[4], NEJOOD FAISAL ABDULSATTAR[1], MUSTAFA HAMID HASSAN[1], ALI HASHIM ABBAS[1], FATIMA HASHIM ABBAS[5], AREEJ ALASIRY[6], AND M. TURKI-HADJ ALOUANE[6]

[1]Department of Computer Technical Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna 66002, Iraq
[2]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Johor 86400, Malaysia
[3]Department of Computer Science, College of Science, Nawroz University, Duhok, Kurdistan Region 42001, Iraq
[4]Department of Computer Technical Engineering, College of Information Technology, Mazaya University College, Dhi-Qar, Annasiriyah 64001, Iraq
[5]Medical Laboratories Techniques Department, Al-Mustaqbal University College, Hillah, Babil 51001, Iraq
[6]College of Computer Science, King Khalid University, Abha 62529, Saudi Arabia

Corresponding authors: Mohammed Ahmed Jubair (mohammed.a@sadiq.edu.iq) and Salama A. Mostafa (salama@uthm.edu.my)

This work was supported by the Deanship of Scientific Research at King Khalid University through General Research Project under Grant GRP/269/43.

ABSTRACT Nowadays, VANET (Vehicular Ad hoc Network) is one of the key aspects of developing advanced intelligent transportation systems. Due to its huge mobility and rapid topology alteration, the network exposes to link failure that affects the firmness of the network and causes delay and congestion. Additionally, the dynamic change in the network routing affects the network's security, making it vulnerable to various attacks, and results data loss. An efficient and highly secured routing protocol is needed to overcome these drawbacks. Subsequently, this research proposes a new routing protocol that combines the Quality of Service (QoS)-aware Cluster Head (CH) selection and hybrid cryptography named QoS+. The QoS+ protocol is mainly divided into QoS-based CH selection and hybrid cryptography modules. The CH selection module based on QoS parameters attempts to provide reliable and stable clusters and improve the firmness and connectivity during the communication process of the network. The hybrid cryptography module contains Advanced Encryption Standard (AES) and Elliptic Curve Cryptosystems (ECC) algorithms. It attempts to improve the security and privacy of the network. The QoS+ protocol is evaluated by a developed VANET simulator using NS2 software. The simulator consists of a network model, a load model, and an attack model. Various speed and transmission ranges and gray hole and wormhole attacks are used in the simulator. The outcome calculated from the performance analysis shows that the proposed QoS+ protocol has a 7% to 24% higher message success rate, 500 to 800 higher packets normalized routing load, 350 to 550 Kbps higher throughput, 5% to 17% higher efficiency, and 50ms to 12ms lower end-to-end delay when compared with the earlier works of ECHS and KMSUNET. The proposed QoS+ protocol also achieves superior performance in terms of CH efficiency, cluster member efficiency, and average cluster number with various speeds and transmission ranges.

INDEX TERMS Vehicular ad hoc network (VANET), quality of service (QoS), network security, cluster head (CH).

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

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) is the division of the mobile ad hoc network, mainly applied in the Intelligent Transmission System (ITS). To facilitate the communication process from one place to another, VANETs use wireless devices. The distinctiveness of the VANETs is huge and high-speed mobility, the most dynamically varying topology, and variable structures. The general types of VANETs are Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Later, Vehicle to- Roadside units (V2R) are included with it [1]. Additionally, VANET enables automobiles to interact with one another without the need for infrastructure. It has acquired popularity due to its security and cost efficiency.

Creating a routing system that can manage a high-mobility environment in VANET is still challenging. As a result of increased mobility and different topology, data might become outdated, raising concerns about disconnectedness and packet loss among vehicle nodes [2], [3], [4]. Most researchers introduced routing protocols to improve the security and traffic model in the VANETs. Nevertheless, this is an open research area, and we need improvement in the communication protocol of VANETs. Different types of software are presented to validate the communication protocols' performance. The most common conventional software is Network simulation and testing to authenticate the performance of various ad hoc communication protocols, as in [2].

Because of VANETs behavior, sustaining the firmness of the network becomes a challenging task. Its stability and communication are significant in enhancing the network's overall performance. The stability of the network can be achieved by controlling the factors such as location, direction, movements, connection, speed, and density. Clustering is one of the traditional models that help improve network stability [3]. This approach's core idea is to decrease energy consumption by creating clusters and selecting cluster heads and gateways [4]. On the other side, providing security to the network will improve its stability of it, and it also helps the network to protect itself from vulnerable attacks [5], [6], [7]. To address the mentioned defects in the network, in this paper, we introduced a new service (QoS)-aware cluster head (CH) selection and hybrid cryptography (QoS+) routing protocol to meet data transmission, energy, and security issues present in the network.

The QoS+ protocol encompasses two concepts to improve network routing: clustering and hybrid cryptography. The clustering technique aims to improve the network's energy, efficiency, and firmness of the VANETs, even with high-speed mobility and dynamically varying environment. Hybrid cryptography with the combination of Advanced Encryption Standard (AES) and Elliptic Curve Cryptosystems (ECC) algorithms aim to improve the confidentiality of the data in VANETs. The paper has three main contributions:

- Propose a new QoS+ routing protocol that combines the Quality of Service (QoS)-aware Cluster Head (CH) selection and hybrid cryptography. The fundamental cause of the proposed QoS+ routing protocol is to reduce the energy consumption, delay, loss of packets, and routing overhead of the network. In QoS+, malicious activities are detected and prevented using a hybrid cryptography algorithm.
- Integrating a hybrid cryptography module in the QoS+ routing protocol that contains Advanced Encryption Standards (AES) and Elliptic Curve Cryptosystems (ECC) algorithms. It attempts to improve the security and privacy of the network. The networks are exposed to different types of attacks, including black and gray hole attacks and wormhole attacks.
- Testing and evaluating the QoS+ protocol in a VANET environment with varying QoS metrics. The simulated VANET consists of normal, trusted, and malicious nodes. The QoS+ protocol can manage to classify the nodes and data transmission in such a way that ensures reducing the network's energy consumption and maintaining the network's security. The parameters that are concentrated for the process of results analyses are network throughput, message success ratio, normalized routing load, packet loss, energy efficiency, and energy consumption.

The rest of this paper is organized as follows. Section 2 presents the related works. Section 3 shows the construction model of the VANET network, including the system model, network model, load model, and attack model. Section 4 discuses the details analysis of the proposed routing protocol. In Section 5, VANETs simulation and evaluation results are analyzed. Finally we draw conclusions from our work in Section 6.

II. RELATED WORK

In [8], the author created a centralized and localized congestion control. This method greatly improves performance by measuring the parameters, such as network throughput, end-to-end delay, and packet loss ratio. However, energy and delivery ratio calculations are missing. In [9], the author introduced a Fuzzy-Based Cluster- Management System (FBCMS) to decrease energy consumption in VANETs. The network connectivity is concentrated mainly, and it shows better results. However, the other parameters are not shown.

In [10], the author created a novel approach, namely a centralized cluster-head deployed intrusion detection system (IDS), mainly used to reduce network packet loss during data transmission from source to destination. This method greatly helps to overcome the problem caused by the high mobility of vehicles. If we apply this method in a network with huge numbers of vehicles, the detection time taken is very high, which will increase the network delay. In [11], the author used Discriminant Analysis (DA) and Linear Discriminant Analysis (LDA) to secure the network from various kinds of attacks. Various machine learning methodologies are used in IDSs in VANET to protect the network from attacks [12]. The

TABLE 1. Merits and demerits of the earlier research works.

