Santos J. and Moreira *EURASIP Journal on Wireless Communications and Networking* (2019) 2019:204
https://doi.org/10.1186/s13638-019-1518-x

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

An evaluation of reputation with regard to the opportunistic forwarding of messages in VANETs

Luz M. Santos J.[1,2*] and Edson Moreira[2]

Abstract

A mechanism for trust management is required in vehicular ad hoc networks (VANETs) to record the behavior of the vehicles. However, it is a complex matter to follow the historical behavior of the vehicles, since their identities are protected by pseudonyms, which are constantly changing to prevent tracking. In our proposal based on a centralized reputation system, being a vehicle well behaved in the opportunistic forwarding of messages comprises two components: reputation for messages creation and for messages forwarding. The vehicles can forward messages at a given time, and the types of messages that are sent in each transaction may require a vehicle reputation score. In this case, the decision of a vehicle to accept a message is based on the reputation of the sender vehicle that created or forwarded the message. We describe the reputation system through the first three levels of a functional ontology and finite state machines. We evaluate the system by means of simulations in an urban scenario to obtain the reputations of forwarding and generation of messages, varying the number of misbehaving vehicles. It was found that a centralized reputation scheme reflects the behavior of the vehicles insofar as feedback is delivered to the reputation server.

Keywords: Vehicular ad hoc network, Reputation system, Trust management, Security and privacy

1 Introduction

The emergence of vehicular ad hoc networks (VANET) has generated new challenges and requires an even deeper consideration of reputation, as it is one of the ways to trust in vehicles or drivers sending messages. A distributed trust management system would allow to a vehicle to realize an assessment of the direct experience with other peers, although there is no guarantee that it will interact with the same vehicles in the future. Maintaining the reputation history of other vehicles is difficult when each vehicle is anonymous and is changing its pseudonym periodically. Storing information about the reputation of a large number of vehicles could lead to scalability problems. In addition to the above factors, the distributed approaches are focused on selecting dynamic groups of vehicles and algorithms that require a considerable number of messages to be exchanged and thus could take longer to make a decision.

A considerable effort has been made to develop distributed trust management systems for VANETs, based on the assumption that it is not possible to rely on a centralized system for this network. The first reason for adopting a centralized system is that the vehicles are regulated and governed by a centralized authority. Hence, it is natural to adopt a centralized scheme [1]. In addition, a centralized architecture may be preferable to a decentralized due to simpler management, control, and safety. Today, it is possible to plan a centralized reputation system that involves new technologies such as long-term evolution (LTE); this could be the most efficient way of connecting the vehicles to the Internet [2] and not just depending on connections via Roadside Units (RSUs). The main advantage of a centralized system is to have a global knowledge of the behavior of all vehicles that participate in the VANETs. The complexity of calculating the reputation score is left to the central infrastructure, which means that the vehicles can process other higher priority tasks.

This paper is based on work [3] that presented a centralized reputation system with the identity of the vehicles protected with the pseudonym mechanism. We also

*Correspondence: lsantos@unipamplona.edu.co
[1]Systems Engineering, Universidad de Pamplona, Pamplona, Colombia
[2] Maths Science Institute and Computing-ICMC, University of São Paulo, São Carlos, Brazil

extend work in [4] which considers that reputation management based on ontology could drive many aspects of VANETs and particularly can serve as a reference for the production of feedback that will feed the reputation of the vehicles. In our application, the vehicles can forward messages at a given time and the types of messages that are sent in each transaction may require a vehicle reputation score. In this case, the decision of a vehicle to accept a message is based on the reputation of the sender vehicle that created or forwarded the message. For this, the reputation certificate (RC) of a vehicle is attached to the messages that are generated or forwarded by it. We propose a centralized reputation system, which works with a composed reputation by including different behavioral factors. In our case, the reputation of being a suitable vehicle to forward a message is related to two behavioral factors: for the generation of messages about road conditions and for the cooperation in the forwarding of messages. We evaluated through simulations the average reputation obtained by the vehicles, varying the number of misbehaving vehicles.

The remainder of this paper is organized as follows: Section 2 describes the methods; Section 3 work related to reputation systems for trust management in VANETs; Section 4 general description about the opportunistic forwarding of messages; Section 5 definition of the reputation system through the first three levels of a functional ontology and finite state machines; Section 6 simulation setup including motivational scenario, mobility and network parameters, planning of experiments, and discussion of the results of the simulations; and Section 7 summary of the conclusion.

2 Methods

Evaluating VANETs applications in real world environments is very expensive and requires a lot of effort. For the evaluation of this work, simulations were carried out with the goal to validate our reputation system under a grid scenario. The metrics and factors used were selected from some works of the state of the art (see Section 6.3). The simulation environment in VANETs included the following: Simulation of Urban MObility (SUMO 0.21.0) [5] used for the vehicular traffic model, Objective Modular Network Testbed in C++ (OMNET++ 4.6) [6] used for the communications network, the vehicular environment framework network in simulation (Veins 3.0) [7] required for the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications. Crypto++ 5.6.2 [8] was included to provide public cryptographic schemes such as Elliptic Curve Cryptography (ECC). A library of security was developed for VANETs, so that it could import classes from Crypto++ and implement a new pseudonym class with the methods to sign and verify messages.

3 Related work

In this section, first, we focus on work related to centralized reputation systems and recent studies about trust management in VANETs. Second, we relate opportunistic forwarding algorithms in VANETs. The works cited include the properties of scalability, robustness, and awareness of security issues. Some works treat privacy concerns with schemes of group signatures or pseudonyms. The approach [9] used a single-hop reputation announcement, and [10] proposed a multi-hop version which uses the carry-and-forward method. The proposals seek to evaluate the reliability of messages and aggregation of reputation scores. However, these schemes lack privacy protection since the messages and feedback are linkable and not anonymous. An adversary is able to conduct an attack on the traceability and learn the path of a target vehicle. The author in [11] formulated a generic abstraction for an authenticated anonymous announcement scheme using reputation systems. Our system adds the composed reputation by two behavioral factors.

A reputation-based announcement scheme that considers privacy for VANETs was proposed by the authors in [12]. Here, the reputation server rather than the receiver vehicle takes the decision as to whether an announcement is trustworthy or not, since only vehicles deemed reputable by the reputation server are given signing keys, and the signatures do not reveal what the reputation scores are. In [13], Chen et al. provided a full description of a new cryptographic primitive, which enables a scheme to address a secure channel for the retrieval of new signing keys used in [12]. This work does not present analyses and experiments to calculate the delay of the cryptographic functions and the number of messages that the implementation of the scheme should have. Another centralized approach called Reputation-based Global Trust Establishment scheme (RGTEs) was proposed in [1]. A vehicle searches in its database for the reputation score of the neighbor vehicle, if not, the vehicle query it at a centralized entity through of a RSU. Nevertheless, the scheme lacks experimentation and does not address privacy issues.

In recent studies, [14] proposed a blockchain-based anonymous reputation system (BARS) to break the likability between real identities and public keys to preserve privacy. The work by [15] proposed a trust-based dueling deep reinforcement learning approach (T-DDRL) for communication between vehicles; it deployed a dueling network architecture into a logically centralized controller of software-defined networking (SDN). The authors in [16] used trust-based methodology to find location with the help of trustworthiness of the node. In [17], Kumar et al. proposed an enhanced trust-based mechanism to select trusted nodes through which messages are transmitted.

Eziama et al. [18] proposed a trust model with respect to machine/deep learning (ML/DL).

Opportunistic forwarding algorithms have been studied for many years. Xiao et al. [19] focused on TOUR, a single-copy opportunistic routing algorithm, in which a time-sensitive forwarding set is maintained for each node by considering the probabilistic contacts in delay-tolerant networks (DTNs). The authors in [20] proposed a distributed optimal Community-Aware Opportunistic Routing (CAOR) algorithm. To reduce redundancy caused by multi-hop broadcast, a direction-aware broadcast protocol was proposed in [21]. A centrality prediction method based on K-order Markov chains to solve the problem of centrality prediction in mobile social networks (MSNs) was proposed in [22]. Huang et al. [23] proposed a clustering scheme named as the credit-based clustering (CBC) scheme for point of interests' (POIs') geo data sharing in vehicular social network (VSN). In [24], Zhou et al. surveyed the recent advances in the data offloading techniques through VANETs.

