Wireless Networks (2019) 25:4639–4661
https://doi.org/10.1007/s11276-018-1756-6

Trust model for secure group leader-based communications in VANET

Hamssa Hasrouny[1,2] · Abed Ellatif Samhat[2] · Carole Bassil[3] · Anis Laouiti[1]

Published online: 17 May 2018

Abstract

VANET aims to improve safety for all road users. Vehicles exchange safety messages over wireless communication links which are prone to multiple attacks. To enhance the existing security of V2V communications, we propose in this paper a security framework based on vehicles behavior analysis. We define a Hybrid Trust Model (HTM) and a misbehavior detection system (MDS) where a trust metric is assigned to every vehicle depending on its behavior. Using this trust metric, a classification of the vehicles into malicious or honest is done. HTM is based on-the-fly group formation which helps to manage the communication between vehicles and the back-end system by selecting the most trustworthy node as group leader (GL). Vehicles and GL will cooperate with each other within the group and with the back-end system to detect the malicious node and to notify the Misbehavior Authority. The latter takes appropriate actions to limit the consequences of the malicious behaving node. Performance evaluation of HTM and MDS is carried out using Groovenet Simulator. Results show the efficiency of the proposed model to select the trustworthy vehicles and to monitor their behaviors, as well as to classify them and to deactivate the malicious ones.

Keywords Trust evaluation · Performance · Misbehavior detection · Security · Group formation · Decentralized

1 Introduction

VANET (Vehicular Adhoc Network) ecosystem consist of vehicles with on board units (OBUs), roadside units (RSUs) set up along the roadways and a back-end system offering various services (registration, authorization, revocation…). All these entities are interacting together for traffic control and improving road safety. The communication is either V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) or hybrid via DSRC (Dedicated Short Range Communication) in a single or multi-hop mode [1]. After exploring the related works in the security architectures [2], standards [3], protocols, attacks, approaches and solutions in VANETs [4], many open issues require more investigation. Some of these issues are the capability of the network to self-organize within a high mobile network environment, the trustworthiness evaluation of nodes participating in VANETs and their misbehavior detection, the revocation process and the Certificate Revocation List (CRL) management and distribution.

Security is one of the main concerns in VANETs, and trust is a key element of security that prevents generic attacks on the network [5, 6]. The trust value is used to measure the belief between two entities (the truster and the trustee). Its value allows us to determine if we can trust the trustee or not (related to a situation and a time). The trust evaluation plays a vital role in the security and quality in VANET since this latter is based on data exchange (safety/non-safety applications) among vehicles. Vehicles can behave selfishly or maliciously for individual benefits. They can falsify or alter the exchanged safety messages which endanger people's life [7]. Trusting a malicious node

✉ Hamssa Hasrouny
hamssa.hasrouny@telecom-sudparis.eu

Abed Ellatif Samhat
samhat@ul.edu.lb

Carole Bassil
cbassil@ul.edu.lb

Anis Laouiti
anis.laouiti@telecom-sudparis.eu

[1] Telecom SudParis, SAMOVAR, CNRS, University Paris-Saclay, 9 rue Charles Fourier, 91011 Evry Cedex, France

[2] Faculty of Engineering-CRSI, Lebanese University, Hadath Campus, Hadath, Lebanon

[3] Faculty of Science II, Lebanese University, Fanar Campus, Fanar, Lebanon

can lead to unpredicted threats, like affecting the network efficiency, large consumption of resources and exposure to attacks. Especially, if this malicious node is the group leader (GL) which has a crucial role within the group; it is responsible for group keys generation and distribution based on group members' activities. This issue implies that the GL must be the most trustworthy vehicle to accomplish these objectives. Throughout the literature, group formation enhances vehicular safety in VANETs [1, 8–11]. It is a valid strategy to strengthen privacy, to provide authentication, and to limit the unauthorized access. The group-based authentication reduces the communication with the infrastructure. Through group signature, it ensures integrity, non-repudiation, confidentiality, and anonymity. Therefore, using a trust evaluation technique becomes a must to ensure a safe and secure driving environment in VANETs. Thus allowing vehicular sensing networks (VSNs) in smart cities to benefit from VANET secure V2V and V2I communications, to transmit and integrate reliable and important information related to a city's operation [12].

Different families of trust evaluation approaches exist [7, 13–18]: policy-based approach, monitoring based approach, and the hybrid approach. In the Policy approach, it allows expressing the different attributes, the actions to perform and the different conditions to establish trust. In Monitoring approach, it is based on monitoring solutions to evaluate the trust level of an entity. It is calculated with different strategies: either direct or indirect evaluation. The direct calculation is based on the exchange of attributes or combined parameters in P2P (Peer-to-Peer) networks. The indirect calculation (or reputation) is based on the feedback of the different entities participating in the model. Finally, the Hybrid approach aims to combine both to evaluate the trust. All these models are based on two types of architectures: centralized or decentralized frameworks. For the centralized, a central node will be delegated to monitor all communications, analyze the historical data and evaluate the trust level. While for the decentralized, each node can have the role of a truster and a trustee. Each one may evaluate the trust level of any other entity. A trusted module has to be installed then in each node. Figure 1 illustrates the different trust evaluation approaches mentioned above.

In this paper, we focus on the trustworthiness evaluation of vehicles participating in VANET and their misbehavior detection within groups. Vehicles will organize themselves into groups where each group is managed by a group leader. The GL can communicate directly with the members of its group, i.e., vehicles are located within its radio range. Notice that vehicles may belong to more than one group; in that case, they can play a relay role and allow multi-hop communication between different groups. The most critical issues to be resolved are: how to define the trust parameters and evaluate them, and how to combine the different evaluations and share feedbacks among participant vehicles. The proposed solution detailed in the coming sections will answer all these concerns. The main contributions of this paper are:

- We propose a group-based Hybrid Trust Model (HTM) within a secure architecture based on the combination of centralized and decentralized management to monitor vehicles' behavior.
- We design a mechanism to evaluate the trust value used for selecting the most trustworthy vehicles as potential group leaders and detecting any malicious vehicle that can behave in a bad way.
- We define a misbehavior detection system (MDS) using misbehavior detection rules at the back-end and within vehicles to mitigate the effect of malicious vehicles (even if the malicious is a GL).

The rest of the paper is organized as follows: Sect. 2 presents some existing related works. Section 3 details the proposed Trust Model. Simulation results evaluating the performance of our scheme are given in Sect. 4. In Sect. 5, we expand the assets of the proposed Trust Model. Finally, we conclude in Sect. 6.

2 Related works

In this section, we review some existing schemes, observe their merits and limitations and compare their choices. Many researchers investigated the Trust evaluation within VANETs [15–39] using various techniques. For the trust computation, it can be either based on the direct calculation for predefined parameters between two communicating vehicles (sender and receiver), or indirect calculation based on the neighboring opinion sent to the receiver about the sender for evaluation, or hybrid mode which is the combination of both cases direct/indirect. To evaluate the trust of a certain vehicle, the decision making can be either centralized in an entity within the infrastructure, or decentralized through participating vehicles, or combination of both centralized/distributed. For the participation, it can be either proactive or reactive. Proactive means controlling a situation rather than responding to it; while reactive means the opposite. For the misbehavior detection scheme, it is broadly divided into two categories: data-centric and non-data centric. The meaning of data-centric is to believe on information rather than the source of information which means detect misbehavior basis of collected information (e.g., beacons, alert message..) while in some scheme, the misbehavior is detected by a Trusted Authority

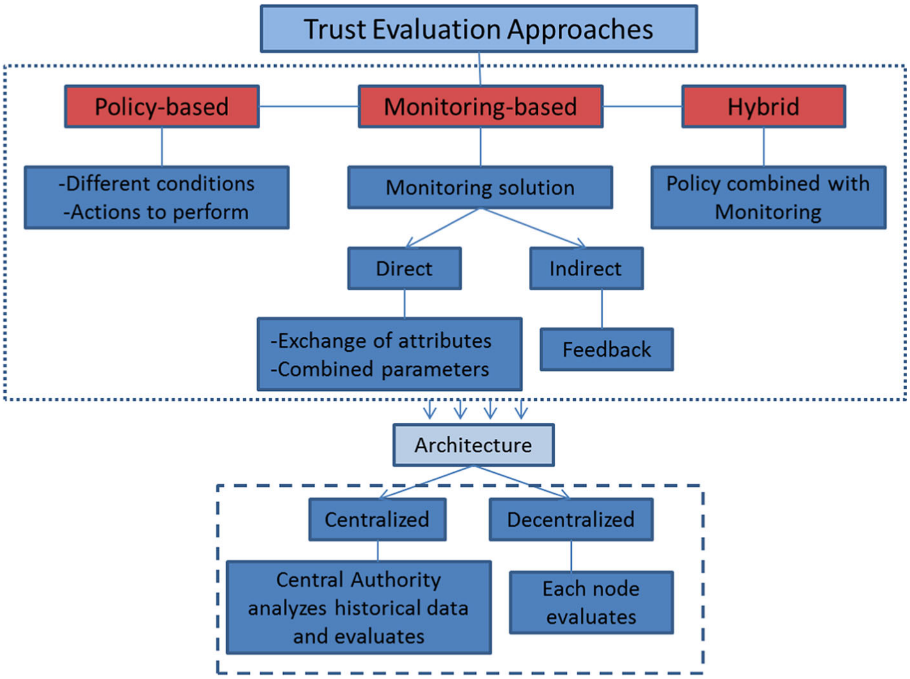


Fig. 1 Different trust evaluation approaches

(TA) itself, which may require additional overhead and long time for detection.

Trust establishment approaches can be divided into an infrastructure based trust or self-organizing based trust [15]. Within the infrastructure models [25–27], trust establishment relies on verifying certificates provided to vehicles, while in the self-organizing models [28, 29] the trust establishment is realized based on cooperation between vehicles. Infrastructure based trust can have either centralized or distributed decision-making management.

Both models (infrastructure or self-organizing) can be either Entity or Data oriented. Entity oriented models maintain the trust of other nodes individually, i.e., no need for the third party. While Data oriented models are based on similarity mining technique used for identifying similar messages or similar vehicles [16, 28–36]. Messages correlation or vehicles verification provides appropriate trust metrics values based on direct, indirect or hybrid calculation [17]. Trust metric values are used for nodes classification and establishment of a secure and reliable communication between them [30].

The privacy is better preserved in the self-organizing trust models [28, 29] than in the infrastructure ones; VANET users are anonymous within their groups in group-based VANET communications. The group members are anonymous for outsiders, i.e., only group managers (group-leaders) can trace their group members. Additionally, the self-organizing simplifies the process of building trust based on received messages. Thus provide better and more confident decisions for selecting the most appropriate GL by considering the trust value of vehicles from different participants.

The proposed solutions mentioned above [15–38] designed particularly for VANET partially cover the security requirements mentioned in [39]. Those requirements are Privacy, Adaptive to rapid network changes, Scalability, Realistic (real test scenarios), Low network overhead, Decentralization. Table 1 shows a comparison between the existing solutions based on the different techniques and characteristics mentioned above.

Some of the existing gaps in the previously proposed trust solutions are: (1) in data oriented models, they deal more with trustworthiness of the data received from other nodes rather than the nodes themselves; so trust is purely based on events disseminated by entities, and it needs to be established regardless of any prior interaction with these entities [25, 31]; (2) sometimes the evaluation of specific information could be tampered or unavailable when needed; attack detection techniques are missing, especially for sophisticated attacks such as “Sybil attack”. A lack of a risk analysis for the proposed models [20, 30]; (3) in combined models, reputation relies on the existence of other peers that have enough knowledge and can be trusted. The absence of these peers will degrade the evaluation [31]; *iv*.network overhead can be increased by continuous routing and security updates [34].

As a result, this triggers further research in this field for potential improvements to define a new framework for a trust model in VANETs. In this paper, we propose a Hybrid Trust Model (HTM) that covers the major security requirements mentioned in [39].

Table 1 Comparison between different Trust Models

	Specifications	Self-organizing trust	Infrastructure based trust
Cooperation	Centralized		[25]
	Decentralized	[28–30, 34, 35]	[23, 24, 27, 32, 36]
	Hybrid		[16, 17, 26]
Certificate	Certificate-based trust	[28, 29]	[16, 25–27]
Data analysis	Entity oriented	[30, 34, 35]	[24, 27, 32, 33, 36]
	Data oriented		
	Static info (event)	[28–31, 35]	[16, 18, 24, 31–33, 36, 37]
	Dynamic info (vehicle)	[28, 34]	[31]
Trust and behavior	Location based		[36]
	Direct/indirect trust calculation	[17, 20, 26, 30, 34]	[17, 19, 26]
	Privacy preserving	[28, 29]	[22]
	Misbehavior detection	[20, 28]	[17, 26, 33, 38]

Table 2 compares our proposed model to some existent trust evaluation and misbehavior detection systems based on a list of criteria. We define this list to highlight the ability of these systems to evaluate the trustworthiness of participating nodes in a rapidly changing network with the possibility of several frequent attacks, preserving the privacy of the participants and with low network overhead. The authors in [5, 37] analyze the probabilistic and deterministic approaches (individually and combined) to estimate trust for VANET security. The probabilistic approach determines the trust level of the peer vehicles based on received information. The deterministic approach measures the trust level of the received message by using distances calculated using received signal strength (RSS) and the vehicle's geolocation (position coordinate). A combination of the probabilistic and deterministic approaches gives better results compared to individual approaches. [38] propose an algorithm DMN (Detection of Malicious Nodes) in VANETs improves DMV (Detection Malicious Vehicle) Algorithm regarding an effective selection of verifiers for detection of malicious nodes and hence improves the network performance. The comparison in Table 2 shows the efficiency of our proposed model that will be detailed in the next section.

