IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 October 2023, accepted 25 October 2023, date of publication 2 November 2023, date of current version 9 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3330105

RESEARCH ARTICLE

Trust Model for Reliable Grouping-Based Communications in Vehicular Ad-Hoc Networks

MUHAMMAD HALEEM JUNEJO[1], AB AL-HADI BIN AB RAHMAN[1], (Senior Member, IEEE), RIAZ AHMED SHAIKH[2], KAMALUDIN MOHAMAD YUSOF[1], AND SHAHIDATUL SADIAH[1], (Member, IEEE)

[1]Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Johor Bahru, Johor 81310, Malaysia
[2]School of Computing Sciences, University of East Anglia, NR4 7TJ Norwich, U.K.

Corresponding author: Ab Al-Hadi Bin Ab Rahman (hadi@utm.my)

This work was supported in part by the Ministry of Higher Education under the Fundamental Research Grant Scheme (FRGS) under Grant FRGS/1/2020/TK0/UTM/02/62, and in part by Universiti Teknologi Malaysia (UTM) through the UTM Flagship/CoE under Grant Q.J130000.5023.10G05.

ABSTRACT This paper presents a high-reliability Grouping-Based communications trust model in Vehicular Ad-hoc Networks (VANET). The proposed solution consists of two distinct components: First, the Dynamic Group Head Selection (DGHS) scheme to improve the Group Head's (GH) stability by considering the reliability of the communication link with the Road Side Unit (RSU). Second, a hybrid Dynamic Trust Model (DTM) scheme improves trustworthiness by considering the node's dynamic conditions and records. Average GH Lifetime and Average Query Success Rate were used as metrics to evaluate the performance of the grouping algorithms to those of Cluster-Based Location Service (CBLS) and Trust-based Security for Message Exchange (TSME). The proposed DTM was compared to TSME and MiTM Attack Resistant Trust Model (MARINE). With a maximum density of 900 vehicles, DTM improves the average GH lifetime by 43% compared to CBLS and 19% compared to TSME. Similarly, DTM increases the query success rate by 10% compared to the CBLS and 23% compared to the TSME, even at the slowest speed (40 km/h). In terms of node density precision, DTM decreases by around 5% for MARINE and 10% for the TSME approach. In conclusion, it has been shown that the proposed schemes are reliable for various position-based VANET applications that need precise positioning and trusted messaging.

INDEX TERMS Grouping-based communications, trust model, vehicular ad-hoc networks.

I. INTRODUCTION

The vehicular ad-hoc Network (VANET) ecosystem consists of vehicles equipped with on-board units (OBUs), roadside units (RSUs) placed along roadways, and a back-end system that provides different services (registration, authorization, revocation, etc.). VANETs improve road safety, vehicle security, and driver privacy against attacks. There have been 10.8 million annual automotive accidents in the United States since 2000, resulting in over 36,000 annual fatalities and another 24,000 annually connected to collisions with other vehicles and costing more than $100 billion annually [1]. All vehicles get their positions through the Global Positioning System (GPS) and send them to the existing nearby location server. Location service is also responsible for collecting periodic location updates and responding to location queries about the current position of the vehicles [2], [3]. Many unresolved issues were found after investigating the associated works in the security architectures, standards, protocols, attacks, techniques, and solutions in VANETs. The capability of the network to self-organize in a highly mobile network environment, the evaluation of the trustworthiness of nodes participating in VANETs, and their misbehavior detection are a few of these issues. Moreover, group-based location service

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

schemes are categorized into static and dynamic group-based location services. Vehicles are grouped to formulate a group based on specific rules. At least one Group Head (GH) exists in every group designated as a moving local location server [4], [5]. The other vehicles in the group are named Group Members (GMs). The dynamic group-based location service relies on dynamic grouping. Dynamic grouping is also termed mobile grouping. It depends on the mobility parameters such as speed and position to make the groups. Group-based location service schemes have more scalability, reliability, and communication overhead advantages than non-group-based ones. Furthermore, dynamic grouping is more flexible than static grouping [2], [3].

The group's stability depends on essential parameters, such as speed, distance, direction, number of neighbors, link lifetime, destination, signal-to-noise ratio, fixed-size road segments, road id, and density [5]. These parameters are used to elect GH and GM associated with this group. Due to rapid topological changes in VANETs, speed is considered the most important parameter in forming groups [6]. The group's stability can be increased by combining different parameters while still meeting the needs of various applications [7]. The non-optimal GH election parameters lead to unnecessary grouping around the intersection, where the communication overhead and collision of messages around the intersection increases, affecting the location updates and location queries of GMs. The inter-group interference, congestion, contention, and message loss were also increased due to frequent grouping variations [4], [8]. Possibly, vehicles may send incorrect location data during network communication. Due to these issues, group instability increases. So, there is a need to improve the existing group maintenance schemes to improve the performance of the location service. The scientific community has contributed substantially to solving safety, security, and technical design problems. However, dealing with safety, security, and privacy criteria is the most important part of utilizing VANETs efficiently. In this way, the research community has developed ideas for making VANETs safer [9], [10], [11], [12]. Unfortunately, conventional cryptography solutions are unsuitable for lightweight communication to provide network security. Furthermore, it can't guarantee the reliability and quality of messages, which can cause undesirable effects [13], [14], [15]. As a result, trust-based defences against inside attacks for VANETs are produced [13], [16]. Trust is defined in the context of VANET as the confidence one vehicle has in another to carry out the required activity. Vehicles may determine if a person can trust the information based on some factors, including the opinions of their neighbors, the credibility of the communicating vehicle, and their previous interactions with the communication vehicle.

Numerous lightweight cryptographic primitives have recently been developed to replace more complex algorithms like block ciphers, hash functions, and stream ciphers. Therefore, high mobility, unreliable communication links, and frequent changes in the topology lead to challenging situations inside VANET. The unreliable link with the RSU and non-optimum grouping formation. Furthermore, establishing and assessing trust in received communications in such a short period is challenging, especially for lightweight communication with limited resources. The processing and communication overhead associated with message authentication and dissemination rises as the number of messages in the network rises. This work tackles the problem and suggests a low-cost message authentication and distribution system. This study proposes a group-based trust model in a dynamic environment using centralized and decentralized administration to monitor vehicles' behavior. In addition, it provides a method for evaluating the trust value utilized in choosing the most trustworthy vehicles as possible group leaders and identifying any malicious vehicle that may operate in an untrustworthy manner. This research aims to develop a lightweight trust model with improved group stability in a dynamic environment. This paper is organized as follows. In Section II, related work is presented. Section III discusses the materials and methods. Section IV shows the results and discussion, while Section V demonstrates the paper's conclusion.

II. RELATED WORK

Table 1 compares the grouping-based trust models for VANET. Asoudeh et al. [17] propose a Group Based Position Service (CBLS) approach that uses dynamic grouping to give a vehicle's location. First, each car broadcasts its Group Head Election Value (GHEV), determined by the speed, distance, and number of directly linked vehicles to its neighbors. Then, each vehicle compares the CHEV against its value. If a neighbor's CHEV is better, the vehicle advertises it. GH instability persists owing to the lack of a well-defined group formation range. This is because every car broadcasts its information to its adjacent vehicles, and those vehicles give that information to nearby vehicles. In this way, all vehicles in the vicinity are updated. As a result, CHEV does not certify a GH vehicle with consistent speed and the least distance from other cars.

Pal et al. [18] determine the group centroid based on vehicle location by considering the speed and distance from the centroid. The GH is chosen from among the vehicles within the centroid's range. However, the variable numbers of cars in each vehicle's neighbor table impact the centroid's uniqueness, making it difficult to predict the range of group formation. Additionally, GH is chosen without taking the RSU's dependability into account.

Khan et al. [19] came up with an idea for a trust model (TM) in VANET that was built on group-based procedures. The GH determines trust and sends that number to a trusted authority (TA). TA removes a hostile node from a network based on GH's knowledge. The continuous reporting required by the proposed approach is the main drawback, as it significantly decreases network efficiency and generates a large approach overhead. In addition, there is a lack of

TABLE 1. Grouping-based trust models for VANET.