4 Application of opportunistic forwarding of messages

The application deals with the generation and opportunistic forwarding of messages by following the store-carry and forward mechanism. Table 1 lists the common terms used in this work . In [25], Yokoyama et al. define opportunistic communications as being occasional communications among vehicles. Sensitive messages that inform about the traffic conditions and events occurred in the roads are generated by vehicles and sent to a central monitoring system. This system carries out the role of the observer node (ON) which provides feedback to report the truth or falsity of the content of the messages. Intermediate vehicles forward the message to the RSU where the message is delivered to the final destination. After this, the vehicles involved for creating and forwarding the message will receive feedback. As a result of the forwarding process, the ON can receive several copies of the same message, but it only generates feedback for the vehicles involved in the first copy of the message that it receives. The subsequent messages that have the same identification as the message are considered duplicates and are rejected.

Table 1 List of terms

Term	Description
OBU	On-board unit
RSU	Roadside unit
ON	Observer node
OV	Observer vehicle
EV	Evaluated vehicle
CV	Creator vehicle
FV	Forwarder vehicle
$K1$	Reputation for messages generation
$K2$	Reputation for messages forwarding
Rep	Total reputation of a vehicle
δ	Weight for messages generation
$1-\delta$	Weight for messages forwarding
α	Weight for the last feedback
$1-\alpha$	Weight for the historic reputation
CA	Certificate authority
RS	Reputation server
RC	Reputation certificate
RCI	Reputation certificate identification
CC	Check code
LR	Last rating

A vehicle may play the role of an evaluated vehicle (EV) which is a vehicle that receives feedback or the role of observer vehicle (OV) if it is the destination of the message. Here, we define two kinds of EV: the creator vehicle (CV) that receives feedback as an individual agent (which generates messages) and the forwarder vehicle (FV) that receives feedback as a cooperative agent (which forwards messages). When a message arrives at the central monitoring system, the FV receives positive feedback, regardless of the nature of the message. The scheme rewards the altruistic vehicles with the goal of encouraging the cooperation in the forwarding of messages. The punishing of selfish vehicles has not been the main focus in this work; however, our scheme could be able to detect that vehicles are not participating in the forwarding of messages and thus reducing the reputation for this behavioral factor. Researches about the impact of selfish behaviors are being developed on systems as peer to peer [26], in which their solutions could be adapted to VANETs. The forwarding protocol and its evaluation are beyond the scope of this paper.

Figure 1 shows the ontological structure required for inferring the reputation of the vehicle; the reputation of being a suitable vehicle to forward a message is related to two behavioral factors: for the generation of messages about road conditions ($K1$) and for the forwarding of messages ($K2$). These are calculated from Eqs. 1 and 2.

$$K1 = (K1 \times (1-\alpha) + \mathrm{LR} \times \alpha) \tag{1}$$

$$K2 = (K2 \times (1-\alpha) + \mathrm{LR} \times \alpha) \tag{2}$$

where LR is the rating that receives a vehicle in the last feedback. LR takes a discrete value because the event advertised by a vehicle is only evaluated as true or false, without possibility to intermediate assessments. Thus, it was given $+1$ for a true event (positive feedback) and -1 for a false event (negative feedback) in $K1$. For $K2$, LR only

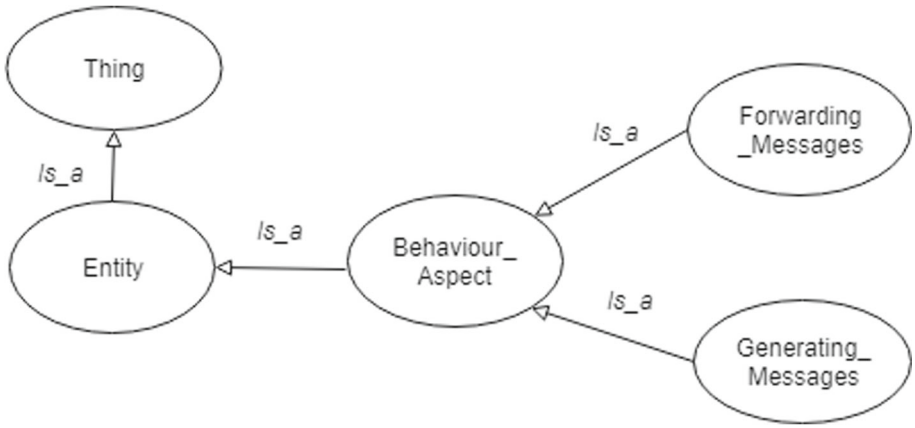

Fig. 1 Reputation of a vehicle

takes positive feedback. α is the weight given to the *rating* reported in the last feedback, and $(1-\alpha)$ is the weight given to the historical reputation score. α can take a value between 0 and 1; in our implementation, α was initialized in 0.2 to consider a minor influence of the last feedback in the results of $K1$ and $K2$. However, the system decreases quickly the reputation of a vehicle if it presents continues negative feedback.

Thus, the total reputation of a vehicle (Rep) is calculated from Eq. 3 as a weighted mean. It multiplies $K1$ and $K2$ by the weights and adds the results up. δ is the weight fixed for the generation of messages ($K1$) and is a value between 0 and 1. $(1-\delta)$ is the weight attributed for the forwarding of messages ($K2$). In our evaluation, we want obtain the effects of the weight for the generation of messages on the total reputation of the vehicle, because we consider two scenarios: with low weight ($\delta = 0.2$) and with medium weight ($\delta = 0.5$) (see Section 6.3).

$$\text{Rep} = (K1 \times \delta + K2 \times (1-\delta)) \tag{3}$$

As a result, the vehicles could obtain a Rep on the scale $[-1, 1]$, which is similar to other proposals in VANETs as the scale $[0, 1]$ used in [17]. Our scale meets the design goals of reputation management, which allows reflecting the behavior of the vehicles and reacting quickly to abrupt changes of the same.

5 Reputation system description

This section describes the reputation system through the first three layers of a possible functional ontology, see Fig. 2. It is very important for VANETs to define a formal specification of conceptualization that covers data interoperability and the attributes of reputation, security, and privacy among the different agents involved in transport systems. Concepts were taken of the work [3], a centralized reputation system with the identity of the vehicles protected with pseudonym mechanism. A first approach involving an ontological representation of the reputation system was outlined in [4], and a proof-theoretic translation of this model was formulated in [27]. We improved the ontology by using benchmarks of the concepts of the body of knowledge of the FOAF Vocabulary Specification 0.99 [28] and the PROV Ontology recommended by the W3C [29]. Certificate authority (CA), reputation authority, and transit regulatory authority are demarcated as the *foaf:Organization*. Vehicles, reputation server (RS), and roadside unit (RSU) are the main agents in our system, *prov:Agent*. The vehicles can play different roles: creator vehicle (EV) and forwarder vehicle (FV), which receive either positive or negative feedback from another peer or node on its behavior in the network.

Reputation, feedback, data message, geographical area, and behavioral factors are defined as *prov:Entity*. The geographical area can be friendly or unfriendly. In a friendly area, the level of threat is low (few negative feedbacks) and the vehicles can disable the review of the reputation of the peer vehicles. In an unfriendly area, the level of threat is high (many negative feedbacks) and the vehicles must enable the review of the reputation of the peer vehicles. The driver and passenger are conceptualized as *foaf:Person*. The current pseudonym, security certificate, and reputation certificate (RC) are considered *foaf:Document*. And finally, evaluation of reputation and pseudonym changing are considered to be important activities in our scheme and described as, *prov:Activity*.

