The Journal of Systems and Software 165 (2020) 110561

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

In Practice

QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks

Hamideh Fatemidokht, Marjan Kuchaki Rafsanjani*

Department of Computer Science, Faculty of Mathematics and Computer, Shahid Bahonar University of Kerman, Kerman, Iran

ARTICLE INFO

Article history:
Received 17 August 2019
Revised 19 February 2020
Accepted 20 February 2020
Available online 26 February 2020

Keywords:
Clustering
Quality of Service (QoS)
Stability
Vehicular ad hoc networks (VANETs)

ABSTRACT

Vehicular ad hoc networks (VANETs) are considered as a subset of mobile ad hoc networks (MANETs) that can be used in the transportation field. These networks considerably improve the traffic safety and accident prevention. Because of the characteristics of VANETs such as self-organization, frequent link disconnections and rapid topology changes, developing efficient routing protocols is a challenging task. To address this issue, clustering is an appropriate approach in a mobile environment. Clustering aims to partition the vehicles into a number of clusters based on some predefined metrics such as velocity, distance and location. In this paper, a clustering routing protocol, named QMM-VANET, which considers Quality of Service (QoS) requirements, the distrust value parameters and mobility constraints, is proposed. This protocol specifies a reliable and stable cluster and increases the stability and connectivity during communications. This protocol is composed of three parts: (1) computing the QoS of vehicles and electing a trustier vehicle as a cluster-head, (2) selecting a set of proper neighboring nodes as gateways for retransmitting the packets and (3) using gateway recovery algorithm to choose another gateway in case of failure of the link. NS-2 simulator is utilized to illustrate the performance of our proposed protocol in a highway scenario. The performance analyses display that the QMM-VANET protocol can achieve low end-to-end delay and high packet delivery ratio and maintain the network stability.

1. Introduction

Vehicular ad hoc networks (VANETs) are a special type of mobile ad hoc networks that mobile devices are connected via wireless links without using a fixed infrastructure (Basagni et al., 2004). VANETs are designed to improve road safety, accident prevention and traffic management. Indeed, the life of people that travel on the road are directly affected by traffic management and safety. Despite the similar features between MANET and VANET such as self-management, self-configuring, limited bandwidth and shared radio transmission conditions, there are several differences in their architecture, applications and characteristics. Indeed, the performance of VANETs depends on many features, compared to MANETs, such as high mobility, unbounded network size, variation of topology, unlimited energy and storage resources (Touil and Ghadi, 2017; Hasrouny et al., 2019). VANETs applications are classified into two categories. Safety applications like cooperative traffic monitoring, collision prevention and optimization of a route to a destination; and comfort or non-safety applications such as weather forecasting and the place of the nearest petrol station, restaurant or hotel and their prices (Basagni et al., 2004; Touil and Ghadi, 2017; Hasrouny et al., 2019; Lim and Manivannan, 2016; Sharef et al., 2014; Al-Sultan et al., 2014; Fatemidokht and Kuchaki Rafsanjani, 2018).

Vehicular ad hoc networks are a major network communication topic in intelligent transportation systems (ITSs). These networks support communications between close vehicles and as well as among vehicles and roadside equipment (Al-Sultan et al., 2014; Zhang and Zhang, 2016). Therefore, vehicles share different types of information, such as traffic, the conditions of roads and safety information in order to raise traffic efficiency, road safety and traveling comfort. The different types of communications in VANETs are categorized into vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communication (V2I). The Application Unit (AU), On-Board Unit (OBU) and RoadSide Unit (RSU) are various hardware and software components that make communication between vehicles. OBUs are wireless communication devices that periodically broadcast information to RSUs and nearby vehicles (Al-Sultan et al., 2014; Tzeng et al., 2015). Fig. 1 demonstrates a vehicular ad hoc network. Due to the characteristics of VANETs such as high mobility and sparse distribution of the vehicles on the road, maintaining the stability in these networks is a critical is-

* Corresponding author.
E-mail addresses: h.fatemidokht@math.uk.ac.ir (H. Fatemidokht), kuchaki@uk.ac.ir (M. Kuchaki Rafsanjani).

https://doi.org/10.1016/j.jss.2020.110561
0164-1212/

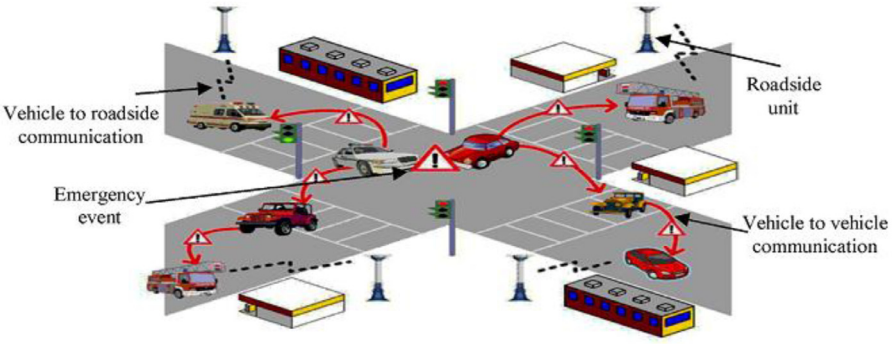

Fig. 1. Vehicular ad hoc network (Sharef et al., 2014).

sue among many challenging tasks that has major impact on the communication. Indeed, stability is a situation in which the communication in the network can continue in a regular and successful way without unexpected changes. Therefore, the network stability and communication are the significant concerns that have extraordinary impact on the performance of the network. Stability can be influenced by direction, distance, mobility, connectivity and density. Achieve stability is simplified by using clustering strategy (Sutagundar et al., 2016). At present, many researches focus on vehicular packet transmission and clustering to improve the performance of these networks (Huaug et al., 2013).

Indeed, clustering simplifies scalable and stable network structures and communications and aims to partition the vehicles into a number of clusters based on certain rules. Each vehicle in the cluster structure can play a different function such as cluster-head, gateway or member. In a cluster, the cluster-head acts as the access point and manages traffic control and QoS presentation. All vehicles communicate directly in the one cluster. Otherwise, the communication between them has to rely on the cluster-heads. In the other words, the cluster-head is a local coordinator in its cluster and performs adjustment of intra-cluster transfer and forwarding of data. The amount of information used to store the network state is reduced by clustering. Also, routing based on clustering improves the capacity of VANET. Indeed, clustering creates a virtual backbone of communication that cause to effective delivery of data in VANETs and improves the utilization of rare resources like bandwidth (Bali et al., 2014; Daeinabi et al., 2011; Wang et al., 2015; Lin and Gerla, 1997; Bylykbashi et al., 2019).

Considering that the vehicles on the roads can be formed as clusters, routing based on clustering is suitable for vehicular ad hoc networks. Since the routing scheme is generated and maintained by the vehicles, without any help of a fixed backbone or a base station, secure clustering-based routing is an important issue for VANETs. Also, consideration of the QoS metrics assigned to the topology of VANET to group the vehicles, is an essential issue. Several clustering routing protocols for VANETs are proposed in the articles (Wang et al., 2008; Kakkasageri and Manvi, 2012; Hafeez et al., 2012). In these protocols, cluster-head is selected based on different criteria such as relative speed and direction. However, the overhead for communications in these protocols is high. Also, there are clustering routing protocols that ignore malicious vehicles in the network so that are vulnerable to attack of these vehicles (Abdel Wahab et al., 2013; Zhang et al., 2011; Touil and Ghadi, 2018; Sivagurunathan et al., 2009; Kwon et al., 2015; Khan et al., 2018; Mehmood et al., 2017). Moreover, there are QoS-based clustering protocols in the literature. In these protocols the various QoS metrics like bandwidth, end-to-end delay and energy are considered for choosing cluster-head. Also, these protocols consider the different QoS constraints like bandwidth and delay during the choosing optimal routes (Clausen T et al., 2001; Santa et al., 2009; Badis and Agha, 2005; Otrok et al., 2011). However, they do not investigate the high mobility of vehicles that makes these protocols ineffective for VANETs.

To address the aforementioned defects, in this paper, the cluster-based protocol for VANET is proposed that considers different QoS parameters such as bandwidth, velocity, distance, number of neighbors and distrust value to choose trustworthy cluster-heads so that stability, security and connectivity can be improved. Indeed, this paper proposes a routing protocol named QMM-VANET that considers Quality of Service (QoS) requirements, mobility constraints and the distrust value parameters. This protocol includes three parts: (1) calculating the QoS value of vehicles and choosing a trustworthy vehicle as a cluster-head, (2) choosing a set of appropriate neighboring nodes as gateways and (3) using gateway recovery algorithm to choose another gateway in case of link failure so that stability is maintained in these networks that have a significant impact on communications.

The rest of this paper is organized as follows. Section 2 presents related works. Our proposed clustering routing protocol for VANET is described in Section 3. Section 4 offers result of network simulations and finally the conclusion is presented in Section 5.

1.1. Contributions of this paper

The proposed QMM-VANET clustering protocol chooses trustworthy cluster-heads based on different QoS parameters. Bandwidth, velocity, distance, number of neighbors and distrust value are the metrics that are considered to calculate the value of QoS for each vehicle. Indeed, bandwidth is the vehicle's level of capability to supply the services of packet transmission and is considered to ensure the reliability of the network. Velocity and distance help to selection cluster-heads with regard to the mobility constraints in VANETs. Whereas, distrust value is used for assessment and monitoring of forwarding behaviors of vehicles. A monitoring of the malicious vehicle algorithm is used to detect abnormal vehicles in the network. A vehicle can be selected as cluster-head, if it has the maximum local QoS value. Then, the elected vehicle selects the set of proper gateways for transmitting the packets and connecting the clusters. Eventually, a recovery process, which is selected alternative gateways with acceptable QoS, is used to handle the link failures. The advantages of our proposed clustering protocol are briefly mentioned as follows:

1- The basic purpose of the QMM-VANET protocol is to increase the packet delivery ratio and improve the percentage of stability and connectivity.
2- Cluster-heads are chosen based on the local maximum value of QoS so that the mobility and distrust metrics are considered. This method in turn results to improve the connectivity, stability and VANET security efficiency.

3- In the QMM-VANET protocol, an algorithm in order to monitor the vehicles behavior is used so that can detect malicious vehicles in the network.
4- In the QMM-VANET protocol, after choosing cluster-heads by using to take into account the various QoS parameters, the cluster-head selects a set of appropriate neighboring nodes as gateways.
5- In order to hold the connection of network and decrease the re-choices and the overhead, the proposed protocol utilizes a gateway recovery algorithm to choose another gateway in case of occurrence of link failure.

2. Related work

Several clustering algorithms have been proposed for vehicular ad hoc networks, which form stable clusters among the vehicles using various techniques. They can be categorized into six categories as follows: predictive clustering, backbone based clustering, Mac based clustering, traditional clustering, hybrid clustering and secure clustering (Bali et al., 2014). Various clustering routing protocols for VANETs are discussed and compared in detail in (Bali et al., 2014; Cooper et al., 2016). Several techniques have been proposed to elect a cluster-head such as lowest-ID algorithms (Lin and Gerla, 1997; Baker and Ephremides, 1981), highest-degree algorithms (Lin and Gerla, 1997; Gerla and Tsai, 1995) and weighted clustering algorithm (WCA) (Chatterjee et al., 2002). In this section, some of the clustering algorithms proposed for VANETs are reviewed. A summary of the discussed protocols is presented in Table 1.

