Vehicular Communications 12 (2018) 75–87

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Robust and trust dynamic mobile gateway selection in heterogeneous VANET-UMTS network

Baraa Sharef [a], Raed Alsaqour [b,*], Mahmoud Alawi [d], Maha Abdelhaq [c], Elankovan Sundararajan [d]

[a] Department of Information Technology, Faculty of Information Technology, Ahlia University, Manama, Bahrain
[b] Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, 93499 Riyadh, Saudi Arabia
[c] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia
[d] Research Center for Software Technology and Management, Faculty of Information Science and Technology, National University of Malaysia, 43600, Bangi, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 15 July 2017
Received in revised form 17 January 2018
Accepted 2 February 2018
Available online 6 February 2018

Keywords:
Vehicular ad-hoc network
Mobile gateway selection
UMTS
VANET-UMTS
Heterogeneous network

ABSTRACT

Vehicular ad-hoc network (VANET) technology is serving variable applications as it uses moving vehicles as nodes in a network to create communication independent of a central infrastructure. Various types of VANET problems have emerged because of the absence of a central infrastructure as well as the random movement of the vehicles. VANETs cannot cope with network segmentation because of frequently disconnected networks in sparse environments. Therefore, several solutions have been proposed in the literature, such as integrating the VANET with other infrastructure networks by static gateways that have been fixed along the road. However, protocols based on static gateways can provide connectivity only in areas where they are deployed. Thus, the distribution and requirement of static gateways are the main drawbacks of these protocols. In this paper, a new routing protocol for robust and trust mobile gateway selection (RTMGwS) has been proposed. RTMGwS protocol uses the characteristics of vehicle movements and variant routing parameters to select an optimal mobile gateway with high robust and trust connection to an infrastructure network. The protocol is designed to spread the advertisement messages by the mobile vehicle gateway over the integrated network architecture of VANET and universal mobile telecommunications system (VANET-UMTS) without flooding the network and seamless handovers. The proposed protocol has been validated using SUMO and NS2 simulators over highways environment. The simulation results show encouraging performance in terms of increasing the packet delivery ratio and overall throughput, reducing control packet overhead and minimizing connection delay.

1. Introduction

Vehicular ad-hoc network (VANET) technology is one of the growing fields of research that integrates the potential of new generation wireless networks into vehicles [1]. VANET aims to serve different applications where it uses moving cars as nodes in a network to establish communication that is independent of a central infrastructure. VANET does not have a fixed infrastructure and centralized administration. Therefore, VANET has the key advantages of flexible network topology and lower cost of administration and maintenance [2,3].

Routing in the VANET network is highly complex because of its highly volatile topology and mobility speed [4]. Several specialized routing protocols have been developed for VANET. The VANET protocols, with various techniques, improve network performance to a certain extent but still suffer from network partitioning because of high mobility [5]. This phenomenon has recently prompted researchers to switch their efforts in investing, studying, and developing new solutions to overcome the problem.

In the literature, heterogeneous wireless network is one of the interesting solutions that integrates the VANET with other infrastructure networks, such as cellular networks, WLAN, and the Internet [6]. The proposed protocols in heterogeneous vehicle to infrastructure (V2I) network make vehicular communication more reliable and minimize unwanted delays in different vehicular applications that the VANET does not provide [7]. A good example of a heterogeneous wireless network is the combination of IEEE 802.11p-based VANET and the universal mobile telecommunication system (UMTS) network that produces a more robust network with respect to coverage area and speed [8,9]. By combin-

* Corresponding author.
E-mail address: raed.ftsm@gmail.com (R. Alsaqour).

https://doi.org/10.1016/j.vehcom.2018.02.002
2214-2096/

ing UMTS and VANET, a high data rate will be combined with wide-range communication. In the visualized VANET/3G network, one mobile vehicle can act as a mobile gateway to other vehicles to access the UMTS network in its nearness by receiving the data from the relay vehicle (via its IEEE 802.11p interface) and relaying the data to the UMTS network when connected by its 3G universal terrestrial radio access network (UTRAN) interface.

A mobile vehicle gateway refers to a dual-interfaced vehicle that relays data to the UMTS backhaul network from other vehicle sources. The mobile vehicle gateway is enabled with the dual interfaces of VANET IEEE 802.11p and the UMTS UTRAN networks. Commonly, the integration between VANET and different infrastructure networks is achieved through a static gateway that is fixed along the road. Conventionally, the static gateway is an access point in which the vehicles use for connection to the outer network. The main drawbacks of the static gateway are the cost associated with each gateway and the number needed to cover an area. The costs include the hardware, operational, installation, and maintenance costs. Moreover, due to the moving speed of the vehicles, the connection to this type of gateway is not stable. The vehicles may connect and disconnect frequently which hinder the seamless connection to be achieved. By contrast, the protocols based on the static gateway can only provide connectivity in areas where they have been deployed. Recently, protocols based on mobile gateway concept overcome the restriction of a static gateway in which the static gateways are replaced with mobile vehicles that function as mobile gateways.

Thus, this study proposed a new robust and trust mobile gateway selection (RTMGwS) protocol to obtain the benefit of different facilities, such as the continuous connection to the Internet and other mobile services when traveling on the road. Furthermore, this routing protocol has been designed to satisfy the requirement of the multiple applications of VANET, particularly in the case of the applications that required high security as well as the best quality of services. Particularly, the proposed RTMGwS routing protocol aims to provide four main contributions.

1. The RTMGwS protocol can efficiently expand the coverage service areas of the infrastructure communication technologies, such as WiMAX, UMTS, and LTE, as well as provide Internet connectivity for all participant VANET vehicles even if they are outside the limited coverage area of infrastructure base-station transceivers (BSTs).
2. The RTMGwS protocol can serve deferent VANET applications in terms of quality of service and security, whereas the link between sources and destination, i.e., UMTS-BST via the mobile gateway, has been selected based on the most critical routing parameters, thereby potentially improving the performance of different applications.
3. The RTMGwS can reduce the delay caused by a handover mechanism, whereas the VANET vehicles have a set of available alternative routes to always obtain seamless handover. Moreover, RTMGwS initially proposed at least one guaranteed mobile gateway to other mobile vehicles in a proactive procedure, thus reducing the cost of the gateway discovery mechanism introduced by source vehicles.
4. The RTMGwS protocol can provide seamless connectivity in case an infrastructure BST is disrupted or the service is weak. In this case, all VANET vehicles, which move within its coverage area, will lose the signal or experience bad services. The RTMGwS routing protocol adapts ad hoc technology with the concept of the mobile gateway and integrates with the infrastructure technology to efficiently overcome such a problem.

The rest of the paper is organized as follows. In Section 2, the related work is briefly discussed. Section 3 presents the RTMGwS protocol in detail. Section 4 discusses and analyzes the simulation results of RTMGwS protocol, and Section 5 presents the conclusion of the paper.

2. Related works

Several mobile infrastructure-based routing protocols that overcome the restriction of fixed road side units (RSUs) were proposed in the literature. Mobile infrastructure routing protocols use the concept of mobile gateways, in which RSUs are replaced with mobile vehicles that function as mobile gateways [10].

The authors in [11] proposed the mobile infrastructure-based VANET routing (MIBR). MIBR is a position-based reactive routing protocol in which buses are important during route selection and data transfer. The quality of transmission for every single road segment and the various transmission capabilities of different vehicles are considered in the protocol design. The design estimates the density of every road segment based on the bus line information. In MIBR, the source node uses global positioning system (GPS) to obtain the destination information. Every single bus includes two assorted wireless interfaces and a single interface that comprises other vehicles. During routing, the protocol approximates the next road segment and the hop counts and stores the information in a route table. When the packet is near a junction, the subsequent road segment is selected. This process consumes less bandwidth.

In [12], the authors recommended the mobile gateway routing protocol (MGRP) to increase the packet delivery ratio and decrease the average hop count by using both intervehicle- and infrastructure-based communication to route packets. Like other position-based routing protocols, MGRP assumes the presence of a GPS and digital map that enables each vehicle to build its neighbor table (including neighboring vehicles, directions, and speeds) that assist in routing. Furthermore, digital maps indicate the traffic load condition of roads. The MGRP is based on the concept of mobile gateways that are proposed in MIBR; the gateways use buses as a mobile gateway with a fixed route. However, their connectivity is limited by scheduling time and the region covered by the bus routes. Unlike MIBR, MGRP uses vehicles, such as taxis, as mobile gateways.

In [13], prediction-based routing (PBR) is focused on providing Internet connectivity to vehicles. In PBR, ordinary vehicles use the WLAN interface, and vehicles that have both WWAN and WLAN interfaces act as mobile gateways that connect to the Internet. The PBR algorithm assumes that every single vehicle is aware of its individual location via GPS or other services. The protocol benefits from significantly less inconsistency in vehicle movement patterns on highways to predict the duration and expiration of a route from a client vehicle to a mobile gateway vehicle. Before a route malfunction is predicted, PBR pre-emptively looks for a new direction to prevent the loss of service. Regardless of the efficiency of the PBR algorithm in the mobile gateway scenario, whether the situation is realistic remains unclear. The methods on how a vehicle can reveal its wireless Internet connection with others when that connection is remain unclear, although the incorporation of micropayments might be an interesting field of research. Internet providers who are charged for the use of roaming WAN-connected vehicles might be financially capable. However, additional evaluation might be needed to determine feasibility. Furthermore, the mobile gateway's wireless WAN connections must have sufficient bandwidth to support the demand of numerous client vehicles.