Figure 3 shows the main properties established in our system. A vehicle is a domain of the following properties: *hasReputationLevel*, *hasReputationGlobal*, *hasReputationCertificate*, *hasSecurityReputation*, *hasCurrentPseudonym*, *hasPassenger*, *hasDriver*, and *usesArea*. A data message is a domain of the following properties: *hasContent*, *isGeneratedBy*, *isForwardedBy*,

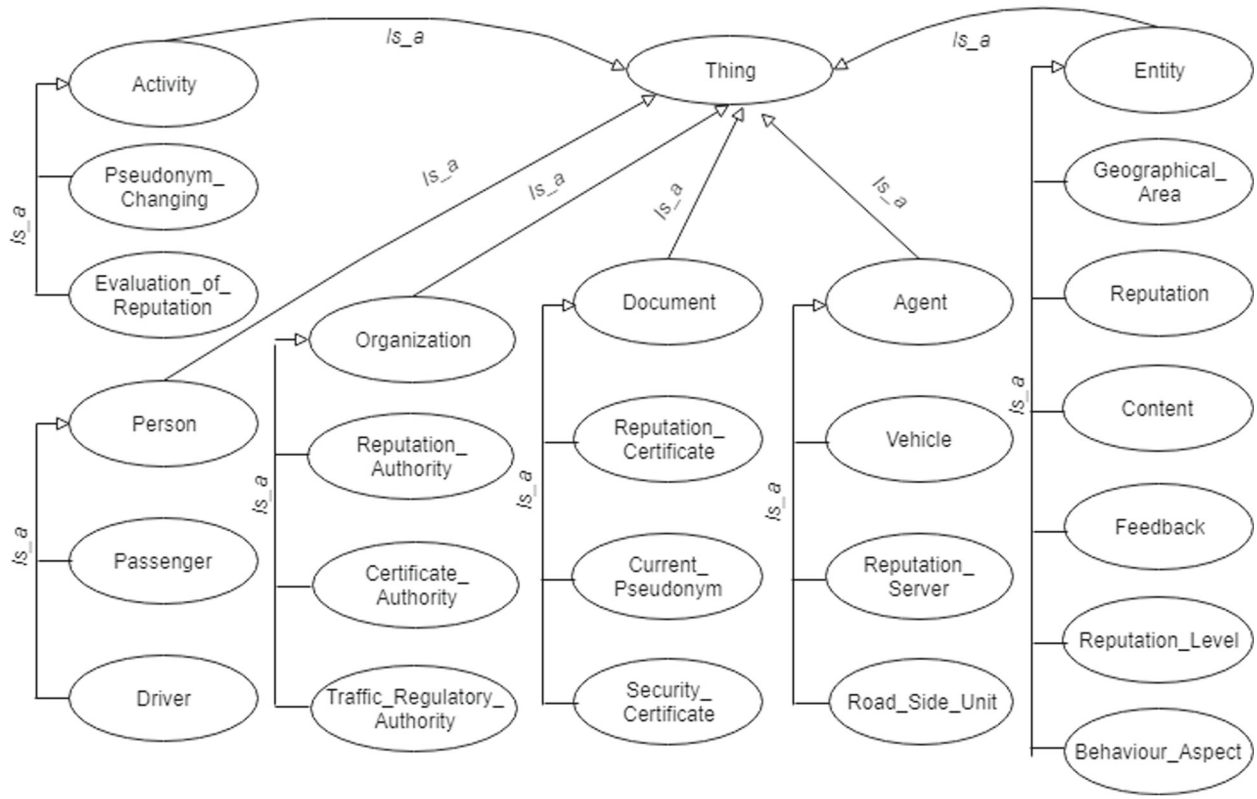

Fig. 2 First three layers of a possible functional ontology

and *isAddressedTo*. A feedback *isGivenBy* an observer vehicle (OV) or observer node (OV), *evaluateTo* evaluated vehicle (EV), *isBasedOn* content of a data message and *isSentTo* the reputation server (RS). Reputation *isCalculatedFrom* behavioral factors and *isUpdatedBy* the reputation server. A reputation certificate *isDownloaded-From* the reputation server and *hasFieldReputation*. The reputation level *isDiscretisedFrom* the reputation. The current pseudonym *isChangedBy* the activity pseudonym changing. This activity *isAssociatedWith* the vehicle. The behavior on the roads *isReportedBy* the traffic regulatory authority. The activity of the reputation evaluation *dependsOn* the geographical area, which *isDeterminedBy* the reputation server. The reputation authority *isInChar-geOf* the reputation server. The certificate reputation *isIssuedBy* the certificate authority.

Table 2 describes the messages used in our system which can make the communications possible.

5.1 Operation of the system in the vehicle

The basis of VANETs is the exchange of data between entities, and making a decision on received data/event is usually based on information provided by other entities [30]. Our proposal is entity-centric, which means the trustworthiness of data is evaluated according the reputation of providing entities. So we present the vehicle as a finite state machine (FSM) to represent its different states and all its functionality of security and privacy, so that not only represent a decision making based on trustworthiness. The "primitives" used in the specification of the FSM of the vehicle are described in Table 3. The system operates in seven states in the vehicle, as shown in Fig. 4. The vehicle starts in the *registering* state where it is registered in the RS with the security certificate that was previously acquired from the CA. Here, the vehicle acquires its initial RC, loads its initial pseudonym, and schedules the next change of pseudonym. The vehicle from the *registering* state goes to the *listening* state where it waits for the reception of one of the messages (DM, RQM, SIM, HRM, or ACM), or the execution of an event (confirm_evt, area_evt, forward_evt, change_evt or send_evt), or the request of the user to send data messages. Depending on the type of received message or event, the vehicle goes to another state.

If the message type is ACM, the vehicle goes to the *system updating* state. The vehicle extracts the "area information" from the *ACM*; if the area is equal to zero, the vehicle enables the *friendly* configuration; otherwise, the

Fig. 3 Main object properties

vehicle enables the *unfriendly* configuration. Then, the vehicle schedules the forwarding of ACM to the neighbors of one hop and returns to the *listening* state.

If the message type is RRM, the vehicle also goes to the *system updating* state. The vehicle decrypts the message, extracts its RC from RRM, updates its local data, allocates the variable *rc_time* to the time of the system (this variable controls the request of a new RC), and returns to the *listening* state.

If the message type is HRM, the vehicle also goes to the *system updating* state. The vehicle stores in cache the incoming HRM message, the sender vehicle of which is the candidate to select the next hop of a DM. After this, it returns to the *listening* state.

If the message type is SIM, the vehicle goes to the *feedback reporting* state, where it checks into cache if there is any feedback or data message pending to send to the RSU. As long as the cache is not void (F represented in Fig. 4),

Table 2 Kind of messages in the system

Message	Source	Destination
DM Data message	Vehicle	Observer
FM Feedback message	Vehicle	RS
RQM Reputation-query message	Vehicle	RS
RRM Reputation-response mess	RS	Vehicle
ACM Area condition message	RS	Vehicles
SIM Signaling message	RSU	Vehicles
HM Hello message	Vehicle	Vehicles
HRM Hello response message	Vehicles	Vehicle

Table 3 Primitives used in the FSM of the vehicle

Primitive	Description
rtd_rcv(message)	Reception of a message
utd_send(message)	Sending of a message
request_user(data)	Request of the user to send a message
make_pkt(parameters)	Creation of a message
not_corrupt(message)	Verifying of the integrity of a message
decrypt(message)	Decryption of the message
extract(message,field)	Extracts a field from the message
add-lista(message)	Adding the fields *CC*, *RCI* to the mess
update(parameter)	Updating of variables
evaluate_rep()	Verifying of the reputation
select_dest()	Selection of the next hop
store_cache()	Storing of information in cache
schedule(evt)	Scheduling of a new event
confirm_evt()	Verifying of the truth of data
area_evt()	Enabling the forwarding of ACM
forward_evt()	Enabling the forwarding of DM
change_evt()	Calling for changing of pseudonym
send_evt()	Enabling the sent of DM
is_observer()	Determining of the destination
is_true()	Determining the truth of a message
time()	Returning of time of the system