Daeinabi et al. (2011) have proposed an efficient clustering algorithm suitable for highway scenario, named VWCA, in vehicular ad hoc networks. Vehicular clustering based on the weighted clustering algorithm (VWCA) considers different parameters to choose cluster-heads such as the number of neighbors, the direction of vehicles, the entropy and the distrust value. This algorithm improves the stability, connectivity, and security of VANETs. They have proposed a monitoring of malicious vehicle (MMV) algorithm to compute the distrust value used in the VWCA. Moreover, they have proposed an adaptive allocation of transmission range (AATR) technique so that each vehicle can find its neighbors dynamically.

Wang et al. (2008) have proposed a position based clustering algorithm for large multi-hop vehicular ad hoc networks. In this protocol, the cluster formation is based on the geographic position of vehicles and traffic information. A predefined maximum distance between the cluster-head and members is used to control the cluster size. However the overhead for V2V and V2I communications in this protocol is high.

Kakkasageri et al. (2012) have proposed a multi agent dynamic clustering scheme for vehicular ad hoc networks. Dynamic clustering divides vehicles into the cluster on the fly. Vehicle speed, direction, connectivity degree to other vehicles and mobility pattern are the main parameters to form a moving dynamic cluster. In this scheme, cluster-head is selected based on stability metric derived from connectivity degree, average speed and time to leave the road intersection. The proposed scheme improves cluster formation time, cluster member selection time, cluster head selection time and control overheads. However, in this scheme, all vehicles need to have relatively strong computational resources.

Hafeez et al. (2012) have introduced a novel cluster-head selection criterion. Cluster-head is selected based on stability criteria such as relative speed and distance between adjacent vehicles. Since the driver's behaviors, the relative speed, the inter distance are subjective, the fuzzy logic inference system is used to deal with this uncertainty. The proposed scheme achieves a highly stable cluster topology. However, due to the distributed processing overhead, the message transmission efficiency decreases.

Abdel Wahab et al. (2013) have introduced VANET QoS-OLSR protocol for Vehicular Ad hoc Networks. VANET QoS-OLSR is a QoS-based clustering protocol that investigates a tradeoff between QoS requirements and rapid topology change constraints. This protocol encompasses the following components: QoS-based clustering using Ant Colony Optimization (ACO), MPR retrieve algorithm and mechanism of fraud prevention. The bandwidth, the number of neighbors, the velocity and the residual distance are the major metrics that are considered to calculate the QoS value per vehicle. VANET QoS-OLSR protocol can increase the packet delivery ratio, reduce the end-to-end delay and the communications overhead and maintain the network stability.

Zhang et al. (2011) have presented a multi-hop clustering algorithm to establish stable vehicle clusters. In this scheme, the mobility metric is introduced to represent the mobility level of mobile nodes. The relative mobility is calculated based on two consecutive messages received from the same vehicle in N hop distance. Also the aggregate mobility value is computed by each vehicle. This value is the sum of relative mobility values for all the neighboring vehicles in N-hop. In this scheme, the vehicle with a minimum aggregate mobility value is selected as cluster-head.

Touil and Ghadi (2018) have presented a clustering protocol to facilitate management and data dissemination of messages, which is based on dynamic clustering integration and passive approach. Due to dynamic clustering, clusters are formed by collaborating vehicles together. Then vehicles send periodically measures about the speed and position to other vehicles belonging to the same cluster. The proposed protocol has four distinct phases: neighbor discovery process, dynamic cluster head selection, formation of clusters and update of clusters. In order to clustering-based data dissemination, neighbors determine before launching the clustering process. For this purpose, vehicles broadcast a message between them to inform other neighbors and create a neighbors table. The cluster head selection process has been used to choose the foremost vehicles as CHs based on the speed and position. The simulation results show that the proposed protocol reduces significantly the number of missed packets in comparison to orderly diffusion and other algorithm.

Sivagurunathan et al. (2009) have presented a self-organized public key management mechanism based on clustering. The vehicles are divided into the number of clusters based on moving pattern. The proposed model is based on the existence of a web of trust between the vehicles that provides secure routing service. However, the proposed system is vulnerable to the intrusion of malicious vehicles.

Kwon et al. (2015) have proposed a novel clustering scheme that considers neighbor vehicles mobility. The proposed scheme selects a vehicle with the lowest neighbor vehicles mobility as the cluster-head in order to efficient and reliable clustered formation. The number of neighbor vehicles that are entering into or leaving from its transmission range is used to measure the neighbor vehicles mobility. This scheme can improve the number of cluster head change and the rate of network topology change.

Clausen T et al. (2001) have proposed Optimized Link State Routing (OLSR). It is a famous unicast routing protocol for MANETs. Santa et al. (2009) have improved this protocol to use in to VANETs. In OLSR, a set of MultiPoints Relay (MPR) nodes is selected by every vehicle, which is used to retransmit the packets. MPR nodes decrease the overhead of flooding message. OLSR is a proactive routing protocol that each node has a route to every other node in the network. However, the overhead of message for retaining the routes is high. Badis and Agha (2005) have designed QOLSR protocol for ad hoc wireless networks using OLSR. This protocol considers the QoS constraints during the selection of optimal paths. Due to the QOLSR chooses the optimal paths in terms of bandwidth and delay and ignores the mobility of vehicles; it is un-

Table. 1
A summary of the discussed protocols.

Authors	Advantages	Disadvantages
Badis and Agha, 2005	The protocol considers the QoS constraints such as bandwidth and delay during the selection of optimal paths.	The protocol ignores the mobility of vehicles and it is unable to deal with VANETs.
Wang et al., 2008	The cluster formation is based on the geographic position of vehicles and traffic information. The protocol is suitable for large multi-hop vehicular ad hoc networks	The overhead for V2V and V2I communications in this protocol is high.
Sivagurunathan et al., 2009	The model is based on the existence of a web of trust between the vehicles that provides secure routing service.	The system is vulnerable to the intrusion of malicious vehicles.
Santa et al., 2009	In the protocol, a set of MultiPoints Relay (MPR) nodes is selected by every vehicle, which is used to retransmit the packets. MPR nodes decrease the overhead of flooding message.	The overhead of message for retaining the routes is high
Tian et al., 2010	The proposed algorithm generates fewer overhead of routing control and also holds stable route to transfer more packets of data.	The proposed algorithm does not consider the important parameters such as delay, throughput and number of packets loss.
Daeinabi et al., 2011	The protocol improves the stability, connectivity, and security of VANETs.	The protocol can be only used in highway scenario.
Zhang et al., 2011	The mobility metric is used to represent the mobility level of mobile nodes.	The protocol is vulnerable to attack of malicious vehicles.
Otrok et al., 2011	The protocol considers the QoS of the vehicles like residual energy and bandwidth during the selection of cluster-head and MRPs.	The protocol ignores the mobility of vehicles for computing the QoS.
Kakkasageri and Manvi, 2012	The proposed scheme improves cluster formation time, cluster member selection time, cluster head selection time and control overheads.	All vehicles need to have relatively strong computational resources.
Hafeez et al., 2012	The proposed scheme achieves a highly stable cluster topology.	The message transmission efficiency decreases, due to the distributed processing overhead.
Abdel Wahab et al., 2013	The protocol can increase the packet delivery ratio, reduce the end-to-end delay and the communications overhead and maintain the network stability.	The protocol does not consider the security.
Schleich et al., 2014	They improve small-world properties of vehicular ad hoc networks such as maximizing the clustering coefficient and minimizing the difference between the average path length (APL) of the considered graph and the APL of corresponding random graphs.	The solutions constructed by the proposed heuristics are restrictive in the number of points of injection.
Kwon et al., 2015	The scheme can improve the number of cluster head change and the rate of network topology change.	The algorithm does not investigate the important parameters such as overhead, throughput and security.
Hadded et al., 2015	The protocol improves the cluster lifetime duration and communication overhead.	The protocol does not investigate security and efficiency of channel access in VANETs that each cluster-head is accountable for allocating bandwidth to whole its cluster members.
Taherkhani and Pierre, 2016	The proposed strategy improves the throughput, delay and packet loss ratio.	Due to the proposed algorithm uses the machine learning algorithm, a great number of computation and processes that takes a long time are conducted.
Wahab et al., 2016	The deployment technique based on cluster-head dissolves the detection problem because of high mobility of the vehicles and decreases the drawback of IDS based on distributed single node.	In dense network, this technique has low rate of detection and high time of detection. Also, the additional liability of IDS on the resource CH affects the CH performance and ultimately disrupts the entire performance of network.
Alheeti et al., 2017	The introduced IDS discovers the attack before it generates considerable harm and also is independent any costly RSUs and hardware.	In the introduced IDS, very few nodes are used to test. Also, QDA and LDA techniques, which are separately used on a dataset to educate and test, can cause to false positives and environment results.
Touil and Ghadi, 2018	The protocol reduces significantly the number of missed packets in comparison to orderly diffusion and other algorithm.	The protocol ignores malicious vehicles in the network.
Ozera et al., 2018	In this protocol, the vehicles have large connectivity and more secure are chosen as the cluster-head.	The protocol does not consider important parameters for the simulation and does not carry out wide simulations.
QMM-VANET (Our proposed protocol)	Our proposed protocol specifies a reliable and stable cluster and increases the stability and connectivity during communications. Also, it uses the monitoring of vehicles behavior that can detect malicious vehicles in the network.	Our proposed protocol only consider in highway scenario.

able to deal with VANETs. Then, Otrok et al. (2011) have introduced the QoS Optimized Link State Routing (QoS-OLSR). This protocol considers the QoS of the vehicles like residual energy and bandwidth during the selection of cluster-head and MRPs. However, it ignores the mobility of vehicles for computing the QoS.

Tian et al., 2010 have presented a clustering routing algorithm for VANETs based on Euclidean distance. The proposed algorithm divides the vehicles into clusters using the position and moving direction of vehicles. Each vehicle broadcasts a beacon message in the network. This message has ID, longitude, direction, hop count and time. When a vehicle receives a beacon message, it checks the beacon hop count value. Then it discards this beacon, if hop count value is larger than the maximum value. The distance between the vehicles is calculated by each vehicle and the vehicle with the minimum distance is selected as cluster-head. The simulation results demonstrate that the proposed algorithm generates fewer overhead of routing control and also holds stable route to transfer more packets of data.

Schleich et al. (2014) have focused on the specific class of vehicular ad hoc networks and improve their small-world properties. Indeed, they find the minimal set of injection points to provide backend connectivity and optimize the small-world properties of networks such as maximizing the clustering coefficient and minimizing the difference between the average path length (APL) of the considered graph and the APL of corresponding random graphs. The Non-dominated Sorting Genetic Algorithm-II (NSGAII) and the Multi-Objective version of the CHC algorithm (MOCHC), which are accurate evolutionary algorithms, are used to find a set of good compromise solutions. The obtained results show that NSGAII was more accurate and MOCHC provided a more varied set of solutions. Also, five heuristics (two centralized and three decentralized) were proposed and compared versus the solutions provided by the evolutionary algorithms. The results provided by heuristics are really competitive results and non-dominated with respect to the best solutions found by the evolutionary algorithms.