The authors in [14] proposed a mechanism that allows the vehicles to discover nearby gateways and select the best one based on several performance metrics. The metrics considered for gateway selection (GWS) are, number of hops to gateway, gateway through-

put, traffic load and route expiration time. The gateways were assumed to be fixed and placed alongside the road. The gateways use neighbor discovery protocol (UDP) to proactive broadcast its existence to 1-hop neighbor. The broadcast message carries important parameters that were used by the vehicles for GWS. Moreover, if the vehicle did not receive any gateway advertisement message, it reactively sends gateway solicitation message to discover the available gateways. When the vehicles received the gateway advertisement message, they extract the information included in the message and compute the gateway index for each gateway. Each metrics assign its weight depend upon the application requirement. In case of voice over Internet protocol (VoIP), delay is priority factor for this application. In order to achieve small delay, number of hops in metric should be given higher weight compare to other metrics. Moreover, for video streaming, throughput is crucial. This leads to assign highest weight to gateway throughput metric compare to other metrics. The mechanism improves 10-20% throughput of the system performance. However, using fixed gateway, especial in VANET scenario, increases the number of handover due to the high speed of the vehicles. This leads to frequency network disconnection which makes seamless connection difficult to be achieved.

By contrast, the study in [9] introduced a heterogeneous integration of VANET and 3G networks by using the mobile vehicle gateways. The proposed architecture, called clustering-based multimetric adaptive mobile gateway management (CMGM), aims to allow mobile data access for vehicles anywhere and anytime. For mobile vehicle gateway selection, three metrics were used, which include UMTS received signal strength (UMTS-RSS), mobility speed, and link stability. A clustering mechanism was used for the mobile gateway candidates (GWCs), and the clustering depends on the movement direction. In addition, UMTS-RSS and IEEE 802.11p transmission ranges are clustered. The GWCs that are close to the cluster center are always selected as the cluster head (CH). Ordinary vehicles use CHs to communicate with the UMTS network. Particularly, the proposed mechanisms can be performed on top of any VANET routing protocol. CMGM is investigated on top of the ad hoc on-demand distance vector (AODV) routing protocol. The proposed algorithm is complicated with respect to the cost of creation and the maintenance of the clusters for a speedy VANET environment. Moreover, the time and signaling traffic used for CH selection and clustering formation are bigger than those of data traffic exchange. Furthermore, CMGM focuses on the definition of a mechanism that selects the minimum number of optimal mobile gateways to ignore the bottleneck at the UTRAN channels rather than expand the coverage zone area.

In [8], the simplified gateway selection (SGS) scheme has been proposed to extend the coverage zone of the VANET network, and the calming of the frequent handover process provides a seamless connection to the UMTS infrastructure network. The SGS supposes that each vehicle equipped with UMTS-UTRAN interface connects to the UMTS-BST infrastructure mode and IEEE 802.11p interface to connect to the VANET mode. The source vehicles find mobile gateways and use three parameters in selecting the best mobile gateway, namely, UMTS-RSS, available route capacity, and route life time (RLS). In this study, the suggested solution follows the same integration architecture used in SGS. Moreover, the proactive strategy used the reactive strategy to assist the sources located far from the coverage services of UMTS-BST. The SGS scheme might be obtained on the top of any VANET routing protocol similar as [9]. Therefore, the SGS scheme is investigated in [8] along with both destination-sequenced distance vector (DSDV) and AODV. The SGS can increase the network coverage area by the integration of vehicles to the UMTS network. Nevertheless, it will suffer from high delays if the zone area of the VANET network is large. On the contrary, the connection over a long distance between source vehicles and selected mobile gateways lowered the transmission rate and yields to either longer periods of transmissions on the channel or several medium access control (MAC) retransmissions. Moreover, the proposed scheme in this study caused high overhead when the number of source vehicles is high.

3. Proposed Robust and Trust Mobile Gateway Selection (RTMGwS) routing protocol

In this section, the RTMGwS protocol is explained in detail. However, prior to the protocol's explanation, some assumptions used for this study are addressed. First, we assume that every vehicle is furnished with a positioning system and geographical map that allow it to reach the location and dimensions of the road as it forms an area for the zone's broadcast. Second, the vehicle's u coordination is denoted as (X_u, Y_u). Third, every vehicle could calculate its own speed V_u and direction θ_u. The vehicle links are recognized when their distance is less than their transmission range R. Fourth, the entire network node clock is synchronized, and thus the time duration may be obtained when the two nodes remain in contact after the two neighbor motion parameters are identified.

3.1. System model

The topology of our envisioned integration of VANET and 3G UMTS is depicted in Fig. 1. The architecture comprises IEEE 802.11p-based VANET vehicles, a UMTS Node B, and the main components of the UMTS core network. Communication over the VANET network is multihop, and VANET nodes communicate with each other on a peer-to-peer basis. The main components of the UMTS network are the general packet radio service (GPRS) support node (SGSN), radio network controller (RNC), gateway GPRS support node (GGSN), and BST [14]. VANET mobile gateway accesses the UMTS network via Node B BST using the UTRAN interface. UMTS network is connected to the external IP networks by GGSN. The GGSN is responsible for converting circuit-switched data from the external network to packet-switched data. SGSN is responsible for routing data packets to the correct RNC from GGSN and vice versa.

The prime objective of the architecture is to determine the mobile vehicle gateways, which can assist other vehicles move in the area where Internet is not accessible because of the BST disruption. As shown in Fig. 1, three VANET regions were observed under BSTs: A, B, and C coverage. These regions are termed as 3G active regions, where the UMTS signal strength is intense in BST A and BST C. However, if the BST B is disrupted, the UMTS signal strength is almost nonexistent. The active regions may overlap, depending on the intelligent transportation system (ITS) management. Vehicles, equipped with IEEE 802.11p and UMTS interfaces, lying within or moving into the 3G active region, are called candidate mobile vehicle gateways (CMGws). Ordinary vehicles (OVs) are those that move within the disrupted BST area. Among CMGws, a number of initial mobile vehicle gateways (I-MGws) per movement flew are selected using different parameters. The I-MGws aims to extend the UMTS-BST services by broadcasting their agent messages to the opposite direction of the route within a restricted broadcasting zone, and the OVs, which are moving towards them, will be aware of their existence. Some of the OVs are selected as relay vehicles in the RTMGwS routing protocol to rebroadcast the agent messages, which in turn assists the source vehicles to find the paths toward the I-MGw vehicles proactively. In addition to the proactive discovery, the reactive gateway discovery was enforced in the RTMGwS routing protocol to assist the vehicles that are located far from the I-MGw vehicles; thus, the agent-advertisement messages may not be received. Each of the discovery mechanism will be described in detail in the subsequent sections.

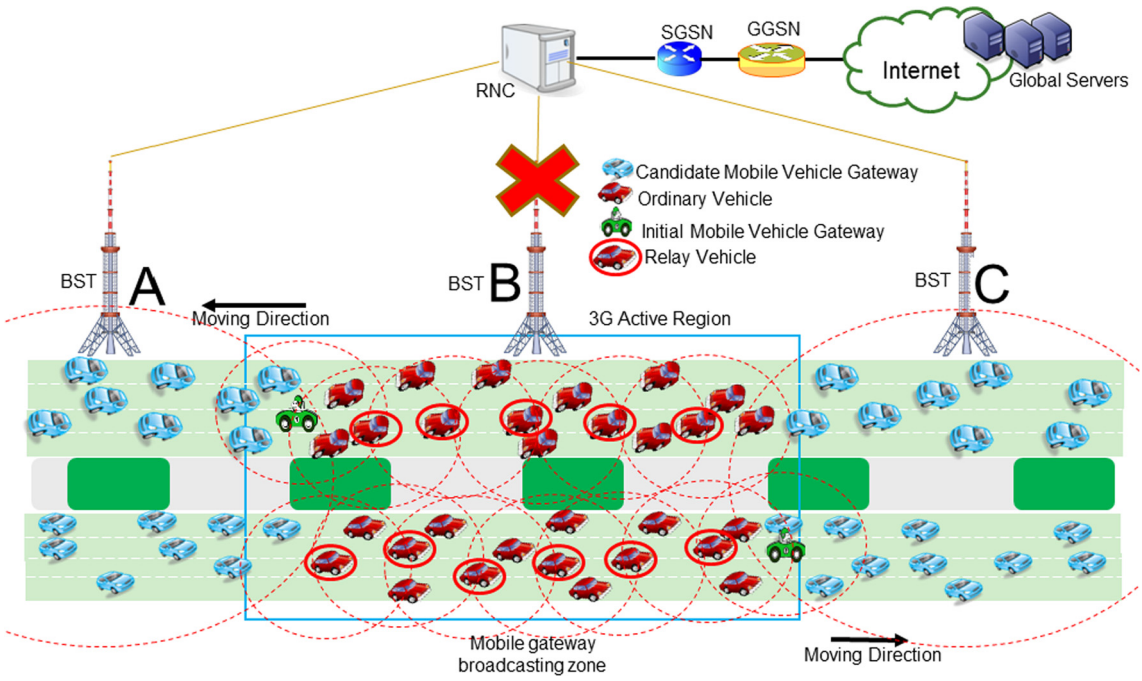

Fig. 1. Architecture of the proposed RTMGwS routing mechanism.