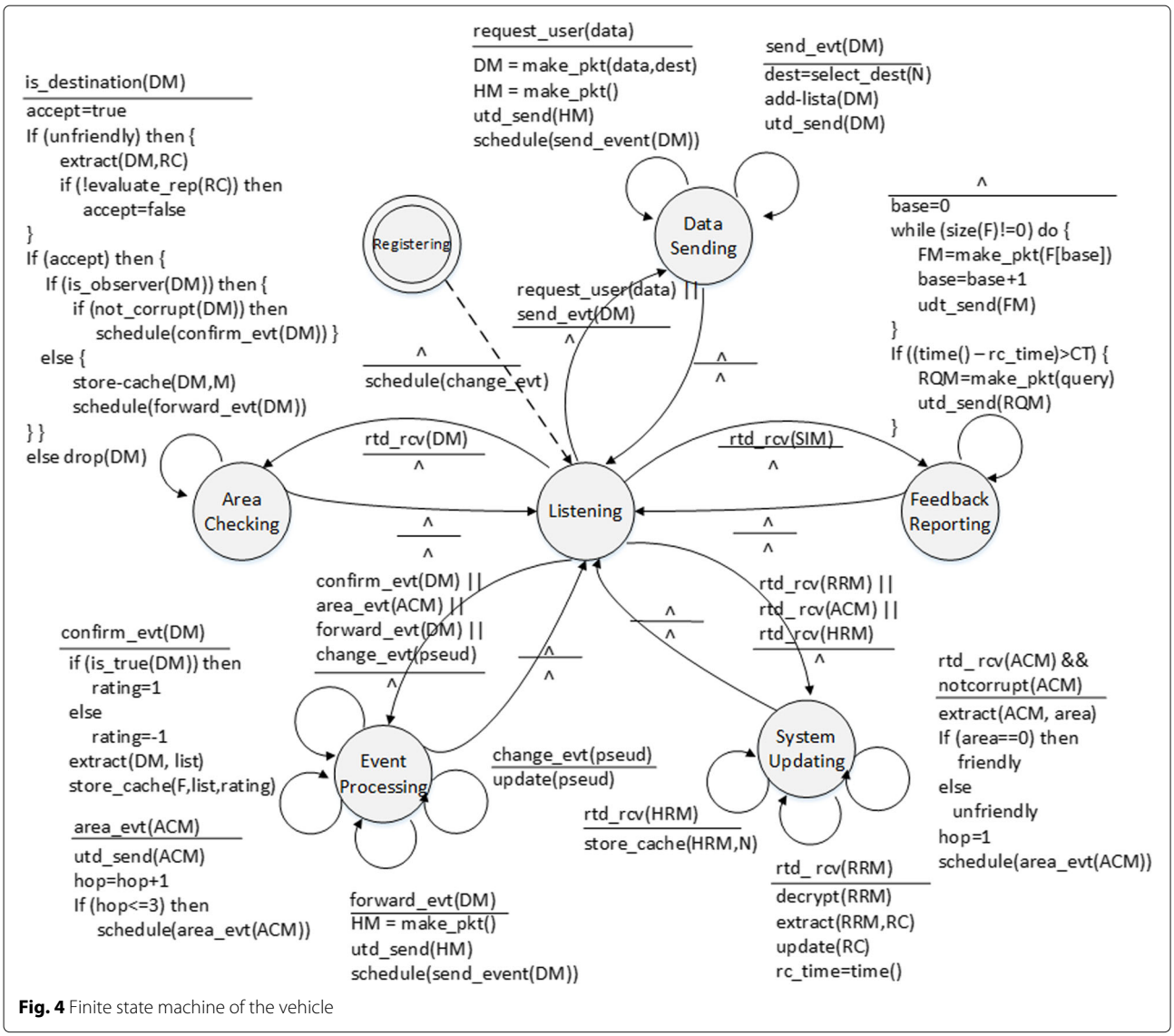

Fig. 4 Finite state machine of the vehicle

the vehicle forwards FM or DM messages to the RSU to address to the destination. Following this, the vehicle examines the time condition for updating the reputation certificate. If the condition is met, the vehicle creates and sends a RQM message to request its last reputation certificate and returns to the *listening* state.

If the message type is DM, the vehicle goes to the *area checking* state. If the DM is addressed to the vehicle, this verifies if the configuration is *unfriendly* and reviews the reputation of the sender vehicle of DM. The vehicle does this by extracting the RC from DM. Then the vehicle decides whether to accept or reject the message. Otherwise, if the configuration is *unfriendly* the message is accepted. After this, the vehicle determines its function; if it is an intermediate vehicle (FV) selected by a forwarding protocol, the vehicle stores the message and schedules its forwarding. If it is an observer vehicle (OV), it checks the integrity of the message and schedules the event for confirming the truth of the content of the message. Finally, the vehicle returns to the *listening* state.

If the user requests a data message to be sent, the vehicle goes to the *Data Sending* state. The vehicle creates the DM and HM messages, sends the HM to its neighbors, and schedules the event send_evt(). After this, the vehicle returns to the *Listening* state. The vehicle also goes to the *Data Sending* state when it is triggered a send_evt(). Then, the vehicle selects the next hop of the message between the neighboring vehicles that answered to HM, adds its data (reputation certificate identification—RCI and check code—CC) in the *list* field, and finally sends DM. Then, sender vehicle returns to the *Listening* state.

If the vehicle receives others events goes to the *event_processing* state. If it is the confirm_evt(), the vehicle evaluates and confirms the truth of the content of DM, extracts the list of EVs from DM, and stores in the cache the corresponding feedback. If it is an area_event(), the vehicle forwards the previous ACM message, counts another hop, and evaluates the conditions required to continue scheduling the area_evt(). If it is the forward_evt(), the vehicle creates and sends a HM message and schedules a send_evt(). Finally, if it is a change_evt(), the vehicle receives the new pseudonym and updates its current pseudonym. Then, the vehicle returns to the *listening* state.

5.2 Operation of the system in the reputation server

In this section, the functions of our system in the server are explained through a FSM. RS operates in five states, as shown in Fig. 5. The server from the *starting* state goes to the *listening* state where it waits for the reception of one of the messages (FM or RQM). Depending on the type of the received message, the RS goes to different states. The new primitives used in the specification of the FSM of the server are described in Table 4.

If the message is FM, the server goes to the *feedback processing* state. First, the reception of the message is checked to ensure the authenticity and integrity of the message. If the message is correct, the server extracts the fields *list* and *rating* from the FM. Then, it starts a cycle for updating the reputation of the evaluated vehicles (EVs) with their behavioral factors included in *list*. At this stage, the reputation aggregation algorithm is carried out. Then, the server returns to the *listening* state.

If the type of received message is RQM, the server goes to the *Answering* state and the RS checks the authenticity of the message. If the message is correct, the server extracts the check code (CC) from the RQM. If the CC is confirmed, the server extracts the RCI identification from RQM, searches the current reputation certificate of the vehicle, and finally creates and sends a RRM message. Then, the server returns to the *Listening* state.

If an area_evt() is received, the server goes to the *Area Updating* state. The server evaluates the condition of each geographical area in the system to determine if is unfriendly or friendly. The RS creates and disseminates an ACM message and provides information about the classification of the area through a RSU. Following this, the server returns to the *Listening* state. If a new vehicle enters, the registry process is carried out, the initial reputation certificate is sent to the vehicle, and thus the vehicle begins to take part of the system.