Trust Model	Topology	Technique	Advantage	Disadvantage
[19]	Distributed	Grouping with watchdog	Effective misbehaviour detection	High overheads
[20]	Centralized	Weighted voting and logistic regression	Quickly identify malicious nodes propagating false information in the network	A high number of solaces are required for event authentication
[21]	Distributed	Group heads with payment punishment mechanism	Cooperation and active participation of nodes, thus avoiding the presence of selfish behaviour	Biased GH selection in rural locations due to limited neighbours
[22]	Distributed	Credit change based on node behaviour	Evacuation of selfish nodes from the network	Inability to differentiate between direct and indirect
[23]	Distributed	Multi-faceted approach	scalable in a dynamic environment	Robustness not addressed
[24]	Distributed	Similarity mining mechanism	help the vehicular use to decide on trusting the received data	No global information on message similarities
[25]	Distributed	Sociological trust evaluation model	Provide security and privacy	Missing architecture to merge all that values
[27]	Distributed	Trust calculation based on information similarity, information conflict and routing path similarity	Real-time validation of received messages	Complex trust model and inefficient in spare scenarios
[30]	Distributed	Direct bust evaluation	Identification of vehicles with fake locations	Trust calculation for every message, inefficient in urban scenario
[31]	Centralized	Trust calculation based on Group head selection	Framework with intrusion detection for different attacks	Assumption of stable group availability
[32]	Centralized	Reputation-based trust calculation	Intelligent eviction of the malicious nodes	Blind reliance on vehicular sensors
[33]	Centralized	Trust calculation based on message classification and DSRC protocols	Lightweight trust model to distribute messages via DSRC protocols	Assumption that malicious nodes behave constantly
[34]	Centralized	Grouping and random walk algorithm	Trustworthiness is evaluated in an infrastructure-less environment	Assumption of uniformly distributed malicious nodes
[35]	Centralized	Beacon-based trust mode	Revokes internal attackers in the privacy-enhanced network	High overheads

information regarding the network communication between the GH, TA, and vehicles.

Ahmed et al. [20] provide a hybrid TM that uses a trust computation model based on a logistic approach to detect nodes introducing erroneous information into the network. This trust architecture gathers reliable information about occurrences at the evaluator nodes through various sources, including direct observation. Once the actual occurrence has been confirmed, the sender node's behavior is classified as authentic or malicious. This technique weighs votes and uses a logistic trust function to determine trust. This trust model recognizes adversarial nodes disseminating false information throughout the network. This approach may not be feasible in rural regions since there are insufficient information sources.

In short, the trust management models presented previously are insufficiently dynamic to VANETs' properties. For example, a few studies [36], [37] proposed handling a certain type of message, while others [38], [39], [40] utilized decentralized trust mechanisms, which is impractical in a VANET's dynamic environment. Furthermore, some other works [28], [41], [42], [43] attempted to counteract a certain kind of attack, which might be a limitation. On the other hand, several other works were meant to counteract a particular kind of challenge, such as authentication [43], privacy [44], [45], or localization [46], [47]. Therefore, in contrast to existing methods, an adaptive TM is required to exchange messages in VANETs, along with a grouping algorithm to deal with the dynamicity of such networks.

III. PROPOSED METHODS

Due to the dynamic nature and variable speed of VANETs, the proposed trust-based message exchange scheme has been divided into two parts. The first stage divides the network into groups and assigns a particular group to each isolated vehicle. One node has been elected as a group head to manage and control the group activities. The dynamicity and variable speed of the VANET have been handled through this grouping scheme. The second part deals with trust management based on the reputations of vehicles as well as the dynamicity and variable speed of the VANET. The trust in the messages has been calculated based on three indicators: location closeness, the number of forwarders, and time closeness.

A. DYNAMIC GROUP HEAD SELECTION (DGHS) SCHEME

Each GH functions as a lower-level location server in the group-based location service. GH updates the positions of its GMs to RSU, which performs as a server at a higher level. The stability of the GH has a significant impact on the operation of the location service. Location service methods based on the static grouping methodology split the region into several segments, with the collection of vehicles in each segment constituting a group. GH is chosen based on where a vehicle is in the segment. All the other vehicles in the groups become GMs and join the group. The static group-based methods are susceptible to frequent GH changes, and groups also overlap owing to the group formation range. A GH travels with its GMs in the dynamic grouping. The values of various metrics, including distance, speed, direction, and the number of neighbors, are considered when choosing the GH. Each vehicle broadcasts its Group Head Fitness Value (GHFV) in the dynamic group-based location service concept. This procedure continues until an optimal GH vehicle is chosen.

The calculated GHFV decides that the unstable vehicle should be the GH. Furthermore, existing group-based location service schemes choose GH without considering the RSU's connection dependability. Some current research on generic grouping uses link status to choose GH. However, these techniques do not guarantee that the GH will remain stable while concurrently interacting with the RSU and GMs. These problems contribute to increased GH instability, which reduces GH's lifespan. This issue impacts both the location queries and the location updates. Therefore, this scheme is integrated with the grouping that increases the dependability of the GH with the RSU. GH election is based on calculating its fitness to work as a GH. In this scheme, the fitness value is a weighted sum of vehicles' V_i average speed variation (ASV_i), distance from the centroid (CD_i), time to link the vehicle V_i with RSU (TL_RSU), the direction of vehicle movement w.r.t RSU (DirV_i) and the total number of connected neighbors (NV_i). Calculates the vehicle's average speed variation with other network vehicles to ensure a stable GH.The following are defined for the proposed DGHS scheme:

$$ASV_i = \frac{1}{n}\sum_{j=0}^{n-1} Vv_i - Vv_j \tag{1}$$

The time to link the vehicle with the RSU,

$$TL\_RSU = \frac{S(V_i) \times \sqrt{(RSU_x - V_{ix})^2 + (RSU_y - V_{iy})^2}}{Vi} \tag{2}$$

where V_i is the speed of vehicle i, RSU_x and RSU_y are the x and y coordinates of the RSU, respectively, and V_{ix} and V_{iy} are the coordinate locations of the vehicle i, respectively. $S(V_i)$ is the direction movement of the vehicle, given by:

$$S(V_i) = \begin{cases} 1, & \text{if } d_1 >= d_2 \\ -1, & \text{if } d_1 < d_2 \end{cases} \tag{3}$$

where d_1 is the distance between the RSU and V_i at a beacon interval t, and d_2 is the distance between the RSU and V_i the next interval $t + 0.1$. $S(V_i)$ is essentially a function whose value is 1 when the vehicle approach the RSU, and -1 when it moves away from the RSU. A vehicle moving away from RSU has a lower chance of the election as it may exit the trust zone.

Equation (2) simply states that the lower vehicle speed has a higher TL_RSU value; ultimately, these vehicles have a higher possibility of becoming a GH. However, a vehicle with a lower speed is unstable with respect to its neighbor's vehicles and frequently leaves a group.

The total number of connected vehicles is the number of neighboring nodes whose acknowledge beacon message has been received.