Author	Year	Proposed method	Merits	Demerits
Fatemidokht and Rafsanjani [22]	2020	Proposes QoS-based monitoring the malicious activity (QMM-VANET).	Outcome parameters are PDR, delay, and network stability.	Parameters such as throughput, overhead, control packets, energy efficiency, and consumption are not concentrated.
Alghamdi [23]	2018	CH selection and security using encryption	Outcome parameters are energy consumption, energy efficiency, delay, and packet loss.	Parameters like packet delivery ratio, network throughput, routing overhead, and hop count are not concentrated.
Paranjothi and Atiquzzaman [24]	2021	Fog–based Rogue Node Detection (F–RouND)	The parameters which are concentrated are delay, overhead and False–Positive Rate.	The major parameters such as energy consumption, energy efficiency, packet delivery ratio, and throughput and packet loss are not considered in this research.
Banikhalaf and Khder [25]	2020	Efficient Cluster Head Selection (ECHS)	It shows better results in terms of network lifetime, packet loss, overhead, and network delay. The simulation outcome shows better network lifetime, packet loss, overhead, and network delay results.	Major parameter such as packet delivery ratio, network throughput, and hop count is not concentrated.
Alaya and Sellami [26]	2021	Efficient Key Management Scheme (KMSUNET)	This method improves the packet delivery rate and energy efficiency.	The throughput proposed by the network is low that needs to be concentrated.

method used in the paper is clustered Self-Organized Map (SOM).

Similarly, in [13], the author introduced a newer model called a trust-aware model for both the operation, such as intrusion detection and protection. The results improved the network's overall performance with a small number of vehicles in it. It is not sure that the same results will be obtained when applying this model with a huge number of vehicles.

In [14], a game-theoretic-based incentive mechanism is proposed to process the idea of collaborative detection, which improves resource utilization. In [15], the perception of cluster-based mobility prediction is done in VANETs. Some research uses a clustering-based 3D channel model to extract multi-path components (MPC) to improve energy efficiency [16]. In [17], clustering-based detection algorithms are used to improve the network's quality of QoS. It helps to reduce the detection efficiency significantly, improving the overall energy efficiency of the VANETs.

In [18], the idea of a multi-hop clustering algorithm is proposed by the author to improve the reliability of the network. Likewise, several graph-based algorithms are introduced, such as a graph-based algorithm utilizing graph partitioning and graph theoretic algorithms using spatial reuse [19], [20], [21]. In [22], the author proposed a cluster-based routing protocol to improve the network QoS, called QoS-based Monitoring the Malicious activity (QMM-VANET). The protocol consists of cluster head (CH) selection, best neighbor selection, and gateway recovery algorithm. The simulation is done through NS2 in the highway scenario. The significant parameters concentrated for the outcome performance analysis are packet delivery ratio, delay, and network stability. However, parameters such as throughput, overhead, control packets, energy efficiency, and consumption are not considered. These are the major drawbacks of this research work.

In [23], the author introduced a new model to reduce congestion and increase network security. This method consists of the concepts like CH selection and security using encryption. The major parameters calculated in the research are energy consumption, energy efficiency, delay and packet loss. However, core parameters like packet delivery ratio, network throughput, routing overhead, and hop count are not concentrated. These are the drawbacks of this approach. In [24], the author developed a trust with cryptography model to improve the performance of the VANET network called Fog–based Rogue Node Detection (F–RouND), which is dynamic in nature. The parameters that were considered in this research are delay, overhead, and False–Positive Rate. However, the major drawback of this research is that major parameters such as energy consumption, energy efficiency, packet delivery ratio, and throughput and packet loss, were not taken into consideration. In [25], the author suggests that clustering is the best technique to improve the energy efficiency of the network. Therefore, in this research Efficient Cluster Head Selection (ECHS) method is proposed. In this work, a centralized clustering model is used. The simulation outcome shows better network lifetime, packet loss, overhead, and network delay results. However, parameters, such as packet delivery ratio, network throughput, and hop count, were not considered. The throughput and packet delivery ratio are the core parameters for the betterment of the network. Hence, as those parameters were not considered is a research drawback. In [26], the author proposed an Efficient Key Management Scheme (KMSUNET), an encryption method used to improve network security. This method greatly improves the packet delivery rate and energy efficiency. Nevertheless, network throughput proposed was low. Table 1 shows the merits and demerits of the earlier research works.

These are some of the earlier research work related to network energy efficiency and security. We summarized the main drawbacks of each work. Thereafter, in this work, we introduced QoS-aware CH selection and hybrid cryptography (QoS+) to improve performance in terms of network routing efficiency and security.

III. SYSTEM MODEL OF THE VEHICLE

The mechanism and models of the VANETs that are used in this study are illustrated here; They are network model, load model, and attack model.

A. NETWORK MODEL

In VANET network, the information is transmitted through vehicle communication. The major equipment of the vehicles is On Board the Unit (OBU), a Global Positioning System (GPS), and radar which are mainly used to distribute location, acceleration, momentum, and braking status to the nearest vehicle. The types of communication used here are V2V and V2I communication for multi-hop data transmission.

B. LOAD MODEL

The load model used in this study is Green shield's load flow [27]; here, the traffic mainly covers the urban and highways areas. This model is chosen because it is simple and enhance accuracy in real-time scenarios. The parameters used in the calculation are density (D) and speed of vehicles (V_{speed}). The expression is given to show the connection between speed and density.

$$V_{speed} \propto \frac{1}{D} \tag{1}$$

$$V_{speed} = C_{window} \frac{1}{D} \tag{2}$$

where C_{window} denotes the contention window value, which is based on the vehicle coverage area; here, speed is negatively correlated with density. So, if the density reaches its maximum at a certain point, the speed reaches zero at the same point, and vice versa. The point where density reaches its maximum is denoted by D_max, and the point where speed reaches its maximum is represented as S_max.

C. ATTACK MODEL

Various kinds of attacks are present in VANETs. This work mainly concentrates on gray-hole attacks and false information attacks.

1) GRAY HOLE ATTACK

During communication, specific processes will be done. These processes include: data forwarding, discarding, modifications of packets in the route, and eavesdropping. At this time, two or more malicious vehicles are created, and some malicious activities are created by sending packets with the help of a private transmission path to minimize the intermediate hops.

2) WORMHOLE ATTACK

During the process of this attack, two or more malicious vehicles are created from various positions, which join with one another and result in the formation of a private tunnel. During the execution of this attack, those malicious vehicles produce maximum RSSI value signals to influence other ordinary vehicles in their coverage area. Those vehicles are chosen on the optimal route toward the destination. Then, the data transmission is initiated, and the malicious vehicle transmits all the received information to another malicious vehicle on the opposite side of the tunnel.

IV. THE QoS+ ROUTING PROTOCOL

The main aim of this research is to improve the network's confidentiality and routing efficiency. In the earlier studies, due to attacks, the network privacy is compromised. Furthermore, due to the huge mobility in dynamically varying VANET networks, the routing efficiency of the network is reduced. This leads to a reduction in the overall performance of the network. In this study, a novel approach is developed to overcome these issues and mainly divided into two parts: QoS-aware CH selection and AES-ECC-based key generation. The overall workflow diagram of the proposed protocol is given below.

A. CLUSTERING IN ROUTING PROTOCOL

In this subsection, we initiate clustering protocol in VANET to optimize the process of CH selection. CH is chosen according to distance, threshold, velocity, density, and speed. Additionally, this protocol sustains the firmness and connectivity of the network. At first, this CH algorithm selects the trusted node as the CH. Then, CH selects a group of appropriate neighboring nodes as gateways, especially for retransmission and cluster connection. In the last stage, if any link failure occurs, the alternative gateways are selected by the gateway recovery algorithm. The geographical position of the network nodes is obtained by using GPS. Here, transmissions are omnidirectional. The vehicles are divided into three categories in the network: (1) Trusted vehicles: A vehicle that generates data in a trusted manner with normal behavior. (2) Normal Vehicles: These are common nodes in the network. (3) Malicious Vehicles: In case the unusual activities of the nodes are identified, the distrust value of the vehicle increases than its threshold value. Those nodes are termed malicious vehicles. The cluster head election algorithm is mainly used to elect the appropriate CH and divide the network into groups. It consists of four steps in the selection of required parameters.