3 Proposed trust model

In this paper, we propose a Hybrid Trust Model (HTM) to evaluate vehicles behaviors and estimate their corresponding trust metric values. HTM serves to judge vehicles trustworthiness and reports to Misbehavior Authority (MA) which takes appropriate actions to deactivate the malicious node. The node with highest trust metric value will be a potential GL for its neighboring vehicles. The architecture of this Trust Model is based on a secure, modular and distributed PKI architecture adopted by NHTSA (National Highway Traffic System Administration) [40], and on group formation and GL-based communication. We adopt the NHTSA architecture and the group-formation to benefit from several security advantages detailed in Sect. 5.

This model involves a monitoring system processing based on the cooperation between vehicles and the validity of their broadcasted data. It is a continuously and dynamically monitoring process changing at each received values of monitoring. HTM provides a secure environment that can mitigate the potential attacks or minimize their duration on VANETs. The cooperation within the Trust Model is a combination of centralized and distributed entities which aims to preserve participants' privacy and tries to maintain low network overhead. For each node, the Trust

Table 2 Comparison between trust evaluation and misbehavior detection models

Solution	Low network overhead	Delay intolerant	Robustness/security	Privacy	Decentralized	Short-lived association	Misbehavior detection
Our proposed model	x	x	x	x	x	x	x
[37]	x	x			x		
[5]		x			x		x
[38]	x	x			x		x

metric is based on direct and indirect calculation, transmitted to the nearest GL which transfers all trust metrics to the back-end system through the nearest RSU. RSUs are widespread on the roadside to fulfill specific services to the back-end system. One of these services is relaying information between OBUs and the back-end system and vice versa. However, in the absence of RSU in range, OBUs may relay information in a multi-hop V2V scenario to reach an RSU. In the back-end system, the Certificate Authority (CA) will compute a global trust metric for each participating node. At different stages, the trust metric has a threshold when exceeded a node is considered trustworthy; otherwise, a proposed set of rules is used to filter out the malicious ones. A Risk Analysis for the proposed trust model is detailed in our previous work [6].

3.1 Architecture

The reference model of the HTM architecture and its components is briefly described in Fig. 2 below. The proposed trust model is composed mainly of two parts: A) back-end system and B) vehicular groups. Part ‘A’ corresponds to NHTSA architecture. Its main entities are classified based on their functionalities into four groups. These groups are: policing, certificate processing, communication with vehicles and Misbehavior Detection/Revocation. Part B is composed of groups of vehicles communicating with each other, with GLs and with the back-end system through the RSUs. RSU is a base station set up along the roadway to allow vehicles to back-end system communication using DSRC protocol. Through RSUs, vehicles can report misbehaviors, receive certificate revocation lists (CRLs) and other traffic/safety updates from the back-end system. It depends on the road type (secondary road, interstate highway…) to determine how many RSUs would appear to be optimal for DSRC communications; the primary objective is to achieve the required coverage. RSUs inter-distance can be considered of 1000 m, which represents the maximum transmission range of DSRC protocol.

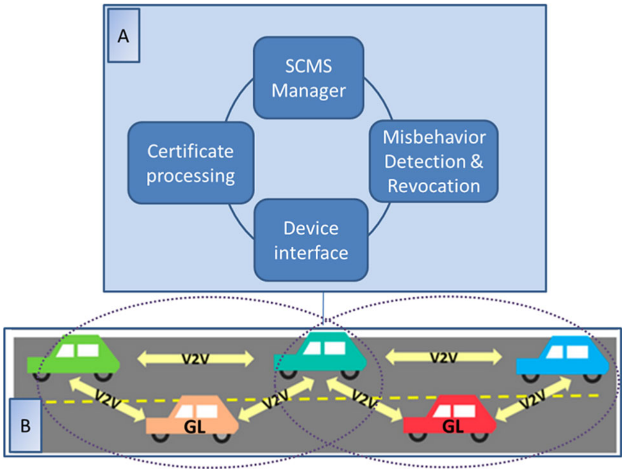


Fig. 2 Trust model components

NHTSA architecture is based on PKI and contains interconnected entities based on their role [1, 40]. NHTSA system contains functional entities responsible for:

- *Management and policies*: The Security Certificate Management System (SCMS) Manager is the entity responsible for generating security policies for the whole system.
- *Long-term certificates enrolment for OBUs*: the Enrolment Certificate Authority (ECA), the Device Configuration Manager (DCM) and Certification Services are the entities that interconnect together to generate the long-term enrolment for vehicles within the vehicular network.
- *Short-term digital certificates (pseudonyms) for OBUs*: The Root Certificate Authority (CA), Intermediate CA, Linkage authority 1 and 2, Pseudonym CA, Registration Authority (RA) and the Request Coordinator collaborate with each other to assure the anonymity of the participant vehicles within the system.
- *Misbehavior detection and certificate revocation:* Misbehavior Authority (MA), Location Obscurer Proxy (LOP) and the Certificate Revocation List (CRL) Store cooperate to ensure the continuation of the trusted nodes only, by producing/publishing CRL and misbehavior reports in VANET.

For the grouping, there are many ways to form groups in VANETs. We consider on-the-fly group formation where a group leader is elected, and group membership is managed dynamically. It is the most useful way due to its flexibility, but it is mainly challenging for group leader election. A group is formed when there are at least two vehicles within their radio range on the road. A group is composed of the vehicles in a zone of 300 m of radio range around the moving GL. At the initialization, if there is no vehicle in the immediate neighborhood of $v1$, then $v1$ the first vehicle that authenticates in time to the back-end system through the RSU in a certain zone will be elected as the GL. The second vehicle that authenticates to the back-end system in the same zone will be elected as Backup Group Leader (BGL). Later on, it will depend on vehicles behavior (trust metric values) on the road to elect the GL; the vehicle with the highest trust metric value in a group will be considered as potential GL and the second highest trust metric value will be considered as BGL. In case of departure of the GL, we consider two scenarios: (1) GL decides to leave the group near an exit point; (2) GL is out of coverage. In the first scenario, GL informs the back-end system through the RSU about its departure; the back-end system will delegate the GL responsibilities to the BGL, the new GL candidate in its group. At that time, the group will be reformed. It happens that not all vehicles handled by the outgoing GL are in the radio range of the BGL. Those vehicles will try to join another group. In the second scenario, the vehicles members of its group will detect its absence by not receiving periodical beacons from it every 100 ms. They remove it from their neighbors' table after a period of 200 ms and try to join another group.

Every elected GL defines a group id (GID) and broadcasts it to neighboring vehicles. Vehicles are required to use group keys to communicate with a group. The key generation process depends on the schema type we have: either static, e.g., the number of group members is assumed to be fixed or dynamic, e.g., the prospective number of group members is unknown [41]. We have on-the-fly group formation which represents a dynamic schema. For the key generation process, the GL generates its own private key $\mathrm{Pr_{GL}}$, the public key of the group $\mathrm{Pu_{gr}}$ [41], and the symmetric key for the group $\mathrm{K_{gr}}$. $\mathrm{Pr_{GL}}$ is used to issue membership certificates to the prospective group members. $\mathrm{Pu_{gr}}$ is used to identify group members. $\mathrm{K_{gr}}$ is used to encrypt confidential data between group members, e.g. the trust metric values of neighboring vehicles.

A user with a key pair of public and private keys can apply the signature generation algorithm to produce a digital signature on some message. The digital signature ensures the authenticity of the signer based on asymmetric or public-key cryptography. It involves a signer and potentially many verifiers and stands in conflict with privacy. For group communication, we use group signature scheme that ensures authentication with privacy. Users can authenticate themselves on behalf of a group, rather than on individual basis. The group signature incorporates multiple secret private keys with one group public key. The generation of secret signing keys is during the join process of the prospective group members to a group. The admitted group member receives its secret signing key from the GL whereas the GL obtains some (secret) information used later to broke the anonymity of the new member in case of any misbehaving.

Upon the group formation, the GL broadcasts the following keys for all vehicles within its group: the symmetric group key ($\mathrm{K_{gr}}$) encrypted with each vehicle public key $\mathrm{P_u}i$, the public key of the group ($\mathrm{Pu_{gr}}$) encrypted with the symmetric group key ($\mathrm{K_{gr}}$) and signed with the GL private key.

In case of any entry to a group, the GL verifies the new vehicle and give it its secret signing key, $\mathrm{Pu_{gr}}$, and $\mathrm{K_{gr}}$ of the group. Upon exit from a group, the GL updates the authenticated members of the group with new $\mathrm{Pu_{gr}}$ and new $\mathrm{K_{gr}}$.

Vehicles periodically broadcast signed beacons to neighbors. Each includes the short-term certificate of the sender in its header and its digital signature in the trailer [3]. The attached certificate ensures trust in the system while the signature is used for verifying the integrity of the beacon's content. The short-term certificate includes a validity period, the public key of the sender and the digital signature of the authority that issued this certificate. The digital signature is generated by creating a hash of the beacon content and the timestamp using SHA-256, and inputting the hashed content to the Elliptic Curve Digital Signature Algorithm (ECDSA). For every exchange, a vehicle needs to verify the sender if it is not already verified, checks if its certificate is still valid and not revoked, and then verify its signature. The verification of its identity consists of verifying its certificate, i.e., confirms that the digital signature on the certificate included in the beacon is digitally signed by the CA that issued it to the sender. The receiving device should already have a copy of the authorizing certificate for the authority stored onboard. In case it does not, it requests the authorizing certificate from the sending device (Peer-to-Peer certificate distribution). This process is repeated for any number of CAs up to the root CA, which authorizes the entire system. For the validity of a certificate, it consists of checking the validity period then its presence on the Certificate Revocation List (CRL). For the verification process of the digital signature, the sender public key in the attached certificate is used to reverse the signature process, i.e., take the encoded string, decode it with the sender public key, generate the original string and then compare with the sending device information.

Without group formation, the receiving vehicle will verify the certificate of each neighbor and its digital signature using the public key of the issuing CA and the public key of the sender. This procedure produces a delay in the communication process and sometimes overhead over the network (in case of absence of the authorizing certificate onboard of the receiving device). With the group formation, all group members are using the group certificate, and the same public key of the group ($\mathrm{Pu_{gr}}$) to verify any signature generated by the group signing key of any group member. This procedure will reduce the delay and overhead of the certificate and digital signature verification and ensure the anonymity of the group members.

Many attackers can compromise the security of this infrastructure, the vehicles, the data exchanged between vehicles or the infrastructure, and the communication between different parties in VANET. Thus, the grouping and its particular cryptographic mechanism combined with the NHTSA entities ensure that this model architecture will mitigate the risks of these attacks [6].

After presenting the model architecture, we will move to the next section to describe the model work cycle.

3.2 Trust model work cycle

Consider a group of vehicles in Fig. 3 within a geographical area of 300 m radius circulating in a cooperative driving. Each vehicle v monitors all its 1-hop neighbors. For Trust evaluation, we will use the following notations in Table 3.

A new vehicle *i* with public P_u and private P_r keys at the Department Motor Vehicles (DMV) will enroll in the back-end system through the Device Configuration Manager (DCM) before entering the vehicular networks. The DCM plays a role in the bootstrap process by ensuring that a device is cleared to receive its enrollment certificate from the Enrolment Certificate Authority (ECA) and it also provides a secure channel to the ECA. Vehicle *i* will get successively its long-term certificate from ECA and its initial trust value, $T_{glob}(i)_0 = 0.5$ (which means vehicle *i* is a vehicle neither honest nor malicious). This initial global trust value is modified following its behavior on the road. NHTSA has suggested that this bootstrapping function need to take place at the time of OBU manufacture to facilitate the identification of defective equipment [42].

Then vehicle *i* requests its short-term certificates used for privacy preservation within VANETs. This certificate request is signed using the private key corresponding to the public key of the long-term enrollment certificate. This process is done either at the vehicle dealers' locations or gas stations via a new entity named short-term Certificate Issuer Proxy (sh-tCIP). Once the back-end system verifies its digital signature, e.g., the request is coming from a valid device. Vehicle *i* will have P_ui, P_ri associated with the long-term enrollment certificate and a bunch of short-term certificates changing every 5 min. The short-term certificates are used by a vehicle's OBU to authenticate and validate sent and received basic safety messages in VANET and later on for signing misbehavior report in case of detection of any malicious behavior. Once this first step is achieved the vehicle *i* has to join a group of vehicles. It will broadcast signed beacons with its private key corresponding to the public key in the short-term certificates. Beacons are periodical messages broadcasted between vehicles every 100 ms and used to inform neighbors about vehicle position, direction, velocity…Vehicle *i* will get its secret signing key, the public key of this group Pu_{gr} used for asymmetric group signature and the symmetric key of the group K_{gr} used to encrypt confidential data between group members. It happens that a vehicle *i* receives the choice to join several groups; it will launch the join process with their GLs. After verification of vehicle *i* within the GL on-board unit, vehicle *i* will get different secret signing keys and different public group keys from GLs in the different groups for groups' signature. Vehicle *i* will act as a relay between those different groups. A broadcasted alert signed by a member of group1 will be received by vehicle *i* which in turns will sign it by its different secret signing keys received from different GLs and thus the message will be broadcasted via vehicle *i* to different groups. Figure 4 shows the enrollment and join to group process of a vehicle *i* within the Hybrid Trust Model.