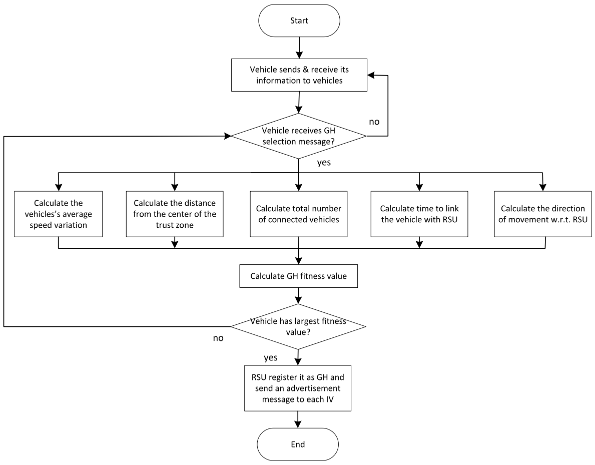
Start
Vehicle sends & receive its information to vehicles
Vehicle receives GH selection message?
no
yes
Calculate the vehicles's average speed variation
Calculate the distance from the center of the trust zone
Calculate total number of connected vehicles
Calculate time to link the vehicle with RSU
Calculate the direction of movement w.r.t. RSU
Calculate GH fitness value
Vehicle has largest fitness value?
no
yes
RSU register it as GH and send an advertisement message to each IV
End

FIGURE 1. Flowchart of the proposed DGHS model.

$$N_{V_i} = \frac{\sum ack}{n} \tag{4}$$

where n is the total number of nodes in the trust zone and N_{V_i} is total number of connected vehicles.

$$FVV_i = \frac{w_1}{ASV_i} + \frac{w_2}{CD_i} + \frac{w_3}{TL_{RSU}} + w_4 \times N_{V_i} + w_5 \times DirV_i \tag{5}$$

where w_1, w_2, w_3, w_4 and w_5 are weighting factors. Different weighting factor combinations were employed to obtain the optimal values that guarantee a good balance among the proposed scheme's selection metrics. Particularly, the sensitivity of these weighting factors to the GH lifetime was evaluated to determine the best-balanced set of these weights. The weighting factor group (0.1, 0.2, 0.4, 0.2, 0.1) has shown the greatest results regarding the highest GH lifetime. This implies GH's stability mostly relies 20% on the CD_i, 20% on nearby vehicles, and 40% on TL_RSU. However, the vehicle's average speed variation and movement direction effects are at least 10% each. Therefore, (5) turn into following (6):

$$FVV_i = \frac{0.1}{ASV_i} + \frac{0.2}{CD_i} + \frac{0.4}{TLR_i} + 0.2 \times N_{V_i} + 0.1 \times DirV_i \tag{6}$$

The current scheme improves the group's stability by making GHs last longer. This is done by choosing a GH that is the most stable with respect to its neighbors in terms of mobility, has the most stable connection to RSU, and has many neighbors. This scheme operates in three phases. In the third phase, each vehicle in the GH range determines its Group Head Fitness Value (GHFV) based on its average speed variation, TL_RSU, and N_{V_i}. Finally, each phase's output is used as the input for the next phase. Figure 1 describes the GH election procedure.

The GH's reliability is crucial for the group-based location service. The non-optimal group formation range and the inconsistent connection of GH with the RSU prevent current research from fully enhancing the performance of location services via GH selection criteria. GH's lifespan may be increased by considering the right mobility characteristics, such as distance, speed, TL_RSU, N_{V_i}, and direction.

A GH is furthermore elected from the GHFV range of vehicles based on the average speed variation, distance from the center of the trust zone, N_{V_i}, TL_RSU, and the direction of movement with respect to the RSU. Finally, the vehicle with the biggest GHFV is elected to be a GH. The complete algorithm of the proposed scheme is given in Algorithm 1.

Algorithm 1 Dynamic Group Head Selection (DGHS)

```
Require: *GHCR*: Group Head Covered Range; *NV*: Number of vehicles in *GHCR*; *Pos_RSU*: Position of RSU; ($C_x$, $C_y$): Trust zone center; *BMs*: Broadcast messages, *GHSM*: Group Head Selection Message.
    $V_i$ sends *BMs*
    $V_i$ receives *BMs*
    $V_i$ receives *GHSM*
    //calculate total number of connected nodes
    $N_{V_i} = ack\_count/NV$
    for j = 0; j <= NV; j++ do
        //calculate average speed variation
        $CASV = CASV + (Vi - Vj)$
    end for
    $CASV = CASV/N_{V_i}$
    //calculate distance from center of trust zone
    $CD = \sqrt((x_i - C_x)^2 + (y_i - C_y)^2)$
    //compute displacement 1 and 2
    $d_{t1} = \sqrt{(RSU_x - V_{ix1})^2 + (RSU_y - V_{iy1})^2}$
    $d_{t2} = \sqrt{(RSU_x - V_{ix2})^2 + (RSU_y - V_{iy2})^2}$
    //determine direction of $V_i$
    if $d_{t1} > d_{t2}$ then
        $dirV_i = 1$
    else
        $dirV_i = 0$
    end if
    //compute the $TL\_RSU$
    $TL\_RSU = (S(V_i) * sqrt((RSU_x - V_{ix})^2 + (RSU_y - V_{iy})^2))/V_i$
    //Compute fitness values $FV_i$ to RSU to select GH
    $FV_i = 0.1/CASV + 0.3/CD + 0.4/TL\_RSU + 0.2 * N_{V_i} + 0.1 * dirV_i$
    return $FV_i$
```

B. DYNAMIC TRUST MODEL (DTM) SCHEME

Roadside Unit (RSU) is the trusted unit in the model. RSU provides initial trust value to all vehicles in the region of interest. All vehicles have a unique trust value in the region. RSU generated an alert message to inform about a malicious vehicle in the region of interest. This alert message helps vehicles in the region not trust the information received from the malicious node.

The group head evaluates the trustworthiness of the propagating message and the group member's reputation (fitness) value to determine the authenticity of an event in VANET, therefore achieving the goal of assuring the secure communication of VANET. This study aims to develop secure trust-based messages in a lightweight VANET. The first step is to develop a safe grouping algorithm for VANETs. The trust management plan is the focus of the second stage, which consists of the following assumptions:

- Event messages have been sent by vehicles.
- Each vehicle sent its GHFV to the GH.
- A vehicle with a lower fitness value is synonymous with a malicious vehicle.
- GH cannot be considered unsafe.
- The sender's closeness to the event site increases the authenticity. Conversely, the authenticity score drops as temporal closeness drops.
- The higher the probability of modifying the event, the greater the number of vehicles reported the same event.

the reputation messages, *GMlist* is given by:

$$GMlist[i] =< V_{id}, SMV_i, FV_i, t_{add} > . \tag{7}$$

where V_{id} is the event message forwarded by vehicle V_i, and SMV_i is the number of successful message delivery, initially, its value is zero. Then, each successful delivery adds (t_{add}) one and unsuccessful delivery minus 1 in its value.

Additionally, a vehicle observing an event sends out *Mevent*, given by:

$$Mevent =< V_{id}, (V_{ix}, V_{iy}), type, (x, y), t_r > \tag{8}$$

A vehicle V_i forwards an event message identified by V_{id}; reports an observed event to GH by specifying its type: $type \in$ *{accident, road liberation, traffic information}*, (x, y), the coordinates of the event's location, (V_{ix}, V_{iy}) the location of the vehicle V_i where it generated the message, and t_r as the reporting time.

The GH verifies its accuracy based on the node fitness value and other indicators given by the location closeness:

$$L_c = 1 - S(V_i) \times \frac{\sqrt{(E_x - V_{ix})^2 + (E_y - V_{iy})^2}}{A_c} \tag{9}$$

where E_x and E_y are the coordinates of occurrence of the event E, and A_c is the coverage area. If the vehicle has already crossed the event, then L_c is higher than in another case where the vehicle is approaching the event. The function is used to find the direction of the reporting vehicle after calculating two beacon messages. The closer the respondent is to the event location, has higher the L_c score.