Hadded et al. (2015) have proposed an Adaptive Weighted Cluster Protocol (AWCP) for VANETs. This protocol uses the average-distance weight factor, average-speed weight factor and number of neighbors weight factor in order to make the clusters structure. Each vehicle broadcasts a HELLO message containing the necessary information such as position and speed. After reception of a HELLO message from its on-hop neighbors, each vehicle computes its weight function and broadcasts a beacon message containing its weight. Then, the vehicle with the minimum weight value in neighbor list is selected as the cluster-head. The simulation results demonstrate that AWCP improves the cluster lifetime duration and communication overhead.

Taherkhani and Pierre (2016) have introduced a centralized and localized data congestion control strategy for VANETs using a machine learning clustering algorithm. This strategy includes three units: congestion detection, data control and congestion control. In congestion detection unit, the measurement channel usage level is used to detect data congestion in the channels. Then in data control unit, the data are gathered, filtered and clustered by machine learning algorithms. In this strategy, the *K*-means algorithm that is a famous unsupervised learning algorithm is used for clustering the large data set in VANETs. The congestion control unit adjusts the proper value of communication parameters such as transmission rate, transmission range, contention window size and AIFS for each cluster. Then, RSUs send these communication parameters to the vehicles stopped before the red traffic light to control congestion. The proposed strategy improves the throughput, delay and packet loss ratio.

Ozera et al. (2018) have presented a Fuzzy-Based Cluster-Management System (FBCMS) in VANETs. Indeed, they present two models of this system named FBCMS1 and FBCMS2 in order to clustering in VANETs. FBCMS1 model considers three input parameters of linguistic named Group Speed (GS), Security (SC) and RelativeAcceleration (RA) to select the cluster-head. Whereas, in FBCMS2 model in addition to the mentioned parameters, a novel parameter named DegreeofConnectivity (DC) is considered. In these models the trapezoidal and triangular membership functions are used for fuzzy logic controller (FLC). Also, the FBCMS1 and FBCMS2 models include 27 rules and 81 rules, respectively. The results of the simulation show that using high value of GS, SC, RA and DC is caused the vehicles have large connectivity and more secure are chosen as the cluster-head. Also, the comparison of between FBCMS1 and FBCMS2 demonstrates that the FBCMS2 can operate better than the FBCMS1 in the vehicles management in the cluster.

Wahab et al. (2016) have proposed a centralized cluster-head deployed intrusion detection system (IDS) for VANETs that detects the packets drop. In this IDS, the cluster-heads monitor and gather data related to the MPR nodes behavior. Indeed, cluster-heads in each cluster are built as IDS. Then, the obtained data are utilized by the SVM in order to investigate the node for malevolence. If a node is detected as malicious, its information is sent to the other cluster-heads. This deployment technique based on cluster-head dissolves the detection problem because of high mobility of the vehicles. Due to the cluster-head has the whole information of all clusters and builds as IDS, the proposed technique decreases the drawback of IDS based on distributed individual node. However, in dense network, this technique has a low rate of detection and high time of detection. Also, the additional liabilities of IDS on the resource CH affect the CH performance and ultimately disrupt the entire performance of the network.

Alheeti et al. (2017) have used Quadratic Discriminant Analysis (QDA) and Linear Discriminant Analysis (LDA) for the discovery of Denial of Service (DOS) and black-hole attacks within VANETs. The behavior of malicious is firstly produced by using the edition of the AODV protocol. Afterwards the mobility is produced by Simulation of Urban Mobility (SUMO) and is fed to NS2 that is a network simulator in order to produce the trace files. These trace files include some beneficial features that are utilized in order to educate and test the introduced IDS. Indeed, this IDS uses QDA and LDA in order to educate and test for differentiation between abnormal and normal behavior. The introduced IDS discovers the attack before it generates considerable harm and also is independent any costly RSUs and hardware. However, in the introduced IDS, very few nodes are used to test. Also, QDA and LDA techniques, which are separately used on a dataset to educate and test, can cause to false positives and environment results.

3. QMM-VANET: the proposed clustering routing protocol

In this section, we introduce the QMM-VANET protocol to optimize the cluster-head selection procedure that optimizes the communications between clusters in the network and chooses cluster-head according to various parameters like proportional bandwidth, distance, velocity and distrust value in order to take care of trade-off of requirements of QoS and limitation of mobility. Indeed, these parameters are considered for optimizing the selection of cluster-head in order to ensure that the load is properly distributed across the whole network. Also, this protocol maintains the stability and connectivity of the vehicular network. In QMM-VANET protocol, at first the cluster-head selection algorithm elects a trustier vehicle as a cluster-head; In fact, every vehicle elects a cluster-head. Then, the elected cluster-head selects a set of proper neighboring nodes as gateways for retransmitting the packets and connecting the clusters. Finally, the gateway recovery algorithm selects alternative gateways when occur link failures. In QMM-VANET protocol is assumed that vehicles are equipped with a Global Position-

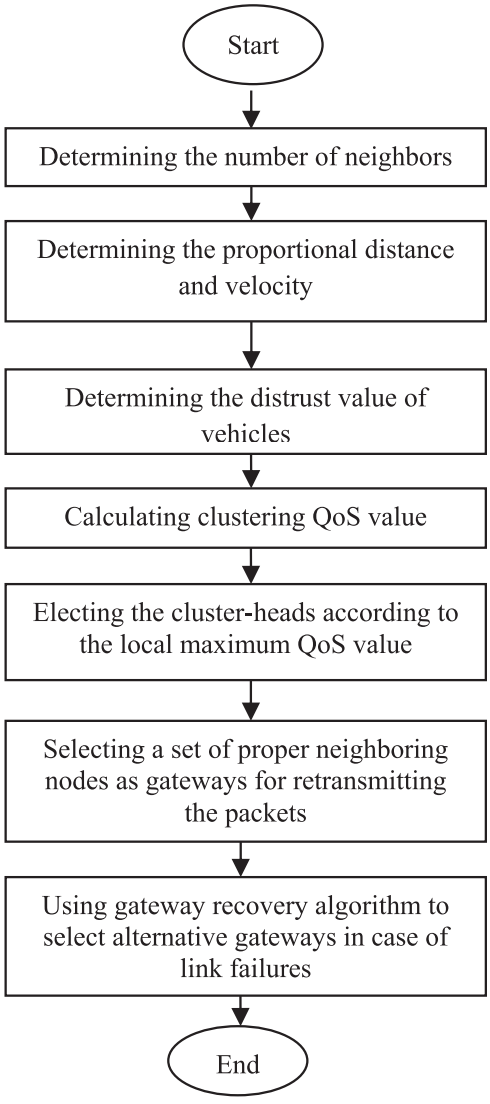

Fig. 2. The flowchart of the QMM-VANET algorithm.

ing System (GPS) that is used to acquire the geographical position of nodes in the network. In this protocol, all transmissions are omni-directional and all vehicles utilize the identical physical mode for transferring and receiving data. Also, in order to transfer data effectively, broadcast transmission of data and store-and-forward methods are combined. When a vehicle goes out of its cluster, it firstly investigates that can it be a member of another cluster? If there is such a cluster, it abandons its current cluster and joins to the novel one. Fig. 2 demonstrates the flowchart of QMM-VANET algorithm.

In order to select a trustworthy vehicle as a cluster-head, we consider the QoS value (Abdel Wahab et al., 2013) and the distrust value that will be defined in Section 3.1.1. The QoS value of the vehicle V represents the QoS requirements. Whereas, the distrust value of the vehicle V demonstrates distrust value of forwarding behaviors of this vehicle. Considered criteria to compute the QoS value per vehicle are: bandwidth, number of neighbors, distance and velocity, which the bandwidth is used to investigate the capability level of vehicles to transmit the packets, the number of neighbor provides the connectivity level and the distance and velocity parameters are used to preserve network stability. Each vehicle has two lists named black list and white list. The white list contains the list of neighbors that their distrust values are lower

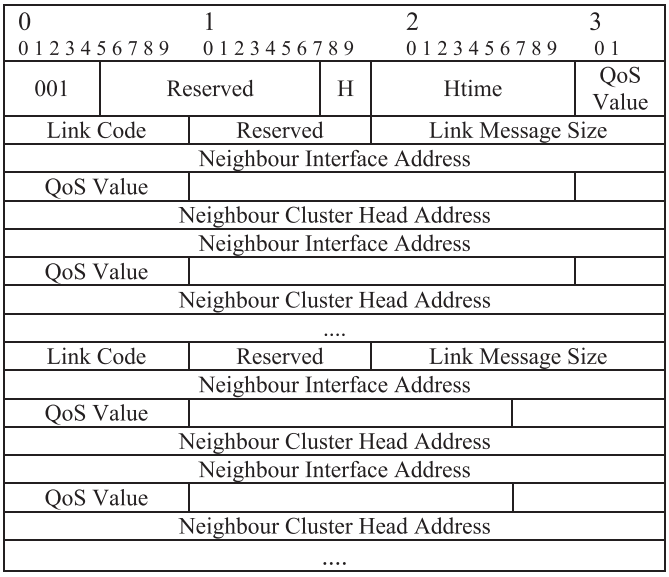

Fig. 3. HELLO message format (Abdel Wahab et al., 2013).

than the threshold value, whereas the black list includes of neighbors that their distrust values are larger than the threshold value. The vehicles in the network can be classified into three categories (Daeinabi et al., 2011):

- **Honest vehicles:** a vehicle that forwards and generates messages correctly and has a normal behavior.
- **Abnormal vehicles:** a vehicle that drops or duplicates packets and propagates false information in the network.
- **Malicious vehicles:** if the unusual behavior of a vehicle is replicated and its distrust value becomes larger than a threshold value, this vehicle is a malicious vehicle.

3.1. The cluster-head selection algorithm

The cluster-head selection algorithm that elects the proper cluster-head and divides the network into clusters has four steps to choose its required parameters. Each vehicle broadcasts HELLO messages (Fig. 3) containing its QoS value in the network. Then, the vehicles use election messages to broadcast their votes. Each vehicle votes to the vehicle with the maximum QoS metric value in neighborhood table. The selected vehicle sends an Ack message to serve as a cluster-head. In order to ensure a trustworthy selection procedure, the cheating prevention procedure is considered. Indeed, an encryption mechanism is used during the selections. For this purpose, the Ack message contains the public key of the selected vehicle as a cluster-head. This key is applied using the intermediate nodes to encrypt their QoS value. This algorithm is explained in algorithm (1). The required parameters for the QoS metric model are:

Step 1: determining the number of neighbors for vehicles

Each vehicle has a neighborhood list. For this purpose, each vehicle broadcasts a hello message periodically to all neighbors in the network. When a vehicle receives a message from another vehicle, it stores the ID of a vehicle and the corresponding position, speed and distrust value of that vehicle in its neighborhood list. Therefore, the number of vehicles located in neighborhood list of the vehicle V specifies the number of neighbors of this vehicle, which is presented by N_v.