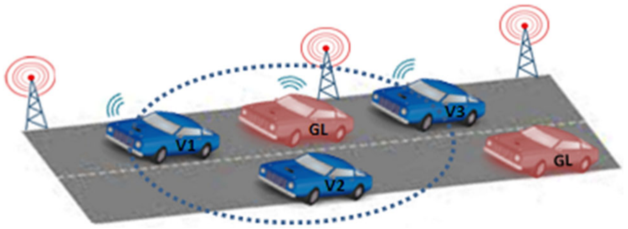


Fig. 3 Vehicular groups

The neighboring vehicles receiving vehicle *i* signed beacons use the corresponding public key of the group to verify *i,* add it to their neighborhood table and record its information in their database. Beacon is usually issued every 100 ms, a checker every 2 × 100 ms will update the neighbors' table about the vehicle status if (alive or not) and remove stale entries to a history table. We define 200 ms to remove a neighbor from neighbors table because we tolerate missing at least one beacon from it otherwise it will be considered not in the neighbors' radio range. Table 4 illustrates the structure of neighbors table.

Each vehicle in the group must monitor all the trust metric parameters. Certain parameters are related to the communication, others are related to the transmission/reception of a vehicle, some parameters are given by the Global Positioning System (GPS) or sensors, and others are based on variables calculation. Such metrics can be categorized into: critical, intermediate and optional. Figure 5 illustrates the monitoring process of vehicle *i* on its neighbors. A vehicle *i* enters a certain area, after joining the group. It will broadcast and receive beacons from neighbors. The gathered information is stored in the Event Data Recorder (EDR) of the vehicle *i,* and the computation process of the trust evaluation will take place. Without loss of generality, all vehicles within the network monitor each other to undertake the trust evaluation that is detailed in next section.

Based on these parameters, the calculation of the trust metric of each vehicle is done as detailed below in the coming sections. This trust metric has a lifetime (200 ms) which is an essential indicator in a rapidly changing topology (VANETs) because it reflects the connection status. No need to keep the outdated trust metric of a certain vehicle that is not my neighbor anymore.

Table 3 Notation for trust evaluation

$T_dv(i)$	"Direct Trust", which evaluates the judgment of vehicle *v* on any vehicle *i* = direct observation
$T_rv(i)$	"Indirect Trust", which evaluates the judgment of vehicle *v* on vehicle *i* based on *v*' neighborhood opinions = other peer recommendation
$T_{tot}v(i)$	"Total Trust" of vehicle *i* calculated by vehicle *v*. It is based on the combination of Direct and Indirect Trust
$T_{glob}(i)_0$	Initial "Global Trust" of vehicle *i* given through the DCM for newly cars entering VANET. It is initialized to **0.5**, which means the newly entered car is neither honest nor malicious. This initial global trust will be updated based on vehicle *i* behavior in VANETs
$T_{glob}(i)$	"Global Trust" of vehicle *i* stored in the back-end system. It represents the updated global trust of vehicle *i* stored within the back-end system database

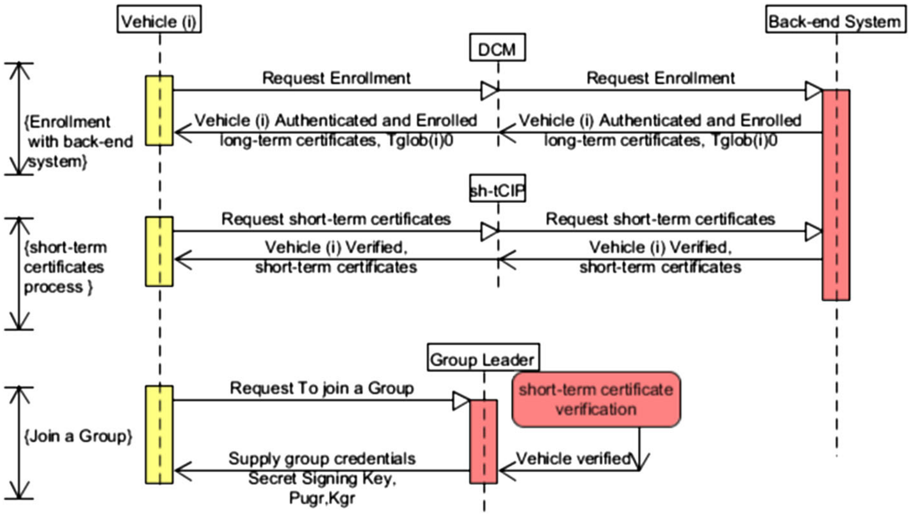

Vehicle (i)
DCM
Back-end System
{Enrollment with back-end system}
Request Enrollment
Request Enrollment
Vehicle (i) Authenticated and Enrolled long-term certificates, Tglob(i)0
Vehicle (i) Authenticated and Enrolled long-term certificates, Tglob(i)0
sh-tCIP
{short-term certificates process }
Request short-term certificates
Request short-term certificates
Vehicle (i) Verified, short-term certificates
Vehicle (i) Verified, short-term certificates
Group Leader
{Join a Group}
Request To join a Group
short-term certificate verification
Vehicle verified
Supply group credentials Secret Signing Key, Pugr,Kgr

Fig. 4 Enrollment and join to group process of vehicle *i* within the trust model

Table 4 Neighbors table

Neighbor ID	Contact time	Status
(Pseudo- ID, for privacy)	Time for first beacon message	GL, or normal participant

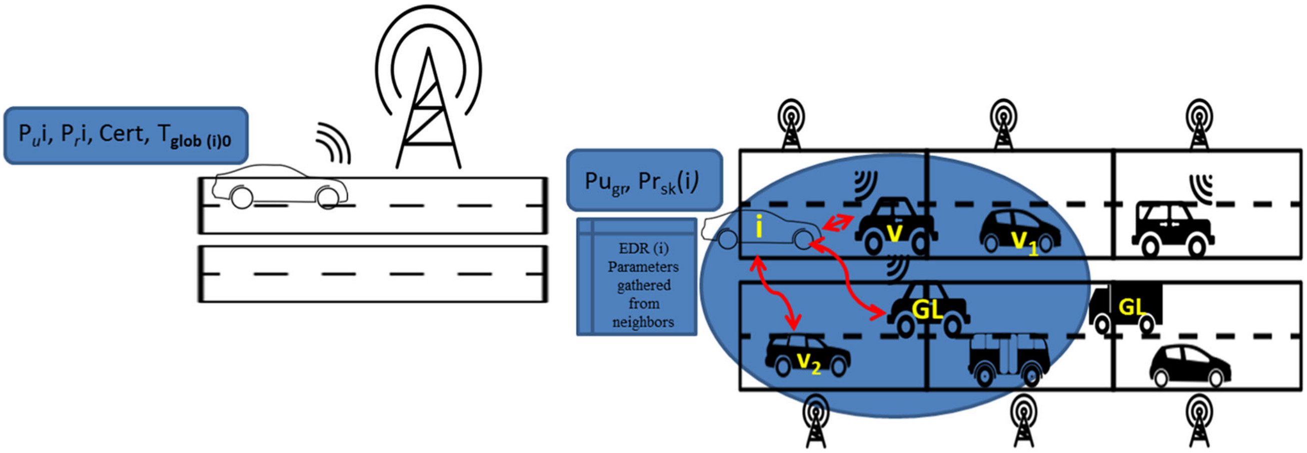

$P_u i$, $P_r i$, Cert, $T_{glob\ (i)0}$
Pu_{gr}, $Pr_{sk}(i)$
EDR (i) Parameters gathered from neighbors
i
v
V_1
GL
V_2
GL

Fig. 5 Monitoring process of vehicle *i*

3.3 Trust computation

In this sub-section, we present all the parameters that intervene in the Trust computation. Our Trust Model is based on direct observation and other peer recommendation. The direct observation is called direct Trust and based on evaluating data received directly from one hop, while the peer recommendation is called indirect Trust and based on forwarding evaluated data by a third party which is a neighbor in our case. The Trust computation is calculated in two cases:

- *Normal mode*: is the case where only beacons are broadcasted between vehicles, no emergency messages are circulating. Beacons are broadcasted between vehicles connected within one hop (within the same range) every 100 ms.
- *Event mode*: is the case where an event happens (emergency or warning message broadcast).

Safety messages include information about the vehicle's behavior. SAE J2735 [43] defines the design specifications for the safety messages [40]. The Basic Safety Message (BSM) is split into two parts: Part I has priority and is transmitted more often, and BSM Part II contains a set of data elements that can vary, and are only broadcasted when an event happens. Part II is then appended to Part I data and broadcasted [40]. Beacons are the BSM part I; alert messages (emergency or warning) are BSM part I concatenated with BSM part II. Emergency messages are like 'Vehicle Crash', 'Vehicle on Fire', 'Vehicle out of Control'… while warning messages are like 'Ice Ahead', 'Emergency Vehicle is Coming', 'Road Closed Ahead'…BSM also needs certain preliminary elements that help a receiving device to know what it is receiving. Those elements are Message-ID, Message count, and Temporary ID. Message ID represents the different types of messages defined by SAE Standard J2735 and sent over DSRC; if it is equal 2, i.e., it is a Basic Safety Message. Message count represents a number in sequence from 0 to 127 assigned to the sent BSM. It helps the receiving vehicle to appropriately put the messages in order and be aware of any missing messages from the sender. Temporary ID is of four-byte string array randomly-generated number that allows a receiving device to associate messages sent from the same device together without knowing the real identity of the sender. This temporary ID is changed to every 5 min when the BSM short-term certificate changes. Having the temporary ID and the certificate change at the same time reduces some of the risk to track a device. In our model, we use this field for vehicle pseudo-ID.

Each disseminated message includes a short-term certificate of the sender in the message header and the signature of the vehicle in the message trailer as illustrated in Fig. 6.

In this model, all neighboring vehicles are supposed to monitor each other and participate in the calculation of the different trust metrics. For that, let us define the following:

3.3.1 Direct trust computation: Normal mode

The beacon is composed of V_{ID}, current position, velocity, status. Where V_{ID} stands for vehicle's pseudo identity, current position stands for its geographical position, velocity its vehicle driving velocity and status (operating mode: Ad hoc mode⋯). The direct trust of a certain vehicle *i* calculated by a certain vehicle *v* is based on many parameters detailed below. These parameters are used in Eq. (1) to reflect the vehicle behavior. Let us consider one of these k parameters 'the velocity' which measures the speed of a vehicle *i*. It is broadcasted in the beacon sent by vehicle *i* to its neighboring vehicle j. When j receives the beacon, it applies the following normalization criteria, which is also illustrated in Fig. 7:

- If the velocity of $i > +25\%$ of the road speed limit or if the velocity of $i < -25\%$ of the road speed limit, then the trust metric m_k reflecting the velocity will be 0.1.
- If the velocity of *i* is between -25 and -15% of road speed limit or if the velocity of *i* is between $+15$ and $+25\%$ of the road speed limit, then the trust metric m_k reflecting the velocity will be 0.5.
- If the velocity of *i* is between -15 and -10% of road speed limit or if the velocity of *i* is between $+10$ and $+15\%$ of the road speed limit, then the trust metric m_k reflecting the velocity will be 0.7.
- If the velocity of *i* is between -10 and $+10\%$ of road speed limit, the trust metric m_k reflecting the velocity will be 0.9.

The geometric mean is applied to the different parameters considered in this case; we use the geometric mean to calculate the direct trust. Referring to [44], a geometric mean is often used to take into account the simultaneous effects of the different parameters. Hence, the direct judgment on vehicle *i*, T_d v(*i*) done by any other vehicle *v*, will be calculated based on the following equation:

$$T_d v(i) = \left[\prod_{j=1}^{k} \alpha_j m_j\right]^{1/k} \tag{1}$$

where α_j is a weight factor, and m_j is the trust metric reflecting one of the many parameters: related to the communication and the transmission/reception of a vehicle, or given by the GPS or other sensors, or based on variables

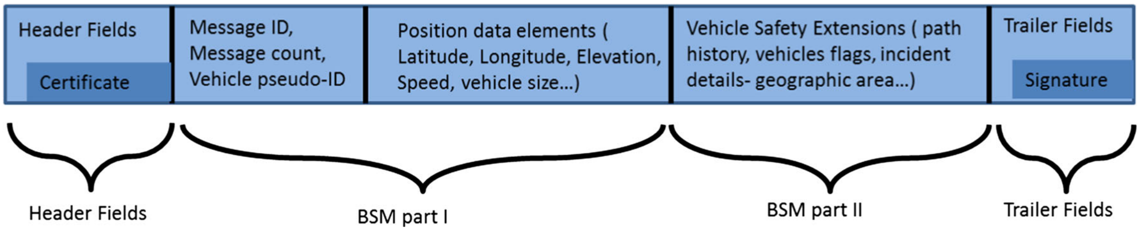


Fig. 6 Safety message format

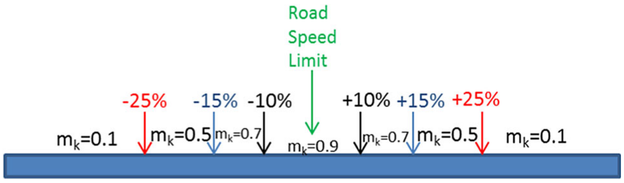


Fig. 7 Normalization of velocity parameter for direct trust calculation

calculation. The k parameters that could be considered include the following:

- *Active frequency:* computes the number of received messages from a certain vehicle every 100 ms, it must be equal to 1. If this is greater than 1, notify the MA to check if it is malicious (DoS or other attacks).
- *Velocity:* measures the speed of a vehicle broadcasted in the beacon.
- *Received Power* (RP): helps to detect the location of the transmitting vehicle. The greater is the received power; the closest is the transmitting vehicle. We rely on this parameter to check the nearest vehicle to a certain location and thus should generate the precise information.
- Number of *confident neighbors* N_v: presents the number of confident neighbors within the vehicle radio range. A confident vehicle means having a trust value exceeding a certain threshold.
- *Internode distance d_i*: measures the distance between the monitored vehicle i and the monitoring vehicle v in the same lane. This distance has a threshold d_{norm} (normal distance expected between two consecutive vehicles, v in front of i). If the internode distance between v and i calculated by vehicle v is less than d_{norm}, then vehicle i is probably a malicious one that wants to cause an accident. Otherwise, if the internode distance calculated is greater than d_{norm}, then vehicle i may slow the traffic to produce congestion.
- *Traffic rules obey*: measures for every vehicle bypassing speed and changing lane indicators received from the radar and updated within vehicles at each stop light. Those includes:
    - s_i: bypassing speed indicator. How often the vehicle exceeded the speed limit.
    - l_i: changing lane indicator.