3.2. Proactive mobile gateway discovery mechanism in RTMGwS

Internet access is provided by mobile vehicle gateways located in the 3G active region of BSTs, and vehicles initially need to find these mobile vehicle gateways for communication. To accomplish the proactive gateway discovery task, we consider the optimized dissemination of alarm messages (ODAM) [15], which is based on geographical multicast and determines the multicast group following the driving direction and the positioning of the vehicles in a geographically restricted area using geo-casting capabilities. However, in this paper, we have proposed a new mechanism for the initial mobile gateway discovery using the optimization in [15], and the selected mobile gateway plays a role as I-MGw based on specific parameters. I-MGw periodically broadcasts gateway advertisement messages in a geographically restricted area that covers the non-signaling coverage zone between two UMTS-BSTs, as shown in Fig. 1. This method restricts the broadcasting within the specific area and prevents further broadcasting messages that exceed the concerned area, thereby exhausting the network resources.

Proactive mobile gateway discovery aims to propagate the advertisement messages in VANET through multiple hop fusion. The broadcast zone of a gateway is a rectangular box needs a message, originated from a certain preselected I-MGw vehicle, should not be broadcast outside the gateway zone. This area defined the maximum number of hops to the mobile vehicle gateway and is calculated based on the distance between BSTs, transmission range of the BSTs, and density of the vehicles (whether it is a highway or city with traffic congestion) [16].

In order to reduce the overhead during the gateway discovery process, a new mechanism of broadcasting messages that restricts broadcasts to a predefined geographical zone while allowing only some relays to rebroadcast the advertised messages is suggested. Each advertised message contains the I-MGw address, relay address, message sequence number, and broadcast zone, the stability parameters (sender position, sender speed, and sender direction) and are used by each mobile vehicle receiving the message to predict the link lifetime. Moreover, the advertised message contains the number of hops, route load capacity, and trust of each mobile vehicle. I-MGw initially sets the relay address to their own address; the route expiration time, route load capacity, and trust to a large value; and the number of hops to 0. The message structure is shown in Table 1. Moreover, Fig. 2 depicts the process of RTMGwS.

Table 1
Agent-advertisement message fields.

Field	Description
I-MGw	Address of initial mobile vehicle gateway
Relay	Relay address
SeqNo.	Message sequence number
Location	Geographical location of the sender
Speed	Speed of the sender
Direction	Direction of the sender
Z_m	Message broadcast zone
RLT	Life time of the route
NHop	Number of hops
LCap	Residual load capacity of a route
Trust	Trust of the path

The selection process of the proposed routing protocol consists of five main stages: initial mobile gateway selection, relay selection, weighting, route establishment, and handoff stage.

3.2.1. Initial mobile gateway selection

The initial mobile gateway selection is based on the traffic flow toward the BSTs. By contrast, once mobile vehicles enter the BST coverage zone, they calculate the UMTS-RSS, which was received from the UMTS-BST. If the UMTS-RSS is greater than a specific received signal strength threshold (RSS_{Th}), it indicates itself as I-MGW. Moreover, we have considered the trust parameter as the second condition in mobile gateway selection to obtain the most secured services of the other participated mobile vehicles, which are located in the VANET zone area (i.e., all mobile vehicles located toward the UMTS-BST coverage zone). The advantage of I-MGw selection is twofold. First, it expands the coverage area of the UMTS-BST seamlessly. Second, it can reduce the process of gateway discovery from the sources located toward the UMTS-BST coverage zone by providing at least one guaranteed initial mobile gateway to serve between the sources and BST.

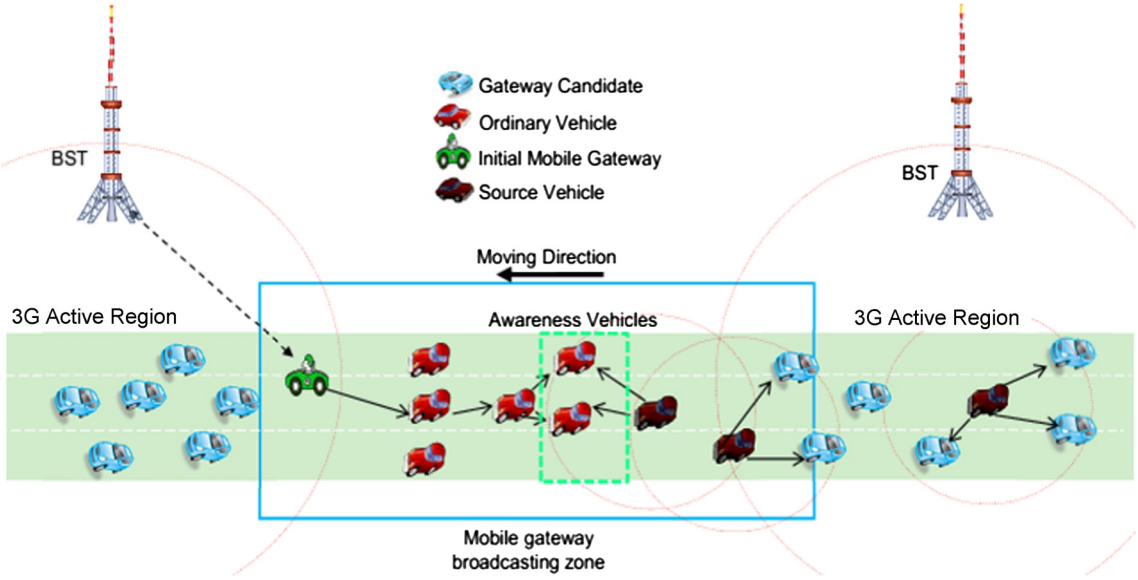

Fig. 2. Different cases of reactive mobile gateway discovery.

3.2.2. Relay selection

After indicating the I-MGw, the selection progress will turn to the relay selection stage. By contrast, if the mobile vehicle (MV) indicated itself as I-MGW, it broadcasts the agent-advertisement message in the opposite direction to all neighboring mobile vehicles within the predefined mobile gateway broadcasting zone. Each vehicle, upon receiving the agent-advertisement messages, retrieves the broadcast zone message information (see Table 1) and the direction of the sender from the received message. The received OVs calculate the robustness and the route's trustworthiness from the parameters integrated into the agent-advertisement message to select the next relay. The neighbor who received an ordinary mobile vehicle discards the agent-advertisement message if it is not located in the broadcast zone, the sender direction angle is different by more than $\pi/4$ [9], or the message $SeqNo = PrevSeqNo$. As stated earlier in the suggested routing protocol, not all vehicles rebroadcast advertisement messages because only certain vehicles identified as relays send such messages to different vehicles. RTMGwS routing protocol selects relays by the means of contention. However, the contention is based on robust and trust parameters to select the next relay. The robust parameter represents three different subsets of parameters: route life time (*RLT*), residual load capacity (*LCap*), and number of hops (*NHops*). In addition, the trust parameter is used to ensure that the selected relay is a trusted relay.

A. Robust parameters

The parameter that depends on vehicles mobility and traffic congestion variables in the calculation of route selection is the robust parameter in the current study.

1. Route Lifetime (RLT)

Hasty changes in VANET vehicles position cause the route to fail frequently [8,9,13,16]. We adapt the *RLT* prediction based on [13] and [8] functions as follows.

The creation of the agent-advertisement messages causes the mobile gateway to insert its position and velocity, thus setting $RLT = \infty$. As the message is received by *IV*, the information is extracted from the message (position and velocity). It will calculate the link life time (*LLT*) among the two closest mobile vehicles using Eq. (1).

$$LLT = \frac{R - |D_{sd}|}{|v_s - v_d|} \tag{1}$$

where D_{sd} is the distance between the source and destination within the communication range R. The complete distance between the closest vehicles and v_s and v_d is the adjacent vehicle velocities. If the *RLT* value in the advertising message is larger than *LLT*, the *RLT* field advertising message will be changed to a new value, or the present value will remain the same. *RLT* changes continuously until the advertising message reaches the *SV*. The *RLT* is contained in the advertising message; that is, the links' minimum lifetime. Equation (2) shows the RTL calculation, where n is the number of link.

$$RLT = \min \sum_{i=0}^{n} LLT_i \tag{2}$$

2. Available Load Capacity (LCap)

In the VANET-UMTS integration network, if the selected mobile gateway vehicle serves a number of vehicles more than its capability, a higher packet loss and delay are observed because of congestion on that selected gateway. In a multiple scenario, multiple routes can have common intermediate vehicles in the route from *SV* to *GV*. This process also causes a bottleneck on that route or on the mobile gateway and *IV* buffers. Thus, the *SV* selects the route based on the available *LCap* to overcome these problems.

LCap, or available load capacity, can be described as any vehicle's minimal available load capacity [17,8], which includes the *IVs* and *GV*. As the *IV* receives the agent-advertisement messages during the relay selection phase, the available load capacity is computed. If a vehicle x's maximum load capacity is $C_{\max}$ and the latest traffic load is TL_x, when handled by x, the vehicle x is $LCap_A$. The available load capacity is computed as follows in Eq. (3).

$$LCap_A = C_{\max} - TL_x - b \tag{3}$$

where the back-off value that gives the vehicle protection from overloading is b. The TL_x calculation can be based on the following Eq. (4).

$$TL_x = \sum_{j=1}^{s} Pr_j Ps_j \tag{4}$$

where TL_x is the vehicle$x$ latest traffic load that relays traffic from s traffic sources, and the average packet arrival rate and average

packet size of the traffic from source j are denoted by Pr_j and Ps_j individually. The overall capacity of the residual load $LCap_i$ of the route i is the vehicles' minimum available load capacity. *LCap* is computed based on Eq. (5), where j is in a route that includes *GV*.

$$LCap_i = \min \sum_{j=1}^{n} LCap_j \tag{5}$$

3. Number of Hops (NHop)

In network communication, a hop is one portion of the path between the source and destination. Data packets pass through intermediate vehicles and mobile gateway on the way. Whenever packets are passed to the next vehicle, a hop occurs. In calculating the number of hops in each path between the source and destination each time an intermediate vehicle receives a message, the vehicle modifies the routing table records, incrementing the number of hops by one. In certain cases, when the source vehicle transmits the data packet, it will transmit the packets through the path with a minimum number of hops.