Time closeness, T_c is a way to show how recently an event was reported. An estimated time or the reporting vehicle, T_{re} is given by:

$$T_{re} = \frac{\sqrt{(E_x - V_{ix})^2 + (E_y - V_{iy})^2}}{V_{vi}} \tag{10}$$

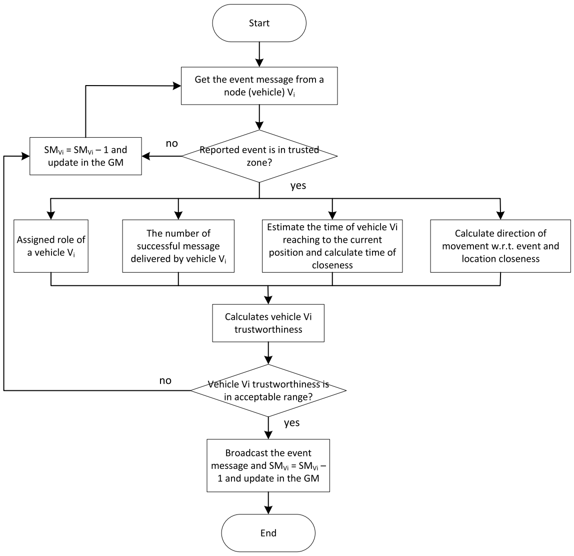
Start
Get the event message from a node (vehicle) V_i
Reported event is in trusted zone?
no
yes
$SM_{Vi} = SM_{Vi} - 1$ and update in the GM
Assigned role of a vehicle V_i
The number of successful message delivered by vehicle V_i
Estimate the time of vehicle Vi reaching to the current position and calculate time of closeness
Calculate direction of movement w.r.t. event and location closeness
Calculates vehicle Vi trustworthiness
Vehicle Vi trustworthiness is in acceptable range?
no
yes
Broadcast the event message and $SM_{Vi} = SM_{Vi} -$ 1 and update in the GM
End

FIGURE 2. Flowchart of the proposed DTM model.

if $|t_r - (T_{re} + t_e)|$ is less than a constant δ (t_e is the estimated time), then the message is rejected, otherwise,

$$T_c = \frac{1}{t_r - t_e} \tag{11}$$

where V_{vi} is the speed of the reporting vehicle. T_c thus estimates the time reporting of the vehicle. The past data held by RSU contains SMV_i the number of successful message deliveries by vehicle Vi, and is also used to develop confidence. A vehicle may be considered trustworthy if it provides a specialized or authorized function, such as a school bus, ambulance, or police car. The node's weight can reflect its trustworthiness and the data it reported to some degree. A node in VANETs should belong to one of the three levels.

Figure 2 shows the flowchart of the proposed DTM scheme. The node trustworthiness is calculated based on the vehicle's assigned role, the time to reach the event place, the number of successfully delivered messages, and the direction of movement with respect to the event. The complete algorithm of the proposed scheme is given in Algorithm 2.

Algorithm 2 Dynamic Trust Model (DTM)

```
Require: $Mevent$: Event message; $GH$: group head; $RSU$:
    Roadside Unit; $GHCR$: Group Head Coverage Range.
  //calculate dynamic threshold
  //$N_{event}$ is number of nodes reporting an event
  $N_{RE} = 1 - \frac{1}{N_{event}}$
  if $ID_{vi}$ == police or rescue services then
    $R_{vi} = 1$
  else if $ID_{vi}$ == other government vehicles then
    $R_{vi} = 0.5$
  else
    $R_{vi} = 0$
  end if
  //computer direction of movement w.r.t. RSU
  if $(x, y)$ lies in the $GHCR$ then
    $d_{t1} = \sqrt{(E_x - V_{ix1})^2 + (E_y - V_{iy1})^2}$
    $d_{t2} = \sqrt{(E_x - V_{ix2})^2 + (E_y - V_{iy2})^2}$
    //determine direction of $V_i$
    if $d_{t2} > d_{t1}$ then
      $dir V_i = -1$
    else
      $dir V_i = 1$
    end if
  end if
  //calculate $L_c$
  $L_c = 1 - S(V_i) \times \frac{\sqrt{(E_x - V_{ix})^2 + (E_y - V_{iy})^2}}{A_c}$
  //calculate $T_{re}$
  $T_{re} = \frac{\sqrt{(E_x - V_{ix})^2 + (E_y - V_{iy})^2}}{V_{vi}}$
  if $|t_r - (T_{re} + t_e)| < \delta$ then
    //reject the message
    $SMV_i = SMV_i - 1$
  else
    $T_c = \frac{1}{t_r - t_e}$
    $T_{vi} = L_c + T_c + R_{vi} + N_{RE}$
    $SMV_i = SMV_i + 1$
    //Broadcast the message
  end if
  //update and return $GMlist$
```

C. SIMULATION FRAMEWORK

The final step is the examination of the proposed work's performance. The group stability schemes' performance was simulated, tested, and compared to other group-based location service schemes, and trust model effectiveness was compared with existing trust models. In this analysis, we integrate real-world road topology and real-time data from a database into a microscopic mobility model to generate realistic traffic flows along the highway. In VANETs, two kinds of simulators are utilized to simulate vehicles: a network simulator and a traffic simulator. Traffic simulators are used to replicate road traffic behavior, whereas network simulators are utilized to simulate network protocols. A variety of simulation frameworks, such as Network Simulator 2 (NS2), Objective Modular Network Testbed in C++ (OMNET++), Optimized Network Engineering Tool (OPNET), and Matrix Laboratory (Matlab), have been designed and developed. However, OMNeT++ is favored since it is a C++ simulation platform that allows for creating and executing network simulations while being extensible, modular, and based on components. The computer system used for the experimental purpose was equipped with 16GB RAM and a core i7 processor with a clock speed of 3.8 GHz.

The proposed schemes followed the simulation setting and environment of CBLS to adopt a more realistic scenario. The Doha map is considered in this research because the same map was used by benchmark research CBLS [48].

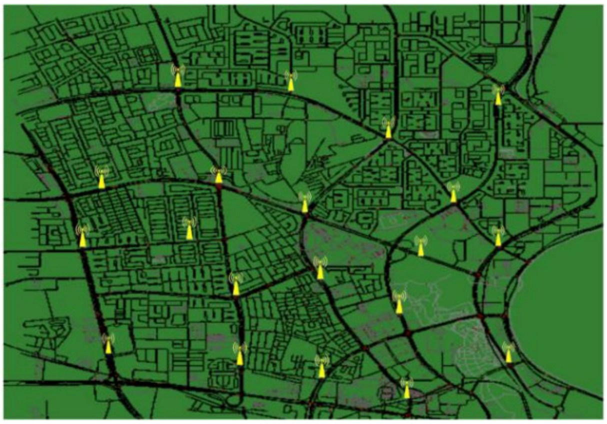

FIGURE 3. Part of the Doha map used in the simulation.

TABLE 2. Parameters used in the simulation environment.

Parameter	Unit	Value
Simulation Area	KM^2	6×6
MAC	-	802.11p
Simulation Time	min	15
Number of RSUs	-	20
Transmission range of a vehicle for urban roads	M	500
Transmission frequency	Hz	10
RSU update interval	s	5
Number of lanes in each direction		Single lane
Vehicles' density		100-900
Vehicles' speed	KM/hour	40-100
Average speed	KM/hour	40

Dimensions are obtained for the simulation scenario (latitude:25.3440 to 25.2899 and longitude: 51.4666 to 51.5266). The map, shown in Figure 3 was obtained from the OpenStreetMap database. CBLS relied on 6 × 6 km to conduct simulations. Twenty RSUs were set up as fixed-location servers in different places to cover the simulated area. The road is separated into 800m portions to cover the effective range on both sides of the vehicles. In accordance with the VANET specification, vehicles must transmit a beacon at a rate of 10Hz. Therefore, the transmission rate of beacon messages from all vehicles was set to 10Hz so that the exact locations of vehicles could be found. The simulation time of one thousand seconds was used to yield findings. To justify the density of vehicles 150 to 950, one lane in each direction was employed to simulate vehicles. The physical and MAC layers are set up by IEEE 802.11p guidelines. Table 2 lists the simulation parameters. Simulations are run by taking the maximum speed variations between 36-108 km/h.

The range of communication for each vehicle was assumed to be 400m. The efficiency of the proposed technique was evaluated under two conditions, the speed, and density of the vehicles. In a city, the average speed for a vehicle is 30 km/h [49]. In this research, the average speed of the vehicles was taken to be 40 km/h. Additionally, simulations are run with varied densities of vehicles; a scenario with 350 vehicles indicates high density, while 250 vehicles reflect medium density and 150 vehicles represent low density. The number of vehicles classified as low to high density ranges from 100 to 1000 and from 100 to 350, respectively. In this research, the number of vehicles in the network ranges from 100 to 900 to depict the network's condition. In the first scenario, the maximum speed of the vehicles ranges from 40km/h to 100km/h, but the average density of vehicles on the road stays the same (13–16 cars/km/lane). The average density is 13 to 16 vehicles per kilometer of road, about 620 cars in a 6km by 6km area. In the second scenario, the maximum density of vehicles varies from 100 to 900 while the average speed stays at 40km/h.