Within the proposed Trust Model, the direct trusts calculated by vehicle i should be broadcasted to neighboring vehicles. Receiving vehicles will register and use these direct trusts later in their indirect trust calculations. These direct trusts are encrypted with the symmetric key of the group (K_{gr}) then concatenated with the beacon signed by each group member signing key used for group signature. Thus we ensure the confidentiality and integrity of these disseminated values for authenticated group members only.

3.3.2 Indirect trust computation: Normal mode

The Reputation or indirect trust determines the trustworthiness of a vehicle based on the opinions provided by its neighbors. The Reputation or indirect calculation aims to gather and aggregates feedbacks about an entity from other participants (its neighborhoods). Thus the indirect trust of vehicle i, T_r v(i), is an average value calculated based on all direct trusts of vehicle i received from v's neighborhood. We use for this purpose the arithmetic mean. Referring to [44], the arithmetic mean is relevant any time several quantities added together to produce a total and where the individual data points are not dependent on each other.

Within each vehicle v, the indirect trust of neighboring vehicle i, is calculated using Eq. (2):

$$\mathrm{T_r}v(i) = \frac{1}{N}\sum_{j=1}^{N} T_d^j(i) \tag{2}$$

where j, represents a neighboring vehicle of vehicle v; N, represents the number of neighbors sending beacons that contain the direct trust of vehicle i, T_d(i); $T_d^j(i)$, represents direct trust of vehicle i calculated by neighboring vehicle j. It intervenes in the calculation of indirect trust of vehicle v over vehicle i.

3.3.3 Total trust computation: Normal mode

The total trust combines the direct and indirect trust for any vehicle. The total trust is calculated in three steps at three levels: within vehicles, GL and Infrastructure (RSU). The total trust is used to evaluate the trustworthiness of a vehicle.

3.3.3.1 Vehicle level

At vehicle level, the total trust of any vehicle i calculated by a vehicle v and is given by the Eq. (3):

$$\mathrm{T_{tot}}v(i) = \beta * T_d v(i) + (1 - \beta) * T_r v(i) \tag{3}$$

where 0.5 < ß<1, this could be justified by the fact that we considerably trust the direct calculation and we will not neglect the neighboring opinions referred to as the indirect calculation.

Therefore, every vehicle v will fill its database with the values of the direct, indirect and total trusts of all neighboring vehicles i as shown in Table 5. i varies from 1 to n. Where n represents the number of v neighbors.

Within each vehicle, old values within the trust database are updated iteratively following the smoothing move procedure in the following equation:

$$\text{New value} = \alpha * \text{new value} + (1 - \alpha) * \text{old value} \tag{4}$$

where $0.5 < \alpha < 1$, which means we use smoothing update procedure and not overwriting old values. We consider this range since we are more interested in the recently calculated values. The total trust list in Table 5 is used for vehicle trustworthiness evaluation within the vehicles control process (detailed later in Sect. 3.4).

Finally, every vehicle v sends periodically (each 150 ms) its neighboring vehicles total trust list $\mathrm{T_{tot}v}(i)$ to the GL which in turn computes the average total trust for vehicles within its radio range.

3.3.3.2 GL level

At the GL Level, the average Total Trust for vehicle i calculated by a GL is given by Eq. (5):

$$\mathrm{T_{totm}}(i) = \frac{\sum_{j=1}^{n} T_{tot}^{j}(i)}{n} \tag{5}$$

where i, is any vehicle within the GL radio range; n, number of occurrence of vehicle i Total Trust within the GL database; $T_{tot}^{j}(i)$, is the Total Trust of vehicle i calculated by vehicle j.

Moreover, the GL sorts its trust list periodically in descending order thus the most trustworthy vehicle is on top of the list. We consider that even if the GL was not the top list member, no changes in the GL election until the current GL leaves the group. Each time, the GL is passing by an RSU, it transfers the updated Total Trust of any vehicle i, $\mathrm{T_{totm}}(i)$ only. These vehicles average total trusts participate in the selection process of the potential GL in coordination with the back-end system (CA, MA, LOP).

Table 5 Trust database of vehicle v

Vehicle	$\mathrm{T_d v}$ (i)	$\mathrm{T_r v}$ (i)	$\mathrm{T_{tot}v}(i)$
i	Direct trust/v	Indirect trust/v	Total trust/v

3.3.3.3 Infrastructure (RSU) level

At the RSU level, two cases occur for the global trust computation of any vehicle i, $\mathrm{T_{glob}}(i)$:

- When vehicle i belongs to *one group* only, then its global trust $\mathrm{T_{glob}}(i)$ is equal to its average total trust $\mathrm{T_{totm}}(i)$ calculated by one GL. So $\mathrm{T_{glob}}(i) = \mathrm{T_{totm}}(i)$.
- When vehicle i belongs to *several groups*, then the RSU calculates the geometric mean of the $\mathrm{T_{totm}}$(i) received for this vehicle i as in Eq. (6). (e.g., if i belongs to two groups then its $\mathrm{T_{totm}}$(i) will be calculated by two GLs).

$$\mathrm{T}_{glob}(i) = \left\lfloor \prod_{k=1}^{N} T_{Totm}(i)^{1/N} \right\rfloor \tag{6}$$

N, number of groups to which vehicle i belongs.

RSU (infrastructure) as big data-center will merge and update these trust metrics using the smoothing update procedure mentioned in Eq. (4) above and result in a global trust metric for each vehicle. This global trust metric $\mathrm{T_{glob}}(i)$ is used for vehicle evaluation, results classification and then deactivation of malicious ones. More details about vehicle behavior evaluation are expanded in the next section. Figure 8 summarizes the handover process of the different trust metric calculated between the vehicles, GLs and the infrastructure.

After the global trust computation in the normal mode, we will move to the next section to evaluate the global trust computation in the event mode.

3.3.4 Total trust computation: Event mode

The calculations are pretty much the same. For the direct and indirect trust calculation in event mode, we apply the same formulas as in normal mode presented above but with slightly different parameters. We add the following parameters for direct trust evaluation:

- *Forwarding index:* presents the ratio of the number of forwarded messages over the number of transmitted ones.
- *Forwarding delay:* express the difference between timestamps of a received message and forwarded one.
- *Hope count:* shows the number of hops traveled by messages.

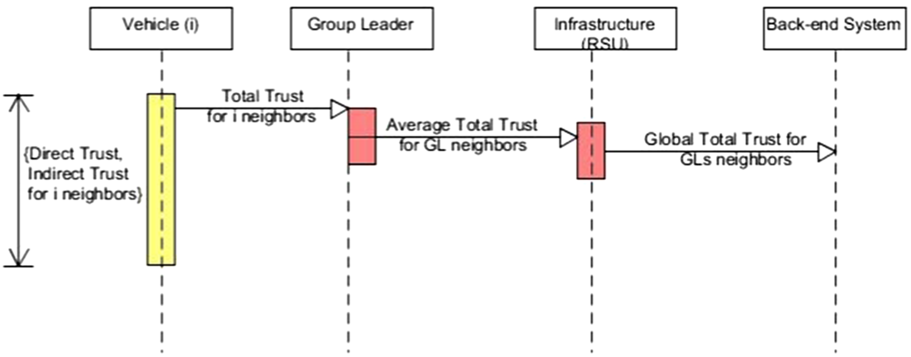

Vehicle (i)
Group Leader
Infrastructure (RSU)
Back-end System
{Direct Trust, Indirect Trust for i neighbors}
Total Trust for i neighbors
Average Total Trust for GL neighbors
Global Total Trust for GLs neighbors

Fig. 8 The handover process of the calculated trust values between vehicles, GLs and the Infrastructure (*RSU*)

- *Signal strength*: based on the position included within the beacon and the received signal strength detected by the receiver sensors; a trustworthy node is considered as the closest one to the Event.

Similarly to normal mode, same steps are adopted for indirect, total and global trust calculation in event mode. Figure 9 illustrates the whole life cycle of event dissemination in the HTM. We consider the following scenario; *v*ehicle A in group1 detected an accident on the road. It generates a safety message signed with its secret signing key and concatenates it with direct trust values already calculated for its neighboring vehicles encrypted with the symmetric key of group1 K_{gr1}. Based on direct interaction, neighboring vehicles receive the transmitted safety message, verify sender A by the public key of group1 and evaluate the direct trust of A based on the value of its parameters mentioned above (velocity, active frequency, forwarding index, forwarding delay, hop count….). The encrypted direct trust values attached to the safety message are stored in the Event Data Recorder of receiving vehicles and are used in the indirect trust calculation. For each neighboring vehicle, we calculate direct trust based on Eq. (1), indirect trust based on Eq. (2) and total trust based on Eq. (3). Several Total trust values are transmitted to GLs which in turn merge similar data based on Eq. (5) then transmit average trust values through the nearest RSUs to the back-end system. This latter generates global trust values for vehicles based on Eq. (6) and stores them in its database using Eq. (4). After a cryptographic resolution for the newly calculated direct trust values and the safety message, each neighboring vehicle of A encrypts its direct trust values, signs the received safety message with its secret signing key, concatenates them together and relays to neighboring vehicles in its radio range (Next forwarder). Thus the multi-hop messages dissemination is achieved.

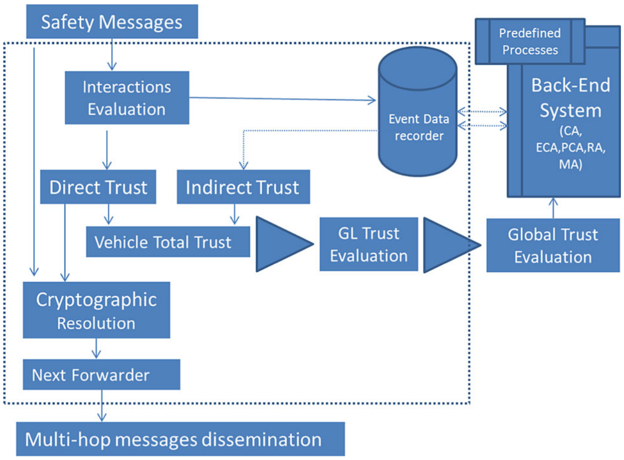


Fig. 9 Trust evaluation process in event mode

We will move to the next section to evaluate the vehicle behavior within the vehicular networks.

3.4 Evaluating vehicle behavior

The trust metric in its different stages has a certain threshold when exceeded; the vehicle is considered trustworthy. Otherwise, a simple set of rules is used to filter out the malicious ones. We consider that each vehicle (including GL—the vehicle with the highest confidence score) controls and sends its report directly to the Misbehavior Authority (MA) [6, 40]. The MA generates the final decision related to trustworthiness in our proposed Model. Moreover, we propose a cooperation between vehicles and GLs in the control process. Since sometimes there are some attacks/attackers can be detected by a vehicle and cannot be detected immediately by the GL.

In the following, we proceed by classifying vehicles between honest, intermediate and malicious. An honest vehicle represents a vehicle with good behavior. A malicious vehicle is a vehicle with bad behavior. An intermediate vehicle is a vehicle with doubtful behavior; it will be under inspection for a certain period (between 300 ms and 5 min). If its misbehaving continues after the period expiry, then it will be considered as a malicious vehicle. Therefore:

- The GL controls and generates its report to MA.
- Every vehicle controls and notifies the GL which in turn notifies MA. If the GL is not reachable

(neighboring vehicles are not receiving beacons from it within a period of 200 ms), then the vehicle can directly notify the MA to take appropriate actions.

- MA analyzes the received data and takes appropriate actions.

3.4.1 Group leader controls

Based on Eq. (5), each GL calculates $\mathrm{T}_{\mathrm{totm}}(i)$, the average total trust for each vehicle i within its radio range. To compute the trust threshold $\mathrm{T}_{\mathrm{thresh}}$ within the GL, we use the following equation:

$$\mathrm{T}_{\mathrm{thresh}} = \frac{\sum_{i=1}^{n} T_{totm}(i)}{n} \tag{7}$$

where n represents the number of vehicles within the GL Database (number of vehicles already verified with the GL). i denotes any vehicle within the GL radio range.