B. Trust parameter

Trust parameter focuses on calculating the trust level of all participating mobile vehicles rather than on the vehicles' mobility conditions of the VANET network. This parameter aims to achieve reliable and secure communication from sources to destination. Thus, the work suggested by [18] and extended by [19] is used as the work's trust model in the current study.

Definition 1 *(Trust).* $Trust(u)$ is the representative of the vehicle u's trust score during the periodical time t. $Trust(u)$ range is $(0 \leq Trust(u) \leq 100)$. The vehicle's untrustworthy element is denoted by 0, and the most trustworthy vehicle is denoted by 100.

Definition 2 *(Direct trust).* If the transmission between vehicle A and vehicle u is m times throughout the periodical time t, the degree of ith time satisfaction is $S(u,i)$, $S(u,i) \in [0,1]$. The value denotes by 1 shows that the vehicle u absolutely satisfies vehicle A. At 0 value, the vehicle u completely dissatisfies vehicle A and is not trustworthy. $TF(u,i)$ is also assumed as the weight of ith transmissions. The direct trust of vehicle u is defined as

$$Direct_{Trust}(u) = \frac{\sum_{i=1}^{m} S(u,i) * TF(u,i)}{\sum_{i=1}^{m} TF(u,i)} \tag{6}$$

Definition 3 *(Indirect trust).* The indirect trust of vehicle u is measured based on the recommendations of other vehicles and is defined as follows:

$$INDirect_{Trust}(u) = \frac{\sum_{i=1}^{m} Tu(i) * Direct_{trust}(i)}{\sum_{i=1}^{m} Direct_{trust}(i)} \tag{7}$$

where $Tu.\ i.\ .$ is the direct trust of vehicle u relative to vehicle i, and $DirectTrust.\ i.\ .$ is the direct trust of vehicle i. The trust of vehicle u is given by

$$\begin{aligned} Trust(u) &= \alpha * Direct_{trust}(u) + \beta * INDirect_{Trust}(u) \\ &= \gamma * Trust_i(u) \end{aligned} \tag{8}$$

where $Trust_i.\ u.\ .$ represents the trust score collected for vehicle u during the last periodical time $t.\ .\ ,.\ .$, and $.\ .$ are the weights of direct trust, indirect trust, and trust scores, respectively, as collected during time $t.\ .\ ,.\ .$, and $.\ .$ range from 0 to 1.

Definition 4 *(Path trust).* The trust value of the ith path Pi is

$$TP_i = \Delta - \frac{\Delta - T_{\min}}{T_{\min} - \mu}, \tag{9}$$

where Δ is the average trust score of vehicles in the path calculated using Eq. (8). $T_{\min}$ is the minimal trust value in the path. μ. is the boundary value between distrust and trust. $T.\ Pi.\ .$ is the trust value of the ith path P_i.

3.2.3. Simple Adaptive Weight (SAW) technique

For selecting the best relay using the above-mentioned metrics, a multimetric relay selection method based on SAW technique has been proposed to satisfy the different attributes or metrics, such as the weight of importance level, score evaluation, and relay outranking based on the priority [20,21]. In SAW technique, each metric can have either a positive or negative criterion. In this case, *RLT, LCap*, and *Trust* are metrics with positive criteria, which optimality increase with increasing criterion values. On the other hand, the *NHop* is a metric with negative criteria. The best score of any criterion is 1 and the worst is 0.

Metric with a positive criterion

$$S_i = \frac{M_i - M_{\min}}{M_{\max} - M_{\min}} \tag{10}$$

Metric with a negative criterion

$$S_i = \frac{M_{\max} - M_i}{M_{\max} - M_{\min}} \tag{11}$$

where S_i is the scaled metric value of the metric; $M_{\max}$ is the maximum value of the metric; $M_{\min}$ is the minimum value of the metric; M_i is the value of the metric.

After normalizing each metric to the comparable scale, a user-weighting factor should be defined to specify the priority in relation to metric significance. The neighbor *OV* calculates the weight of each forwarded I-MGw messages as

$$W_i = \sum_{i=1}^{4} \left(M_i[PF] * S_i \right) \tag{12}$$

where *PF* is a priority factor selected by the neighbor *OV*.

For the contention over all I-MGw vehicles that result from the calculation of SAW, the timer set stage applies. By contrast, the neighbor *OV* sets the timer $t_i(W_i)$ for each received I-MGws' advertisement messages based on the weight W_i of each I-MGw vehicle as follows.

$$t_i(W_i) = T(1 - W_i) \tag{13}$$

where T is the maximum forwarding delay [14,18].

When receiving an agent-advertisement message, the neighbor *OVs* will wait for time that is computed by the timer before rebroadcasting the message as shown in Eq. (13). If during this time it receives a message that originated from the same I-MGw with the same message *SeqNo.* (that is, another mobile vehicle has retransmitted the message), it will cancel the timer and discard both messages. Otherwise, it re-broadcasts the message after the timer has expired. In case there are more than one I-MGw vehicles broadcasting messages, the proposed protocol will select only one relay for each I-MGw to prevent flooding the network by rebroadcasting the messages for several I-MGw vehicles from all neighbor OVs.

3.2.4. Route establishment

When the mobile source vehicle receives an advertisement message, it performs the route establishment process to the UMTS-BST by pre-selected I-MGws. Each source vehicle will have access to one or more I-MGw presented proactively by relays in this manner, and then the source vehicle should decide which gateway it must connect with. The decision, at this point, will perform identically to the procedure of weight computational stage in the multimetric relay selection method based on the information enclosed in each relay vehicle table.

The I-MGw vehicle will be selected based on the SAW calculation with a maximum weight W_i in the overall received I-MGw messages. Notably, the route establishment to I-MGw vehicles does not consider the I-MGw-RSS as a parameter in the selection mechanism of the proposed RTMGwS routing protocol because the I-MGw vehicles were previously selected with the I-MGw-RSS > RSS_{Th} and move toward the UMTS-BST. The I-MGw-RSS increases whenever it moves toward the UMTS-BST as stated in [8,9].

Therefore, the I-MGw-RSS parameter is not a valued parameter because the I-MGw-RSS increases gradually. Furthermore, the services of the pre-selected I-MGw vehicle will be migrated to its relay periodically by a handover mechanism. Algorithm 1 clarifies the proposed multimetric relay selection method based on SAW technique for proactive mobile vehicle gateway discovery.

3.3. Reactive mobile gateway discovery mechanism in RTMGwS

Reactive gateway discovery is executed to associate the proactive gateway discovery in two main cases; (1) a source vehicle does not receive any advertisement messages from its neighbors, and (2) several vehicles located in the coverage area of the BST have enabled their UTRAN interfaces as seen in Fig. 2.

In this case, gateway solicitation messages (*GWSOL*) are reactively sent until they reach either a vehicle that is already aware of a route to an *I-MGw* called awareness vehicles (*AVs*) or *CMGws* vehicles directly. *CMGws* are assigned to each vehicle moving within the UMTS network, and its UMTS-RSS and trust are larger than the RSS_{Th} and $Trust_{Th}$ thresholds, respectively. When the *GWSOL* message reaches the *AV*, the route reply (*RRep*) message is sent directly to the vehicle that is willing to connect to the Internet. If more than one *RRep* message exists, the source vehicle simply selects the most robust and trusted route to the I-MGw similar to the procedure followed in the Multi-Metrics Relay selection algorithm.

However, when the route request (*RReq*) message reaches the *CMGws* directly, the *RRep* message is sent back to the vehicle. Upon receiving the *RRep* messages from more than one *CMGw* vehicle, both robust and trust parameters will be considered to select the optimal path to the *CMGw* vehicles. Moreover, we followed the same procedure proposed in [8] in the reactive gateway discovery by using the proposed parameters in our study to select the optimal mobile gateway; the same handover mechanism will be performed as well. The only difference is that broadcasts can be stopped when the *GWSOL* message reaches an *AV* or reaches a *CMGw* vehicle. Algorithm 2 of selecting the optimal mobile gateway reactively is shown as follows.

3.4. Handoff mechanism

In order to perform a seamless handover over different selected I-MGws, we have considered that each relay, once it enters the coverage zone of UMTS-BST, may it selected to play a role as I-MGw as seen in Fig. 1. Since it already established a route to number of sources vehicle, no more advertising routing packets need to establish a new route which it in turn caused unnecessary bandwidth consumption. Therefore, relays once located inside the coverage zone of UMTS-BST, it will calculate the UMTS-RSS received from UMTS-BST. If the UMTS-RSS greater than RSS_{Th}, it indicates itself as I-MGw. However, in such case, it is not required to achieve the condition of trust parameter where it has been achieved in advance in relay selection stage. After selecting the relay to play a role as I-MGw then the old I-MGw stop broadcasting the advertisement messages.