- Step 1: Decide the number of neighbors for the vehicles using its neighbor table. That neighbor table consists of node location, speed, and density. The QoS value is a calculation using clustering and the QoS matrices. This calculation is carried out by using the neighbor table. The mathematical expression of the value of QoS is given below:

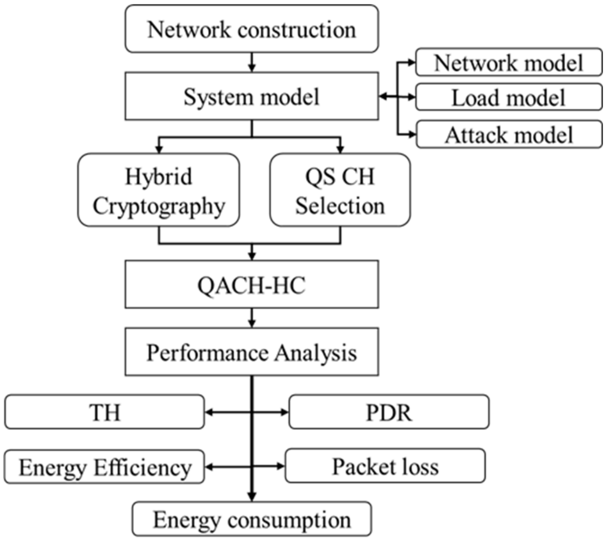


FIGURE 1. Work flow diagram of the QoS+ routing protocol.

$$QoS_{value} = (B_e \times S_{avg} \times \frac{D_{value}}{V_{value}})/T_v \qquad (3)$$

where B_e *and* N_v are the networks' existing bandwidth and average speed of the vehicles. D_{value} is the vehicle's distance ratio, and the term V_{value} is the vehicle's velocity ratio. And finally, T_v is the trust value of the vehicle. This trust value is the combination of the calculation of direct and indirect trust factors.

- Step 2: Data Communication models and rank-based CH selection are made to construct effective communication.
- Step 3: Speed and Density of the vehicle determination, mainly used to maintain the stability of the network.

1) QOS-BASED ROUTE SELECTION

In the process of the multi-path routing model after the election of CH based on the QoS, each CH will transmit the hello packets to its neighbors, which is in the coverage distance D_min. To preserve the neighbor details properly, each CH maintains the routing table. At the end of each transmission, the neighbor table gets updated. Figure 2 shows the significant blocks of the hello packet.

Source ID	Initial Power	Buffer	Link performance

FIGURE 2. Blocks of hello packets.

Link Stability: To select the next hop, link stability calculation is essential for the CH. The set of neighbors of the present cluster head CH_i is denoted as N_i. Link stability calculation includes power, link performance, and buffer factor. The link stability of the network is mathematically expressed below.

$$Link\ Stability = \{P_{initial,j} + B_{buffer,j} + LP_{ij}\} \qquad (4)$$

where, $P_{initial,j}$ is represented as the initial power of present neighbor CH_j, $B_{buffer,j}$ is represented as the current neighbor CH_j buffer size, LP_{ij} is represented as the present CH_i and the present CH_j link performances. The expression to calculate the LP_{ij} is given below:

$$LP_{ij} = \frac{SINR_{ij}}{D_{j\ to\ destination}} \qquad (5)$$

Here, $SINR_{ij}$ denotes the signal interference to noise ratio of the link among the present CH (CH_i) and the present CH neighbor (CH_j), and $D_{j\ to\ destination}$ denotes the travel distance between the present CH neighbor (CH_j) and the destination. To find the next hop, the math expression is given below:

$$Hop_{next} = Max\ \{Link\ Stability\} \qquad (6)$$

The stable link is found using these calculations, and the source CH transmits the route request packet (RREQ) to the next neighbor. In Figure 3, the blocks of the RREQ packet are given.

Sender ID	Receiver ID	Path ID	Link Stability	R_{time}	C_{delay}

FIGURE 3. Blocks of RREQ Packets.

In the figure, R_{time} refers to the packet received time, and C_{delay} represents the packet communication delay. Using this parameter, the end-to-end delay of each packet can easily be calculated. Control packets are reduced, automatically reducing the network overhead, which saves power. The node's trust value is calculated using direct and indirect trust. The direct trust calculation among any two nodes according to the process of predefined communication, which is nodes X and Y. The core metrics considered in this calculation are the total number of transmitted packets and time factor attenuation. The expression for direct trust is mathematically explained below:

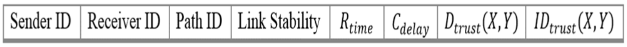
$$D_{trust}(X, Y) = \frac{\sum_{i=1}^{time} A^{t-i} Q^{i}_{XY}}{Q} \qquad (7)$$

where Q $= \sum_{i=1}^{time} A^{t-i}$, $A^{t-i} = (0 < A < 1)$, represents the time attenuation function, Q^{i}_{XY} represents the number of packets transmitted from node Y to X at each time instance. The number of transmitted packets and the trust value is directly proportional. If the transmitted packet counts increase, the trust value automatically increases. If nodes X and Y do not communicate, then $D_{trust}(X, Y)$ is set to default value 1.

In the process of trust evaluation of the node, the indirect trust factor calculation is also essential. The indirect trust factor and the nodes X and Y depend on past histories such as abnormal leaving, abnormal joining, normal leaving, and normal joining. The expression for indirect trust is mathematically explained below:

$$ID_{trust}(X, Y) = \frac{1}{f} \sum_{i=1}^{f} DT^{d}_{i}(d) \qquad (8)$$

where f is the overall count of neighbors present at the time duration. Finally, the route reply packet is transmitted by including the direct trust and indirect trust calculations. In Figure 4, the blocks of the RREP packet are given.



Sender ID	Receiver ID	Path ID	Link Stability	R_{time}	C_{delay}	$D_{trust}(X,Y)$	$ID_{trust}(X,Y)$

FIGURE 4. Blocks of rreq packets.

2) DATA COMMUNICATION MODEL

The data communication model is subdivided into two subsections. They are intra-cluster communication and inter-cluster communication. Both are described below:

- Intra Cluster Communication: At the time of the localization period, a normal node transmits the request message to its CH using D_min, which is the travel distance between the CH and the normal node. CH aggregates the collected data, and it is termed aggregated data.
- Inter-Cluster Communication: At the end of data aggregation, inter-cluster communication is initiated. During this period, the optimal path is selected, and the aggregated data gets transmitted to another CH or the Base Station (BS). Here the other CH represents the relay CH, which is selected based on the rank factor. The rank factor is determined using the initial power, signal strength, and the normal nodes inside the cluster. The rank factor is calculated based on the following equation. The CH, on its own, maintains a routing table to store all the transmission details. If the CH rank is high, then during the process of inter-cluster communication, it is highly possible to achieve better Quality of Service (QoS). In case the BS is out of the coverage area of the CH, then CH will select the neighbor CH with a higher rack factor to transmit the data to the BS. If multiple numbers of CH are present with a similarly high rank, then any CH can be chosen randomly by the present CH. The mathematical expression for the calculation rank factor is given below:

$$rank_{CH} = \frac{P_{initial}(CH_i)}{\rho \times n \times P_{max} \times |RSS\,(BS, CH_i)\,|} \tag{9}$$

where ρ is represented as the weight factor from (0,1), $P_{Initial}\,(CH_i)$ is represented as the present initial power of the CH_i, n is the count of normal alive nodes inside the cluster, P_{max} is the maximum initial power of the normal node, and $RSS\,(BS, CH_i)$ is represented as the signal strength between the BS and the CH.