The arithmetic mean is used to calculate the average value of independent events [44]. Different total trust values of vehicle i calculated by different vehicles j are independent of each other. For that reason, we used the arithmetic mean in the $\mathrm{T}_{\mathrm{thresh}}$ calculation.

A set of rules is used in each GL to classify every vehicle i within its radio range based on the following:

If the average total trust of vehicle i, $\mathrm{T}_{\mathrm{totm}}(i)$, calculated by the GL exceeds its trust threshold ($\mathrm{T}_{\mathrm{thresh}}$) then vehicle i is considered an honest vehicle. Otherwise, if the average total trust of vehicle i, $\mathrm{T}_{\mathrm{totm}}(i)$, falls between $(\mathrm{T}_{\mathrm{thresh}})/2$ and $\mathrm{T}_{\mathrm{thresh}}$, then vehicle i is considered an intermediate vehicle. The GL puts vehicle i under inspection for a specified period t; if t expires and vehicle i remains with its same behavior, then the GL considers vehicle i as a malicious one and notifies the MA. Differently, if the average total trust of vehicle i, $\mathrm{T}_{\mathrm{totm}}(i)$, is less than the half of the trust threshold value, $(\mathrm{T}_{\mathrm{thresh}})/2$, then vehicle i is considered a malicious vehicle. The GL notifies the MA. This set of rules is also illustrated in Fig. 10.

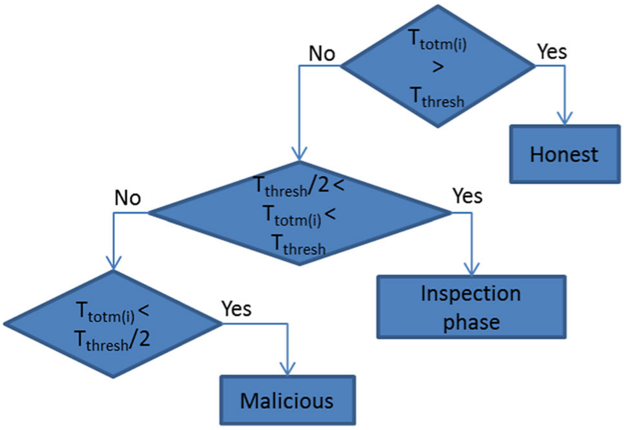


Fig. 10 GL trustworthiness evaluation

3.4.2 Vehicle-to-vehicle control

There is a difference in the evaluation process of vehicles behavior between normal and event mode. We introduce an accordance parameter that differs in both cases. The coming subsections detail the vehicle-to-vehicle control respectively in normal and in event mode.

3.4.2.1 Vehicles control: Normal mode A normal mode presents the case where only beacons are broadcasted between vehicles; no emergency messages are circulating in the vehicular networks. In normal mode, we introduce a new parameter $\mathrm{A}v(i)$: "accordance parameter" of a vehicle v over vehicle i calculated in the following equation:

$$Av(i) = \frac{\mathrm{T_d}v(i)}{\mathrm{T_r}v(i)} = \frac{\text{direct trust of i calculated by } v}{\text{indirect trust of i calculated by } v} \tag{8}$$

The accordance parameter $\mathrm{A}v(i)$ is the ratio of direct trust of vehicle i $\mathrm{T_d}(i)$ calculated by vehicle v, over its indirect trust calculated by neighbors.

We also compute the trust threshold within each vehicle v as in Eq. (9):

$$\mathrm{T}_{\mathrm{thresh}}(v) = \frac{\sum_{i=1}^{n} T_{tot}(i)}{n} \tag{9}$$

where i varies from 1 to n; n represents the number of v neighbors.

The accordance parameter $\mathrm{A}v(i)$, the trust threshold $\mathrm{T}_{\mathrm{thresh}}(v)$ and the direct trust of vehicle i, $\mathrm{T_d}v(i)$, are inputs for vehicle v to judge the trustworthiness of vehicle i. The set of rules used within each vehicle v to classify neighboring vehicle i consists of the following:

If the accordance parameter of vehicle v over vehicle i, $\mathrm{A}v(i)$, is 1, i.e., the judgment of vehicle v over vehicle i is similar to the feedback received from v's neighbors regarding vehicle i. We consider the direct trust of vehicle v over vehicle i, $\mathrm{T_d}v(i)$, if it is greater than the trust threshold calculated within vehicle v, $\mathrm{T}_{\mathrm{thresh}}(v)$, then vehicle i is considered an honest vehicle; otherwise, vehicle i is considered a malicious one.

If the accordance parameter of vehicle v over vehicle i, $\mathrm{A}v(i)$, is greater than 1, i.e., the judgment of vehicle v over vehicle i is different from the feedback received from v's neighbors regarding vehicle i. We consider the direct trust of vehicle v over vehicle i, $\mathrm{T_d}v(i)$, if it is greater than the trust threshold, $\mathrm{T}_{\mathrm{thresh}}(v)$, then vehicle i is considered an honest vehicle; otherwise, vehicle i is considered an intermediate vehicle under inspection phase.

If the accordance parameter of vehicle v over vehicle i, $\mathrm{A}v(i)$, is less than 1, i.e., the judgment of vehicle v over vehicle i is different from the feedback received from v's neighbors regarding vehicle i. We consider the direct trust of vehicle v over vehicle i, $T_d v(i)$, if it is greater than the trust threshold, $T_{thresh}(v)$, then vehicle i is considered an intermediate vehicle under inspection; otherwise, vehicle i is considered a malicious one;

As mentioned before, the inspection period is used for monitoring intermediate vehicles. Its duration varies between 300 ms to 5 min. If this period expires and the misbehaving continues, vehicle v notifies the GL which in turn investigates and informs the MA.

The set of rules within each vehicle v is also illustrated in Figs. 11, 12 and 13.

3.4.2.2 Vehicles control: Event mode For evaluating vehicle behavior based on the reputation of a certain event, we adopted a model similar to that discussed for the normal mode with a slight difference. An event can be an alert (emergency or warning) as described in Sect. 3.3. The accordance parameter $Av(i)$ used as input for the model, is declared in Eq. (10):

$$Av(i) = \frac{Rep_{i(E)}}{Rep_{v(E)}} \tag{10}$$

For evaluating vehicle behavior based on a certain event, we consider as in [30] the reputation of a vehicle v related to this event $Rep_v(E)$. An Event Reputation aims to gather and aggregates feedbacks about the event from other participants [18]. To calculate the event reputation, we proceed as follows. If an event E occurs in a certain zone, we assume that vehicle i is in the zone of this event. If it detects it (with sensor), then $Rep_i(E) = 1$, if it does not detect it by its sensor but receives it through a message received from others then $Rep_i(E) = 0$.

$Rep_i(E)$: the reputation of vehicle i relative to this event E.

$Rep_v(E)$: the reputation of vehicle v relative to this event E.

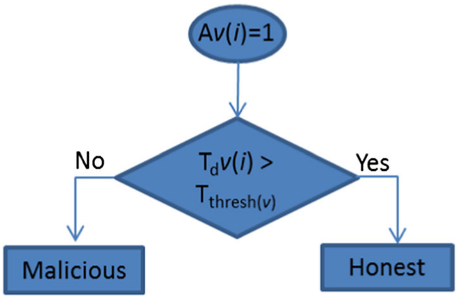


Fig. 11 Vehicles evaluation based on accordance parameter $Av(i) = 1$

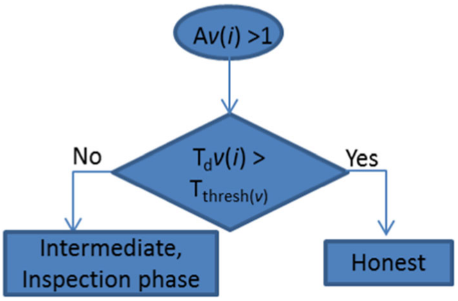


Fig. 12 Vehicles evaluation based on accordance parameter $Av(i) > 1$

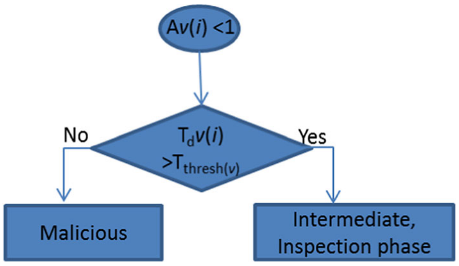


Fig. 13 Vehicles evaluation based on accordance parameter $Av(i) < 1$

Thus for a vehicle v outside the zone but adjacent to vehicle i, $Rep_v(E)$ is calculated based on Eq. (11):

$$Rep_v(E) = \frac{\sum_{i=1}^{i=|S|} Rep(E) * d_i * T_d v(i)}{\sum_{i=1}^{i=|S|} d_i * T_d v(i)} \tag{11}$$

where S = {set of vehicles receiving the warning related to this event and are in the vicinity of vehicle v}. d_i is the distance between vehicle i and event E. $T_d v(i)$ direct trust of vehicle i computed by vehicle v.

The set of rules used in each vehicle v for neighboring vehicle i classification is detailed below in Figs. 11, 12 and 13.

3.4.3 Misbehaviour authority controls

For updating the trust metric values in the database, we consider the trust metrics history at the Infrastructure (RSU) level only. Vehicles and GLs are very dynamic and with limited resources. Every vehicle and GLs evaluate vehicle trustworthiness and notify MA. MA is the only authority responsible for taking the appropriate action.

Figure 14 shows the total trust $T_{totm}(i)$ update procedure at the Infrastructure (RSU) level. If the average trust value for any vehicle i ($T_{totm}(i)$) transmitted by GLs at successive iterations k and k + 1 are close to each other in term of value, the infrastructure (RSU) follows the smoothing update method mentioned in Eq. (4). If these values are far away from each other which reflect the instability in

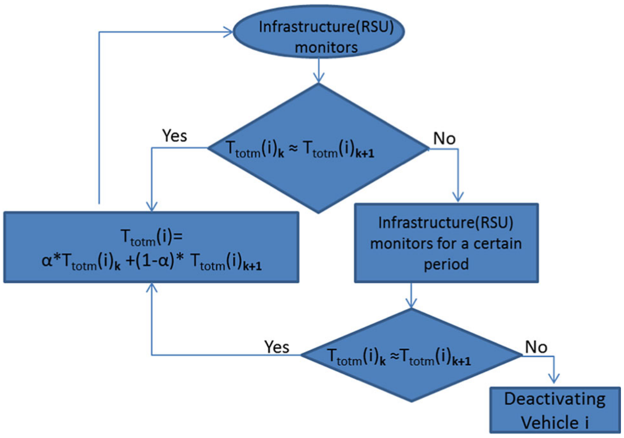

Infrastructure(RSU) monitors
$T_{totm}(i)_k \approx T_{totm}(i)_{k+1}$
Yes
No
$T_{totm}(i)= \alpha*T_{totm}(i)_k +(1-\alpha)* T_{totm}(i)_{k+1}$
Infrastructure(RSU) monitors for a certain period
$T_{totm}(i)_k \approx T_{totm}(i)_{k+1}$
Yes
No
Deactivating Vehicle i

Fig. 14 At infrastructure (RSU)-MA level, average total trust T_{totm}(-*i*) update procedure

vehicle *i* behavior, the infrastructure (RSU) will put vehicle *i* under inspection for a certain period that varies from 300 ms to 5 min before informing the MA that takes the final decision of deactivation. MA can deactivate the malicious node by revoking its related certificates so it cannot participate anymore in the vehicular networks.

If the MA receives a notification from GLs or any vehicle, it runs the following steps shown in Fig. 15:

- If the vehicle was honest and becomes malicious, it is monitored for a period *t* before broadcasting this info and deactivating the malicious vehicle. MA uses white, grey and blacklist. White for honest; grey for doubtful; black for malicious. So the vehicle is moved to greylist.
- If the vehicle was malicious and becomes honest, it will be under inspection for a period *t’* double of the ordinary period adopted *t* (which varies between 300 ms and 5 min), before reclassifying it as an honest node.

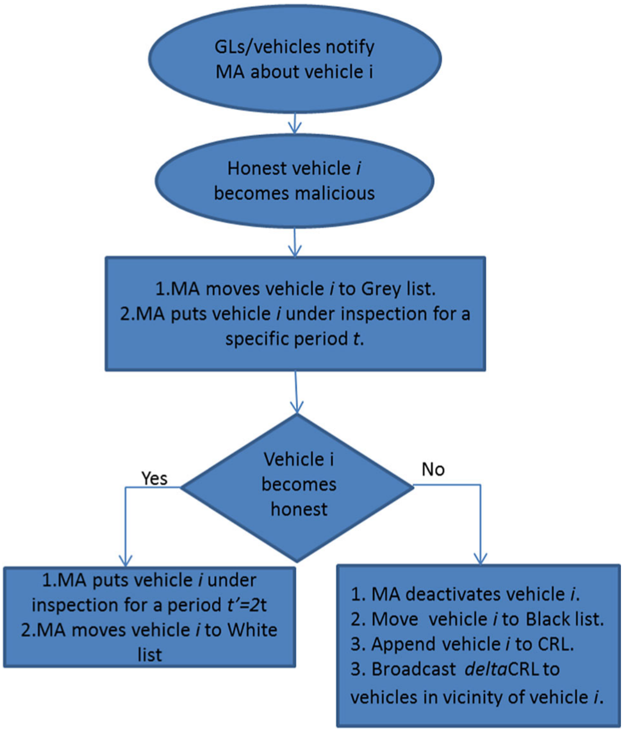

GLs/vehicles notify MA about vehicle i
Honest vehicle *i* becomes malicious
1.MA moves vehicle *i* to Grey list.
2.MA puts vehicle *i* under inspection for a specific period *t*.
Vehicle i becomes honest
Yes
No
1.MA puts vehicle *i* under inspection for a period *t’=2t*
2.MA moves vehicle *i* to White list
1. MA deactivates vehicle *i*.
2. Move vehicle *i* to Black list.
3. Append vehicle *i* to CRL.
3. Broadcast *delta*CRL to vehicles in vicinity of vehicle *i*.