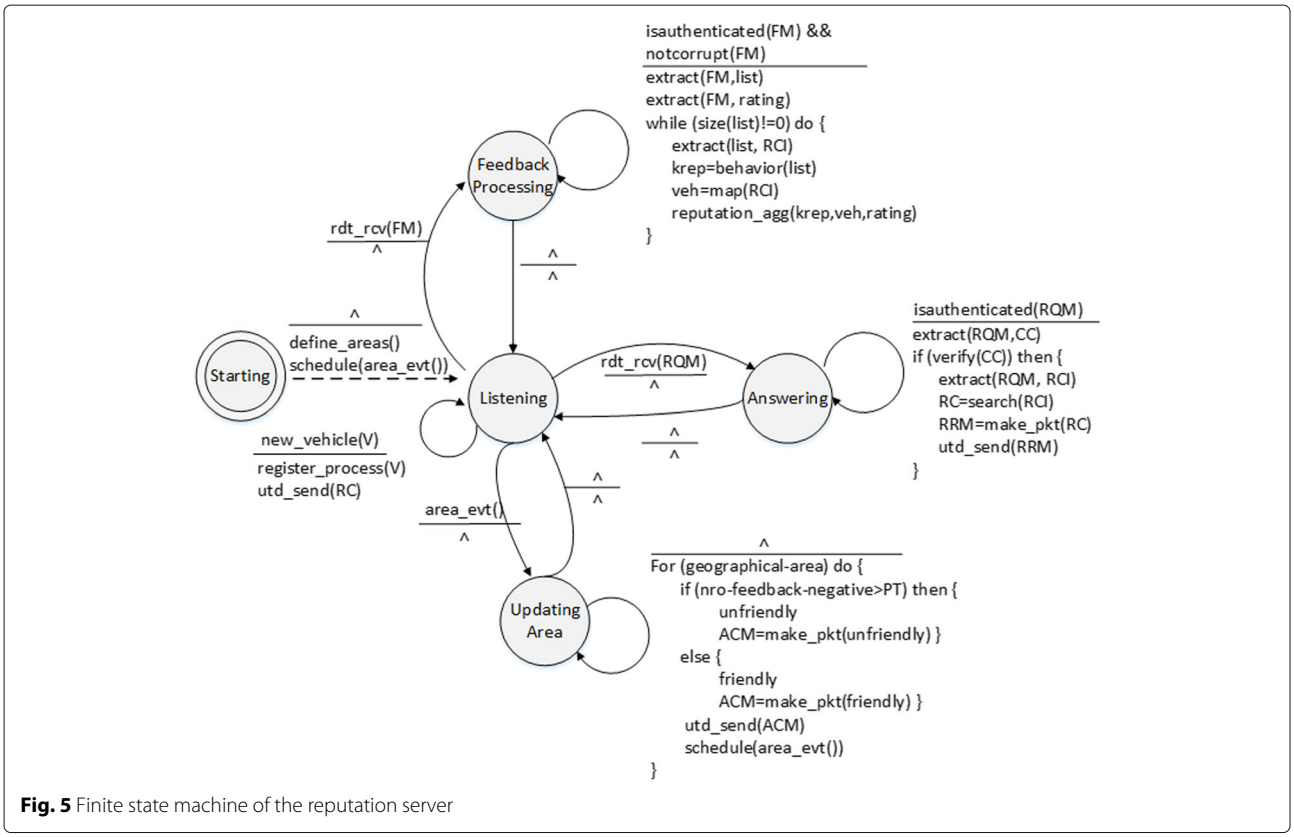

Fig. 5 Finite state machine of the reputation server

Table 4 Primitives used in the FSM of the server

Primitive	Description
verify()	Verification of check code
search()	Searching of reputation certificate
map()	Mapping of identity of the vehicle
reputation_agg()	Executing the reputation algorithm
new_vehicle()	New vehicle in the system
register_process()	Registering of a new vehicle in the system
behavioral()	Determining the behavioral factor

6 Simulation setup

We decided to carry out simulations on the basis of the studies [31, 32]. We took advantage of opportunistic encounters between vehicles to exchange data, and evaluate the opportunistic message forwarding application. This section sets out the motivational scenario for implementing the system; there is an outline of the simulation setup including the parameters of mobility and network and the way the experiments were planned. We also evaluate the average reputation obtained by the vehicles, varying the number of misbehaving vehicles. Finally, we discuss the results of the simulation experiments.

6.1 Motivational scenario

In this section, we explain our application by examining a motivational grid scenario, which is depicted in Fig. 6. The vehicles enter the scenario from different origins, and one RSU is deployed in the center of the grid, which is interconnected to the Internet. It is assumed that the RSU and vehicles are equipped with IEEE 802.11p-based wireless interfaces. Additionally, each vehicle has a built-in Global Positioning System (GPS) device and an on-board unit (OBU) with storage and processing capabilities. The RSU will broadcast signalling messages (SIM) at a regular interval, by means of beacons, and the vehicles start receiving these messages, as soon as they enter in its coverage area. In this way, the vehicles send data messages (DM) saved in its local cache, pending of delivery to the central monitoring system. As well as, the vehicles can update their RCs from the server through the RSU.

There are two kinds of evaluated vehicles (EVs), creator vehicle (*CV*) and forwarder vehicle (*FV*). In Fig. 6, (1) CV_1 creates a DM_1 message and sends it opportunistically to FV_1. (2) FV_1 will store and keep the message and later will opportunistically forward it to FV_2. (3 and 4) DM_1 is forwarded until FV_3 reaches the RSU and sends DM_1 to

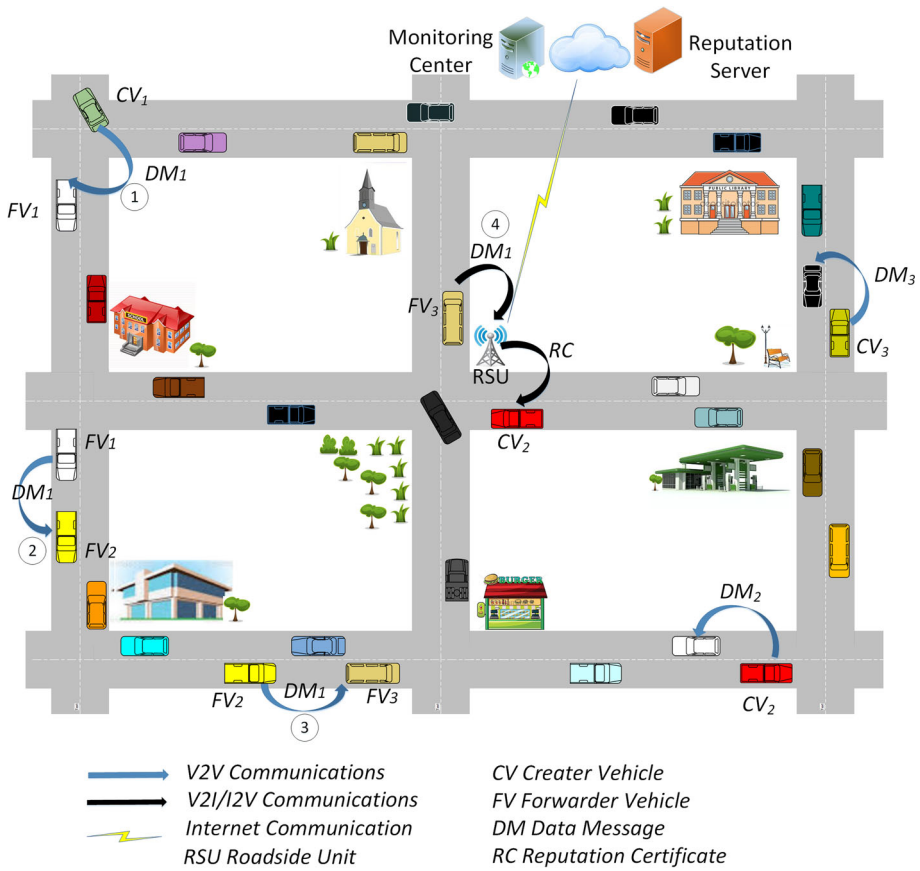

Fig. 6 Motivational scenario: forwarding of messages and sending of feedback to the reputation server

the central monitoring system. At each hop of DM_1, *FVi* extracts the reputation score from the reputation certificate of $FVi - 1$ and checks whether the reputation score of the previous vehicle is within the threshold of trust defined by the application to accept the message. If the condition is true, the message will be accepted. Otherwise, the message will be rejected. The destination of the messages in the simulations, the central monitoring system will give feedback to the CV_1, and the *FVs* responsible for forwarding the message.