3) SPEED AND DENSITY OF THE VEHICLE

The communication is done between the CH and the vehicles using the Green shield's traffic flow [27]. The CH measured individual vehicle densities using the acknowledgment message received from those vehicles. And the vehicle density is expressed below:

$$D = A_{data} \times N \times C_{window} \tag{10}$$

where A_{data} is represented as the acknowledgment data which gets broadcasted from the vehicle, N is defined as the sum of the vehicles present in the region, and C_{window} is the data transmission Variable Contention Window size.

In our network scenario, every single vehicle can do the process of transmission and reception of the data up to 400 m. Since the transmission window of each vehicle consisting of a CH vehicle is 800 m. Hence, we know that the vehicle's speed and density are negatively correlated. The correlation between the speed and density is mathematically expressed below:

$$S = S_{max} - \frac{D}{D_{max}} S_{max} \tag{11}$$

where S_{max} is represented as the vehicle speed at the time of density zero, D_{max} represents the vehicle density at the time of speed zero. To measure the significant speed variation in that collected beacon data, CH separates the vehicle, which transmits the relevant speed measures to the malicious vehicle, and the duration of the contention slot t_{slot} is added.

After recognizing the malicious node, the CH initiates the calculation of the average density D_{avg} and the average speed S_{avg} as so to do the hypothesis test.

$$D_{avg} = \frac{1}{N} \sum\nolimits_{i=1}^{N} D_{initial} t_{slot} \tag{12}$$

$$S_{avg} = \frac{1}{N} \sum\nolimits_{i=1}^{N} S_{initial} t_{slot} \tag{13}$$

Hypothesis testing is done to calculate the malicious activities of the vehicles. In the process of hypothesis testing, the average speed and the individual speed of the vehicle are compared with the data transmission variable Contention Window (C_window) size. Finally, the vehicle that matches the average speed is called the trusted node.

In our research, the hypothesis testing is done using the speed values of the entire network, which includes all the vehicles in it, where the CH node accepts the speed values with positive assurance and the Variable Contention Window (C_window) size of the vehicle. The hypothesis testing H_test is made using the null hypothesis. Suppose H_test is the speed and is acknowledged from the vehicle which maintains maximum speed and C_window. The other nodes are malicious. Here, error may occur only if the speed of the vehicle is low. For this purpose, the measurement of average speed with the received speed of the vehicle is done by calculating its standard deviation (σ). The mathematical expression for calculating the standard deviation (σ) is given below:

$$\sigma = \sqrt{\frac{1}{N} \sum\nolimits_{i=1}^{N} (S_{avg} - S_{initial}) C_{window}} \tag{14}$$

According to the average speed, the standard deviation will vary. The acceptance region's top and bottom limits are $S_{avg} \pm \sigma$. The vehicle with maximum acknowledged speed value from the trusted nodes fall on the acceptance region only if $((S_{avg} C_{window}) - \sigma) < S_{avg} < ((S_{avg} C_{window}) + \sigma)$. Also, the trusted node will reject the speed value outside

TABLE 2. Hypothesis testing (H_{test}).

Column heading	Column heading two	NULL HYPOTHESIS (H_n)
H_test	relative permeability	TRUE
Decision	energy density	$S_{avg}C_{window} = Max$
	demagnetizing factor	$S_{avg}C_{window} = Min$

the acceptance region. Table 2 presents hypothesis testing parameters.

B. HYBRID CRYPTOGRAPHY USING ECC-AES ALGORITHMS

Hybrid cryptography is used in the VANET network to secure the network, and it is based on the hash functions and the traditional cryptography model ECC and AES. The major phases of this security approach are setup initialization, registration, and AES encryption. The description of the process of those phases is given in detail.

Initialization Phase: After the network model selection of VANETs, the setup initialization process will be executed. The design steps are given below:

- Step 1: Every RSU controllers $C_kRSU(1 \leq k \leq n)PK_{private}$ and computes that with the equivalent public key where ($PK_{public} = PK_{private}$). Here, P is represented as a base point for the ECC algorithm, and $PK_{private}$ and PK_{public} are the private as well as the public key of the RSU controllers.
- Step 2: The network controller chooses the private key (CPK), which directs the computation of the public key ($CPUK$). Here, $CPUK = CPK.P$. Therefore, the CPK and $CPUK$ are the private and public keys of the network controller.
- Step 3: In the final stage, the C_kRSU and network controller announce the public data to all and maintain the private key most confidentially for the prospect's use.

Vehicle's registration phase: Any vehicle can register with any roadside unit using data like ID, Password, fingerprint, and biometric pattern. The procedure for the registration phase is given below:

- Step 1: At the starting point, the user I_{user} selects any person's data, user ID (I_{IDU}), password (I_{pass}), and biometric (I_{BIO}). Then, the user I_{user} computes the bio-hash value H(I_{BIO}), as well as submits data ($I_{IDU}I_{pass}$), H(I_{BIO})) to the roadside unit with the help of the secure channel.
- Step 2: In this stage, the $RSU_j(1 \leq j \leq m)$, random number selection is made which is X_j, and this is common to all the users. The computation details are given below.

$$A_j = h(I_{IDU}||I_{pass}) \tag{15}$$

$$A_j{}' = h(I_{IDU}||H(IBIO)) \tag{16}$$

$$B_j = h(I_{IDU}||X_j) \tag{17}$$

$$V_j = h(I_{IDU} + I_{pass}) \tag{18}$$

$$V_j{}' = h(I_{IDU} + H\ (I_{BIO})) \tag{19}$$

$$C_j = B_j + A_j \tag{20}$$

$$\sigma = \sqrt{\frac{1}{N}\sum\nolimits_{i=1}^{N}(S_{avg} - S_{initial})C_{window}} \tag{21}$$

- Step 3: In this stage, the system-based timestamp Tj is taken from the RSU_j and a random number R_j. This step leads to the computation of $TR_j = h(T_j||R_j)$. The default database, which is already present, is now verified by the RSU_j. If those are only one of a kind, then store the R_j and T_j against each I_{IDU} in the secured database.
- Step 4: At last, the RSU_j saves the data such as (V_j, $V_j^{`}$, C_j, C_j, 'TR_j, *and* $Secure_{oper}$) which are present inside the OBU and that are positioned in the user vehicle. This is the procedure for every vehicle in the registration phase.

AES Encryption: After the initialization and registration of the ECC key, it is used in the AES encryption process as the symmetric key. AES encryption method encrypts the ID with the help of the symmetric key. Where $S_{key} = PK_{public} \times PK_{private}$, ID = E($S_{key}$, ID). After the transmission process, it must match the decryption key successfully. Then, the CH measures the ECC key using the PK_{public} and $PK_{private}$. Additionally, the CH checks the MAC code. So the current input becomes $ID^{'} + PK^{'}_{public} + MAC$. Finally, in decryption, the ECC key is the symmetric key for the AES cryptography. Then the final ID becomes $ID{=}D(S_{key}, ID^{'})$.

V. SIMULATION ENVIRONMENT

In general, VANETs consist of a massive number of vehicles with complex topology [27]. Using the software named *NS2 network simulator*, the performance evaluation is carried out [28], [29]. To reach the reported results of the QoS+ protocol, we performed twenty runs for the simulation. The evaluation is represented in comparison with earlier works of Efficient Cluster Head Selection (ECHS) [25] and Efficient Key Management Scheme (KMSUNET) [26]. In NS2, we use SUMO and open street maps to generate mobility. The coverage area of the network is 1500m×1500m. The traffic exchange is done through constant bit rate (CBR) packets with a size of 512 bytes per packet. Table 3 shows the details of the parameters used for the process of simulation.

A. PERFORMANCE PARAMETER DEFINITION

For the process of simulation and result evaluation, the considered parameters are described below:

1) MESSAGE SUCCESS RATIO (MSR)

MSR is defined as the proportion of the messages reaching the receiver to the messages transmitted from the sender.

2) NORMALIZED ROUTING LOAD (NRL)

NRL represents the proportion of all the routing-based control messages transferred to all the vehicles to the number of messages received by the final vehicles.