Fig. 15 Steps taken by MA upon receiving notifications from GLs or vehicles

4 Simulation results

In this section, we run many scenarios to evaluate the proposed Trust Model through simulation studies. Specifically its performance and efficiency of selecting trusty vehicles; how it monitors their behaviors, as well as their classification. Finally, we conclude this section by summarizing simulation results.

For the simulation, we used GrooveNet v2.0.1 [45], an open source hybrid simulator which integrates mobility and network simulator. It simulates communication among vehicles and can load a real street map form Tiger/Line database [46]. Multiple broadcast messages are supported during the simulation: Generic packets and Safety packets. Generic packets are beacons or basic safety messages generated periodically every 100 ms and used to declare vehicle position for neighbors. Safety packets are event-driven packets or alert packets (emergency or warning) broadcasted when a hazardous situation is detected using the classical flooding algorithm. The alert rebroadcast process is limited by the alert message lifetime. A node may receive the same alert several times; this redundancy increases the transmission reliability.

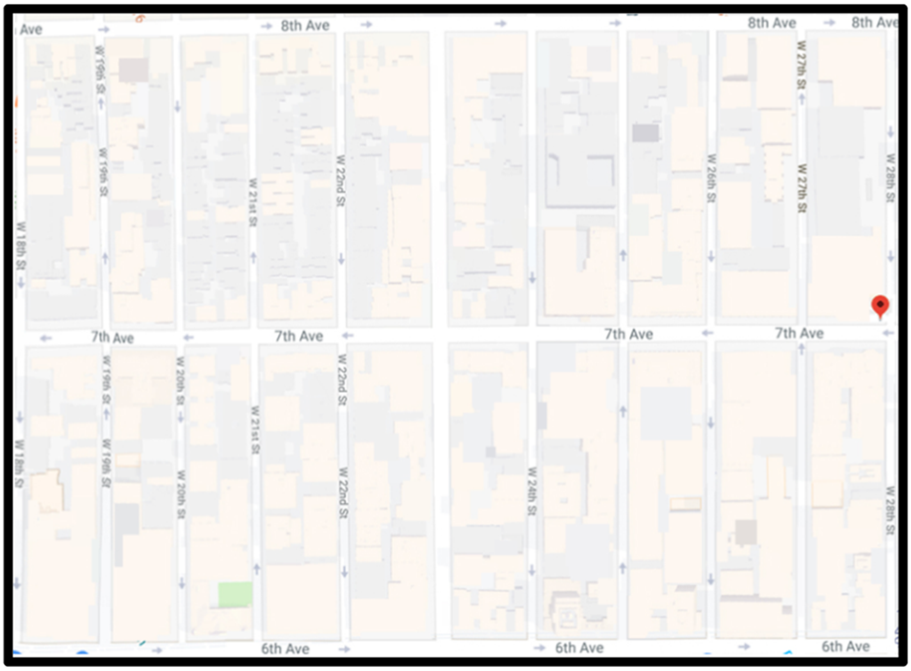
To simulate our proposed Trust Model, we added specific procedures to calculate the trust metrics and classify the vehicles. The most trustworthy vehicle will be elected as a potential group leader, and the misbehaving ones will be excluded from the vehicular networks based on the set of rules for Misbehavior Detection running within vehicles and at the back-end system. The simulation parameters used in our experiments are summarized in Table 6.

The simulation area illustrated in Fig. 16 is a 0.5 Km^2 around 333 7th Ave, New York, Location. Each simulation was run for 15 min in sparse, medium and dense mode respectively with 20, 50 and 100 circulating vehicles. These vehicles are equipped with DSRC for V2V or V2I communication. Initially, vehicles were positioned at 333 7th Ave New York location. Interacting vehicles are allowed to move using the Car Following Model (following GL); a vehicle will not exceed the speed of the vehicle in front of it. Vehicles circulate randomly for a maximum trip

Table 6 Simulation parameters

Parameter	Value
Area	0.5 Km^2
Transmission range	300 m
Transmission rate	3 Mbps
SNR	20dB
Maximum trip distance	1 km
Group leader mobility model	Uniform speed model (*street speed limit*)
Vehicles mobility model	Car-following model
Speed standard deviation	± 25%
Number of vehicles	20, 50, 100
Evaluation parameters	Velocity, number of confident neighbors, forwarding delay
α (weight of current value)	50, 60, 70%
β (weight of direct calculation)	50, 60, 70%
Simulation Time	15 min
Message lifetime	1 min
Iterated simulation	30 times/scenario

Fig. 16 Simulation area



distance of 1 km and return to their initial position using the Sight Seeing Trip Model (shortest path to the origin, at 333 7th Ave New York). The transmission range of vehicle radio is 300 m. Group Leader is moving based on a Uniform Speed Model varying ± 25% of the speed limit of the mentioned street, i.e., GL's speed is uniformly distributed around the speed limit of the street. Without loss of generality, for Eq. (1) we consider three of the trust evaluation parameters, which are the velocity of the vehicle, number of confident neighbors and Forwarding delay.

In our simulation, we consider several scenarios to show the efficiency of the proposed Trust Model:

a. As detailed previously the Hybrid Trust Model is used to evaluate vehicles' behavior based on calculated trust metrics. These values were designed to reflect their real behaviors within VANETs. Using a monitoring tool embedded within the simulator, we can follow circulating vehicles within VANET. For illustration purposes, we pick up three vehicles *v*3, v21, and *v*25. Figure 17 shows their total trust variations over the y-axis versus time over the x-axis while circulating in a medium mode scenario for 15 min. Vehicle total trust varies based on vehicle behavior; it starts with an initial value 0.5 and can reach 0.9 for the most trusted

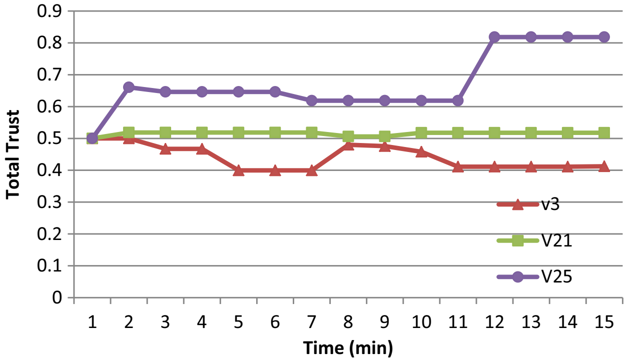


Fig. 17 Total trust variation of three vehicles in medium mode scenario

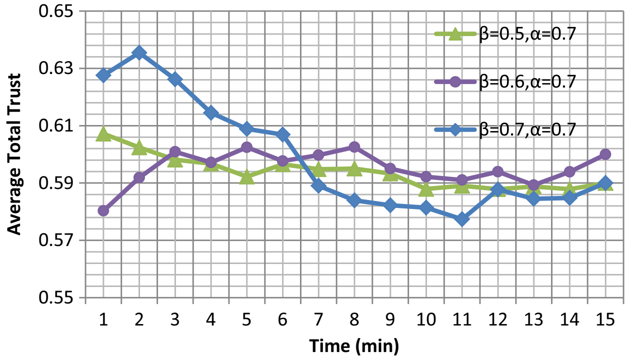


Fig. 19 Average total trust variation of vehicles with α and β parameters in medium mode scenario

vehicles. We notice from Fig. 17 that T_{tot} (v25) started with its initial value 0.5, and then we notice the changes relatively. Its total trust increases after 1 min to 0.66 then at t = 10 an additional increase till 0.81 and remains constant until the end of the simulation. This issue reflects the good behavior of v25. In opposite, v3 started by 0.5 then its total trust decreased continuously based on its bad behavior in the simulation. v21 total trust remains around 0.5 which reflects its intermediate behavior neither malicious nor honest vehicle to trust. All these values reflect the real behavior of these vehicles. These total trust values were calculated for α = 0.7 and β = 0.6, α and β represent respectively the weight of the newly calculated value in Eq. (4) and the weight of the direct trust in Eq. (3). α and ß parameters are multiplicative factors that vary between 0.5 and 1. A focus on vehicles behavior during the first 100 s of the simulation is illustrated in second precision in Fig. 18.

Furthermore, we chose the average total trust of all participating vehicles in medium mode scenario to get a global view of vehicles' behavior within the system. We illustrated these values varying α and ß parameters that intervene in the total trust calculation. Figure 19 shows the average total trust of all participating vehicles over y-axis versus time over x-axis within 15 min in medium mode scenario with different values of α and ß. We present the case of α = 0.7 which means the current calculated value is weighted 70% relative to the most recent calculated one within each computation process, i.e., we use smoothing update procedure and not overwriting old values since we are more interested in the recently calculated values. We show different values of ß greater than 0.5; this choice is justified by the fact that we considerably trust the direct calculation and we will not neglect the neighboring opinions referred to as the indirect calculation. During the next scenarios and without loss of generality, the parameters ß and α for Eqs. (3) and (4) are taken ß = 0.6 and α = 0.7.

b. *Model-Group Formation:* In this context, we show in Fig. 20 that the Trust Model security architecture (GL formation) overcomes the PKI infrastructure in network overhead. We took an example of safety message dissemination, at different snapshots within 15 min. In our model, a safety message contains a header, the payload, and a trailer. The group certificate is included in the header, the safety message details about vehicle

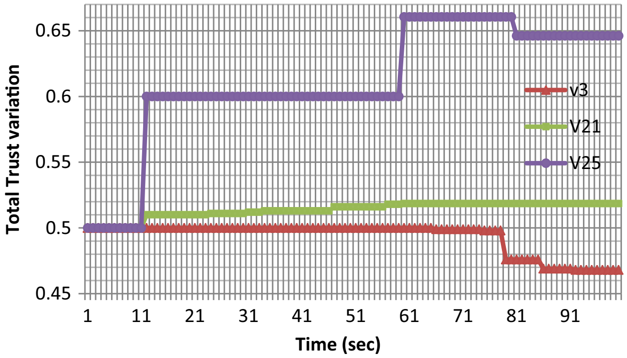


Fig. 18 Total trust variation in second precision of three vehicles in medium mode scenario

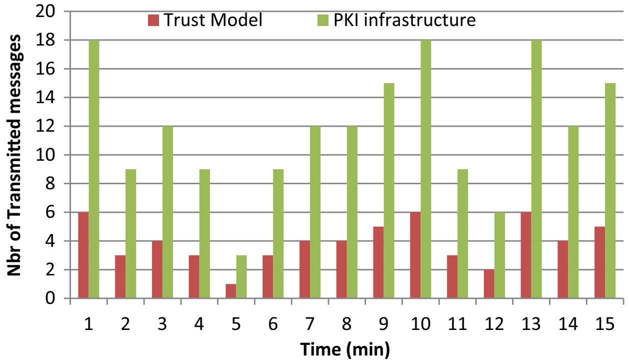


Fig. 20 Comparison of transmitted messages/vehicle in PKI versus trust model architecture

status and alert event are in the safety message payload, and the sender's digital signature is contained within the trailer. This safety message will be broadcasted concatenated with encrypted direct trust vector of neighboring vehicles. In our model, vehicles within the same group are authenticated to the same GL and directly disseminate the safety message to their communication range concatenated with their direct trust vector of neighboring vehicles encrypted with the symmetric key of the group K_{gr}. As the example in Fig. 20, at t = 6 min during the simulation, one of the vehicles had four neighbors, it notifies them about the accident by sending four messages signed precisely by its secret signing private key and concatenated with the encrypted data. While in PKI infrastructure, it should authenticate first each neighbor, and then sends it the safety message concatenated with the direct trust vector of neighboring vehicles encrypted asymmetrically with each neighbor public key. In case the sender has not a copy onboard of the authorizing certificate, this pushes to ask the sender to resend it. Which results in 3 messages/vehicles (1-authorizing certificate request, 2-certificate reply, 3- signed safety messagell encrypted direct trust values of neighbors) giving a total of 12 messages for four neighbors. The results show that our group-based Trust Model scheme outperforms the PKI scheme in saving network overhead during the safety message dissemination.

c. *Safety message dissemination in Trust Model:* Fig. 21 shows the percentage of warned cars in different modes scenarios (sparse, medium and dense). A warning event was triggered every 1 min. For each event, the percentage of warned vehicles is measured. Figure 21 illustrates this percentage during 15 min. The results highlight an adequate penetration of safety messages between vehicles within the proposed Trust Model, varying from 50 to 99%; this reflects good cooperation and leads to a correct and extensive evaluation of trust metric values between vehicles. We also notice in Fig. 21 that the percentage of warned vehicles in medium and dense mode scenarios exceed the percentage in sparse mode, this is due to the density of vehicles. Moreover, we notice that the percentage of warned vehicles in medium mode sometimes exceeds the penetration in dense mode (at time = 3, 8, 13 and 15); this can be interpreted by the fact that some collisions mitigate the dissemination process. Furthermore, Fig. 22 illustrates the maximum traveled distance in meters by warning messages in sparse, medium and dense mode scenarios. Based on vehicles cooperation, the traveled distance could exceed the maximum transmission range of DSRC 1000 m. This penetration reflects the nodes cooperation based on vehicle density for spreading the notifications within the vehicular networks. In fact, the notification travels longer in dense mode than in medium and sparse modes. In addition to the previous results, we also show respectively in Figs. 23 and 24, the collided versus received messages during events dissemination process in medium and dense mode scenarios. These results can be used as an indicator for the channel utilization during the dissemination within the simulation period.