The vehicle's maximum speed is set at 100 km/h. The simulation area is 2km by 2km in size. The maximum node density in this region was 900 nodes. Additionally, 10% of nodes were chosen as malicious nodes that consistently provide phone or fraudulent messages. The kind of vehicle is also decided before the simulation even starts. Thus, 10 % of members' nodes are designated as highly trustworthy nodes like ambulances/fire brigade/rescue teams; 20% of members' nodes are designated as intermediate-trustworthy nodes like government vehicles, and the remaining 70% of nodes are designAated as ordinary private nodes without any prior trustworthiness. Because there are more private vehicles on the road than in the other categories. This simulation's channel bandwidth is 10Mbps on the ideal data rate to prevent message congestion. Additionally, the network's member vehicles all have the same set transmission range. Constant Bit Rate (CBR) with a value of 36kbps and a focus on User Datagram Protocol (UDP) packet generation traffic is used as the source of simulation traffic. In all, the simulation takes around 9000s.

Initiating many runs for each simulated scenario is recommended to gain confidence in the simulation results. Therefore, each simulation scenario in this research contains 30 runs. The initial node placement is redistributed randomly at the start of each simulation, using a new random seed so that all initial circumstances are unavoidably distinct.

D. PERFORMANCE EVALUATION

The performance of the three proposed schemes has been assessed in three separate phases and compared to the most recent, ISI-indexed, TSME [17], [50], and MARINE [51]. The lifetime of the GH has a direct impact on the group's stability. The GH lifetime is determined by dividing the total GH duration time by the number of group heads, According to Equation 12, the GH lifetime is the average lifetime of GHs for a certain circumstance [49], given by:

$$AverageGHLifetime = \frac{\sum_{i=1}^{n} t_i^m - t_i^{fb}}{n} \tag{12}$$

where n is the total number of group heads formed, t_i^m is the election time for group heads, and t_i^{fb} is the losing time for group heads. The lifetime of the GM has an impact on the group's stability. The GM lifetime is determined by the moment a vehicle joins the group and the moment it leaves, i.e., dividing the total GH duration time by the number of group heads.

The percentage of successfully answered queries to the total queries sent is given by:

$$QuerySuccessRate(\%) = \frac{\sum_{i=1}^{n} successfullyReceivedQueries}{\sum_{i=1}^{n} successfullyTransmittedQueries} \quad (13)$$

The performance is also evaluated by:

- **Precision (P)**: Precision is a fraction of the relative instances included inside the retrieved instances. In this research, the number of nodes properly identified as malicious nodes counts as a relevant instance. A retrieved instance is the total number of nodes correctly and mistakenly identified as malicious nodes. Thus, Precision is defined as TM's ability to precisely forecast an event's trustworthiness, given by:

$$P = \frac{PM}{PU} \quad (14)$$

where PM is the number of real malicious nodes caught probability and PU is the total number of untrustworthy nodes caught (either caught correctly or incorrectly) probability.

- **Recall (R)**: The term Recall is described as the capability of TM to predict absolute malicious content disseminated by the nodes. In this case, PT is the total number of truly malicious nodes.

$$R = \frac{PM}{PT} \quad (15)$$

- **F_Score**: The term F-Score is described as the weighted average of Precision and Recall. Moreover, the accuracy of TM depends on F-Score. The higher F-Score values correspond more accurately to TM. F-Score is defined by:

$$F\_Score = 2 \times \frac{P \times R}{P + R} \quad (16)$$

- **Communication overhead**: Communication overhead is the total amount of packets that must be sent or conveyed from one node to another. Communication overhead refers to the messages sent and received between a sender and a third-party node and between a receiver and a third node.

E. ASSUMPTIONS AND LIMITATIONS

The following assumptions and limitations pertain to this research and are considered in the network scenario:

- GPS technology allows all vehicles to be informed of their location.
- Digital maps depicting vehicles on junctions and roads are standard equipment in every vehicle.
- The transmission range is equivalent and substantial in all vehicles.
- The computing capacities of all vehicles are uniform.

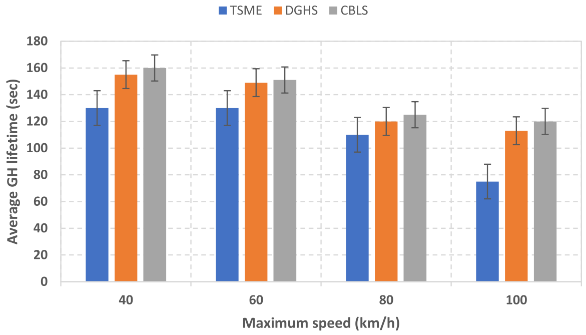

FIGURE 4. Average GH lifetime at different maximum speeds.

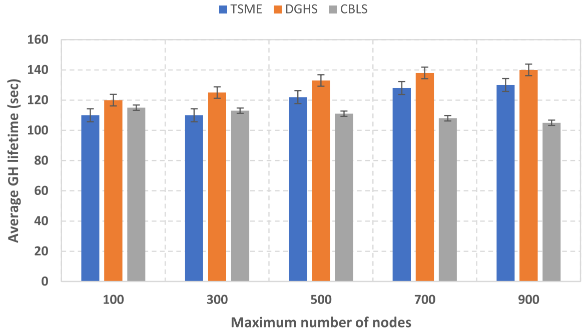

FIGURE 5. Average GH lifetime at different numbers of maximum nodes.

- All vehicles know their destination, speed, and maximal acceleration.

IV. RESULTS AND DISCUSSION

The average lifetime of a GH has a direct impact on the group's stability. The longer GH lifetime indicates that the group configuration is more stable because of its bigger value. The average GH lifetime is calculated by dividing the network's total number of GHs by the sum of all GHs' total durations. The size of the segment affects the GH lifetime. GH passes through the same distance in less time with increased speed.

Figure 4 shows that the suggested DGHS method improves GH lifespan by 21% against CBLS and 33% versus TSME at 40 km/h. As a result of the quick topological changes, Figure 4 illustrates how an increase in speed impacts the performance of three schemes. DGHS scheme demonstrated better performance compared to its competitors at all speeds. DGHS was chosen by getting the average relative speed of each vehicle in the network compared to its neighbors; it helps achieve a better GH lifespan.

Figure 5 depicts the performance of the DGHS, CBLS, and TSME schemes in terms of average GH lifespan vs the maximum number of vehicles in the network. The proposed scheme uses the range and the number of vehicles located within the range of the centroid vehicle to regulate the density. In addition, instead of broadcasting its fitness value

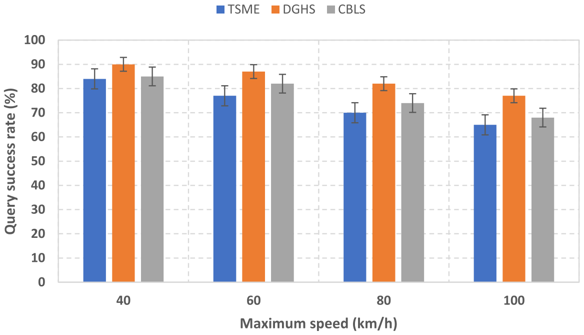

FIGURE 6. Average query success rate of GH at different maximum speeds.

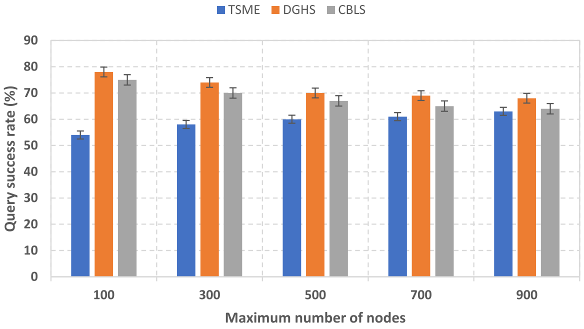

FIGURE 7. Average query success rate of GH at different maximum nodes.