TABLE 3. Simulation parameter.

Parameters	Values
Simulator Version	NS-2.35
Simulation Time	150 ms
Coverage Area	1500*1500 m2
Transmission Range	250 m
No of Vehicles	150
Standard	IEEE 802.11
Propagation Model	Two Ray Propagation Model
Antenna	Omni-directional Antenna
Traffic Type	Constant Bit Rate
Traffic rate	0.01 sec to 0.50 sec
Data Packet Size	512 bytes
Agent Type	Transmission Control Protocol
Routing Protocol	Ah-doc on-demand Vector
Initial Energy	100 J
Idle Energy	0.1 J
Simulator Version	NS-2.35

3) NETWORK THROUGHPUT (NT)

NT calculates the total number of data packets transmitted during the communication process in the entire network. The unit of throughput is Kbps.

4) NETWORK ENERGY EFFICIENCY (NEE)

NEE is defined as the remaining energy that is calculated at the end of the simulation process. The unit of energy efficiency is joules (J).

5) NETWORK ENERGY CONSUMPTION (NEC)

NEC is defined as the energy consumed for each transmission in the network. The unit of energy efficiency is joules (J).

6) END-TO-END DELAY (E2E)

The term E2E is denoted as that it is the average time taken for the process of transmission and reception of the data packets in the network. The unit of end-to-end delay is ms.

B. SIMULATION RESULTS AND ANALYSIS

Figure 5 presents the line graph of MSR calculation. Here, the proposed protocol is compared toECHS and KMSUNET. The X-axis represents the number of vehicles in the network, while Y-axis represents data success rate. From the graph, it is evident that the success rate of the proposed QoS+ protocol is higher than in earlier research works. Due to this, the QoS+ establishes a stable path between source and destination nodes.

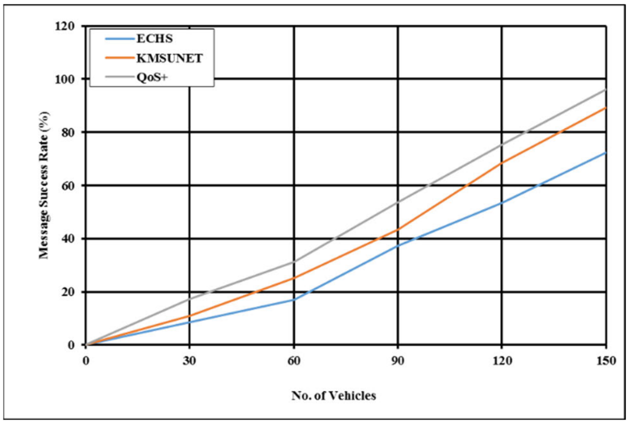


FIGURE 5. Message success rate calculation.

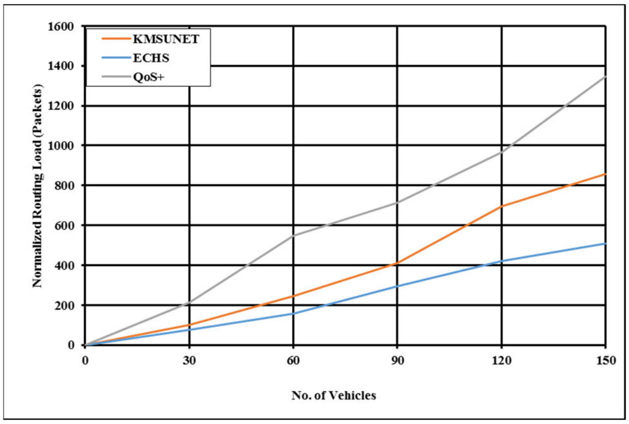


FIGURE 6. Normalized routing load calculation.

TABLE 4. Message success rate and NRL.

Parameters	ECHS	KMSUNET	QoS+
Message Success Rate	72.49 %	89.15 %	**96.14 %**
Normalized Routing Load	508 packets	857 packets	**1346 packets**

Figure 6 showcase the line graph of the normalized routing load calculation. Again, the proposed protocol is compared to ECHS and KMSUNET. From the graph, it is clear that the normalized routing load of the proposed QoS+ protocol is higher than earlier research works because the QoS+ protocol manages the network through dynamic and passive clustering integration. A dynamic cluster is used to team up the vehicles. One the other hand, passive clustering controls the transmission in the network. The normalized routing load values of the proposed method with earlier works are given in Table 4. In Table 4, of the values of message success rate and normalized routing load are shown.

Figure 7 depicts the throughput calculation. The proposed protocol is compared with earlier works such as ECHS and KMSUNET. From the figure, it is avident that the throughput of the proposed QoS+ protocol is higher than in earlier research works. The QoS+ protocol achieves better outcomes than other protocols due to the use of an efficient CH selection approach. This approach decreases the energy consumption and increases the cluster lifetime in the VANET environment. The throughput values of the proposed method with earlier works are given in Table 5.

Figure 8 illustrate the line graph of energy efficiency calculation. Once more, the proposed protocol is compared to ECHS and KMSUNET. The X-axis represents number of vehicles in the network, while the Y-axis represents the

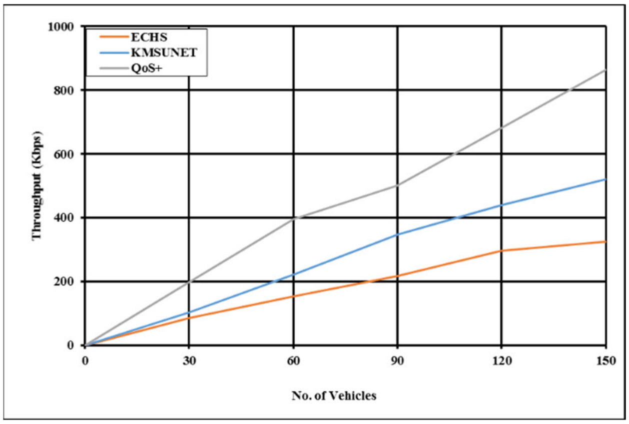


FIGURE 7. Network throughput.

TABLE 5. Network throughput and energy efficiency.

Parameters	ECHS	KMSUNET	QoS+
Throughput	325.17 Kbps	521.49 Kbps	**864.28 Kbps**
Energy Efficiency	60.25 %	72.45 %	**77.58 %**

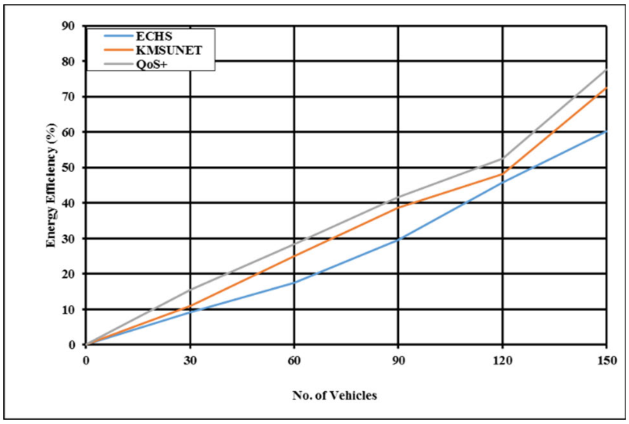


FIGURE 8. Energy efficiency.

network energy efficiency. As shown in the graph, i the energy efficiency of the proposed QoS+ protocol is higher than that of ECHS and KMSUNET. The energy efficiency values of the proposed method with earlier works are given in Table 5. In Table 5, both the values of throughput and efficiency are shown.

Figure 9 depicts energy consumption calculation for proposed protocol QoS+, as well as ECHS and KMSUNET. The X-axis represents the number of vehicles in the network, and the Y-axis represents network energy consumption. The graph shows that the consumed energy of the proposed QoS+ protocol is lower than the energy consumption of ECHS and KMSUNET. The energy consumption values of the proposed method with earlier works are in Table 6.