Now, suppose that CV_2 in Fig. 6 needs to update its RC. First, it will listen to a signalling message (SIM) from the RSU. Second, CV_2 will send a reputation query message (RQM) to the RS. Third, it will receive a reputation response message (*RRM*) from the server through the RSU. Finally, CV_2 will update its RC so that it can be joined to the data messages created or forwarded by it.

6.2 System simulation

The simulation of VANETs includes vehicular mobility, vehicle to vehicle, and vehicle to infrastructure (V2I) communications [33]. Our scheme was evaluated in an urban scenario (a grid of 1 km^2) with five vertical and five horizontal streets, to represent a typical commercial neighborhood. A total of 100 vehicles (approximately 50 km/h) entered the scenario and stayed there travelling throughput the simulation time. The RSU is deployed in the center of the scenario with a communication range of about 250 m. Parameters related to the vehicle properties and grid scenario were defined in SUMO as shown in Table 5. One of the most important parameters is vehicle speed. Additional aspects include acceleration, deceleration, model and length of the car, placement of RSU, and scenario type.

Likewise, parameters relevant to the vehicular communications network were fixed in OMNET++ in the project veins as shown in Table 6. These parameters include transmission power, frequency band, and channel.

Table 5 SUMO configuration parameters

Parameter	Value
Urban area	1 km^2
Number of vehicles	100 vehicles
Maximum speed of *V*	13.9 m/s
Car model	Krauss
Vehicle length	5 m
Vehicle acceleration	0.8 m/s
Vehicle deceleration	4.5 m/s
Sigma	0.5 m

Table 6 Veins configuration parameters

Parameter	Value
Communication range	250 m
Frequency band	5.9 GHz
Channel bandwidth	10 Mhz
Radio propagation model	Simple path loss
Signalling interval	1 s
Header length	11 bytes
Beacon length	128 bytes
Beacon interval	0.33 s
Bit rate	6 Mbps
MAC protocol	IEEE 802.11p
Network protocol	Wave Short Mess. Protocol

6.3 Planning of the experiments

Works that included assessments of the performance of a reputation system in VANET [34] shows variations in the percentage of malicious vehicles, [35] maintains a fixed number of misbehaving nodes, and varies the probability of sending invalid messages; in [36], there is a randomly selected vehicle that broadcasts bogus traffic messages every 10 s, [37] changes the mobility parameters such as the maximum speed of the vehicles and vehicular density. We selected the average reputation as the main response variable like in [38].

In each experiment, we generated a representative number of messages and chose a sample of 40 CVs, a variable percentage of which were malicious vehicles like in [33]. A *malicious or misbehaving vehicle* is a vehicle that will always send fake messages, will forward messages, and will always provide correct feedback of its peers. We suppose that an event in the road occurs every 60 s around the CVs, and thus, these generate a DM every 60 s, which is forwarded to the central monitoring system. We performed simulations for 600 s and executed 5 runs for each experiment. Following, the response variables and factors are defined.

Response variable

- *Average reputation* (AR): this is the arithmetic mean of the reputation score (Rep) that all the vehicles have in the reputation server.

Variable factor

- *Percentage of malicious vehicles* (MV): this is the number of malicious vehicles with regard to the number of CVs; MV used were 12.5%, 25%, 50%, and 75% respectively;
- *Weight δ*: in order to calculate the reputation score of a vehicle (Rep), there are two components with their weights. Reputation for the creation of messages has

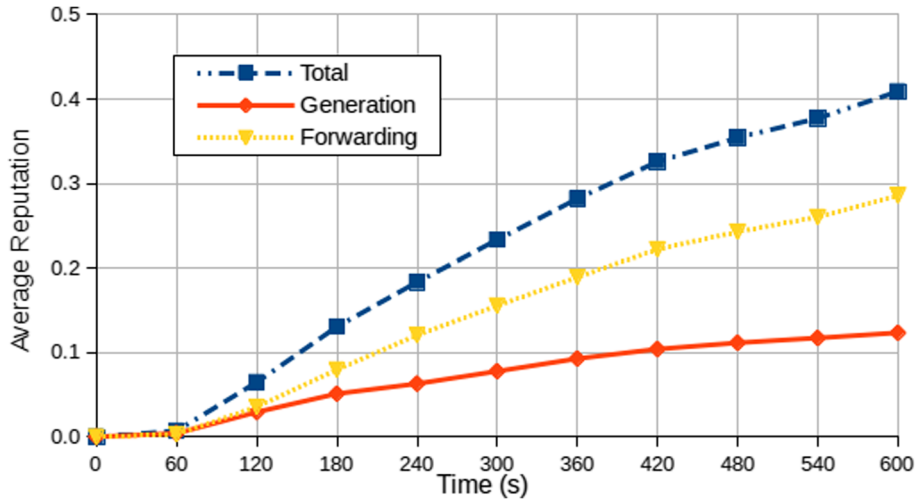

Fig. 7 Results of AR with MV = 12.5%

a weight δ, and reputation for the forwarding of messages has a weight $1-\delta$ (see Eq. 3). δ was set up in 0.2 and 0.5.

Fixed factors

- *Penetration rate*: this refers to the percentage of smart vehicles registered in the reputation system; a penetration rate of 100% is assumed for the experiments;
- *Initial reputation*: this refers to the reputation with which the vehicle starts in the system; in the simulations, the initial reputation is zero;
- *Weight* α: this is the weight given to the last rating reported in a feedback for calculating the reputation of a vehicle and was fixed at 0.2; thus, $1-\alpha$ is the weight given to the historic reputation of the vehicle (i.e., 0.8);
- *Elliptic curve*: this refers to the type of elliptical curve used to implement the functions of elliptic curve cryptographic. We selected the *secp256r* curve, the functions of which include the signing and checking of pseudonyms, reputation certificates, and messages.

6.4 Results and discussions

In this section, there is a discussion of the results of the simulation experiments with δ in 0.5. Figures 7, 8, 9, and 10 show the four scenarios of MV with the results of the average (AR) minute by minute deployed as total

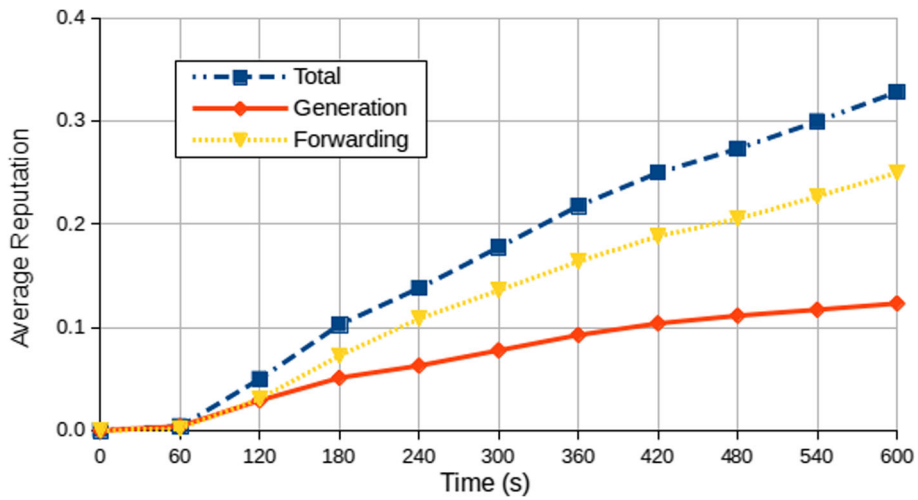

Fig. 8 Results of AR with MV = 25%

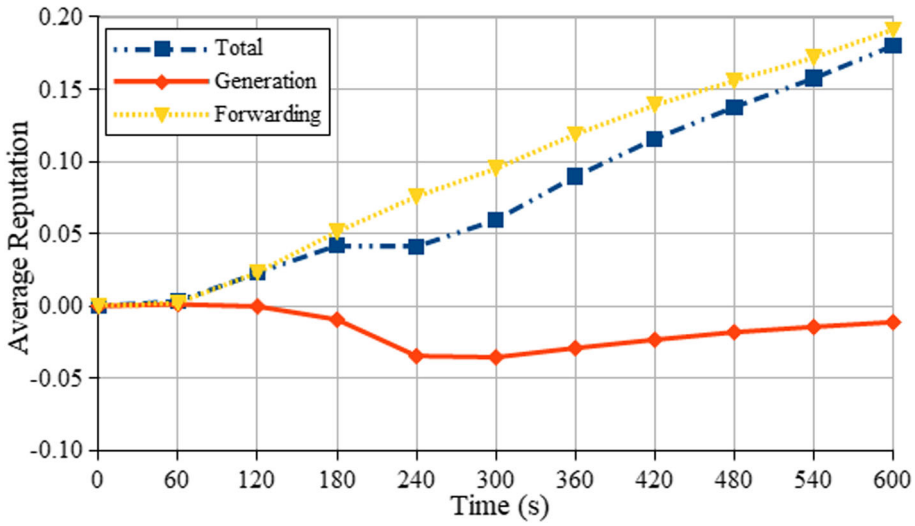

Fig. 9 Results of AR with MV = 50%

for the generation of messages and for the forwarding of messages.