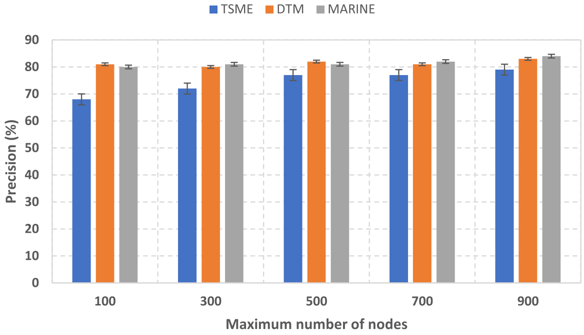

FIGURE 8. Precision values with vehicle density.

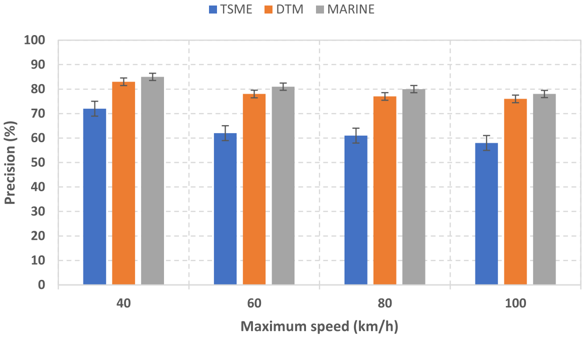

FIGURE 9. Precision values with maximum speed.

throughout the network, it communicates it to the RSU, which increases GH's lifespan.

Figure 6 shows that the DGHS scheme has a higher query success rate than its competitors. At the slowest speed (40 km/h), the proposed approach improves the query success rate by 10% over the CBLS and 23% over the TSME. However, DGHS improves query success rate over the current CBLS and TSME schemes by 14% and 24%, respectively, at the maximum 100km/h.

Figure 7 illustrates the performance of the DGHS, CBLS, and TSME schemes regarding query success rate vs network nodes. The lifetime of each GH and GM in a section in the TSME grows with an increase in density; however, lifetime is only possible for road segments. The CBLS relies on a broadcasting strategy without establishing any range, and when density increases, there is more competition for available communication channels, which results in more messages being lost.

In the proposed DGHS scheme, density is handled by setting the GH election range first and then choosing a GH. Therefore, GH exhibited acceptable stability despite the higher density. When compared to the CBLS and TSME, the proposed DGHS scheme has a query success rate that is enhanced by 12% and 43% for the lowest density (100 vehicles in the network) and by 18% and 20% for the maximum density (900 vehicles in the network), respectively.

The efficiency of the proposed TM is computed against the MARINE and TSME models. The simulation results in this section compare the precision and recall of DTM with MARINE and TSME techniques across different densities, velocities, and percentages of malicious nodes. The requirements for communication overhead are also shown.

The impact of node density on DTM, MARINE, and TSME is seen in Figure 8. When the node density fluctuates, the DTME outperforms the TSME in precision. However, there is no discernible distinction between DTM and MARINE. These three techniques also provide superior precision at increasing node densities. This is accurate given that a larger density of well-behaved nodes increases the likelihood of receiving accurate data from others. For MARINE, precision is reduced by around 5%, while for the TSME method, it is reduced by about 10%. Figure 9 shows how the precision of the DTM, MARINE, and TSME are compared as the nodes move at various speeds. These data demonstrate that the precision values are lower when the vehicles travel more quickly. This is true because information about unreliable vehicles spreads more slowly when the vehicles are going more quickly. The precision value for the DTM, MARINE, and TSME techniques with various percentages of malicious nodes is shown in Figure 10. Precision suffers when a significant portion of the network's nodes are malicious. Both TSME and MARINE show a 10% and 2% reduction of precision at the lowest speed.

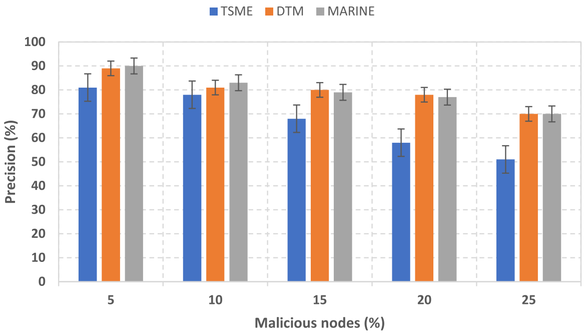

FIGURE 10. Precision values with percentages of malicious nodes participating in the network.

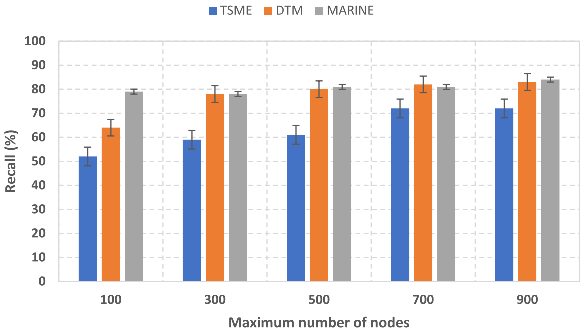

FIGURE 11. Recall values with vehicle density.

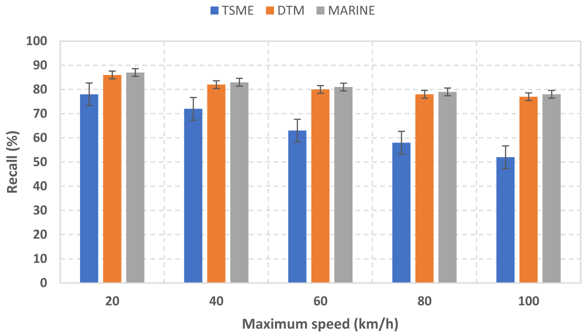

FIGURE 12. Recall values with maximum speed.

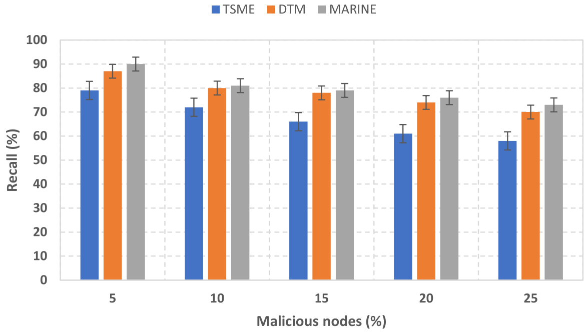

FIGURE 13. Recall values with percentages of malicious nodes participating in the network.

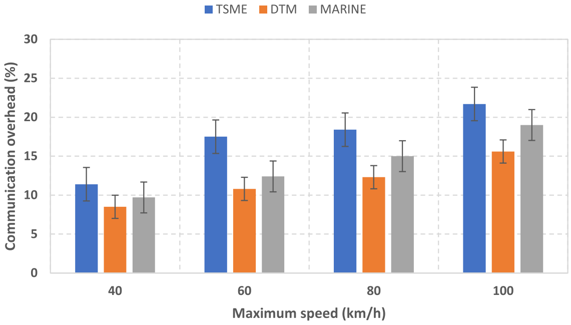

FIGURE 14. Percentage of communication overhead with vehicle density.

The disease causes a greater decline in this number. This is mostly because malicious nodes and impediments impede nodes from communicating accurate data.

The impact of the recall on velocity, density, and the number of malicious nodes are discussed in the following sections. The effect of node density on the recall of DTM, MARINE, and TSME is seen in Figure 11. This graphic demonstrates that these methods have a greater recall score as node density increases. Furthermore, the suggested DTM model is more sensitive to malicious nodes compared to past research. This graph demonstrates that DTM outperforms MARINE and TSME regarding recall scores across various node nodes. Recall of MARINE drops by 2% and TSME has a considerable drop of 20%. When the nodes move at various speeds, Figure 12 compares the recall of the DTM, MARINE, and TSME. This image illustrates how the recall score of various systems decreases when the nodes move more quickly. At the top speed of the vehicles (100 km/h), the percentages were 71% and 58%, respectively. Additionally, the recall value with percentages of malicious nodes participating in the network is shown in Figure 13, where the proposed DTM shows very close value to MARINE.