4. Performance analysis

The effectiveness of the RTMGwS routing protocol was evaluated by combining the SUMO mobility [22] and NS2 [23] network simulators. The SUMO simulator is used to generate the vehicular mobility model used in evaluating the RTMGwS routing protocol, whereas NS2 is used to measure the network performance of the RTMGwS routing protocol. The NS2 version patched with NSMIRICLE [24] was used to support multiple interfaces in a wireless node in the evaluation process. The mobility file obtained from the SUMO was used in NS2 to define the node motion during the simulation.

The simulation parameters used in this study are the same as those used in [8] and [9], both of which are considered benchmarks to compare with the current proposed protocol. However, our study expanded the simulation area over the suggested area in [8] and [9] to increase the probability of connectivity of mobile vehicles located over large dead spot distance areas. The current research problem focuses on issues related to the connectivity over a long-dead spot distance area. Moreover, the simulation time is selected to be sufficiently long that it can potentially roam the entire distance area by mobile nodes as seen in Table 3. We compared RTMGwS with two different strategies of mobile gateway discovery: cluster-based and reactive-based. The cluster-based multi-metric adaptive mobile gateway management mechanism over AODV (CMGM-AODV) routing protocol was selected as one of the cluster-based benchmarking routing protocols to be compared with our routing protocol [7]. The simplified gateway selection over AODV (SGS-AODV) routing protocol was also selected as a reactive-based benchmarking routing protocol in the present study [8]. Moreover, both CMGM-AODV and SGS-AODV were modified by adding the trust parameter of path selection beside their own parameters to conduct a fair comparison.

Hence, two more benchmarking routing protocols are applied: extended MGM over AODV with trust-level (CMGM-AODV-trust) routing protocol and extended SGS over AODV with trust-level (SGS-AODV-trust) routing protocol. The priority factor values of each metric are assigned as 26.8%, 25.5%, 24.9%, and 22.9% for *Trust*, *NHops*, *RLT*, and *LCap* parameters, respectively. These values are obtained after many attempts and error experiments to determine the optimal priority factor of each metric in the gateway selection. Four performance metrics were used to measure the efficiency of the proposed algorithm, which are average end-to-end delay, packet delivery fraction, throughput, and routing overhead which are defined as follow [25].

1. **Average end-to-end delay:** This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is d_i, and the number of packets received by the destination node is $pktd_i$. The average end-to-end delay of the application traffic n is obtained as:

$$Average\ end\text{-}to\text{-}end\ delay = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{pktd_i} \tag{14}$$

BEGIN ALGORITHM 1

Based on each traffic flow of *MVs:*
when the *MV* enters the coverage area of UMTS-BST **do**
  MV calculates the *UMTS-RSS*:
  if *MV-RSS* ≥ RSS_{Th} and *MV-Trust*≥ $Trust_{Th}$ **then**
    MV is indicated as the *I-MGw* vehicle and broadcasts *AGENT-ADVERTISEMENT MESSAGE* within the geographical zone Z_m area (including *I-MGw-addr*, *Relay-Addr*, Z_m, *S, P, D, Trust, NHop, RLT, LCap*);
  end
end
when receiving *AGENT-ADVERTISEMENT MESSAGE* by *OV;* **do**
  if *MV* inside the Z_m area and moves in the same direction as *I-MGw* and *SeqNo* > *PrevSeqNo*.
    then update the *AGENT-ADVERTISEMENT MESSAGE* information by calculating *Trust, NHop, RLT, LCap;* **do**
    calculate the scale metric S_i:
      for each metric, M_i of the *I-MGw*$_i$, where $1 < i < 4$ **do**
        if *Mi [CRITERION] is POSITIVE* **then**

$$S_i = \frac{M_i - M_{min}}{M_{max} - M_{min}}$$

        else if
          Mi[CRITERION] is NEGATIVE **then**

$$S_i = \frac{M_{max} - M_i}{M_{max} - M_{min}}$$

        end if
      end for
    then the weight of each *I-MGw*$_i$ calculated by $W_i = \sum_{i=1}^{4}(M_i[PF] * S_i)$, and the next *Relay*$_i$ is selected with the maximum weight of *I-MGw*$_i$ to rebroadcast the *AGENT-ADVERTISEMENT MESSAGE*;
    Timer set by $t(W_i) = T(1- W_i)$;
      if Timer expired; **do** the selected *Relay*$_i$ rebroadcast the *AGENT-ADVERTISEMENT MESSAGE* of *I-MGw*$_i$;
    end if
  else if
    MV outside the Z_m area or the difference between its direction angle and direction of the sender is more than $\pi/4$ or *SeqNo. = PrevSeqNo*, **then**
    discard the *AGENT-ADVERTISEMENT MESSAGE;*
  end if
  do again to select the next *Relay*$_i$*;*
end
When the selected *Relay* enters the coverage area of *UMTS-BST*, it calculates the *UMTS-RSS*:
  if *Relay*$_i$*-RSS* ≥ RSS_{Th}*;* **then**
    Relay$_i$ is indicated as *I-MGw*$_i$ and sends *THANKS_MESSAGE* to the old *I-MGw;*
  end if
end

END ALGORITHM 1

2. **Packet delivery fraction:** This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, $pktd_i$ is the number of packets received by the destination node in the ith application, and $pkts_i$ is the number of packets sent by the source node in the ith application. The average packet delivery ratio of the application traffic n is obtained as:

$$Packet\ delivery\ fraction = \frac{1}{n}\sum_{i=1}^{n}\frac{pktd_i}{pkts_i} \tag{15}$$

3. **Throughput:** This is defined as the total amount of data (b_i) that the destination receives them from the source divided by the time (t_i) it takes for the destination to get the final packet. The throughput is the number of kilobits transmitted per second. The throughput of the application traffic n is obtained as:

$$Throughput = \frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{t_i} \tag{16}$$

4. **Routing overhead:** This metric represents the ratio of the amount of routing-related control packet transmissions to the

BEGIN ALGORITHM 2

An *SV* broadcasts the *GWSOL* by using the 802.11p interface.
when the *GWSOL* packet is received by a *MV* **do**
  if *MV-TYPE==AV* and moves in the same direction as *SV,* **then**
    AV sends an *RRep* message (including *I-MGw-addr*, *Relay-Addr*, *Trust, NHop, RLT, LCap*);
  else if
    MV-RSS≥RSS_{Th} and *MV-Trust*≥ $Trust_{Th}$ and moves in the same direction as *SV,* **then** it is indicated as an *I-MGw* vehicle and sends the *RRep* (including *Trust, NHop, RLT, LCap*);
  else
    continue to broadcast the *GWSOL* messages to neighboring vehicles;
  end if
    discard duplicate *GWSOL* messages from the same source (if any);
end
when the *SV* receives the *RRep* message **do**
  calculate the scale metric S_i:
  for each metric, M_i of the *I-MGw* vehicle, where *1<i<4* **do**
    if M_i*[CRITERION] is POSITIVE,* **then**

$$S_i = \frac{M_i - M_{min}}{M_{max} - M_{min}}$$

    else if
      M_i *[CRITERION] is NEGATIVE,* **then**

$$S_i = \frac{M_{max} - M_i}{M_{max} - M_{min}}$$

    end if
  end for
end
the *SV* calculates the weight of each *I-MGw*$_i$ vehicle by $W_{I-MGwi}=\sum_{i=1}^{4}(M_i[PF] * S_i)$ **then**
SV selects the optimal mobile gateway with the maximum weight;

END ALGORITHM 2

Table 2
NS2 simulation parameters.

Simulation parameter	Value
Simulation area	1,500 ∗ 14,000 (m^2)
Channel	Channel/WirelessChannel
Radio-propagation model	Propagation/TwoRayGround
Network interface	Phy/WirelessPhyExt
MAC interface	Mac/802 11Ext
Interface queue	Queue/DropTail/PriQueue
Antenna type	Antenna/OmniAntenna
UMTS-RSS threshold	−94 dB m
UMTS-BST transmission range	8 km
Simulation period	2,000 s

Table 3
SUMO mobility parameters.

Mobility parameter	Value
Road type	Highway
Number of lanes	2 lanes
Maximum speed	10 m/s to 35 m/s
Vehicle number	60 to 160

amount of data transmissions. Here, cpk_i is the number of control packets transmitted in the ith application traffic, and pkt_i is the number of data packets transmitted in the ith application traffic. The average routing overhead of the application traffic n is obtained as:

$$Routing\ overhead = \frac{1}{n}\sum_{i=1}^{n}\frac{cpk_i}{pkt_i} \quad (17)$$

The remainder of the simulation parameter values are shown in Tables 2 and 3 respectively.