Figure 7 shows the results of AR for the scenario with 12.5% of the MV (i.e., 5 of the CVs sending fake messages). The results of AR for the generation of messages are positive and less than 0.2. The main reason is that the number of vehicles sending honest messages is greater than the number of vehicles sending fake messages, and hence, few negative feedback was reported. The AR for the forwarding of messages is also positive, greater than AR for the generation of messages and less than the total AR. This is because all the vehicles that forwarded messages received positive feedbacks. Figure 8 shows the results of AR for the scenario with 25% of the MV which are similar to the results of the scenario with 12.5% of the MV.

The results of AR for 50% of the MV are shown in Fig. 9. The results for the generation of messages are negative because the number of vehicles generating fake messages increases, and thus, the number of negative feedback by this factor also increases. The results for the forwarding of messages are positive and higher than the results of the total AR. This is due to that the vehicles continue receiving positive feedbacks despite the increase of malicious vehicles.

Figure 10 depicts the results for 75% of the MV. The influence of the percentage of the MV on the results is

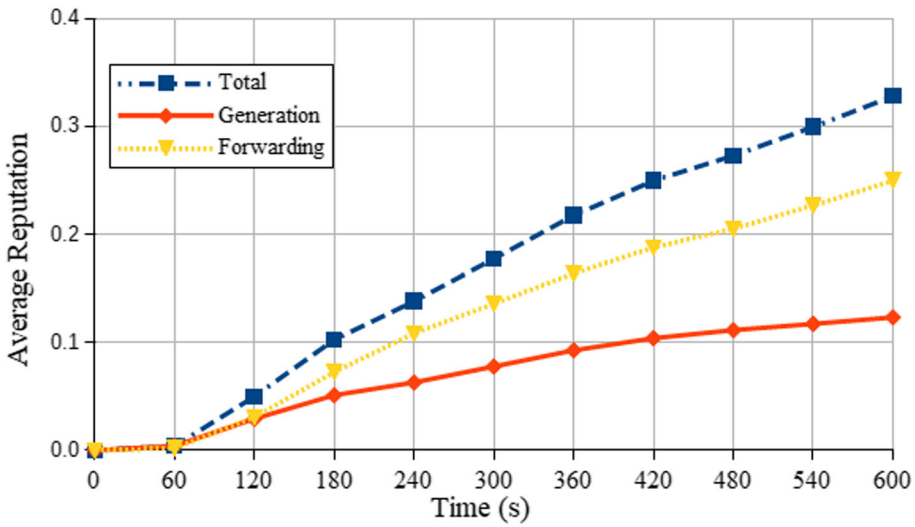

Fig. 10 Results of AR with MV = 75%

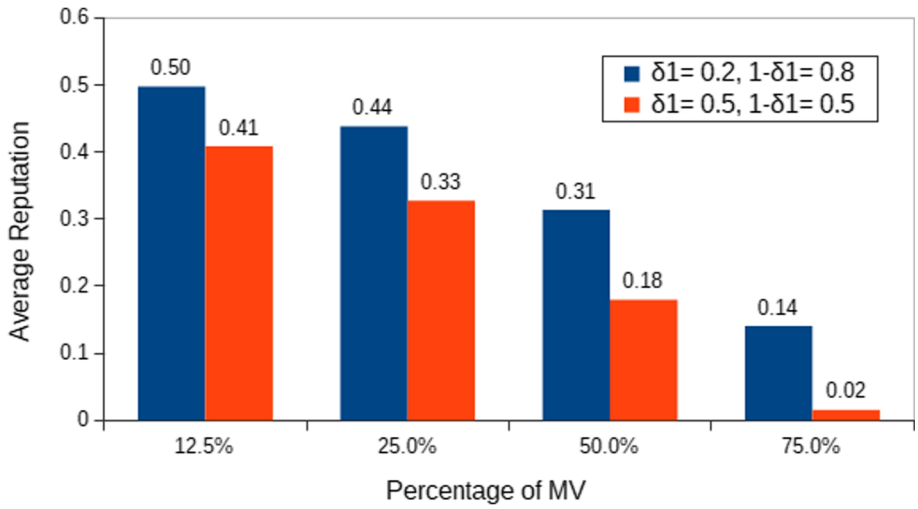

Fig. 11 Average reputation of the vehicles varying δ

more evident in this scenario. The results of the total AR and for the generation of messages are negative, and the results for the forwarding of messages are the lowest with regard to the other scenarios. It is only in the range from 540 to 600 s that the total AR increases a little more than zero. The main reason for this is that only 5 vehicles sent honest messages. The results for the generation of messages did not fall to -0.5 in this case, because the malicious vehicles could also receive positive feedback for the forwarding of the messages.

We also realized experiments with δ fixed in 0.2; Fig. 11 compares the final results of the AR for the eight experiments with two values of δ and varying MV. All the results of AR were positive, this is due to the fact that the number of vehicles receiving feedback for the forwarding of messages surpasses the number of vehicles receiving feedback for the generation of messages. The results showed that AR is influenced by δ; the four results of AR with $\delta = 0.2$ are higher than for the four experiments with $\delta = 0.5$. This is explained on the basis that the weight given for the forwarding of messages increased, and on the contrary, the weight for the creation of messages decreased. It is also observed that by increasing the MV, the results of AR decreased. The reason is that fewer vehicles receive feedback for the forwarding of messages, and the number of vehicles receiving negative feedback for the generation of fake messages increases. As we expected, δ and MV influenced in the results.

7 Conclusions

We did the ontological representation of a reputation system in VANETs and calculated the reputation of the vehicles with regard to the opportunistic forwarding of messages, in which the vehicles received feedback for the behavioral factors of creation and forwarding of messages. We evaluated the performance of the system in an urban scenario under different application parameters. The results revealed that the reputation score of vehicles is influenced by the weights attributed to the factors of creation and forwarding of messages and the weight attributed to the most recent rating. This last weight influenced the number of feedbacks necessary for a vehicle to reach either the maximum or minimum reputation score established for each behavioral factor. The results also showed that the reputation score of the vehicles reflects their behavior, e.g., the scenario where only few vehicles send fake messages obtained the highest reputation score. By contrast, scenarios in which many vehicles sent fake messages obtained the lowest reputation score.

Abbreviations

ACM: Area condition message; AR: Average reputation; CA: Certificate authority; CC: Check code; CV: Creator vehicle; DM: Data message; ECC: Elliptic curve cryptography; EV: Evaluated vehicle; FM: Feedback message; FV: Forwarder vehicle; FSM: Finite state machine; GPS: Global Positioning System; HM: Hello messages; HRM: Hello response message; LTE: Long-term evolution; MV: Malicious vehicle; ON: Observer node; OBU: On-Board Unit; OMNET: Objective Modular NEtwork Testbed; OV: Observer vehicle; RC: Reputation certificate; RCI: Reputation certificate identification; RGTE: Reputation-based Global Trust Establishment; RQM: Reputation query message; RRM: Reputation response message; RS: Reputation server; RSU: Roadside unit; SIM: Signalling message; SUMO: Simulation of Urban MObility; VANET: Vehicular ad hoc network; V2I: Vehicle to infrastructure; V2V: Vehicle to vehicle

Acknowledgements

The authors are thankful to the Universidad de Pamplona-Colombia for supporting this work,;Maths Science Institute and Computing-ICMC, University of São Paulo, São Carlos, Brazil, for supporting the collaboration of coauthors; and Center for Mathematical Sciences Applied to Industry -CEPID-CeMEAI, for providing technological support.