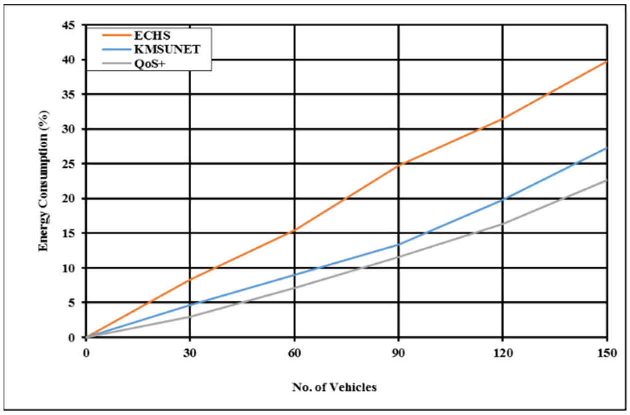


FIGURE 9. Energy consumption.

TABLE 6. Energy Consumption and end-to-end delay.

Parameters	ECHS	KMSUNET	QoS+
Energy Consumption	39.75 %	27.26 %	**22.64 %**
End-to-End Delay	234.168 ms	153.472 ms	**102.458 ms**

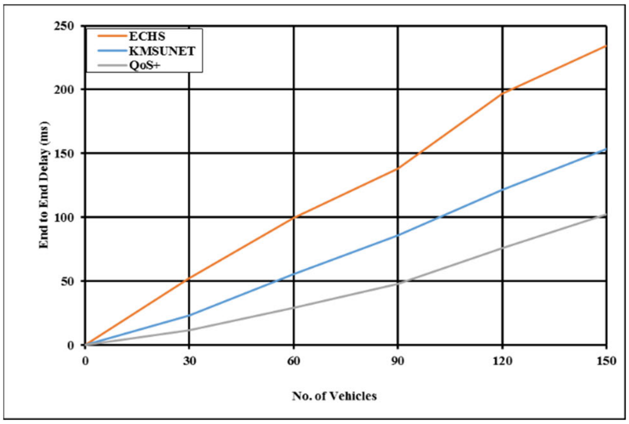


FIGURE 10. End-to-end delay.

Figure 10 shows the graphical representation of end-to-end delay calculation. Similar to previous graphs, the proposed protocol is compared against ECHS and KMSUNET. The X-axis represents the number of vehicles in the network, while the Y-axis represents the network delay. The graph shows that the delay from the proposed QoS+ protocol is lower than that of ECHS and KMSUNET. The end-to-end delay values of the proposed method with earlier work protocols are given in Table 6. Table 6 shows both the network's energy consumption values and end-to-end delay.

After analysing all the parameters and their results, it is clear that our proposed QoS+ routing protocol produces better overall performance when compared with earlier works, ECHS and KMSUNET. Table 7 to Table 10 list the CH efficiency, CM efficiency, and average cluster number, calculated according to the average speed of the network, measured as Km/H. Two scenarios are considered, 100 meters and 200 meters.

TABLE 7. Cluster head efficiency for 100 meters.

Parameters	ECHS	KMSUNET	QoS+
Energy Consumption	39.75 %	27.26 %	**22.64 %**
End-to-End Delay	234.168 ms	153.472 ms	**102.458 ms**

TABLE 8. Cluster head efficiency for 200 meters.

Parameters	ECHS	KMSUNET	QoS+
Energy Consumption	39.75 %	27.26 %	**22.64 %**
End-to-End Delay	234.168	153.472 ms	**102.458 ms**

TABLE 9. Average cluster number for 100 meters.

Average Speed (Km/H)	ECHS	KMSUNET	QoS+
0	12	10	**5**
50	14	12	**8**
100	17	15	**8**
150	19	17	**10**

TABLE 10. Average cluster number for 200 meters.

Average Speed (Km/H)	ECHS	KMSUNET	QoS+
0	9	7	**5**
50	12	11	**7**
100	14	11	**8**
150	16	14	**8**

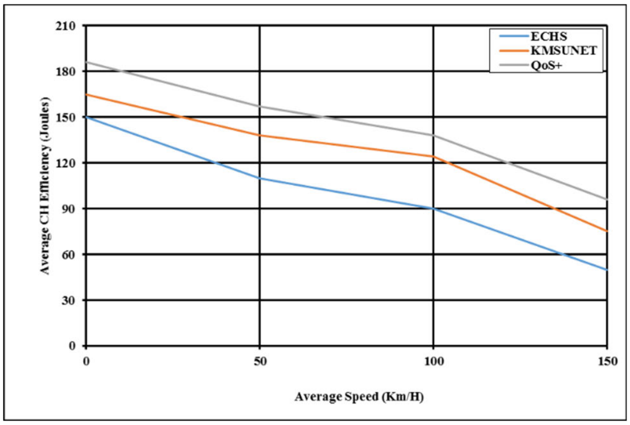


FIGURE 11. CH efficiency for 100m.

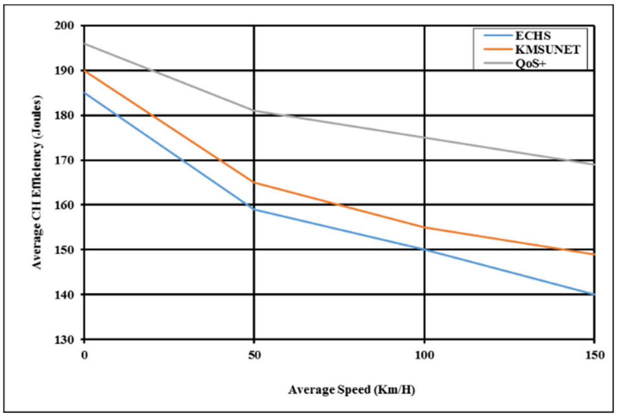


FIGURE 12. CH efficiency for 200m.

Figure 11 and 12 shows the average CH efficiency for the proposed QoS+ against ECHS and KMSUNET under various vehicle speed and transmission range (100m and 200m) settings. The results show that as the speed increases, the average CH efficiency is reduced gradually. This is due to the vehicles' dynamic nature and fast movement. The results prove that if the transmission ranges increase, it increases the CH efficiency because for 150 average speeds at 100m, the CH efficiency of the QoS+ is 96s, but for 200m, the CH efficiency is 169s. Tables 7 and 8 show the values of the cluster head efficiency for 100m and 200m.

The performance calculation of the average cluster number is diagrammatically represented in Figures 13 and 14 for various speeds and transmission ranges (100m and 200m). Here, the performance of the proposed QoS+ is compared with t ECHS and KMSUNET. The values of the average cluster number for 100m and 200m are given in Tables 9 and 10. The results demonstrate that the increase in transmission range decreases the cluster numbers. Because, in general, the transmission range of the present cluster increases, it results in the addition of more cluster members in it. For 150 average speeds at 100m, the average cluster number of the QoS+ is 10, but for 200m, it is 8.

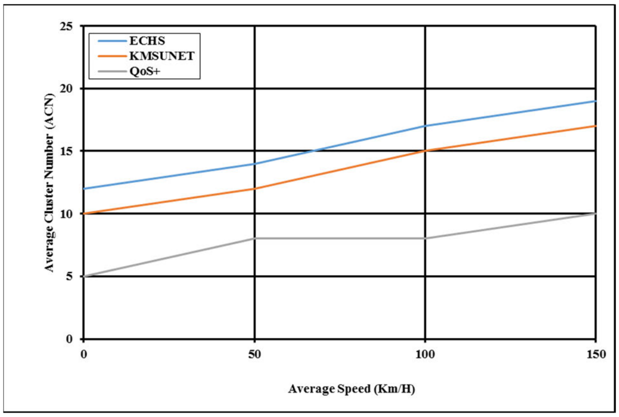


FIGURE 13. Average cluster number for 100m.