Step 2: *determining the proportional distance and velocity*

The distance and velocity of vehicles are considered to retain the network stability. Considering these parameters causes the ve-

hicles divided into clusters with convergent distance and velocity scale. Also, using these parameters ensures to select cluster-heads and gateways with appropriate velocity and significant distance to traverse. Therefore, the lifetime of clusters will be prolonged and the link failures will be reduced.

The velocity ratio (V_ratio) for each vehicle is the ratio of velocity to average speed. The velocity of the vehicle can be any number between 60 and 120 km/h, and average speed is the average total speed traveled on a trip and return trip. Indeed, average speed is the ratio of total distance journeyed by the vehicle in each direction to total time spent on onward trip and return trip (Abdel Wahab et al., 2013). For example, if a vehicle travels at 65 km/h (40.39 mph) and at 100 km/h (62.14 mph) on a trip and return trip, respectively. The average speed is calculated as follows:

$$\begin{aligned} average\_speed &= 2 * 65 * 100/(100 + 65) \\ &= 78.8 \ \ km/h \ (48.96 \ mph) \end{aligned}$$

Therefore, V_ratio is calculated according to the following equation:

$$V\_ratio = velocity/average\_speed \tag{1}$$

The distance ratio (D_ratio) of each vehicle is the ratio of residual distance towards the destination. The distance parameter can be acquired with the GPS (Abdel Wahab et al., 2013). D_ratio is calculated using the following equations:

$$residual\_DIST = MAX\_DIST - CP \tag{2}$$

$$D\_ratio = residual\_DIST/MAX\_DIST \tag{3}$$

where CP is the current position of the vehicle and MAX_DIST is the distance between source and destination.

Step 3: determining the distrust value of vehicles

The distrust value of vehicle V(D_v) shows the behavior of this vehicle when it forwards messages. When a vehicle joins to the network, the initial distrust value $D_v = 1$, which is the same for all vehicles, is assigned to it. Then, the vehicle broadcasts its distrust value to its neighbors. Each vehicle based on this value is placed in either a white or a black list. Malicious vehicles that are recognized through the technique described in Section 3.1.1 should be located in the black list. Other vehicles are placed in the white list.

Step 4: calculating clustering QoS value

Therefore, we offer QoS model pursuant to the combination of the QoS metrics. Indeed, vehicle V can calculate its QoS value using its neighborhood table and obtaining information about the network. QoS value is calculated as follows:

$$QoS_v = \left(B_v \times N_v \times \frac{D_{ratio_v}}{V_{ratio_v}} \right) / \ D_v \tag{4}$$

where B_v and N_v are the available bandwidth and the number of neighbors of vehicle V, respectively. $D_ratio_v$and V_ratio_v represent ratio of remaining distance and ratio of velocity for vehicle V. The distrust value of vehicle V is shown by D_v. Therefore, parameter QoS_v is exchanged between neighborhood vehicles and the vehicle with the maximum QoS metric value in neighborhood table is selected to be the cluster-head. This process periodically updates the information of cluster when a novel vehicle joins the cluster or abandons the cluster.

Algorithm (1): The cluster-head selection algorithm

for each (node v ϵ N) **do**
  Compute QoS_v
  Broadcast hello message containing QoS_v
  Let k ϵ N $\cup${v} be s.t.
$QoS_k := \max\{QoS_j \mid j \epsilon N \cup \{v\}\}$
  Elect k through the election message
end for
for each (selected head k ϵ N) **do**
  Broadcast an Ack message to neighbors
end for

3.1.1. Calculation of distrust value

Due to lack of infrastructure and central management, vehicular ad hoc networks are vulnerable to a number of security threats. Vehicles can cooperate with each other and increase security in the network. The following method is utilized for verifying the behavior of vehicles and isolate malicious vehicles. Flowchart of this method is shown in Fig. 4.

To select a cluster-head, distrust values of vehicles should be calculated. It is worth mention that a cluster key is assigned to each cluster-head, which is specified by its certificate authentication (CA). CA acts as a trusted third party and manages cryptography keys, personalities and certificates of vehicles located in its region.

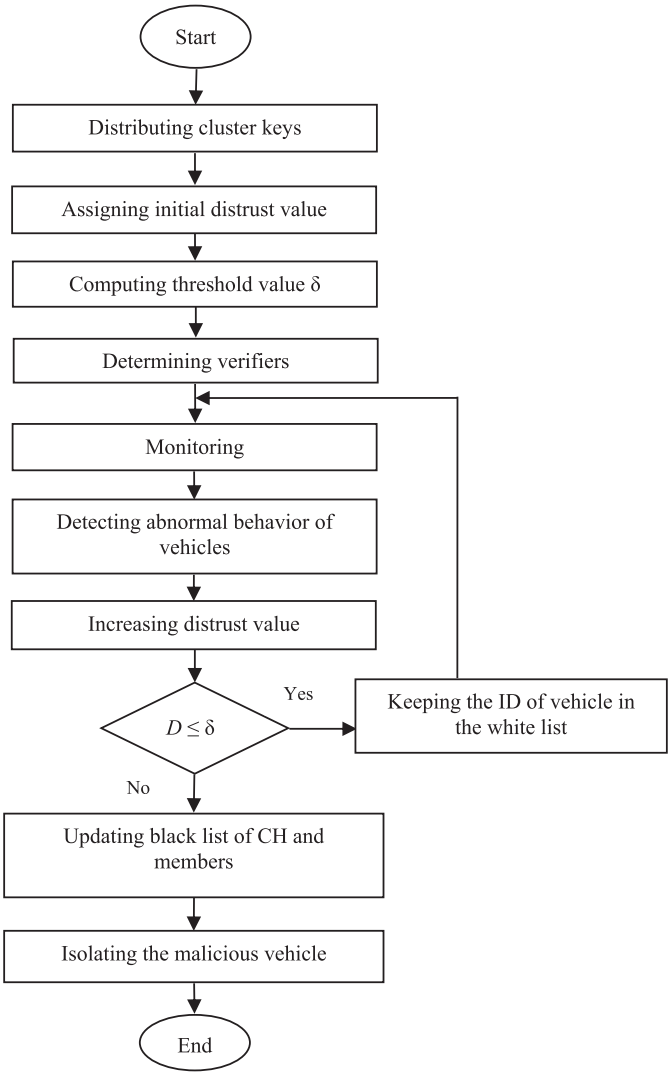

Fig. 4. Flowchart of monitoring of malicious vehicles.

The initial distrust value that is allocated to vehicles when they join to the network is the same for all vehicles. This initial value is set to 1. At first, each vehicle is placed inside the white list and then if its distrust value becomes larger than a threshold value, it moved to the black list.

The threshold value δ is a criterion for updating black and white lists. It is computed in each environment as follows (Daeinabi et al., 2011):

$$\delta = e^{\varphi} \quad 0 \le \varphi \le K_v - 1 \tag{5}$$

where K_v is the average number of vehicles in a certain environment and is computed as:

$$K_v = \left[\frac{N_{avg}}{R_{avg}}\right] \tag{6}$$

where R_{avg} and N_{avg} are the typical transmission range and the average number of vehicles, respectively. According to Eq. (5), the exponent φ is placed in $[0, K_v - 1]$ and the relative value of δ in each enviroment can be determined. Afterwards, the value of δ is saved in all CAs in the specified environment.

In our presented model, some vehicles named *'verifier'* perform the monitoring process. Indeed, the verifier monitors the packet is forwarded correctly or not and investigates the behavior of vehicles in the network. Correct forwarding means a forwarding vehicle transmits a packet to its next hop node sincerely. Therefore, if an abnormal vehicle drops, duplicates or forges the packet, it is not considered as correct forwarding. A neighbor of vehicle V is *'verifier'* if its distrust value is smaller or equal than the distrust value of vehicle V. As previously mentioned, each vehicle has a neighborhood list and knows distrust value of vehicles that are in this list.

In VANETs, Each vehicle plays the role of a router for data packets destined for the other vehicles. When vehicle V plays the relaying role and transmits a packet, its verifiers place in promiscuous mode to check the forwarding behavior of this vehicle. When vehicle V propagates false information in the network, its abnormal behavior detected by each verifier. When verifier u reports the abnormal behavior of vehicle V, other trustier verifier vehicles check the distrust value of the verifier u to be sure that the distrust value of this verifier is lower or equal than the distrust value of vehicle V. When the abnormal behavior of vehicle V is detected by its verifiers, the most trustworthy verifier in the cluster (such as cluster-head) calculates abnormal behavior rate I_v and the new distrust vale for this vehicle by following equations (Daeinabi et al., 2011):

$$I_v = w_1 \sum_{i=1}^{L} \left(\frac{1}{D_i}\right) + w_2 \sum_{i=1}^{L} \left(\frac{1}{|DS_i| + 1}\right) \tag{7}$$

$$w_1 + w_2 = 1 \quad and \quad w_1, w_2 > 0$$

$$D_v(new) = e^{I_v} + D_v(old) \tag{8}$$

where L is the number of verifier vehicles. The parameters D_i and DS_i are the distrust value of the i-th verifier and the discrepancy between the speed of the i-th verifier vehicle and the average speed of monitored vehicle, respectively. w_1 and w_2 are the corresponding weighting factors. These weighting factors are constant values that are specified by trial and error. The increase of distrust value dependent on the abnormal behavior rate and traffic conditions. It means that by increasing the parameter I_v, the distrust value is increased. Also, in high traffic conditions, D_v goes up faster. Note that we assume the most trustworthy verifier in the cluster is cluster-head and has the distrust values of all vehicles in its cluster. When the distrust value of vehicle V changes, the new value of D_v is broadcasted to its neighbors by the cluster-head. Then, the neighbors update their black and white lists using the new information.

If the distrust value of vehicle V is lower than a threshold value ($D \le \delta$), the ID of this vehicle is kept in the white list. Otherwise, the ID of vehicle V is moved to the blacklist and reports to the related CA as a malicious vehicle. CA broadcasts the ID of this vehicle to all vehicles. The vehicles that are distinguished as malicious vehicles and are located in the blacklist are not used as relaying vehicles and are not accepted any packet of them.

In this method, to report the ID of a malicious vehicle to CA, cluster-head uses a digital signature that calculated an authenticator as follows (Kuchaki Rafsanjani and Fatemidokht, 2015):

$$Auth_{RI_{CH}} = Sign(H(information\ of\ malicious\ vehicle),\ keyP_{CH}) \tag{9}$$

CA applies the verification function to corroborate the integrity of information of malicious vehicle, as:

$$Verify\left(Auth_{RI_{CH}},\ H(information\ of\ malicious\ vehicle),\ keyU_{CH}\right) \tag{10}$$

where $H(M)$ demonstrates hash of message M. $keyP_{CH}$ and $keyU_{CH}$ are private key and public key of the cluster-head.