Results of the packet delivery fraction for the proposed RTMGwS routing protocol and four other benchmarking routing algorithms in terms of the number of mobile vehicles are presented in Fig. 3(a). These results show that by increasing the number of mobile vehicles, all the algorithms show increments in their packet delivery fraction. The results emphasize that the best performance was achieved by the RTMGwS routing protocol in the dense area with 160 vehicles. Moreover, the figure curve shows that the packet delivery fraction of the SGS-AODV-trust and CMGM-AODV-trust routing protocols increase marginally and approach the performance of our proposed routing protocol. This result is predictable because the large number of mobile vehicles decreases the probability of transmission failure and more possible paths can be used to reach the destination. However, the proposed RTMGwS routing protocol shows improvement in terms of the packet delivery fraction over the SGS-AODV-trust, CMGM-AODV-trust, SGS-AODV, and CMGM-AODV for the different vehicle numbers (i.e., from 60 to 160 mobile vehicles). This condition is due to the selected mobile gateway periodically advertising gateway messages and the received mobile vehicles updating their

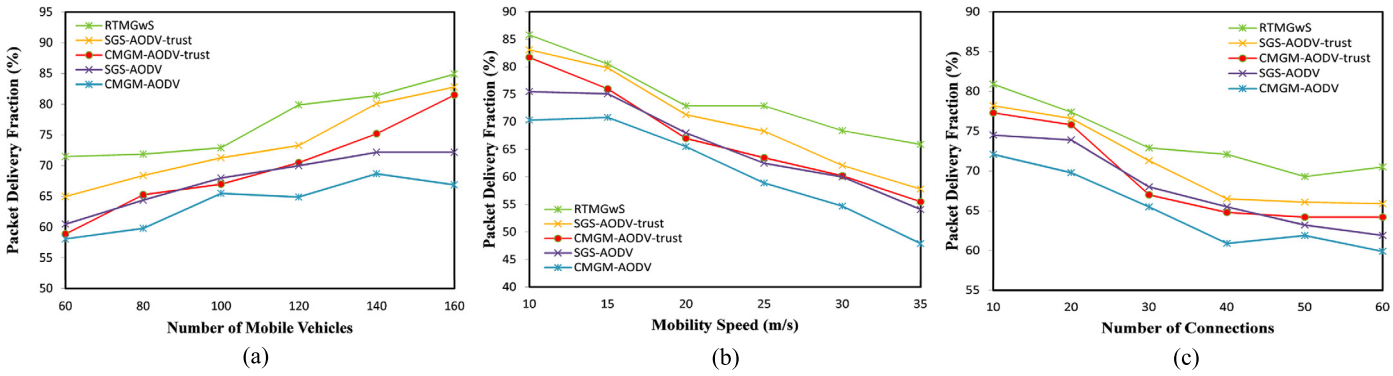

Fig. 3. Packet delivery fraction versus: (a) number of mobile vehicles, (b) mobility speed, (c) connection number.

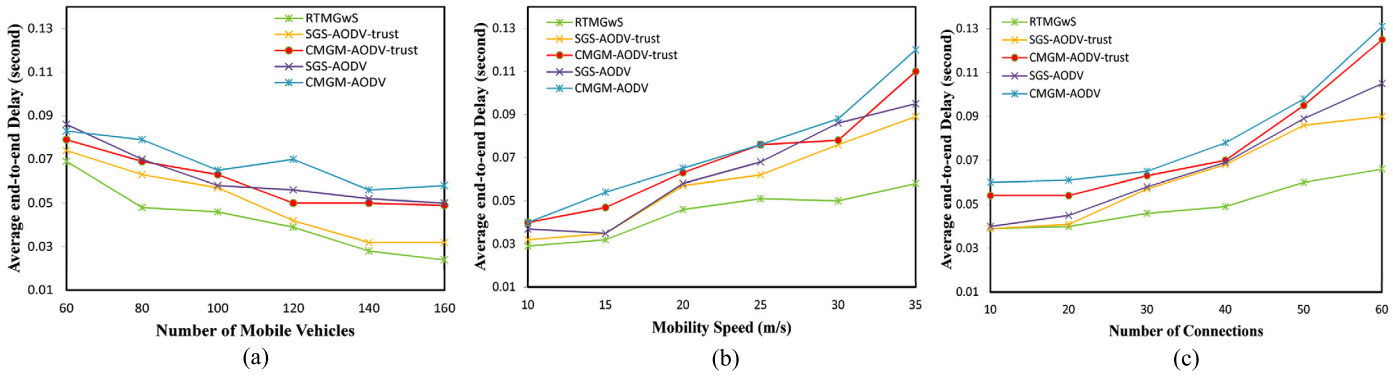

Fig. 4. Average end-to-end delay versus: (a) number of mobile vehicles, (b) mobility speed, and (c) connection number.

route entry in RTMGwS routing protocol. Therefore, the mobile nodes are more likely to have fresher and more optimum routes to a mobile gateway, thereby minimizing the risk for link breaks.

Fig. 3(b) shows the results by varying the mobile vehicle speed. Increasing the speed will result in links with shorter lifetimes, so links become more easily broken. Therefore, all the algorithms show a slight decrease in the packet delivery fraction when increasing the vehicle speed from 10 m/s to 35 m/s. This result also shows that the decrement of the packet delivery fraction in RTMGwS is not as high as that of the other routing protocols when the mobility speed increases to 35 m/s.

All routing protocols show a decrease in the packet delivery fraction, whereas the connection number increases from 10 to 60 as seen in Fig. 3(c). This scenario is due to more connections that exist when more packets will be transmitted in the network, thereby causing a higher occurrence of congestion and packet loss. However, the proposed RTMGwS routing protocol has the lowest percentage of decrement compared with the other four routing protocols.

All the routing protocols show a slight decrease in the average end-to-end delay when the number of mobile nodes increased from 60 to 160, as shown in Fig. 4(a). This scenario is due to the larger number of mobile vehicles minimizing the time spent to recover the link breakages because more path options are available to reach the destination. Similar to the case of packet delivery fraction, CMGM-AODV-trust and CMGM-AODV clearly shows the worst performance again in the end-to-end delay. This condition is ascribed to the longer time that they spend in clustering formation and cluster head selection. Each time the cluster head moves away from the cluster, a new cluster head must be elected. The processes of cluster head formation require considerable time to elapse before they are finished. Moreover, the mobile gateway election process involves only candidate mobile vehicle gateways inside the cluster to be selected as probable mobile gateways. Thus, such instances where the elected mobile gateway is no longer inside the present cluster results in the recurrence of the entire process of mobile gateway discovery and cluster head election. Therefore, the mobile gateway election delay for the CMGM-AODV-trust and CMGM-AODV routing protocols significantly increments. SGS-AODV-trust and SGS-AODV perform better than CMGM-AODV-trust and CMGM-AODV. The proposed RTMGwS routing protocol performs best among all protocol types. The main reason the RTMGwS routing protocol performs better than do the other routing protocols is because it can store updated optimum multiple paths that can serve as backup paths.

Fig. 4(b) shows the results of varying the mobile vehicle speed from 10 m/s to 35 m/s. Incrementing the speed can generate links with shorter lifetimes between each pair of the intermediate nodes, which result in less stable routes. Such routes with short lifetimes cannot maintain a route with a large number of hops. The likelihood of link breakage unexpectedly increases. Therefore, all routing protocols show a significant increase in the end-to-end delay because the mobility speed increases. This scenario is due to the fresher periodic mobile gateway information spreading within the network stored and updated in each mobile node table. Hence, less delay is obtained when the topology changes and the first selected path is no longer available. Nevertheless, the average delay in the case of the SGS-AODV-trust and SGS-AODV protocols increases significantly when the mobility speed increases. This condition is due to the long time consumed between the broadcasting *RReq* messages and received *RRep* messages, especially when frequent handoff occurs in long distance routes. Increasing the mobility speed in the case of CMGM-AODV-trust and CMGM-AODV routing protocols results in an increasing reformulation of clusters and re-selection of the cluster head, which then leads to more time spent to elapse such processes. Thus, this protocol shows the worst average end-to-end delay performance among all routing protocols.

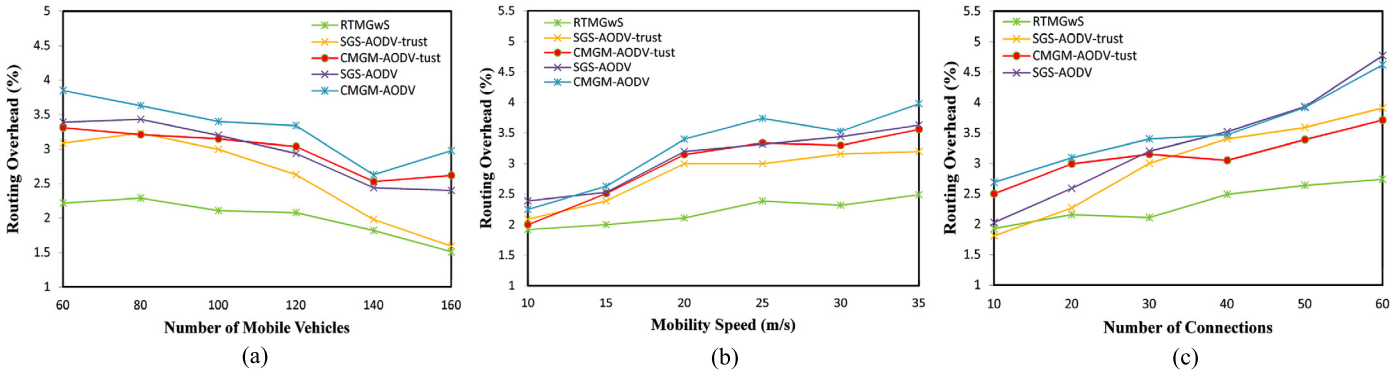

Fig. 5. Routing overhead versus: (a) number of mobile vehicles, (b) mobility speed, and (c) connection number.