The Major disadvantage of the ECHS and KMSUNET methods is that they achieved moderate message success rate, throughput, and normalized load. The ECHS method only concentrated on efficient CH selection, and no approaches were used to protect the network. Due to a lack of security, packet loss may increase, which affects the message success rate and throughput. In the KMSUNET method, the throughput achieved by the network is low. We propose the QoS+ method to overcome this drawback, concentrating on security and routing efficiency. The QoS+ achieved superior network

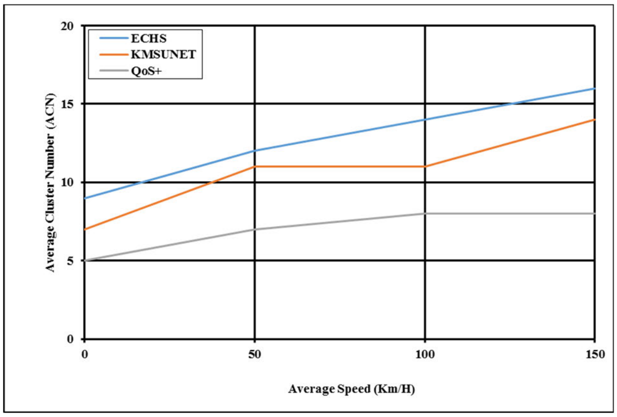


FIGURE 14. Average cluster number for 200m.

throughput, normalized routing load, message success rate, end-to-end delay, energy efficiency, and energy consumption. Additionally, as per the speed and the transmission range, parameters such as CH efficiency, cluster member efficiency, and average cluster number are calculated.

VI. CONCLUSION

VANETs are a group of vehicles that are connected in a wireless medium. Due to the functional characteristics of the VANET network, a few drawbacks are present in it, which affect the overall performance of the VANETs. Massive networks with dynamic mobility and attacks are those. So efficiency and security improvement are popular research topics in VANETs. To achieve those, we introduced a novel approach, namely QoS-aware CH selection and hybrid cryptography (QoS+). Clustering and hybrid security are initiated in the QoS+ routing protocol to maintain security and energy efficiency. The major steps of the proposed protocol are QoS-based CH selection and ECC key generation. The simulation is implemented using NS2. The network's performance is analyzed by calculating the parameters such as network throughput, normalized routing load, message success rate, end-to-end delay, energy efficiency, and energy consumption. Then as per the speed and the transmission range, the calculated parameters are CH efficiency, cluster member efficiency, and average cluster number. The results are calculated and compared with the ECHS and KMSUNET earlier methods. The proposed QoS+ superior outcomes with variable vehicle speed and transmission range in the dynamically changing topology. In future work, we plan to execute this idea in the heavily populated zone, which is the maximum populated, more complex scenario and needs to deal with some other VANET challenges.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through General Research Project under grant number GRP/269/43.

Also, the authors would like to thank the Center of Intelligent and Autonomous Systems (CIAS) at the Faculty of Computer Science and Information Technology (FSKTM), Universiti Tun Hussein Onn Malaysia (UTHM), for supporting this work.

REFERENCES

[1] F. Fakhfakh, M. Tounsi, and M. Mosbah, "An evaluative review of the formal verification for VANET protocols," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, doi: 10.1109/IWCMC.2019.8766783.

[2] S. A. Mostafa, A. Mustapha, A. A. Ramli, M. A. Jubair, M. H. Hassan, and A. H. Abbas, "Comparative analysis to the performance of three mobile ad-hoc network routing protocols in time-critical events of search and rescue missions," in *Proc. Int. Conf. Appl. Hum. Factors Ergonom.* Cham, Switzerland: Springer, Jul. 2020, pp. 117–123.

[3] A. H. Abbas, A. J. Ahmed, and S. A. Rashid, "A cross-layer approach MAC/NET with updated-GA (MNUG-CLA)-based routing protocol for VANET network," *World Electr. Vehicle J.*, vol. 13, no. 5, p. 87, 2022.

[4] M. A. Jubair, S. A. Mostafa, R. C. Muniyandi, H. Mahdin, A. Mustapha, M. H. Hassan, M. A. Mahmoud, Y. A. Al-Jawhar, A. S. Al-Khaleefa, and A. J. Mahmood, "Bat optimized link state routing protocol for energy-aware mobile ad-hoc networks," *Symmetry*, vol. 11, no. 11, p. 1409, Nov. 2019.

[5] A. Touil and F. Ghadi, "Efficient dissemination based on passive approach and dynamic clustering for VANET," in *Proc. 1st Int. Conf. Intell. Comput. Data Sci.*, 2018, pp. 369–378.

[6] A. A. Khan, M. Abolhasan, and W. Ni, "An evolutionary game theoretic approach for stable and optimized clustering in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4501–4513, May 2018.

[7] A. Mehmood, A. Khanan, A. H. H. M. Mohamed, S. Mahfooz, H. Song, and S. Abdullah, "ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET," *IEEE Access*, vol. 6, pp. 4452–4461, 2018.

[8] N. Taherkhani and S. Pierre, "Centralized and localized data congestion control strategy for vehicular ad hoc networks using a machine learning clustering algorithm," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 11, pp. 3275–3285, Nov. 2016.

[9] K. Ozera, K. Bylykbashi, Y. Liu, and L. Barolli, "A fuzzy-based approach for cluster management in VANETs: Performance evaluation for two fuzzy-based systems," *Internet Things*, vols. 3–4, pp. 120–133, Oct. 2018.

[10] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks," *Expert Syst. Appl.*, vol. 50, pp. 40–54, May 2016.

[11] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "Using discriminant analysis to detect intrusions in external communication for self-driving vehicles," *Digit. Commun. Netw.*, vol. 3, no. 3, pp. 180–187, Aug. 2017.

[12] M. Almi'ani, A. A. Ghazleh, A. Al-Rahayfeh, and A. Razaque, "Intelligent intrusion detection system using clustered self organized map," in *Proc. 5th Int. Conf. Softw. Defined Syst. (SDS)*, Apr. 2018, pp. 138–144.

[13] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks," *Comput. Secur.*, vol. 78, pp. 245–254, Jul. 2018.

[14] Y. Guo, H. Zhang, L. Zhang, L. Fang, and F. Li, "A game theoretic approach to cooperative intrusion detection," *J. Comput. Sci.*, vol. 30, pp. 118–126, Jan. 2019.

[15] I. T. Abdel-Halim, H. M. A. Fahmy, and A. M. Bahaa-El Din, "Mobility prediction-based efficient clustering scheme for connected and automated vehicles in VANETs," *Comput. Netw.*, vol. 150, pp. 217–233, Feb. 2019.

[16] M. Yang, B. Ai, R. He, L. Chen, X. Li, J. Li, B. Zhang, C. Huang, and Z. Zhong, "A cluster-based three-dimensional channel model for vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5208–5220, Jun. 2019.

[17] X. Cheng and B. Huang, "A center-based secure and stable clustering algorithm for VANETs on highways," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–10, Jan. 2019.

[18] X. Zhang, Y. Li, and Q. Miao, "A cluster-based broadcast scheduling scheme for mmWave vehicular communication," *IEEE Commun. Lett.*, vol. 23, no. 7, pp. 1202–1206, Jul. 2019.

[19] L. Liang, S. Xie, G. Y. Li, Z. Ding, and X. Yu, "Graph-based resource sharing in vehicular communication," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4579–4592, Jul. 2018.

[20] R. Singh, D. Saluja, and S. Kumar, "Reliability improvement in clustering-based vehicular ad-hoc network," *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1351–1355, Jun. 2020.