d. *The Efficiency of the Proposed Model in Trust Evaluation:* In this scenario, 50% of malicious cars are injected. The malicious cars present misbehaving vehicles, decelerating to slow down the traffic or accelerating to cause an accident. Figure 25 presents the detected percentage of inspected and malicious vehicles (following our misbehavior detection set of rules) over y-axis versus time over x-axis within 15 min in different modes (Sparse, Medium and Dense) scenarios. We notice that in different modes, the detected percentages converged close to 50%. Figure 26 details the number of Honest, Inspected and Malicious vehicles in medium mode scenario where the total number of vehicles is 50 and 50% of

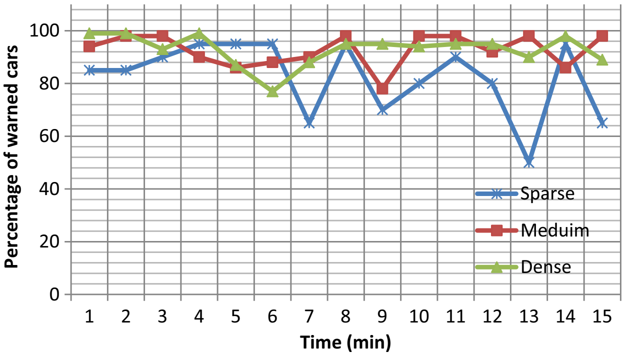


Fig. 21 Percentage of warned cars in different modes scenarios

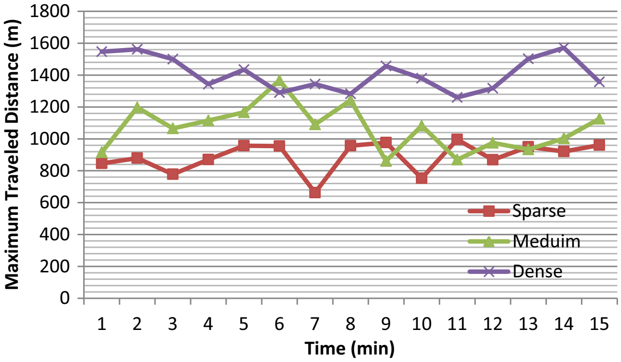


Fig. 22 Maximum distance traveled by warning messages in different mode scenarios

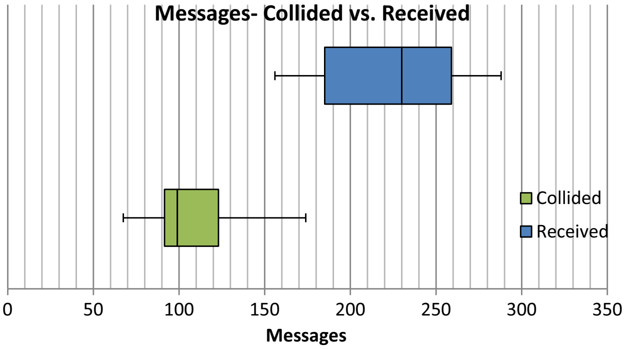


Fig. 23 Comparison of collided versus received messages in case of warning events in medium mode scenario

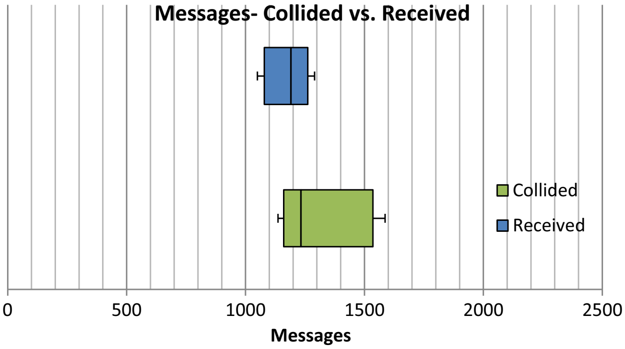


Fig. 24 Comparison of collided versus received messages in case of warning events in dense mode scenario

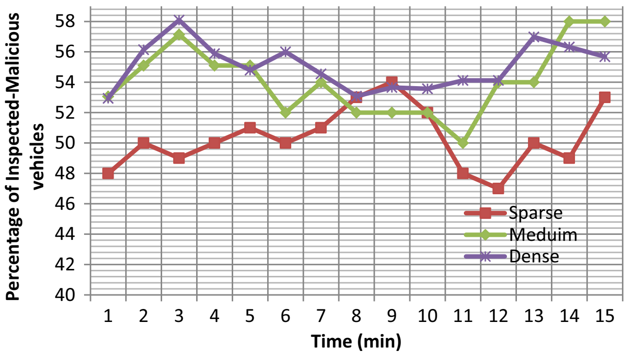


Fig. 25 Detection rate of inspected-malicious for trust model in different modes with 50% malicious cars injected

malicious cars are injected. These figures show the capability of the Trust Model of detecting a good percentage of attackers based on vehicles' cooperation.

e. *Model Behavior for GL Election:* In this subsection, we focus on the average lifetime of a potential GL within different percentages of existing malicious vehicles. GL is the most trustworthy vehicle among other participants in a given neighborhood. Let us consider one of these simulations illustrated in Fig. 27, where the current GL ID is vehicle 1. It shows the potential GL ID over y-axis versus time over x-axis and the percentage value represents the percentage of malicious vehicles at time t. Starting the simulation, vehicle 30 was the most trustworthy vehicle during the existence of 78 and 44% of malicious vehicles respectively. Between Time = 3 till 5 min, vehicle 40 overcomes vehicle 30 behavior and becomes the potential GL with a percentage of existing malicious vehicles varying between 53 and 62%. Between t = 8 till 12, we notice that irrespective of the existence of 44–50% of malicious vehicles, vehicle 6 (an honest vehicle) remains the potential GL for a while (240 s). This point reflects the stability in potential GL behaviors within the proposed Trust Model irrespective of the percentage of existing malicious vehicles. When the current GL decides to leave the group, it delegates its responsibility to the potential GL through the back-end system as detailed previously in the proposed trust model architecture.

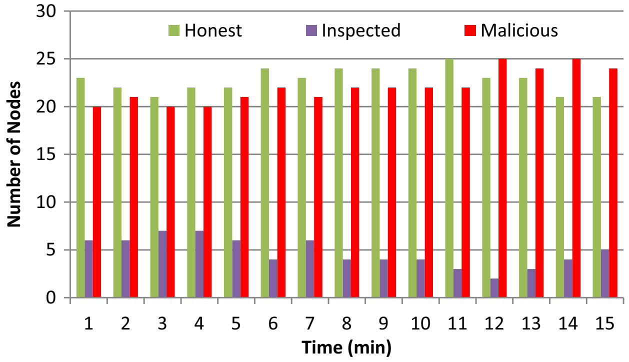


Fig. 26 Number of honest, inspected and malicious nodes in medium mode scenario

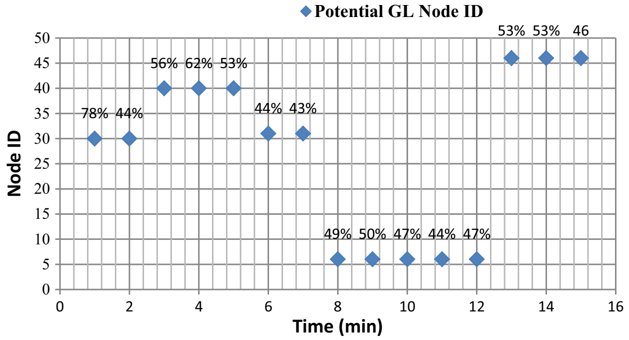


Fig. 27 Average lifetime of potential GL with different percentages of malicious vehicles

f. *Misbehavior detection*:

- *GL level (GL controls):* As explained in Sect. 3.4 and based on Eq. (6), GL controls vehicles' behavior within its radio range. It classifies them based on the set of rules explained in Sect. 3.4.1 and illustrated in Fig. 10. We present one of several snapshots within the simulations. We picked from the GL database four vehicles (*v*17, *v*2, *v*36, and *v*29) from its group that contains 25 vehicles. We use the trust model to evaluate their behaviors; results are shown in Table 7. T_{thresh} is the arithmetic mean of all total trust values of vehicles within GL radio range. In this scenario, we have the GL $T_{thresh} = 0.68$ and $T_{thresh}/2 = 0.34$. We were monitoring the system and noticed that *v*2 accelerated and exceeded the road speed limit over 65mph. This behavior negatively affects its total trust metric. Its total trust varies between $T_{thresh}/2$ and T_{thresh}. This vehicle will be under inspection for a specific period. Inspection period varies from 300 ms to 5 min. If this period expires and the misbehavior continues, a notification will be sent to the MA. Another example: *v*17 was driving normally and cooperating with neighbors during our monitoring phase, its total trust $T_{tot}(i) = 0.72$ which is greater than the T_{threh}, this vehicle will be considered as Honest. As for vehicles 36 and 29, they were over speeding and not cooperative in disseminating safety messages. They were classified as malicious ones as shown in Table 7. This emphasizes the effectiveness of the misbehavior detection set of rules within the trust model.

- *Vehicles level (Vehicles control):* the vehicles beside the GL monitor each other and notify the Misbehavior Authority based on the set of rules mentioned previously in Sect. 3.4.2 and illustrated in Figs. 11, 12 and 13. Let us consider a snapshot from our simulation within vehicle 17. A prototype of the analysis is shown in Table 8; we consider two vehicles (*v*2 and *v*21) from *v*17 neighborhood. The trust threshold within *v*17 is $T_{thresh}(_{v=17}) = 0.588618$. $T_{thresh}(v)$ represents the average of all total trust values within vehicle *v*. During the monitoring period, *v*2 was accelerating over the speed limit, the direct trust of *v*2 calculated by *v*17 is $T_d(_{v=2}) = 0.5812 <<< T_{thresh}(_{v=17})$. The calculated accordance parameter for *v*2, $Av(_{i=2}) > 1$. $Av(i)$ is the ratio of direct trust of vehicle *i* $T_d(i)$ calculated by vehicle *v*, over its indirect trust calculated by neighbors. For *v*2, $Av(_{i=2}) > 1$ means that the direct trust calculated by *v*17 is greater than the indirect trust calculated by the neighbors. *v*2 will be considered intermediate and under inspection phase. Inspection period varies from 300 ms to 5 min. If this period expires and the misbehavior continues, *v*17 informs MA about *v*2 to take appropriate action. Let us consider another example. During the monitoring phase, *v*35 was very cooperative, its direct trust calculated by *v*17 is $T_d(_{v=21}) = 0.875772 >>> T_{thresh}(_{v=17})$, $Av(_{i=21}) > 1$ which means the direct trust calculated by vehicle 17 is greater than the indirect trust calculated by the neighbors. *v*21 will be considered Honest.

Table 7 GL controls

VehID	$T_{totm}(i)$	Status
17	0.72	Honest
2	0.48	Inspection phase
36	0.28	Malicious
29	0.21	Malicious

To conclude, we evaluated the proposed Trust Model through simulation studies. We tested its performance and efficiency of selecting the most trustworthy nodes as potential group leaders and detecting the malicious behaviors. These trust evaluations were based on different metrics to analyze vehicles' behavior within the group while preserving the privacy of the participants and maintaining low network overhead.

5 The efficiency of the proposed trust model

The proposed Trust Model presents many assets listed below:

- The model is a combination of a centralized and decentralized network and communication. The centralization resides in the security infrastructure (back-end system) while decentralization is based on vehicles and GLs cooperation. This point strengthens the solution because it eliminates the drawbacks of the centralized models; because with a centralized model, the back-end system is the center of authentication and authorization for vehicles even during V2V communications thus creates delays and network overhead. In addition to, the single point of failure (back-end system) issue that affects the network performance.

  The group formation is one of the primary solutions for these drawbacks; it is adopted by our Trust Model. It lessens the delays and the periodical contact between vehicles and the back-end system which also causes depletion of infrastructure resources.
- The security requirements are guaranteed by using: digital certificates (long and short terms), digital signatures ($P_u i$, $P_r i$) for authentication, group signature for anonymous signature (on behalf of the group) with

Table 8 Vehicle controls

Vehicle (v)	Vehicle(i)	$T_d(i)$	$T_r(i)$	$T_{tot}(i)$	Status
192.168.0.17	192.168.0.2	0.5812	0.5281	0.55996	Intermediate
192.168.0.17	192.168.0.35	0.8757722	0.575772	0.755772	Honest

Table 9 Summary of the proposed model specifications

	Specifications	Proposed trust model
Cooperation	Centralized	
	Decentralized	
	Hybrid	x
Certificate	Certificate-based trust	x
Data analysis	Entity oriented	x
	Data oriented	
	Static info (event)	x
	Dynamic info (vehicle)	x
Trust and misbehavior	Location based	
	Direct/indirect trust calculation	x
	Privacy preserving	x
	Misbehavior detection	x

privacy preservation and keys frequently changing [11, 40].