Fig. 4(c) shows that the average end-to-end delay for all routing protocols increased when the traffic load increased as expected because the increasing traffic load (concerning the different numbers of connection from 10 to 60) means more collisions, retransmissions, and route recovery. Analyzing the result in Fig. 4(c) shows that the difference between RTMGwS and SGS-AODV-trust is negligible in a light traffic load from 10 to 20 connections, whereas the figure curve is indicative of a significant increase in the average end-to-end delay for SGS-AODV-trust compared with RTMGwS. On the one hand, the average end-to-end delay was initially expected to have been different for the SGS-AODV-trust routing protocol when compared with the RTMGwS. The SGS-AODV-trust protocol must perform better because it generates less overhead given the reactive strategy used in its gateway discovery. Consequently, this should cause a lesser number of collisions. On the other hand, the SGS-AODV-trust protocol must perform worse because it does not send periodic advertisements unlike in RTMGwS, which would provide fresher optimum routes to the mobile gateways in long-term connectivity. Given that several other aspects should be considered, the mechanism of the efficient dissemination of gateway messages by means of a minimum number of intermediate vehicles (i.e., relays) has a significant effect on the results.

CMGM-AODV-trust and CMGM-AODV performed the worst in terms of average end-to-end delay against the other three routing protocols as expected. This result can be explained by the same reason for the case of packet delivery fraction, which transmit the data packets in CMGM-AODV-trust and CMGM-AODV through blocked routes or overloaded mobile gateways. Thus, a long buffering time and high delivery delay occur. Similar to the case of packet delivery fraction, SGS-AODV and CMGM-AODV evidently performed the worst again in the end-to-end delay because they did not consider the trust value of the path nodes. Therefore, they were unable to avoid low-trust nodes. The bad experience of packets being dropped by malicious nodes in the route acted as an implicit signal that the network was congested, and it may have caused the source vehicles' attempt to locate another path toward the mobile gateway. SGS-AODV and CMGM-AODV experienced frequent route recovery, thereby resulting in high packet end-to-end delay.

Regarding the routing packet overhead, all routing protocols were evaluated using different network density scenarios. The number of mobile vehicles varied from 60 to 160 vehicles. Fig. 5(a) shows that all the routing protocols decremented the routing packet overhead as the number of mobile vehicles in the network increased. Increasing the number of mobile vehicles lowers the routing packet overhead because additional possible paths can be selected to reach the destination. Thus, the possibility of regenerating route messages that leads to high routing packet overhead can be lowered. The reason why the RTMGwS has less packet routing overhead is due to the efficient selection mechanism of minimum relays to rebroadcast the messages of the preselected mobile gateways. This mechanism helps to decrease flooding in the network by unnecessary messages.

Hence, the packet routing overhead decreases during the gateway discovery process, especially in the case of link breakages in a sparse area. By contrast, SGS-AODV-trust obtained good packet routing overhead in a dense area, whereas it achieved the worst one in a sparse area as shown in Fig. 5(a). This scenario is due to the reactive gateway strategy used in SGS-AODV-trust performing well, especially when a large number of paths are available to reach the destination. Given the connection mechanism applied in the CMGM-AODV-trust and CMGM-AODV routing protocols, a significant routing packet overhead was achieved. All mobile vehicles must adopt a cluster head to communicate with UMTS-BST even if they are located inside its coverage zone services. Therefore, the hall-integrated network is flooded by routing messages either inside or outside the UMTS-BST coverage zone. This condition may be the reason behind the worst result in terms of the packet routing overhead against the other three routing protocols.

Fig. 5(b) shows that the RTMGwS routing protocol obtained the best packet routing overhead with respect to the mobility speed. Low vehicle motion seemed to lead to a more stable network. To a certain extent, all algorithms show a comparable performance in the speed period between 10 m/s to 15 m/s. However, the routing overhead increment varies in each routing protocol when the mobility speed increments. This condition can be explained by two reasons. The first reason, as previously explained, is that the proposed efficient relay selection can help propagate the most significant information to all mobile vehicles through the messages received by the selected relays rather than flooding the network with unnecessary messages. The second reason is that all mobile nodes in RTMGwS have routes that are fresher and more optimal to a mobile gateway entry in their routing tables. The entire network must no longer be flooded with route messages again for new path establishment, which enables a seamless handover.

However, the network was overflowed by routing messages in SGS-AODV-trust because of the frequent handover process at a high mobility speed. Similarly, a significant number of routing packets in CMGM-AODV-trust must search for a cluster head because CMGM-AODV-trust experiences frequent reformulation of clusters at a high mobility speed. In terms of packet routing overhead, the routing overhead in RTMGwS is dominated by the periodically broadcasted mobile gateway messages unlike the amount of data packet sent by the source vehicles. Therefore, the RTMGwS protocol was evaluated based on different connection numbers, and its performance was compared with the performance of the other four routing protocols simulated in the same environment.

The results in Fig. 5(c) show the trade-off performance of all routing protocols in terms of the routing packet overhead by varying the connection number from 10 to 60 connections. Notably,

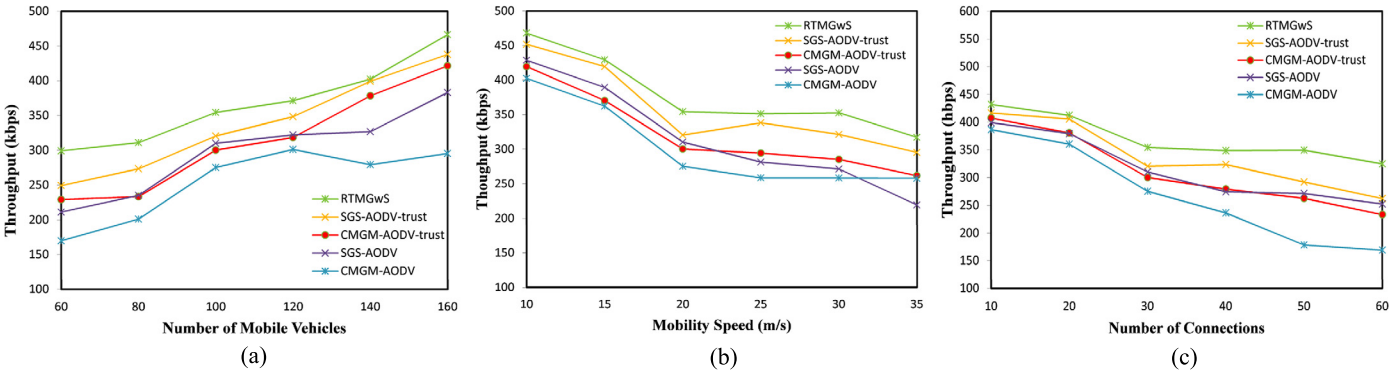

Fig. 6. Throughput versus: (a) number of mobile vehicles, (b) mobility speed, (c) connection number.

the packet routing overhead is relatively lower in all routing protocols for extremely light traffic loads of data packets. Moreover, the figure curve shows a positive record for the SGS-AODV-trust when the connection number varied from 10 to 20 connections when compared with the other four routing protocols. This result is predictable because mobile vehicles in SGS-AODV-trust send route messages on demand when a connection is required. Hence, it generates less packet route overhead. However, all algorithms obtained high packet routing overhead increments against our proposed RTMGwS routing protocol when the traffic load of the data packets is high. This scenario is due to the facilities provided by RTMGwS in performing seamless handover without flooding the network as described earlier. This approach provides a significant performance in high traffic load in terms of the packet routing overhead. Nevertheless, the proposed handover process in the case of SGS-AODV-trust affects the packet routing overhead where all the reactive mobile gateway mechanisms should be repeated once each handover process occurs. The routing packet broadcasts synchronously increase when the source vehicles increase, which causes a large number of collisions and generates a high packet route overhead. Similarly, signaling traffics adopted for cluster head selection and clustering formation in the CMGM-AODV-trust are larger than those of the data traffic exchange. Thus, high collisions occur and a significant packet routing overhead is observed. However, CMGM-AODV-trust obtained a better routing overhead compared with SGS-AODV-trust in the high traffic load of data packets because it was proved by the results shown in Fig. 5(c).

Overall, the worst packet routing overhead results were achieved by SGS-AOVD and CMGM-AODV among all the routing protocols based on the aforementioned scenarios. This result is due to the possible need for SGS-AODV and CMGM-AODV mobile vehicles to generate more route messages when the current path is no longer available because of the node mobility or route packets dropped by misbehaving nodes. Thus, the nodes are prevented from having a route to the destination. This condition can lead to high packet routing overhead in SGS-AOVD and CMGM-AODV.

Fig. 6(a) shows that by increasing the number of mobile vehicles, all the routing protocols show throughput improvement because a larger number of mobile vehicles results in a higher possibility of a broken link to be re-established. Thus, higher throughput occurs in the network. RTMGwS outperforms the other algorithms because of the significant performance of RTMGwS in both dense and sparse areas, in which multiple path to the mobile gateway are available to the intermediate vehicles all the time.

The mechanism of gateway discovery used in SGS-AODV-trust and SGS-AODV routing protocols performs worse in a sparse area where the route breakages redundantly occur. Furthermore, a few mobile vehicles generate few divergent clusters in CMGM-AODV-trust and CMGM-AODV. The selected mobile gateways will be overloaded with data packets when a few clusters have insufficient available mobile gateways, some of which will be discarded and ultimately affect the throughput.