When a malicious vehicle leaves the communication range of its cluster-head and joins to a new cluster, the ID of this vehicle is added in the black list of the new cluster-head and is removed from the black list of the old cluster-head. Therefore, the cluster-heads update their black lists. Then the updated black lists are reported to members of both clusters.

3.2. The gateway nodes selection algorithm

A gateway is a non-cluster-head node that is located within two or more clusters and forwards the information between clusters. Cluster-heads and gateways are the main participants in delivery of data and control packets. In the algorithm of gateway nodes choosing, the cluster-heads choose a set of suitable nodes to become gateways.

When a cluster-head needs to establish a communication with another cluster-head, it broadcasts k forward messages to its 2-hop away nodes by setting the type field as 0, which k is the number of on hop neighbors leading to destination cluster-head. When an intermediate node receives this message, it calculates its QoS value and inserts it in the QoS field. Also, it appends its address in the Intermediate Node Address stack.

When a forward message reached to the destination cluster-head, it includes the list of nodes and their QoS value. The destination cluster-head computes the QoS value of the route by sum of the QoS value of intermediate nodes. Then, it selects the nodes belonging to the route which has the highest value of QoS and located in its cluster as gateways. Afterward, it transforms the forward message into a backward message by setting the type field as 1. Then it unicasts the backward message back to the source cluster-head through the chosen proper route. When the backward message is received by the source cluster-head, the nodes belonging to the proper route and located in the scope of this cluster are selected as gateways. Thus, two cluster-heads communicate together via the gateway nodes. When a vehicle leaves the communication range of its cluster-head and joins to a new cluster, the cluster-heads update their lists and then the updated lists are reported to members of both clusters. The gateway selection algorithm is described in the algorithm (2).

Algorithm (2): The gateway nodes choosing algorithm

```
// a Source cluster-head (Source_CH)
Set "type" field in forward message to 0
Broadcast k forward message 2-hop away
for all (forward message launched from Source_CH to Destination_CH)
do
  if (forward message received at node_i) then
    Compute QoS_i
    if (node_i≠Destination_CH for forward message) then
      Insert QoS_i in the QoS field of forward message
      Append address of node_i in the inter Intermediate Node Address
stack
    else
      Compute the QoS value of the route by sum of the QoS value of
intermediate nodes
      Select the nodes belonging to the route which has the highest
value of QoS and located in its cluster as gateways
      Pass forward message to entrance to convert to backward message
    end if
  end if
end for
for all (backward message returning from Destination_CH to Source_CH)
do
  if (backward message received at node_i) then
    if (node_i == Destination_CH for backward message) then
      Pass backward message for entry in routing table
      Select the nodes belonging to the proper route and located in its
cluster as gateways
    end if
    if (node_i≠Source_CH for backward message) then
        Unicast backward message
      end if
    end if
end for
```

3.3. The gateway nodes recovery algorithm

In VANETs, due to the high speed of vehicles, congestion and interference, link failure is a very common event. An example of link failure is demonstrated in Fig. 5. In this example, node 8, which is a gateway node between cluster 1 and cluster 2, decides to leave cluster 2 and join cluster 3. Hence, the link between clusters 1 and 2 is broken. In order to increase the cluster stability and reduce the network overhead, we use a gateway recovery method. When a message received by the cluster-head, it contains the QoS value of intermediate nodes. The cluster-head sorts the Intermediate Node Address stack in decreasing order based on the QoS values. Thus, when a gateway leaves the cluster, the cluster-head removes the ID of this node from the stack and selects the ID of the first node in the stack as a gateway. This process is replicated till the stack becomes vacant. Therefore, the stability of the network is kept without the repeated re-selections. Algorithm (3) presents the gateway recovery algorithm.

Algorithm (3): The gateway recovery algorithm

```
for each (cluster-head k) do
  Sort the Intermediate Node Address stack (s) in decreasing order based
on the QoS values
  if(a gateway (n) leaves the cluster) then
    s:= s – {n}
    selects the ID of the first node in the stack as a gateway
    if (isEmpty(s)) then
      gateway selection algorithm ()[Algorithm (2)]
    end if
  end if
end for
```

4. Performance analysis

In this section, at first the simulation environment and parameters are presented. Then, the simulation results are discussed and the comparison of QMM-VANET protocol with other protocols is represented.

4.1. Simulation setup

The performance of our proposed approach is evaluated using simulation implemented with NS-2.35 under Linux Ubuntu 12.04. Ns2 is the most popular simulator for academic research and it is more difficult than other software. It is a discrete event and an object-oriented simulator designed for networking research. Also, it models different network architectures, including Wireless LAN, MANET, VANET and satellite. NS2 is written in C++ with an OTcl (Object Tool Command Language) interpreter. Hence, the proposed approach has been implemented by this programming language. MOVE that is the generator of mobility model is used for vehicular networks. It is based on the Java programming language and builds on SUMO (Krajzewicz et al., 2012) (Simulation of urban mobility) that is a time discrete and open-source microscopic road traffic simulation package. This traffic simulator applies XML code to represent the network features such as number of vehicles, velocity, duration and topography. The area of simulation selected is the highway of Kerman city located in the Iran that is shown in Fig. 6 and the simulation area abstraction is demonstrated in Fig. 7. We use SUMO 0.12.0 to generate the vehicle traffic and export a part of the Kerman city map from OpenStreetMap in the form of XML formatted.osm files. A simulation area of 3000 m × 1000 m is used to simulate by varying the number of vehicles from 10 to

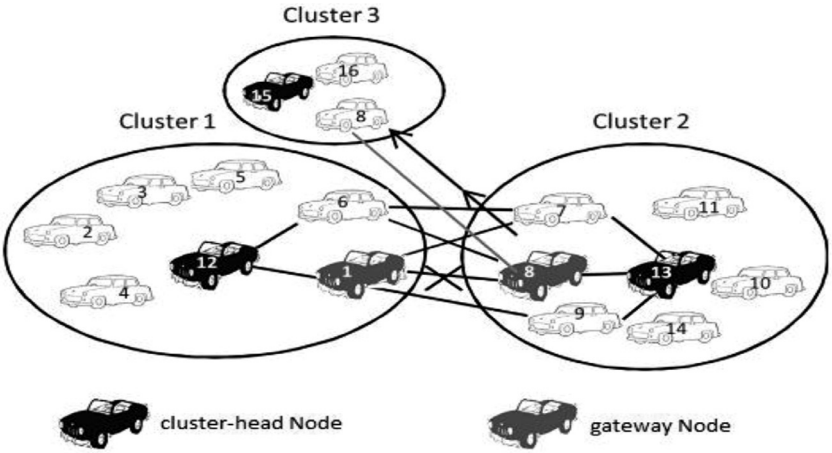

Fig. 5. Link failure example.

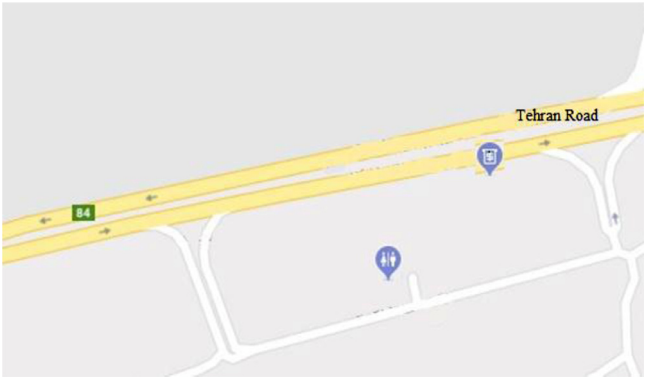

Fig. 6. Area of simulation: highway of Kerman city (Iran).

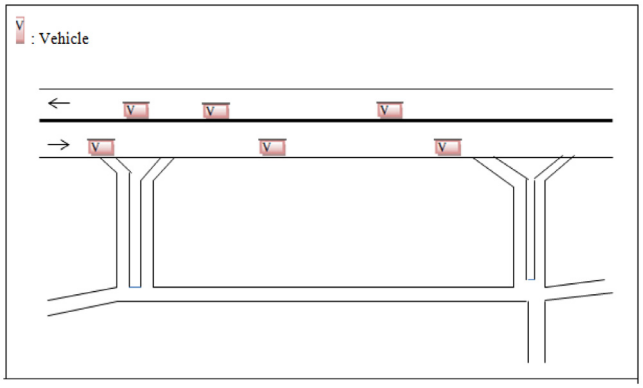

Fig. 7. The simulation area abstraction.

50. Also, the highway topology is applied to simulate the traffic. We assume that all nodes generate a constant bit rate (CBR) peer-to-peer data traffic. Moreover, the vehicle that drops or duplicates packets and changes the content of the packets is considered as malicious vehicle. The percentage of the malicious vehicles in the network is considered 10% of the whole number of vehicles in the network. Also, we take a 95% confidence interval to obtain more precise simulations. The simulation parameters used for NS2 are given in Table 2.

4.2. Experimental results

In this section, a comparison between the VANET QoS-OLSR, the cluster-based QoS-OLSR and the classical QOLSR is illustrated. The classical QOLSR finds the optimal paths using the bandwidth and the delay (Badis and Agha, 2005). The QoS-OLSR uses the bandwidth and the residual energy of each vehicle to compute the QoS function (Otrok et al., 2011). The VANET QoS-OLSR considers the bandwidth, the connectivity and the mobility for calculating the QoS function (Abdel Wahab et al., 2013). Whereas QMM-VANET protocol considers bandwidth, velocity, distance and distrust value to calculate the QoS value for each vehicle.

In QMM-VANET protocol each node encrypts its QoS value and the cluster-heads decrypt the encrypted values by their private keys. Also, each cluster-head encrypts back the QoS values by their public keys. As previously mentioned, each node discovers the highest QoS value to select the cluster-head. Hence, it requires O(log(N)) that N is the number of neighbor nodes. Thus, each node performs O(1) encryption and O(log(N)) to compute the highest QoS value. Also, the cluster-head node encrypts and decrypts TN message that TN is the number of neighbor nodes. Therefore, the computation overhead of each node is $O(TN) + O(1) + O(\log(N)) \approx O(TN)$ that this overhead is small compared to other algorithms.

In our proposed protocol, three messages are broadcasted by the cluster-head to 2-hop away nodes (HELLO, ACK and forward message). While other nodes broadcast two messages named HELLO and election message in the network. Therefore, the communication overhead of this protocol is $3TN_i + 2N_i$, where TN_i and N_i represent the number of 2-hop away nodes and the whole number of nodes, respectively. This communication overhead is admissible compared to other algorithms.

The performance of the proposed protocol is evaluated by comparing it with other clustering protocols in terms of the following criteria (Fatemidokht and Kuchaki Rafsanjani, 2018; Abdel Wahab et al., 2013; Kuchaki Rafsanjani and Fatemidokht, 2015). Although calculations of distrust value have been added to our proposed protocol, the simulation results are close to the VANET QoS-OLSR protocol for some of the criteria such as delay and throughput. In addition, the simulation results show that our proposed protocol improves the investigated criteria such as packet delivery ratio, percentage of stability and percentage of gateways compared to other protocols. Indeed, our proposed protocol determines a stable and reliable cluster and increases the stability and connectivity during communications. Also, it uses the monitoring of vehicles behavior that can detect malicious vehicles in the network.