[21] R. Singh, D. Saluja, and S. Kumar, "Power controlled adaptive range radar for self driving vehicles," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Kuala Lumpur, Malaysia, Apr. 2019, pp. 1–4.
[22] H. Fatemidokht and M. K. Rafsanjani, "QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks," *J. Syst. Softw.*, vol. 165, Jul. 2020, Art. no. 110561.
[23] T. A. Alghamdi, "Secure and energy efficient path optimization technique in wireless sensor networks using DH method," *IEEE Access*, vol. 6, pp. 53576–53582, 2018.
[24] A. Paranjothi and M. Atiquzzaman, "A statistical approach for enhancing security in VANETs with efficient rogue node detection using fog computing," *Digit. Commun. Netw.*, vol. 8, no. 5, pp. 814–824, Oct. 2022.
[25] M. Banikhalaf and M. A. Khder, "A simple and robust clustering scheme for large-scale and dynamic VANETs," *IEEE Access*, vol. 8, pp. 103565–103575, 2020.
[26] B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102779.
[27] M. I. Habelalmateen, A. H. Abbas, L. Audah, and N. A. M. Alduais, "Dynamic multiagent method to avoid duplicated information at intersections in VANETs," *Telecommun. Comput. Electron. Control*, vol. 18, no. 2, pp. 613–621, 2020.
[28] A. K. Kazi, S. M. Khan, and N. G. Haider, "Reliable group of vehicles (RGoV) in VANET," *IEEE Access*, vol. 9, pp. 111407–111416, 2021.
[29] G. P. K. Marwah and A. Jain, "A hybrid optimization with ensemble learning to ensure VANET network stability based on performance analysis," *Sci. Rep.*, vol. 12, no. 1, pp. 1–20, 2022.

MOHAMMED AHMED JUBAIR was born in Iraq. He received the B.Sc. degree in computer engineering from Al-Marrif University, Iraq, in 2012, the M.Sc. degree from the Computer Science Networks Department, Universiti Kebangsaan Malaysia (UKM), Malaysia, in 2017, and the Ph.D. degree from the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia, in 2021. After the completion of the B.Sc. degree, he worked as a Teaching Assistant at Al-Marrif University, from 2012 to 2014. He is currently working as a Senior Lecturer at the Department of Computer Technical Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Iraq. His research interests include software engineering, artificial intelligent, communication systems, networking, and machine learning.

SALAMA A. MOSTAFA (Member, IEEE) received the B.Sc. degree in computer science from the University of Mosul, Iraq, in 2003, and the M.Sc. and Ph.D. degrees in information and communication technology from Universiti Tenaga Nasional (UNITEN), Malaysia, in 2011 and 2016, respectively. He is currently the Head of the Center of Intelligent and Autonomous Systems (CIAS), Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM). He has produced more than 200 articles in journals, book chapters, conferences, and tutorials. He has completed 14 industrial projects and 23 research projects. His specialization and research interests include autonomous agents, adjustable autonomy, human–computer collaboration, machine learning, optimization, and software quality assurance.

DILOVAN ASAAD ZEBARI received the B.Sc. degree in computer science from the College of Science, University of Duhok (UoD), Kurdistan Region, Iraq, in 2011, the master's degree in computer information systems (CIS) from Near East University, North of Cyprus, Turkey, in 2013, and the Ph.D. degree from the Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia (UTM), Johor Bahru, Malaysia, in 2020. He is currently working as a Lecturer at the Department of Computer Science, College of Science, Nawroz University, Duhok, Kurdistan Region. His research interests include artificial intelligence, machine learning, deep learning, medical image analysis, image encryption, biomedical computing, bio-informatics, and steganography.

HUSSEIN MUHEE HARIZ received the B.Sc. degree in communication engineering from the Technical College of Al-Najaf, Al-Furat Al-Awsat Technical University/Engineering, in 2005, and the M.Sc. degree in system and signal processing from Jawaharlal Nehru Technological University Hyderabad (JNTU), Hyderabad, India, in 2014. He is currently pursuing the Ph.D. degree with Tarbiat Modares University (TMU), Tehran, Iran. He is also working as a Lecturer at the Department of Computer Technical Engineering, Mazaya University College, Iraq, in 2014. His research interests include wireless communication and signal processing.

NEJOOD FAISAL ABDULSATTAR received the B.Sc. degree in computer science from the Computer Science and Information Technology College, Qadisiyah, in 2018, and the M.Sc. degree in information technology from Imam Reza International University, Mashhad, Iran. She is currently a Ph.D. Researcher in artificial intelligence engineering with the Internet of Things smart city at the Faculty of Computer Engineering, Bu-Ali Sina University, Hamedan, Iran. She is also working as an Assistant Lecturer at the Department of Computer Technical Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna, Iraq. Her research interests include artificial intelligence (AI), neural networks, information technology (IT), computer networks, the Internet of Things (IoT), and smart cities.

MUSTAFA HAMID HASSAN received the B.Sc. degree in computer engineering from Al-Marrif University, Iraq, in 2012, and the M.Sc. degree from the Computer Science Networks Department, Universiti Kebangsaan Malaysia (UKM), in 2017. He is currently pursuing the Ph.D. degree with the Faculty of Computer Science and Information Technology, Universiti Tun Hussen onn Malaysia (UTHM). He is also working as a Senior Lecturer at the Department of Computer Technical Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Iraq. His research interests include communication systems, artificial intelligent, networking, and machine learning.

ALI HASHIM ABBAS received the B.Sc. degree in communication engineering from the Engineering Technical College of Al-Najaf, Al-Furat Al-Awsat Technical University, in 2010, and the M.Sc. degree in digital system and computer electronics (DSCE) from Jawaharlal Nehru Technological University Hyderabad (JNTU), Hyderabad, India, in 2014, and the Ph.D. degree in communication engineering from University Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia, in 2019. He is currently working as the Head of the Department of Scientific Affairs and Promotions and the Department of Computer Technical Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna, Iraq, in 2021. He is also working as the Dean at the College of Information Technology, Imam Ja'afar Al-Sadiq university, Baghdad, Iraq. His research interests include cluster stability for inter vehicle communication and distributed algorithms, for vehicular ad hoc networks.

FATIMA HASHIM ABBAS received the B.Sc. degree in biology, the M.Sc. degree in biology/zoology, and the Ph.D. degree in biology/zoology from the Science College for Women, Babylon University, Al-Hilla, Iraq, in 2008, 2011, and 2020, respectively. She is currently working as a Senior Lecturer and the Department Coordinator at the Medical Laboratories Techniques Department, Al-Mustaqbal University College, Hilla, Babylon, Iraq.

AREEJ ALASIRY received the B.Sc. degree in information systems from King Khalid University, Abha, Saudi Arabia, and the M.Sc. degree (Hons.) in advanced information systems and the Ph.D. degree in computer science and information systems from Birkbeck College, University of London, U.K., in 2010 and 2015, respectively. She is currently an Assistant Professor at the College of Computer Science, King Khalid University. She also holds the position of the College Vice Dean for Graduate Studies and Scientific Research. Her main research interests include machine learning and data science.

M. TURKI-HADJ ALOUANE received the Senior Electrical Engineering Diploma degree from the National Engineering School of Tunis (ENIT) in 1989, the Master of Science degree in systems analysis and signal processing, in 1991, and the Ph.D. Diploma degree in electrical engineering from ENIT, in 1997. She is currently a Professor at the College of Computer Science, King Khalid University, KSA. In September 1997, she was recruited as an Assistant Professor of electrical engineering at ENIT. In June 2007, she received the National Tenure Diploma in telecommunications from ENIT. In December 2007, she was promoted to an Associate Professor of telecommunications at ENIT. From 2010 to 2012, she was a Visiting Associate Professor at the Electricity Department, Polytechnic School of Tunisia (EPT). Since 2012, she has been a Full Professor of telecommunications at the Information and Communication Technologies (ICT) Department, ENIT. She has coordinated internationally sponsored research projects. Since 1997, she has been leading more than 20 research master's theses and eight Ph.D. theses. She published more than 70 papers in impacted journals and conferences. Her research interests include signal processing (speech, image, and video), machine learning, deep learning, and heuristic optimization.