Fig. 6(b) results show a negative throughput trend for the RTMGwS routing protocol when the mobility speed increases. However, increasing the mobility speed of mobile vehicles affects all five routing protocols in a similar manner. Thus, the throughput rapidly decreases for all underlying protocols when the speed of the mobile vehicles increases from 10 m/s to 35 m/s. The reason behind such throughput outperformance of RTMGwS in different mobility speeds against all other four underlying protocols is because of different aspects. One aspect is the selection mechanism for the minimum and efficient relays hop by hop to prevent flooding in the network and offer different routes to an optimum mobile gateway in advance for all mobile vehicles. A reactive selection of the optimal mobile gateway in SGS-AODV-trust and flooding the network by signaling traffic are avoided, and the time consumed for clustering formation and cluster head selection in CMGM-AODV-trust is decreased. Moreover, decision-making in RTMGwS merges different metrics by considering both the robust and trust levels of the route, which then produces a more holistic routing decision for route selection. Therefore, the larger amount of data packets can be sent through the most robust and trusted route. Furthermore, the capability of storing multiple paths in vehicle routing tables provides a faster and seamless handover in case of topology changes in high mobility speed without flooding the network by further routing packets in the gateway discovery. Thus, higher throughput is achieved in the RTMGwS routing protocol.

The throughput variations against the connection number of the five routing protocols are shown in Fig. 6(c). Increasing the connection number provides more opportunities for building route blocks. Therefore, finding an available route becomes more challenging. The figure curve indicates that the throughput overall routing protocols is high when the traffic load is light, but it decreases as the traffic load increases. Hence, the first set of readings in the figure does not show a large difference in the throughput achieved by the five protocols. However, all the routing protocols show a progressive decrease in throughput as the connection number increases.

The worst throughput was obtained by CMGM-AODV-trust and CMGM-AODV when compared with the other three routing protocols. This result was due to all source vehicles in CMGM-AODV-trust and CMGM-AODV, which use a cluster head to communicate with UMTS-BST, even if they are situated inside its coverage zone. Therefore, the higher the signaling traffic, the more time is spent in formulating the cluster and cluster head selection. This condition generates low throughput. SGS-AODV-trust and SGS-AODV protocols allowed all source vehicles inside the UMTS-BST coverage zone to communicate directly in RTMGwS, thereby decreasing the delay and packet loss caused by frequent network disconnection. Moreover, it lowered the network overflow.

The results presented in Figs. 6(a), 6(b), and 6(c) depict the scenarios of network density, mobility speed, and connection number against throughput, respectively. The results show the effects of implicating the trust parameter in the significant performance of CMGM-AODV-trust and SGS-AODV-trust compared with CMGM-AODV and SGS-AODV. However, CMGM-AODV and SGS-AODV recorded the worst throughput results in the different scenarios because both may have nodes in their paths that have low trust. Therefore, the possibility of maintaining a stable path to the destination is low. Thus, CMGM-AODV and SGS-AODV must flood the network with route messages to find a new path that leads to a higher delay and packet drop. Thus, this scenario results in lower throughput.

5. Conclusion

This study proposes a new routing protocol for RTMGwS. RTMGwS uses the characteristics of vehicle movements and variant routing parameters to select an optimal mobile gateway with high robust and trust connection to the infrastructure network. This protocol is designed to spread advertisement messages by the mobile vehicle gateway over an integrated VANET-UMTS network architecture by performing seamless handovers and without flooding the network. The proposed protocol was compared with CMGM-AODV and SGS-AODV. A modified CMGM-AODV-trust and SGS-AODV-trust were also developed by adding a trust parameter for mobile gateway selection to better compare and investigate the performance of RTMGwS for routing optimization. Moreover, the proposed protocol has been validated using SUMO and NS2 simulators over a highway environment. RTMGwS showed the best performance in terms of packet delivery fraction, end-to-end delay, packet routing overhead, and throughput compared with the benchmarking routing algorithms (i.e., CMGM-AODV-trust, SGS-AODV-trust, CMGM-AODV, and SGS-AODV). RTMGwS considers trust and robust parameters for optimum route selection, which produces better decisions in route selection. RTMGwS also stores multiple paths in mobile vehicles tables received by relays for mobile gateway selection, thereby allowing the proposed protocol to perform better than reactive- and cluster-based gateway discovery routing protocols.

References

[1] B.T. Sharef, R.A. Alsaqour, M. Ismail, Vehicular communication ad hoc routing protocols: a survey, J. Netw. Comput. Appl. 40 (2014) 363–396.
[2] D. Antolino Rivas, J.M. Barceló-Ordinas, M. Guerrero Zapata, J.D. Morillo-Pozo, Security on VANETs: privacy, misbehaving nodes, false information and secure data aggregation, J. Netw. Comput. Appl. 34 (2011) 1942–1955.
[3] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, VANet security challenges and solutions: a survey, Veh. Commun. 7 (2017) 7–20.
[4] M. Abdelgadir, R. Saeed, A. Babiker, Mobility routing model for vehicular ad-hoc networks (VANETs), smart city scenarios, Veh. Commun. 9 (2017) 154–161.
[5] S.M. Bilal, C.J. Bernardos, C. Guerrero, Position-based routing in vehicular networks: a survey, J. Netw. Comput. Appl. 36 (2013) 685–697.
[6] P. Salvo, I. Turcanu, F. Cuomo, A. Baiocchi, I. Rubin, Heterogeneous cellular and DSRC networking for Floating Car Data collection in urban areas, Veh. Commun. 8 (2017) 21–34.
[7] C. Guo, D. Li, G. Zhang, Z. Cui, Data delivery delay reduction for VANETs on bi-directional roadway, IEEE Access 4 (2016) 8514–8524.
[8] M.A. Alawi, R. Saeed, A.A. Hassan, R.A. Alsaqour, Simplified gateway selection scheme for multihop relay in vehicular ad hoc network, Int. J. Commun. Syst. 27 (2014) 3855–3873.
[9] A. Benslimane, T. Taleb, R. Sivaraj, Dynamic clustering-based adaptive mobile gateway management in integrated VANET–3G heterogeneous wireless networks, IEEE J. Sel. Areas Commun. 29 (2011) 559–570.
[10] X. Li, B.-J. Hu, H. Chen, G. Andrieux, Y. Wang, Z.-H. Wei, An RSU-coordinated synchronous multi-channel MAC scheme for vehicular ad hoc networks, IEEE Access 3 (2015) 2794–2802.
[11] J. Luo, X. Gu, T. Zhao, W. Yan, A mobile infrastructure based VANET routing protocol in the urban environment, in: 2010 International Conference on Communications and Mobile Computing, CMC, 2010, pp. 432–437.
[12] H.Y. Pan, R.H. Jan, A.A.K. Jeng, C. Chen, H.R. Tseng, Mobile-gateway routing for vehicular networks, in: IEEE VTSI APWCS, 2010.
[13] V. Namboodiri, L. Gao, Prediction-based routing for vehicular ad hoc networks, IEEE Trans. Veh. Technol. 56 (2007) 2332–2345.
[14] C. Pattichis, E. Kyriacou, S. Voskarides, M. Pattichis, R. Istepanian, C.N. Schizas, Wireless telemedicine systems: an overview, IEEE Antennas Propag. Mag. 44 (2002) 143–153.
[15] A. Benslimane, Optimized dissemination of alarm messages in vehicular ad-hoc networks (VANET), in: High Speed Networks and Multimedia Communications, Springer, 2004, pp. 655–666.
[16] A. Benslimane, S. Barghi, C. Assi, An efficient routing protocol for connecting vehicular networks to the Internet, Pervasive Mob. Comput. 7 (2011) 98–113.
[17] S.H. Bouk, I. Sasase, Multiple end-to-end qos metrics gateway selection scheme in mobile ad hoc networks, in: 2009 International Conference on Emerging Technologies, ICET 2009, 2009, pp. 446–451.
[18] H. Chuanhe, C. Yong, S. Wenming, Z. Hao, A trusted routing protocol for wireless mobile ad hoc networks, in: IET Conference on Wireless, Mobile and Sensor Networks 2007, CCWMSN07, 2007.
[19] H. Shaker, R. Alsaqour, Multipath routing algorithm using an electromagnetic-like mechanism with threshold acceptance for mobile ad hoc networks, Wirel. Pers. Commun. (2014) 1–24.
[20] F.P. Setiawan, S.H. Bouk, I. Sasase, An optimum multiple metrics gateway selection mechanism in MANET and infrastructured networks integration, in: IEEE Wireless Communications and Networking Conference, WCNC 2008, 2008, pp. 2229–2234.
[21] M.A. Alawi, R.A. Saeed, A.A. Hassan, R.A. Alsaqour, Simplified gateway selection scheme for multihop relay in vehicular ad hoc network, Int. J. Commun. Syst. 27 (Dec. 2014) 3855–3873.
[22] D. Krajzewicz, G. Hertkorn, C. Rössel, P. Wagner, Sumo (simulation of urban mobility), in: Proc. of the 4th Middle East Symposium on Simulation and Modelling, 2002, pp. 183–187.
[23] K. Fall, K. Varadhan, The network simulator–NS-2, http://www.isi.edu/nsnam/ns, 2007.
[24] N. Baldo, F. Maguolo, M. Miozzo, M. Rossi, M. Zorzi, ns2-MIRACLE: a modular framework for multi-technology and cross-layer support in network simulator 2, in: Proceedings of the 2nd International Conference on Performance Evaluation Methodologies and Tools, 2007, p. 16.
[25] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, C.-F. Lai, Defending against collaborative attacks by malicious nodes in MANETs: a cooperative bait detection approach, IEEE Syst. J. 9 (2015) 65–75.