Table. 2
Simulation parameters.

Parameters	Values
Time of simulation	400 s, 600 s, 800 s, 1000 s, 1200 s, 1400 s, 1600 s, 1800 s
Dimension	3000 m × 1000 m
Traffic Model	CBR (Constant Bit Rate)
Transmission range	250 m
Data Packet size	512 byte
Topology	Highway with two bands and each band has two lines
Mobility generator	SUMO
Number of vehicles	10, 20, 30, 40, 50
Vehicle speed	60–120 km/h
Idle time	Random value within [0, 1]
Link bandwidth	1 Mbps
Available bandwidth	Idle time × . Link bandwidth
MAC/PHY	IEEE 802.11p
w_1 in Eq. (7)	0.6
w_2 in Eq. (7)	0.4
R_{avg}	300
φ	$(K_v$ -1)/2
Number of simulation runs	10

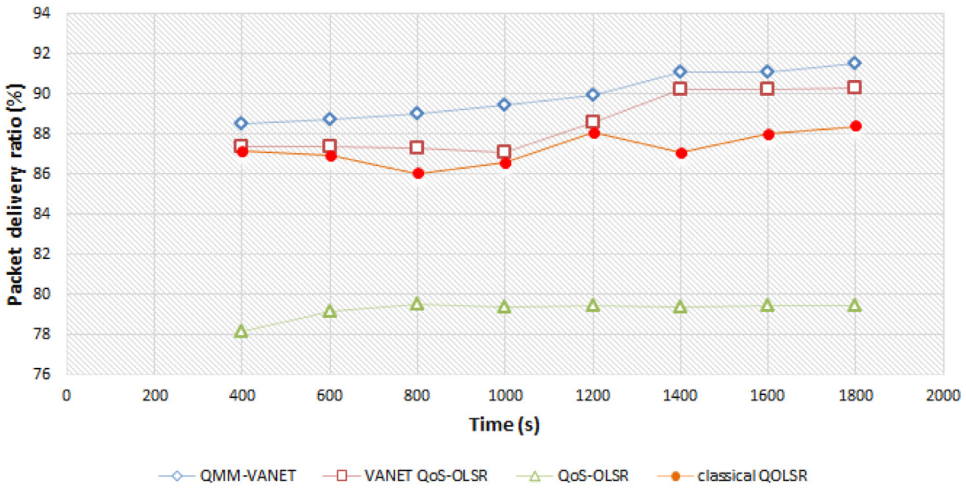

Fig. 8. Packet delivery ratio versus time.

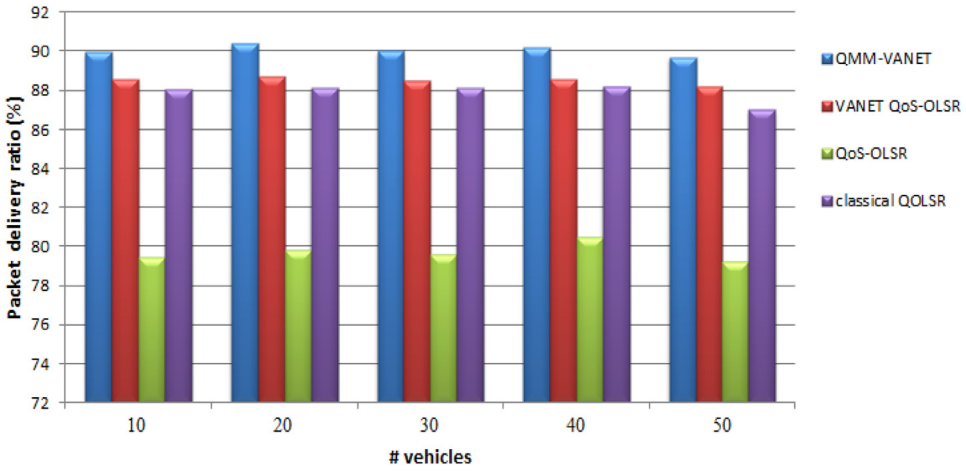

Fig. 9. Packet delivery ratio versus number of vehicles.

- **Packet delivery ratio:** the packet delivery ratio is obtained by dividing the number of packets successfully received by the number of packets originated for a destination.
- **End-to-end delay:** end to end delay refers to the time required to transmit a packet across a network from source to destination.
- **Throughput:** the throughput is calculated by dividing the total number of data bits delivered to destination node during the simulation by the total simulation time.
- **Percentage of stability:** the percentage of stability can be calculated by dividing the number of current vehicles in each cluster to the previous number of vehicles in the same cluster before a slot of time. Indeed, stability of cluster is the average lifetime of a cluster in terms of the number of nodes within that cluster. If over 60% of the nodes are in the cluster, the cluster is intended stable.
- **Percentage of gateways:** this criterion is the percentage of gateways selected using the cluster-head during the communications as the relaying points among clusters.
- **Number of packets loss:** number of packet loss is defined as the number of packets not received at their destination during the simulation time.
- **Path length:** this criterion is described as the average number of hops that used to transmit data between the source node and destination node. The path length can be reflected in the end-to-end delay.

The obtained results of the simulations are shown in Figs. 8–18. In the figures showing the performance parameters vs. time, the number of vehicles is set 20. Figs. 8 and 9 are the packet delivery ratio as a function of simulation time and the number of vehicles, respectively. We can observe in these figures that our proposed protocol increases this ratio; because it is able to increase the percentage of stability and connectivity that the packets are transmitted along a path without packet losses. Indeed, our proposed protocol compared to other protocol increases the packet delivery ratio by 12%.

Fig. 10 shows that the end-to-end delay of QMM-VANET is less than QoS-OLSR and classical QOLSR. This is due to the fact that our proposed protocol increases the connectivity and packet delivery ratio, but due to the calculation distrust value of the vehicles is about 3% more than VANET QoS-OLSR. Fig. 11 is the end-to-end delay of protocols as a function of simulation time. Generally, our proposed protocol in comparison to other protocols decreases the end-to-end delay by 45%. Considering to the obtained results of the packet delivery ratio and end-to-end delay, according to Figs. 12 and 13, the throughput of our proposed protocol is higher than QoS-OLSR and classical QOLSR and about 3% more than VANET QoS-OLSR. Generally, our proposed protocol increases the throughput by 23%.

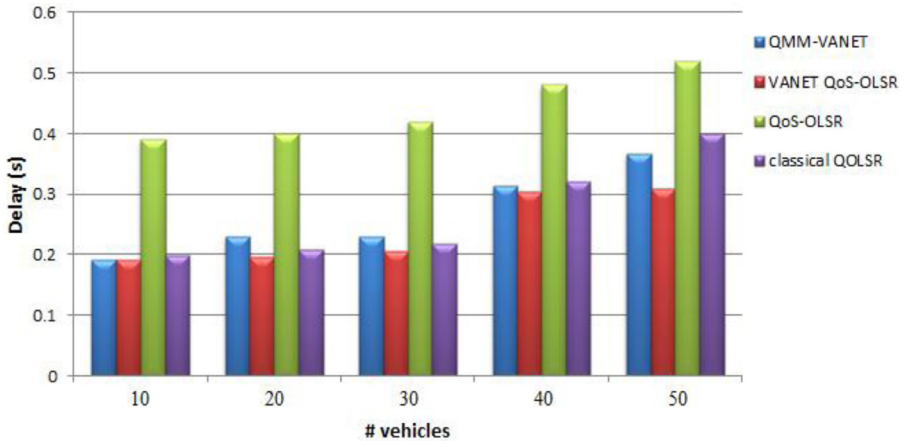

Fig. 10. End-to-end delay versus number of vehicles.

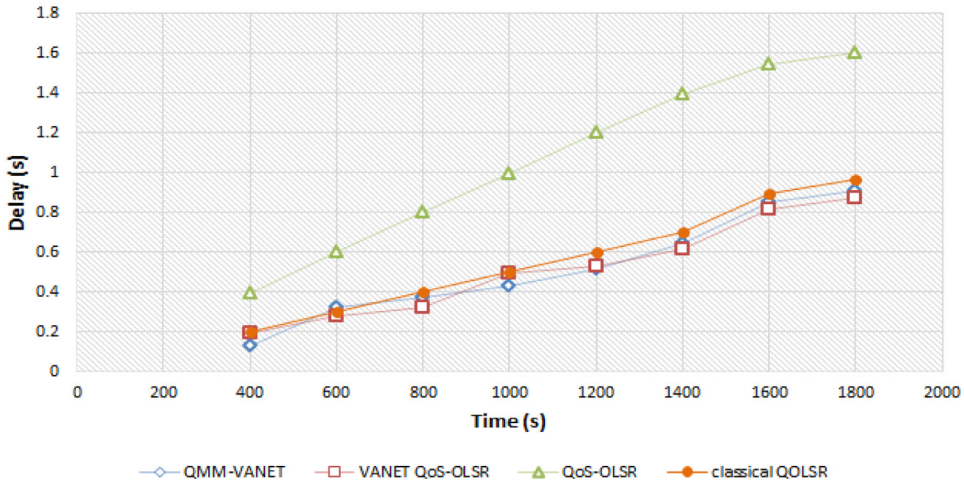

Fig. 11. End-to-end delay versus time.

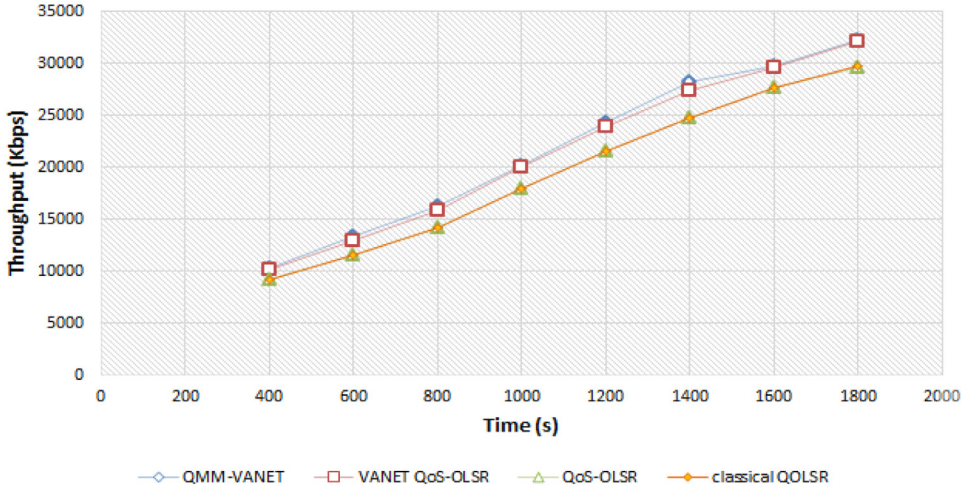

Fig. 12. Throughput versus time.

In Fig. 14 the comparison between the percentage of stability of QMM-VANET and other protocols is shown. This figure represents that in comparison to other protocol the percentage of stability of QMM-VANET is increased by 14%. This is because our proposed protocol uses the distrust value and the proportional distance and velocity to calculate the QoS value per vehicle. It guarantees that cluster-heads and gateways are selected with proper velocity and significant distance to traverse and avoids the repeated disconnections.