Evaluation of DTM, MARINE, and TSME communication overhead is done in relation to different densities, velocities, and numbers of malicious nodes. For example, Figures 14, 15, and 16 illustrate how overhead communication rises together with the node density, velocity, and the number of malevolent nodes.

Figure 14 depicts the impact of density on DTM, MARINE, and TSME communication overhead. The communication overhead grows proportionally with the density of nodes in the network. Comparing the communication overhead, DTM is the most cost-effective option. The effect of speed on the amount of overhead involved in transmitting data is also seen in Figure 16. This figure illustrates how a rise in speed results in a corresponding rise in communication overhead. This is because the cars are moving at such a fast speed that their transmission range no longer overlaps, and as

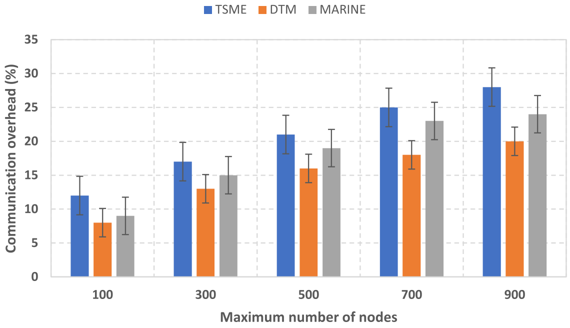

FIGURE 15. Percentage of communication overhead with maximum speed.

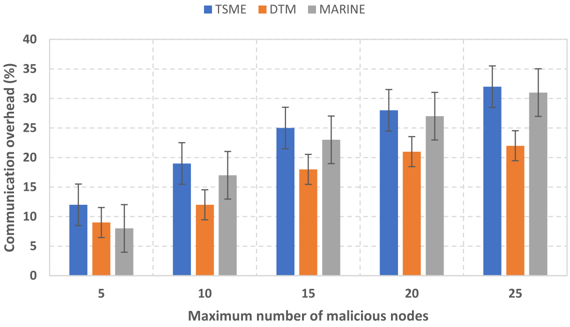

FIGURE 16. Percentage of communication overhead with percentages of malicious nodes participating in the network.

a result, the nodes need to send requests to other nodes in the network.

On the other hand, DTM relies more on the cumulative average speed than individual speed. As a result, DTM adds less communication overhead than MARINE and TSME. DTM thereby outperforms other similar products in terms of cost-velocity at various speeds. The performance of these DTM is shown in Figures 8, 9, and 10 in various scenarios, including one in which the network shows a variable proportion of malicious nodes. These figures demonstrate that malevolent nodes are more responsible for increased communication overhead than either increased velocity or density. Figures 14, 15, and 16 also illustrate how MARINE and TSME have higher communication costs than DTM.

V. CONCLUSION

The design and development of a reliable trust management scheme for group-based VANETs that satisfies message reliability and quality in VANETs with improved performance were successfully implemented. A reliable group head election scheme enhances GH stability by optimizing link reliability. The proposed Dynamic Group Head Selection (DGHS) considers GH and RSU connection-link reliability, improving GH stability. Trust models (TMs) are integrated into the vehicles to assess received communications' trustworthiness.

DTM proposes a lightweight trust model in a dynamic environment that satisfies message reliability and quality in VANETs with improved performance. The proposed DTM improves the overhead regarding authentication and message distribution with an existing technique. The comparison of the proposed models with prior models using the network simulator OMNET++ version 5.3 in conjunction with a real-world scenario created using the traffic simulator, SUMO, is the third significant contribution of this study. The grouping algorithm was compared with CBLS and TSME, and the average success rate and success rate of queries were measured. On the other hand, DTM was evaluated compared to TSME and MARINE. With a maximum density of 100 vehicles, the DGHS technique improves the average GH lifetime by 10% compared to the CBLS and 13% compared to the TSME. However, DGHS, with a maximum density of 900, improves the average GH lifetime by 43% compared to CBLS and 19% compared to TSME. DTM increases the query success rate by 10% compared to the CBLS and 23% compared to the TSME, even at the slowest speed (40 km/h). At a maximum speed of (100 km/h), D increases query success rate by 14% and 24% over CBLS and TSME. Compared to the CBLS and TSME, the suggested DGHS scheme improves query success by 12% and 43% for the lowest density (100 cars in the network) and 18% and 20% for the highest density (900 vehicles). Precision is decreased by around 5% for MARINE and 10% for the TSME approach for node density. TSME and MARINE show 10% and 2% precision reductions at the lowest speed, respectively. In conclusion, it has been shown that the proposed schemes are reliable for various position-based VANET applications that need precise positioning and trusted messaging.

After investigating the outcomes of the various contributions described above, it was discovered that the proposed algorithms provide superior performance over the older model. The research may be expanded by considering the dynamic group formation, group members leaving a group and other factors while modeling VANETs by including attacks. Additional machine learning methods may be trained on the dataset to evaluate the dataset.

REFERENCES

[1] O. J. Adeyemi, R. Paul, and A. Arif, "An assessment of the rural–urban differences in the crash response time and county-level crash fatalities in the United States," *J. Rural Health*, vol. 38, no. 4, pp. 999–1010, 2021.

[2] H. Woo and M. Lee, "A hierarchical location service architecture for VANET with aggregated location update," *Comput. Commun.*, vol. 125, pp. 38–55, Jul. 2018.

[3] V. K. Yadav, S. Verma, and S. Venkatesan, "Efficient and secure location-based services scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13567–13578, Nov. 2020.

[4] M. A. Mujahid, K. A. Bakar, T. S. Darwish, and F. T. Zuhra, "Cluster-based location service schemes in VANETs: Current state, challenges and future directions," *Telecommun. Syst.*, vol. 76, no. 3, pp. 471–489, 2021.

[5] M. D. de Amorim, F. Benbadis, M. S. Sichitiu, A. C. Viana, and Y. Viniotis, "Routing in wireless self-organizing networks," in *Adaptation and Cross Layer Design in Wireless Networks*. Boca Raton, FL, USA: CRC Press, 2018, pp. 325–353.

[6] R. Kaur, R. K. Ramachandran, R. Doss, and L. Pan, "The importance of selecting clustering parameters in VANETs: A survey," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100392.

[7] M. Sood and S. Kanwar, "Clustering in MANET and VANET: A survey," in *Proc. Int. Conf. Circuits, Syst., Commun. Inf. Technol. Appl. (CSCITA)*, Apr. 2014, pp. 375–380.

[8] S. Harrabi, I. B. Jaffar, and K. Ghedira, "Novel optimized routing scheme for VANETs," *Proc. Comput. Sci.*, vol. 98, pp. 32–39, Jan. 2016.

[9] X. Zhang, R. Li, and B. Cui, "A security architecture of VANET based on blockchain and mobile edge computing," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 258–259.

[10] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "VPPCS: VANET-based privacy-preserving communication scheme," *IEEE Access*, vol. 8, pp. 150914–150928, 2020.

[11] B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102779.

[12] R. K. Dhanaraj, S. Islam, and V. Rajasekar, "A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments," *Wireless Netw.*, vol. 28, pp. 3127–3142, Jun. 2022.

[13] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2553–2571, May 2021.

[14] R. Al-Mutiri, M. Al-Rodhaan, and Y. Tian, "Improving vehicular authentication in VANET using cryptography," *Int. J. Commun. Netw. Inf. Secur.*, vol. 10, no. 1, pp. 248–255, 2018.

[15] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A survey on privacy-preserving authentication schemes in VANETs: Attacks, challenges and open issues," *IEEE Access*, vol. 9, pp. 153701–153726, 2021.

[16] R. K. Dhanaraj, S. H. Islam, and V. Rajasekar, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, Aug. 2019.

[17] S. Asoudeh, M. Mehrjoo, N.-M. Balouchzahi, and A. Bejarzahi, "Location service implementation in vehicular networks by nodes clustering in urban environments," *Veh. Commun.*, vol. 9, pp. 109–114, Jul. 2017.