- The efficiency of the group formation mentioned in our previous work [11] to mitigate many attacks.
- The architecture of the reference model assures efficient privacy preservation against insiders and outsiders (no possibility of tracking) [40].
- Trustworthiness of participating nodes in VANET is evaluated.
- The stability and the reasonable convergence of the system are available for GL election.
- Misbehavior reports are sent to specific authority (MA) to take appropriate actions.
- Security attacks over VANET are mitigated using our proposed Trust Model [6].

Finally, Table 9 summarizes the requirements satisfied by our proposed Trust Model compared to previous solutions in related works Table 1.

6 Conclusion

We proposed a Hybrid Trust Model (HTM) for vehicle trustworthiness evaluation depending on their behaviors within VANETs. It is based on secure architecture and on-the-fly group formation. We designed a mechanism to estimate trust values for participating vehicles which are used for their classification; the most trustworthy vehicles are selected as potential GLs, and the misbehaving ones are to be excluded from the vehicular networks. We defined Misbehavior Detection set of rules within vehicles and at the back-end system to mitigate the effect of malicious users and notify the Misbehavior Authority to exclude them from VANETs. We showed by simulation the efficiency of HTM in trust evaluation and the ability of vehicles and GLs to control neighboring participants and to classify them between Honest, Intermediate and Malicious ones. Finally, we compared our proposed model to some existent trust evaluation and misbehavior detection systems. Future work will consider scenarios including specific frequent attacks (Sybil, Blackhole) and inter-groups interaction.

A future project can test the mapping of HTM to FANET (Flying ad-hoc Network) [47, 48] a subgroup of VANETs. It consists of Multi-Unmanned Aerial Vehicle (UAV) systems communicating with infrastructure links [47]. Speed and directions of UAVs are arbitrary, the distance between nodes is very high, and node density is very low. These issues trigger many challenges in FANET, especially in security protocols, groups, and keys distribution.

References

1. Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANET security challenges and solutions: A survey. *Vehicular Communications, 7,* 7–20.
2. ETSI TS 102 940 V1.1.1- ITS—Communications security architecture and security management (2012).

3. IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages: IEEE Std 1609.2-2016.
4. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., et al. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys & Tutorials, 13*(4), 584–616.
5. Rawat, D. B., Yan, G., Bista, B. B., & Weigle, M. C. (2015). Trust on the security of wireless vehicular ad hoc networking. *Ad Hoc & Sensor Wireless Networks, 24*(3–4), 283–305.
6. Hasrouny, H., Bassil, C., Samhat, A. E., & Laouiti, A. (2016). Security risk analysis of a trust model for secure group leader-based communication in VANET. In *Ad hoc networks for smart cities book*, IWVSC Malaysia, Springer, Ch.6 (pp. 71–83).
7. Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine, 46*(6), 164–171.
8. Cooper, C., Franklin, D., Ros, M., et al. (2017). A comparative survey of VANET clustering techniques. *IEEE Communications Surveys & Tutorials, 19*(1), 657–681.
9. Boneh, D., Boyen, X., & Shacham, H. (2004). Short group signatures. In *Annual international cryptography conference* (pp. 41–55).
10. Wu, Q., Domingo-Ferrer, J., & Gonzalez-Nicolas, U. (2010). Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications. *IEEE Transactions on Vehicular Technology, 59*(2), 559–573.
11. Hasrouny, H., Bassil, C., Samhat, A. E., & Laouiti, A. (2015). Group-based authentication in V2V communications. In *Proceedings of IEEE fifth international conference on DICTAP* (pp. 173–177).
12. Wang, J., Jiang, Ch., Zhang, K., et al. (2017). Vehicular sensing networks in a smart city: Principles, technologies and applications. *IEEE Wireless Communications, 25*(99), 1–11.
13. Zhang, J. (2011). A survey on trust management for VANETs. In *IEEE international conference on advanced information networking and applications (AINA)* (pp. 105–112).
14. Tangade, Sh. S., & Manvi, S. S. (2013). A survey on attacks, security and trust management solutions in VANETs. In *IEEE, 4th ICCCNT*, Tiruchengode, India (pp. 1–6).
15. Patel, N., & Jhaveri, R. (2015). Trust based approaches for secure routing in VANET: A Survey. *Procedia Computer Science, Elsevier, 45,* 592–601.
16. Kavitha, M., Tangade, Sh. S., & Manvi, S. S. (2013). Distributed trust & time management strategy in VANETs. In *IEEE, 4th ICCCNT*, Tiruchengode, India (pp. 1–6).
17. Li, X., Liu, J., Li, X., & Sun, W. (2013). RGTE: A reputation-based global trust establishment in VANETs. In *Proceedings of the 5th IEEE international conference on intelligent networking and collaborative systems (INCoS '13)*, China (pp. 210–214).
18. Lo, N.-W., & Tsai, H.-Ch. (2009). A reputation system for traffic safety event on vehicular ad hoc networks. *EURASIP Journal on Wireless Communications and Networking, 2009*, 125348.
19. Primiero, G., Raimondi, F., Chen, T., & Nagarajan, R. (2017). A proof-theoretic trust and reputation model for VANET. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 146–152).
20. Hu, H., Lu, R., Zhang, Z., & Shao, J. (2017). REPLACE: A reliable trust-based platoon service recommendation scheme in VANET. *IEEE Transactions on Vehicular Technology, 66*(2), 1786–1797.
21. Dixit, K., Pathak, P., & Gupta, S. (2016). A new technique for trust computation and routing in VANET. In *Colossal Data Analysis and Networking (CDAN), Symposium on, IEEE* (pp. 1–6).
22. Diep, P. T. N., & Yeo, C. K. (2016). A trust-privacy framework in vehicular ad hoc networks (VANET). In *Wireless telecommunications symposium WTS* (pp. 1–7).
23. Kothari, A., Shukla, P., & Pandey, R. (2016). Trust centric approach based on similarity in VANET. In *International conference on signal processing, communication, power and embedded system (SCOPES)* (pp. 1923–1926).
24. Rivero-Garcıa, A., Santos-Gonzalez, I., Caballero-Gil, P., & Caballero-Gil, C. (2016). VANET event verification based on user trust. In *24th Euromicro international conference on parallel, distributed, and network-based processing* (pp. 313–316).
25. Mármol, F. G., & Pérez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications, 35*(3), 934–941.
26. Zhou, A., Li, J., Sun, Q., Fan, C., Lei, T., & Yang, F. (2015). A security authentication method based on trust evaluation in VANETs. *EURASIP Journal on Wireless Communications and Networking, 1*, 1–8.
27. Liu, Z., Ma, J., Jiang, Z., Zhu, H., & Miao, Y. (2016). LSOT: A lightweight self-organized trust model in VANETs. *Mobile Information Systems Journal*. https://www.hindawi.com/journals/misy/2016/7628231/.
28. Chaurasia, B. K., & Verma, Sh. (2013). Trust based group formation in VANET. *MTTER, 2*(2), 121–125.
29. Tajeddine, A., Kayssi, A., & Chehab, A. (2010). A privacy-preserving trust model for VANETs. In *10th IEEE international conference on computer and information technology (CIT 2010)*.
30. Gazdar, T., Benslimane, A., Rachedi, A., Belghith, A. (2012). A trust-based architecture for managing certificates in vehicular adhoc networks. In *IEEE International Conference on (ICCIT)* (pp. 180–185).
31. Yang, N. (2013). A similarity based trust and reputation management framework for VANET. *International Journal of Future Generation Communication and Networking, 6*(2), 25–34.
32. Rehman, A., Ali, A., Amin, R., Shah, A. (2013). VANET thread based message trust model. In *Eighth international conference on digital information management (ICDIM)*.
33. Xu, H., Hua, L., Ning, Y., & Xue, X. (2013). Detecting the incorrect safety message in VANETS. *Research Journal of Applied Sciences, Engineering and Technology, 5*(17), 4406–4410.
34. Sahoo, R. R., Panda, R., Beherab, D. K., & Naskarcm, M. K. (2012). A trust based clustering with ant colony routing in VANET. In *Third international conference on computing communication & networking technologies (ICCCNT)*.
35. Ltifi, A., Zouinkhi, A., & Bouhlel, M. S. (2015). Trust-based scheme for alert spreading in VANET. In *International conference on advanced wireless, information, and communication technologies (AWICT)*.
36. Ding, Q., Jiang, M., Li, X., & Zhou, X. (2010). Reputation-based trust model in vehicular ad hoc networks. In *IEEE conference on wireless communications and signal processing (WCSP)*.
37. Roy, D., & Das, P. (2017). Trust and group leader based model to avoid broadcast storm problem in vehicular ad hoc networks. *Advances in Computational Sciences and Technology, 10*(4), 575–597.
38. Khana, U., Agrawala, Sh, & Silakari, S. (2015). Detection of malicious nodes (DMN) in vehicular ad-hoc networks. *Procedia Computer Science, 46,* 965–972.
39. Alriyami, Q., Adnane, A., & Smith, A. K. (2014). Evaluation criterias for trust management in vehicular ad hoc networks (VANET). *International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 118–123).

40. Whyte, W., Weimerskirch, A., Kumar, V., & Hehn, T. (2013). A security credential management system for V2V communications. In *IEEE Vehicular Networking Conference* (pp. 1–8).
41. Manulis, M., Fleischhacker, N., Gunther, F., Kiefer, F., & Poettering, B. (2012). Group signatures: Authentication with privacy. Cryptographic Protocols Group, Department of Computer Science, Technische Universiẗat Darmstadt.
42. NHTSA, Preliminary Regulatory Impact Analysis FMVSS No. 150 Vehicle-to-Vehicle Communication Technology for Light Vehicles, Report No. DOT HS 812 359 (2016).
43. Dedicated Short Range Communications (DSRC) Message Set Dictionary, SAE Std. J2735 201 603, March 2016.
44. Bullen, P. S. (2003). *Handbook of means and their inequalities*. Berlin: Springer Netherlands.
45. GroovNet v2.0.1. (2006). Vehicle network simulator. In *Second international workshop on vehicle-to-vehicle communications (V2VCOM)*, San Jose, USA, July 2006, https://github.com/mlab/GrooveNet. Last updated on 2012.
46. https://www.census.gov/geo/maps-data/data/tiger-line.html. Accessed Aug 2016.
47. Wang, J., Jiang, Ch., Zhang, K., et al. (2017). Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones. *IEEE Vehicular Technology Magazine, 2*(3), 73–82.
48. Islam, N., Kowsar Hossain, Md., Nawaz Ali, G. G. Md., & Chong, P. H. J. (2016). An expedite group key establishment protocol for Flying Ad-Hoc Network (FANET). In *5th intere-national conference on informatics, electronics, and vision (ICIEV)*.

Hamssa Hasrouny graduated in Electrical and Electronics Engineering—Communication and data processing from the Lebanese University, Beirut, in 2001 and received a master degree of research M2R in Telecommunication Networks from the Lebanese University (Doctoral School of Science and Technology) and Saint Joseph University (Faculty of Engineering-ESIB), Beirut, in 2012. She is a Ph.D. student at Telecom SudParis, France. Her current research interest is focused on vehicular ad hoc networks (VANETs) security. Since 2008, she was a part-time instructor at the Antonine University—Faculty of Engineering, Bekaa (Zahlé), and since 2014, at the Lebanese International University—Faculty of Engineering, Bekaa (Rayak).

Abed Ellatif Samhat graduated in Electrical and Electronics Engineering from the Lebanese University, Beirut, in 2000 and received a master degree and Ph.D. in computer science from the Pierre et Marie Curie University, Paris, in 2001 and 2004, respectively. From 2005 to 2008, he was within France Telecom group as a Research Engineer at Orange Labs-Paris where he has been involved in several national and European projects including Ambient Networks and Gandalf. In 2009, he joined the Lebanese University, Beirut and he is currently a professor at the Faculty of Engineering. His areas of interest include heterogeneous wireless networks, cross layer design, access selection, mobility management and security.

Dr. Carole Bassil is as an associate professor at the Lebanese University—Faculty of Sciences. She received her B.S in Telecommunication in 1994 and M.S. in Telecommunication and Networking in 1997 from Saint Joseph University. She holds a Ph.D. from Telecom ParisTech (France) in 2005 in the field of VoIP security and a Diploma in Higher-Education Teaching from Saint-Joseph University in 2016. Her current research interests include IoT security and VANET dissemination and security. She is the author of many articles. Between 1999 and 2012, she was a visiting Instructor at Saint Joseph University—Faculty of Engineering. She is IEEE member since 2003, and served as CIO at Lebanese University between year 2016 and 2017. She is also ISO 27001 Provisional Lead Auditor.

Anis Laouiti received his Ph.D. in Computer Science from the Versailles University, France, in 2002. He had been doing his research during and after his Ph.D. at the INRIA/Hipercom team, before he joined the Telecom SudParis, France, as an Associate Professor in 2006. His research covers different aspects in wireless adhoc and mesh networks including protocol design, performance evaluation and implementation testbed. His current research interest is focused on vehicular ad hoc networks (VANETs), MAC layer optimisations and critical data dissemination in VANET and their interactions with the future smart cities and the internet of things networks. He is also investigating sensor/robots automatic deployment mechanisms for surveillance purposes, and IoT for smart industries. He was involved in the IETF-MANET working group and he is one of the co-authors of the OLSR routing protocol (RFC3626). He was involved in several national and European research projects.