In Fig. 15 percentage of gateways as a function of number of vehicles is shown. This figure demonstrates that QMM-VANET, VANET QoS-OLSR and QoS-OLSR reduce percentage of gateways because these nodes are selected using cluster-heads that are a confined number of nodes in network. Also,

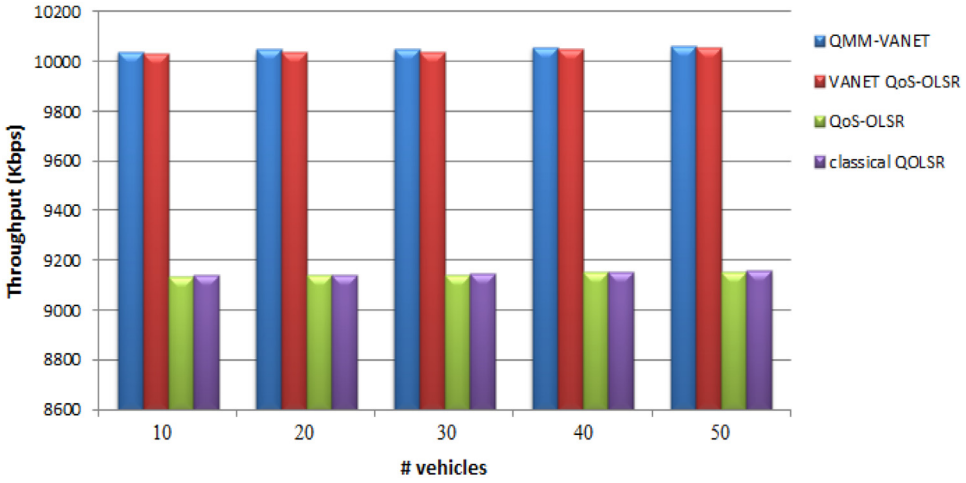

Fig. 13. Throughput versus number of vehicles.

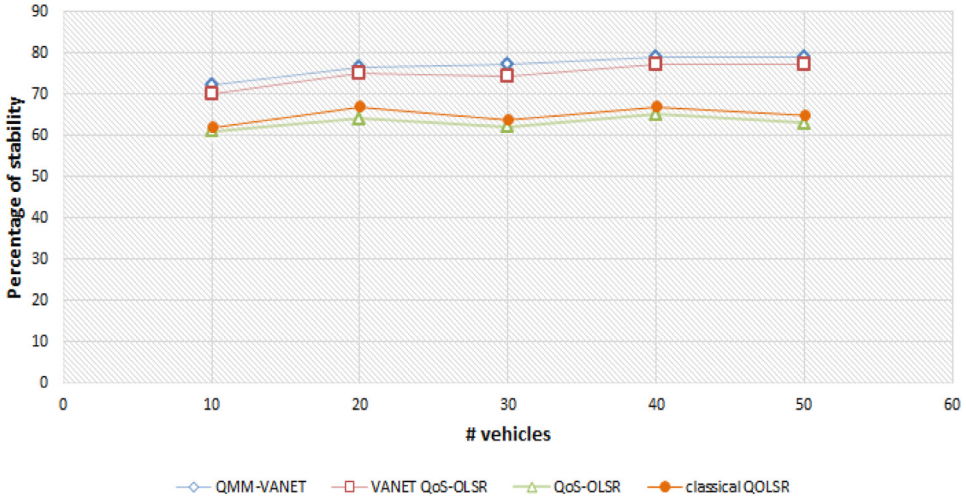

Fig. 14. Percentage of stability versus number of vehicles.

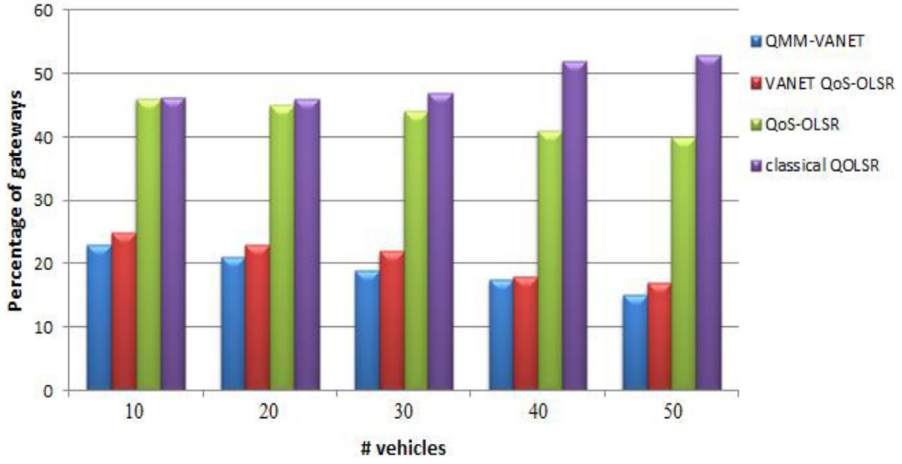

Fig. 15. Percentage of gateways versus number of vehicles.

QMM-VANET protocol is better than VANET QoS-OLSR and QoS-OLSR by reducing the percentage of gateways about 20%. This is since QMM-VANET protocol computes the QoS function using the connectivity factor that lead to select the gateways with higher connectivity. Hence, QMM-VANET protocol can be efficient for dense networks. In Fig. 16 the percentage of gateways of protocols as a function of simulation time is represented.

Fig. 17 compares the number of packet loss obtained by different protocols. Due to the proposed protocol increases the

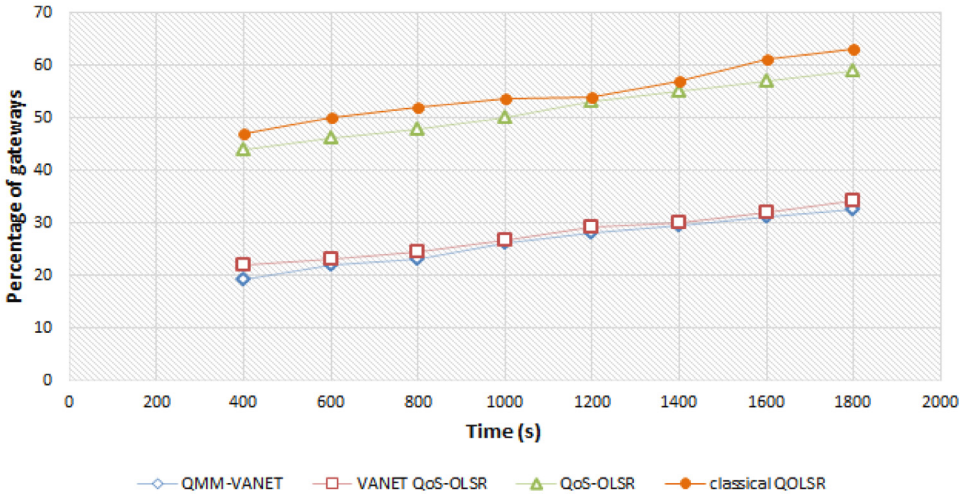

Fig. 16. Percentage of gateways versus time.

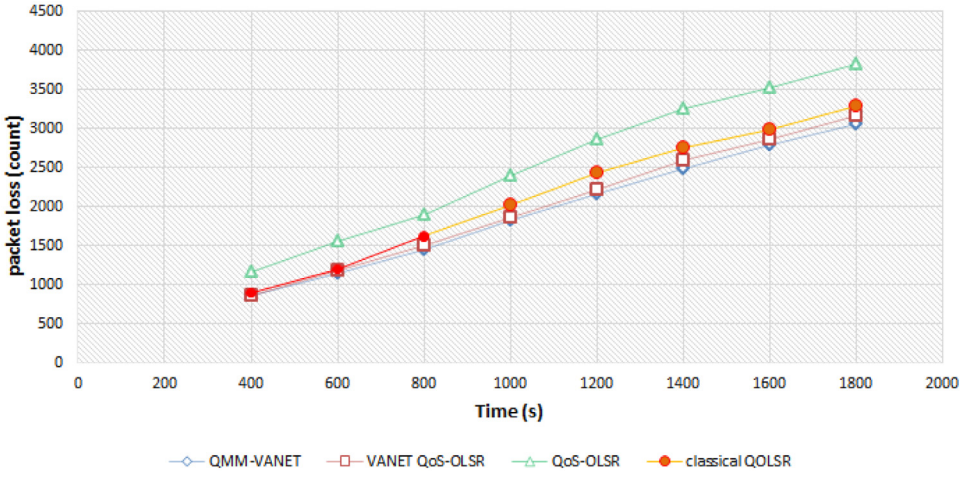

Fig. 17. Number of packet lost versus time.

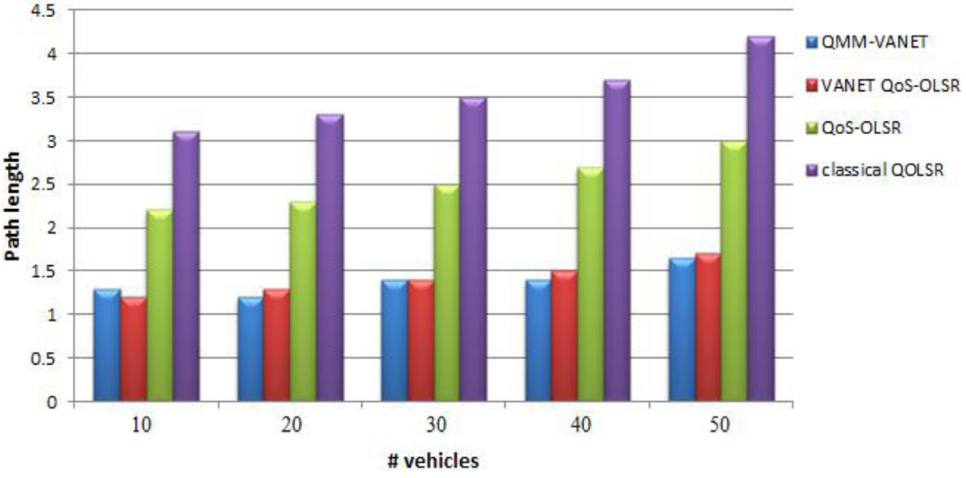

Fig. 18. Path length versus number of vehicles.

percentage of packets transferred, the number of packet loss of QMM-VANET is lower than other investigated protocols about 6%. Fig. 18 represents the average number of hops yielded using the investigated protocols. This figure demonstrates that the number of hops in QMM-VANET protocol is about 3% less than other examined protocols. This is due to the fact that this protocol calculate the QoS function and select the nodes that has the highest value of QoS as gateways.