[18] R. Pal, N. Gupta, A. Prakash, and R. Tripathi, "Adaptive mobility and range based clustering dependent MAC protocol for vehicular ad hoc networks," *Wireless Pers. Commun.*, vol. 98, no. 1, pp. 1155–1170, Jan. 2018.

[19] U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks," *Proc. Comput. Sci.*, vol. 46, pp. 965–972, Jan. 2015.

[20] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali, and S. Begum, "VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead," *J. Sensors*, vol. 2018, pp. 1–17, Jul. 2018.

[21] A. Jesudoss, S. V. Kasmir Raja, and A. Sulaiman, "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme," *Ad Hoc Netw.*, vol. 24, pp. 250–263, Jan. 2015.

[22] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in vehicular ad hoc networks: An economic incentive model based approach," in *Proc. Comput., Commun. IT Appl. Conf. (ComComAp)*, Apr. 2013, pp. 13–18.

[23] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Trans. Syst., Man, Cybern., C*, vol. 41, no. 3, pp. 407–420, May 2011.

[24] N. Yang, "A similarity-based trust and reputation management framework for vanets," *Int. J. Future Gener. Commun. Netw.*, vol. 6, no. 2, pp. 25–34, 2013.

[25] M. Gerlach, "Trust for vehicular applications," in *Proc. 8th Int. Symp. Auto. Decentralized Syst. (ISADS)*, Mar. 2007, pp. 295–304.

[26] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[27] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. Int. Conf. Netw. Syst. Secur.* Cham, Switzerland: Springer, 2013, pp. 94–108.

[28] R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 1652–1669, Nov. 2014.

[29] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: A lightweight self-organized trust model in VANETs," *Mobile Inf. Syst.*, vol. 2016, pp. 1–15, Dec. 2016.

[30] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for VANETs," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 201–206.

[31] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Comput. Elect. Eng.*, vol. 43, pp. 33–47, Apr. 2015.

[32] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Securing vehicular networks: A reputation and plausibility checks-based approach," in *Proc. IEEE Globecom Workshops*, Dec. 2010, pp. 1550–1554.

[33] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[34] R. Shrestha and S. Y. Nam, "Trustworthy event-information dissemination in vehicular ad hoc networks," *Mobile Inf. Syst.*, vol. 2017, pp. 1–16, Nov. 2017.

[35] C. Chen, J. Zhang, R. Cohen, and P. H. Ho, "A trust-based message propagation and evaluation framework in VANETs," in *Proc. Int. Conf. Inf. Technol. Converg. Services*, 2010.

[36] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. Khurram Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[37] S. Goudarzi, A. H. Abdullah, S. Mandala, S. A. Soleymani, M. A. R. Baee, M. H. Anisi, and M. S. Aliyu, "A systematic review of security in vehicular ad hoc network," in *Proc. 2nd Symp. WSCN*, 2013, pp. 1–10.

[38] F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, May 2012.

[39] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.

[40] M. A. Bender, M. Farach-Colton, R. Johnson, B. C. Kuszmaul, D. Medjedovic, P. Montes, P. Shetty, R. P. Spillane, and E. Zadok, "Don't thrash: How to cache your hash on flash," in *Proc. 3rd Workshop Hot Topics Storage File Syst.*, 2011.

[41] F. Boeira, M. Asplund, and M. P. Barcellos, "Vouch: A secure proof-of-location scheme for VANETs," in *Proc. 21st ACM Int. Conf. Model., Anal. Simul. Wireless Mobile Syst.*, Oct. 2018, pp. 241–248.

[42] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. R. Baee, and S. Mandala, "Trust management in vehicular ad hoc network: A systematic review," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, pp. 1–22, Dec. 2015.

[43] L. J. G. Villalba, A. L. S. Orozco, A. T. Cabrera, and C. J. B. Abbas, "Routing protocols in wireless sensor networks," *Sensors*, vol. 9, no. 11, pp. 8399–8421, 2009.

[44] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, "Cuckoo filter: Practically better than Bloom," in *Proc. 10th ACM Int. Conf. Emerg. Netw. Experiments Technol.*, Dec. 2014, pp. 75–88.

[45] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Apr. 2008, pp. 1238–1246.

[46] A. Singh, S. Garg, R. Kaur, S. Batra, N. Kumar, and A. Y. Zomaya, "Probabilistic data structures for big data analytics: A comprehensive review," *Knowl.-Based Syst.*, vol. 188, Jan. 2020, Art. no. 104987.

[47] S. Shah, B. Shah, A. Amin, F. Al-Obeidat, F. Chow, F. J. L. Moreira, and S. Anwar, "Compromised user credentials detection in a digital enterprise using behavioral analytics," *Future Gener. Comput. Syst.*, vol. 93, pp. 407–417, Apr. 2019.

[48] R. Aissaoui, A. Dhraief, A. Belghith, H. Menouar, H. Mathkour, F. Filali, and A. Abu-Dayya, "HCBLS: A hierarchical cluster-based location service in urban environment," *Mobile Inf. Syst.*, Jan. 2015.

[49] D. Zhang, H. Ge, T. Zhang, Y.-Y. Cui, X. Liu, and G. Mao, "New multi-hop clustering algorithm for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 4, pp. 1517–1530, Apr. 2019.

[50] R. Abassi, A. B. C. Douss, and D. Sauveron, "TSME: A trust-based security scheme for message exchange in vehicular ad hoc networks," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–19, 2020.

[51] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-Middle attack resistant trust model in connected vehicles," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3310–3322, Apr. 2020.

MUHAMMAD HALEEM JUNEJO received the B.Eng. degree from the Mehran University of Engineering and Technology (MUET), Jamshoro, and the M.Sc. degree in satellite communication engineering from the University of Surrey, U.K. He is currently pursuing the Ph.D. degree in electrical engineering with Universiti Teknologi Malaysia (UTM). His current research interests include privacy, security, trust management, WSNs, the IoT, machine learning (ML), artificial intelligence (AI), and VANETs.

AB AL-HADI BIN AB RAHMAN (Senior Member, IEEE) received the B.S. degree from the University of Wisconsin–Madison, USA, the M.Eng. degree from Universiti Teknologi Malaysia (UTM), Johor, and the Ph.D. degree from École Polytechnique Fédérale de Lausanne, Switzerland. From 2018 to 2020, he was a Research Engineer with Mediatek Singapore. He is currently a Senior Lecturer with UTM. His current research interests include hardware architecture and design, signal processing, and machine learning.

RIAZ AHMED SHAIKH received the Ph.D. degree from the Computer Engineering Department, Kyung Hee University, South Korea, in 2009. From October 2009 to January 2012, he was a Postdoctoral Fellow with the Computer Security Research Laboratory, University of Quebec, Outaouais, Canada. In 2012, he was an Assistant Professor with the Computer Science Department, King Abdulaziz University, Saudi Arabia. Since August 2022, he has been an Associate Professor with the School of Computing Sciences, University of East Anglia, U.K. His current research interests include privacy, security, trust management, risk estimation, sensor networks, vehicular networks, and the IoT.

KAMALUDIN MOHAMAD YUSOF received the B.Eng. and M.Eng. degrees from Universiti Teknologi Malaysia (UTM) and the Ph.D. degree from Essex University, U.K. He is currently a Senior Lecturer of electrical engineering with UTM. His current research interests include signal propagation, ranging estimation, localization, wireless sensor networks (WSNs), cognitive radio (CR), frequency scanning, software-defined radio (SDR), networking, software-defined networks (SDNs), the Internet of Things (IoT), crowdsourcing, data mining, privacy, security, trust management, policy validation, and VANETs.

SHAHIDATUL SADIAH (Member, IEEE) received the B.Eng. degree in communication network engineering and the M.Eng. degree in electronic and information system engineering from Okayama University, Japan, in 2013 and 2015, respectively, and the Ph.D. degree in information engineering from Hiroshima University, Japan, in 2018. She has been with the Department of Electronics and Computer Engineering, Universiti Teknologi Malaysia, as a Senior Lecturer, since January 2019. Her current research interests include cryptography, information security, digital system design, and computer architecture.