5. Conclusion

Vehicular ad hoc networks (VANETs) include sets of vehicles that are connected through wireless links. Due to the characteristics and wide range of applications of VANETs, designing an efficient routing protocol has become a popular research topic. In this paper, a new vehicular clustering algorithm, called QMM-VANET has been proposed, to maintain the stability of the vehicular ad hoc network. This protocol uses the QoS requirements, the distrust value and mobility constraint parameters to calculate the QoS value for each vehicle. This value is exchanged among neighborhood vehicles and the vehicle with the maximum QoS value is elected as the cluster-head. The major steps of our proposed protocol are: computing the QoS of vehicles and electing a trustier vehicle as a cluster-head, selecting a set of proper neighboring nodes as gateways for retransmitting the packets and using gateway recovery algorithm to select alternative gateways in case of link failures. Simulation results show that QMM-VANET is suitable in the highway scenario and in comparison to other protocols increase the packet delivery ratio by 12% and decrease the end-to-end delay by an average of 45%. This is due to the fact that our proposed protocol increases the percentage of stability and connectivity. Indeed, the QMM-VANET protocol improves the percentage of stability up to 14%. Because the protocol selects cluster-heads and gateways with proper velocity and significant distance to traverse and avoids the repeated disconnections. In the future, the our proposed protocol can be developed to urban scenario, utilized a security algorithm based on key distribution and also detected selfish vehicles in the network by using Swarm Intelligence methods.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Hamideh Fatemidokht: Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Writing - original draft, Visualization, Funding acquisition. **Marjan Kuchaki Rafsanjani:** Conceptualization, Validation, Writing - review & editing, Supervision, Project administration.

Acknowledgement

The work of the authors on this paper was supported by Iran National Science Foundation: INSF (No. 97000901). The authors would like to express their thanks to the anonymous referees for their valuable comments and suggestions that improved the paper.

References

Abdel Wahab, O., Otrtk, H., Mourad, A., 2013. VANET QoS-OLSR: QoS-based clustering protocol for vehicular Ad hoc Networks. Comput. Commun. 36, 1422–1435.
Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., Zedan, H., 2014. A comprehensive survey on vehicular Ad Hoc network. J. Netw. Comput. Appl. 37, 380–392.
Alheeti, K.M.A., Gruebler, A., McDonald-Maier, K., 2017. Using discriminant analysis to detect intrusions in external communication of self-driving vehicles. Digit. Commun. Netw. 3, 180–187.
Badis, H., Agha, K., 2005. QOLSR, QoS routing for ad hoc wireless networks using OLSR. Eur. Trans. Telecommun. 16, 427–442.
Baker, D.J., Ephremides, A., 1981. A distributed algorithm for organizing mobile radio telecommunication networks. In: Proc. the Second International Conference on Distributed Computer Systems April.
Bali, R.S., Kumar, N., Rodrigues, J.J.P.C., 2014. Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions. Veh. Commun. 1, 134–152.
Basagni, S., Conti, M., Giordano, S., Stojmenovic, I., 2004. Mobile Ad Hoc Networking. IEEE Press.
Bylykbashi, K., D.Elmazi, K.M., Ileda, M., Barolli, L., 2019. Effect of security and trustworthiness for a fuzzy cluster management system in VANETs. Cognit. Syst. Res. 55, 153–163.
Chatterjee, M., Das, S.K., Turgut, D., 2002. WCA: a weighted clustering algorithm for mobile ad hoc networks. Clust. Comput. 5, 193–204.
Clausen T, T., Hansen, G., Christensen, L., Behrmann, G., 2001. The optimized link state routing protocol, evaluation through experiments and simulation. In: Proc. IEEE symposium on wireless personal mobile communications.
Cooper, C., Franklin, D., Ros, M., Safaei, F., Abolhasan, M., 2016. A comparative survey of VANET clustering techniques. IEEE Commun. Surv. Tutor. doi:10.1109/COMST.2016.2611524, to be published.
Daeinabi, A., Ghaffhar Pour Rahbar, A., Khademzadeh, A., 2011. VWCA: an efficient clustering algorithm in vehicular ad hoc networks. Netw. Comput. Appl. 34, 207–222.
Fatemidokht, H., Kuchaki Rafsanjani, M., 2018. F-Ant: An effective routing protocol for ant colony optimization based on fuzzy logic in vehicular ad hoc networks. Neural Comput. Appl. 29, 1127–1137.
Gerla, M., Tsai, J.T.C., 1995. Multicluster, mobile, multimedia radio network. Wirel. Netw. 1, 255–265.
Hadded, M., Muhlethaler, P., Zagrouba, R., Laouiti, A., Saidane, L.A., 2015. Using road IDs to enhance clusteringin vehicular ad hoc networks. In: Proc. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia.
Hafeez, K.A., Zhao, L., Liao, Z., Ma, B.M., 2012. A fuzzy-logic-based cluster head selection algorithm in VANETs. In: Proc. IEEE International Conference on Communications, Ottawa, ON., pp. 203–207.
Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A., 2019. Misbehavior detection ande fficient revocation within VANET. J. Inf. Secur. Appl. 46, 193–209.
Huaug, C.J., Wang, Y.W., Chen, H.M., Cheng, A.L., Jian, J.J., Tsai, H.W., Liao, J.J., 2013. An adaptive multimedia streaming dissemination system for vehicular networks. Appl. Soft Comput. 13, 4508–4518.
Kakkasageri, M.S., Manvi, S.S., 2012. Multiagent driven dynamic clustering of vehicles in VANETs. J. Netw. Comput. Appl. 35, 1771–1780.
Khan, A.A., Abolhasan, M., Ni, W., 2018. An evolutionary game theoretic approach for stable and optimized clustering in VANETs. IEEE Trans. Veh. Technol. 67, 4501–4513.
Krajzewicz, D., Erdmann, J., Behrisch, M., Bieker, L., 2012. Recent development and applications of SUMO—simulation of urban mobility. Int. J. Adv. Syst. Meas. 5, 128–138.
Kuchaki Rafsanjani, M., Fatemidokht, H., 2015. FBeeAdHoc: a secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs. Int. J. Electron. Commun. (AEÜ) 69, 1613–1621 July.
Kwon, J.H., Kwon, C., Kim, E.J., 2015. Neighbor mobility-based clustering scheme for vehicular ad hoc networks. In: Proc. International Conference on Platform Technology and Service, Jeju, Republic of Korea.
Lim, K., Manivannan, D., 2016. An efficient protocol for authenticated and secure message delivery in vehicular ad hoc network. Veh. Commun. 4, 30–37.
Lin, C.R., Gerla, M., 1997. Adaptive clustering for mobile wireless networks. IEEE J. Sel. Areas Commun. 15, 1265–1275.
Mehmood, A., Khanan, A., Mohamed, A.H.H.M., Mahfooz, S., Song, H., Abdullah, S., 2017. ANTSC: an Intelligent Na¨ıve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET. IEEE Access 6, 4452–4461.
Otrok, H., Mourad, A., Robert, J.-M., Moati, N., Sanadiki, H., 2011. A cluster-based model for QoS-OLSR protocol. Proc. IWCMC, IEEE, pp. 1099–1104.
Ozera, K., Bylykbashi, K., Liu, Y., Barolli, L., 2018. A fuzzy-based approach for cluster management in VANETs: Performance evaluation for two fuzzy-based systems. Internet Things 3–4, 120–133.
Santa, J., Tsukada, M., Ernst, T., Mehani, O., Gómez-Skarmeta, A.F., 2009. Assessment of VANET multi-hop routing over an experimental platform. Int. J. Internet Protoc. Technol. 4, 158–172.
Schleich, J., Danoy, G., Dorronsoro, B., Bouvry, P., 2014. Optimising small-world properties in VANETs: centralised and distributed overlay approaches. Appl. Soft Comput. 21, 637–646.
Sharef, B.T., Alsaqour, R.A., Ismail, M., 2014. Vehicular communication ad hoc routing protocols: a survey. J. Netw. Comput. Appl. 40, 363–396.
Sivagurunathan, S., Subathra, P., Mohan, V., Ramaraj, N., 2009. Authentic vehicular environment using a cluster based key management. Eur. J. Sci. Res. 36, 299–307.
Sutagundar, A.V., Hubballi, P., Belagali, R., 2016. Stability oriented cluster dynamism in VANET (SOCDV). In: Proc. 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions, Bangalore, India October.
Taherkhani, N., Pierre, S., 2016. Centralized and localized data congestion control strategy for vehicular ad hoc networks using a machine learning clustering algorithm. IEEE Trans. Intell. Transp. Syst. 17, 3275–3285.
Tian, D., Wang, Y., Lu, G., Yu, G., 2010. A VANETs routing algorithm based on Euclidean distance clustering. In: Proc. 2nd IEEE International Conference on Future Computer and Communication, Wuhan. IEEE, pp. 183–187.
Touil, A., Ghadi, F., 2017. Implementation of clustering metrics in vehicular ad-hoc networks. Proc. the Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, pp. 441–449.
Touil, A., Ghadi, F., 2018. Efficient dissemination based on passive approach and dynamic clustering for VANET. Proc. The First International Conference On Intelligent Computing in Data Sciences, Meknes-Morocco, 127. Procedia Computer Science, pp. 369–378.

Tzeng, S.F., Horng, S.J., Li, T., Wang, X., Huang, P.H., Khurram Khan, M., 2015. Enhancing security and privacy for identity-based batch verification scheme in VANET. IEEE Trans. Veh. Technol. doi:10.1109/TVT.2015.2406877, to be published.

Wahab, O.A., Mourad, A., Otrok, H., Bentahar, J., 2016. CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. Expert Syst. Appl. 50, 40–54.

Wang, H., Liu, R.P., Ni, W., Chen, W., Collings, I.B., VANET Modeling, Clustering Design Under Practical Traffic, 2015. VANET modeling clustering design under practical traffic channel and mobility conditions. IEEE Trans. Veh. Technol. 63, 870–881.

Wang, Z., Liu, L., Zhou, M., Ansari, N., 2008. A position based clustering technique for ad hoc inter vehicle communication. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) 38, 201–208.

Zhang, X., Zhang, X., 2016. A binary artificial bee colony algorithm for constructing spanning trees in vehicular ad hoc networks. Ad Hoc Networks doi:10.1016/j.adhoc.2016.07.001.

Zhang, Z., Boukerche, A., Pazzi, R.W., 2011. A novel multi-hop clustering scheme for vehicular ad-hoc networks. In: Proc. the 9th ACM International Symposium on Mobility Management and Wireless Access (MobiWac'11), pp. 19–26.

Hamideh Fatemidokht received her Ph.D. degree in Applied Mathematics department at Shahid Bahonar University of Kerman, Kerman, Iran, in 2017. She received her M.Sc. degree in Computer Science from Shahid Bahonar University of Kerman, Kerman, Iran, in 2013 and received her B.Sc. degree in Computer Science from Vali-e-Asr university of Rafsanjan, Rafsanjan, Iran, in 2010. Her main research interests are Artificial intelligence, Neural Networks, Mobile Ad hoc Networks, Vehicular Ad hoc Networks and Flying Ad hoc Networks.

Marjan Kuchaki Rafsanjani received her Ph.D. in Computer Engineering, Iran in 2009. She is currently an associate professor at the department of Computer Science at Shahid Bahonar University of Kerman, Iran. She has published about 160 research papers in international journals and conference proceedings. Her current research interests include computer networks, artificial intelligence, electronic commerce, grid and cloud computing.