Authors' contributions

LS conceived this study, designed and performed the simulations, analyzed the results, and wrote the manuscript. EM participated in the co-ordination of

the study and data monitoring and drafted the manuscript. Both authors read and approved the manuscript.

Funding
This publication was made possible by a grant from the Universidad de Pamplona-Colombia.

Availability of data and materials
All relevant data are within the paper and its supporting information files on https://github.com/lsantosj/ATSecVanet/tree/master/Results-ARS.

Competing interests
The authors declare that they have no competing interests.

Received: 28 February 2019 Accepted: 18 July 2019
Published online: 13 August 2019

References

1. X. Li, J. Liu, X. Li, W. Sun, in *5th International Conference On Intelligent Networking and Collaborative Systems (INCoS)*. RGTE: a reputation-based global trust establishment in VANETs (IEEE, Xi'an, 2013), pp. 210–214
2. F. Yang, S. Wang, J. Li, Z. Liu, Q. Sun, An overview of internet of vehicles. China Commun. **11**(10), 1–15 (2014)
3. L. M. S. Jaimes, K. Ullah, E. dos Santos Moreira, in *8th IEEE Latin-American Conference on Communications (LATINCOM)*. ARS: Anonymous reputation system for vehicular ad hoc networks (IEEE, Medellín, 2016), pp. 1–6
4. R. M. Vanni P, L. M. Santos, G. Mapp, E. Moreira, in *The Twelfth Advanced International Conference on Telecommunications (AICT)*. Ontology driven reputation model for VANET (IARIA, Valencia, 2016), pp. 14–19
5. German Aerospace Center, Institute of Transportation Systems: SUMO Simulation Urban MObility. http://sumo.sourceforge.net/. Accessed 30 Mar 2017
6. OpenSim Ltd.: OMNeT++ Discrete Event Simulator. https://omnetpp.org/. Accessed 30 Mar 2017
7. Christoph Sommer: Veins Vehicles in Network Simulations. https://veins.car2x.org/. Accessed 30 Mar 2017
8. Crypto++ Community: Crypto++ Library. https://www.cryptopp.com/. Accessed 30 Mar 2017
9. Q. Li, A. Malip, K. M. Martin, S.-L. Ng, J. Zhang, A reputation-based announcement scheme for VANETs. IEEE Trans. Veh. Technol. **61**(9), 4095–4108 (2012)
10. Z. Cao, Q. Li, H. W. Lim, J. Zhang, in *IEEE International Conference On Service Operations and Logistics, and Informatics (SOLI)*. A multi-hop reputation announcement scheme for vanets (IEEE, China, 2014), pp. 238–243
11. A. Malip, Anonymous authenticated announcement schemes in vehicular ad hoc networks. PhD thesis, Information Security Group, Department of Mathematics Royal Holloway, University of London (2014)
12. L. Chen, Q. Li, K. M. Martin, S.-L. Ng, in *International Symposium on Wireless Vehicular Communications (WIVEC)*. A reputation-based announcement scheme that considers privacy (IEEE, Dresden, 2013), pp. 1–5
13. L. Chen, Q. Li, K. M. Martin, S.-L. Ng, Private reputation retrieval in public-a privacy-aware announcement scheme for VANETs. IET Inf. Secur. **11**(4), 204–210 (2016)
14. Z. Lu, Q. Wang, G. Qu, Z. Liu, in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. BARS: a blockchain-based anonymous reputation system for trust management in VANETs (IEEE, New York, 2018), pp. 98–103
15. D. Zhang, F. R. Yu, R. Yang, H. Tang, in *8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet)*. A deep reinforcement learning-based trust management scheme for software-defined vehicular networks (ACM, Montreal, 2018), pp. 1–7
16. S. Das, I. Das, R. P. Singh, P. Johri, A. Kumar, in *Data and Communication Networks. Trust-Based Scheme for Location Finding in VANETs Using Trustworthiness of Node* (Springer, Singapore, 2019), pp. 43–55
17. A. Kumar, S. Bhardwaj, P. Malik, P. Dabas, in *International Conference on Communications and Cyber Physical Engineering*. An enhanced reputation-based data forwarding mechanism for VANETs (Springer, Singapore, 2018), pp. 251–259
18. E. Eziama, K. Tepe, A. Balador, K. S. Nwizege, L. M. Jaimes, in *IEEE Globecom Workshops (GC Wkshps)*. Malicious node detection in vehicular ad-hoc network using machine land deep learning (IEEE, Abu Dhabi, 2018), pp. 1–6
19. M. Xiao, J. Wu, C. Liu, L. Huang, *International Conference on Computer Communications (INFOCOM). Tour: time-sensitive opportunistic utility-based routing in delay tolerant networks*. (IEEE, Turin, 2013), pp. 2085–2091
20. M. Xiao, J. Wu, L. Huang, Community-aware opportunistic routing in mobile social networks. IEEE Trans. Comput. **63**(7), 1682–1695 (2013)
21. H. Zhou, S. Xu, D. Ren, C. Huang, H. Zhang, Analysis of event-driven warning message propagation in vehicular ad hoc networks. Ad Hoc Netw. **55**, 87–96 (2017)
22. M. Ruan, X. Chen, H. Zhou, Centrality prediction based on K-order Markov chain in Mobile Social Networks. Peer-to-Peer Netw. Appl. **12**, 1–11 (2019)
23. C. M. Huang, Y. F. Chen, S. Xu, H. Zhou, The vehicular social network (VSN)-based sharing of downloaded geo data using the credit-based clustering scheme. IEEE Access. **6**, 58254–58271 (2018)
24. H. Zhou, H. Wang, X. Chen, X. Li, S. Xu, Data offloading techniques through vehicular ad hoc networks: a survey. IEEE Access. **6**, 65250–65259 (2018)
25. R. S. Yokoyama, B. Y. Kimura, L. M. Jaimes, E. D. Moreira, in *28th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. A beaconing-based opportunistic service discovery protocol for vehicular networks (IEEE, Victoria, 2014), pp. 498–503
26. Y. Jin, G. Kesidis, J. Shin, F. Kocak, Y. Yi, Impacts of sel sh behaviors on the scalability of hybrid client: server and peer-to-peer caching systems. IEEE/ACM Trans. Networking (TON). **23**(6), 1818–1831 (2015)
27. G. Primiero, F. Raimondi, T. Chen, R. Nagarajan, *IEEE European Symposium in Security and Privacy Workshops (EuroSIP). A proof-theoretic trust and reputation model for VANET*. (IEEE, San Jose, 2017), pp. 146–152
28. Dan Brickley and Libby Miller: FOAF Vocabulary Specification 0.99. http://xmlns.com/foaf/spec/. Accessed 30 Mar 2017
29. W3C: PROV-O: The PROV Ontology. https://www.w3.org/TR/prov-o/. Accessed 30 Mar 2017
30. S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. R. Baee, S. Mandala, Trust management in vehicular ad hoc network: a systematic review. EURASIP J. Wirel. Commun. Netw. **2015**(1), 146 (2015)
31. K. Ullah, L. M. Jaimes, R. S. Yokoyama, E. dos Santos Moreira, in *4th International Conference on Advances in Vehicular Systems, Technologies and Applications*. Advertising roadside services using vehicular ad hoc network (VANET) opportunistic capabilities (IARIA, St. Julians, 2015), pp. 7–13
32. K. Ullah, L. M. Santos, J. B. Ribeiro, E. D. Moreira, in *15th International Conference on Ad-Hoc Networks and Wireless (AdHoc Now)*. Sadp: A lightweight beaconing-based commercial services advertisement protocol for vehicular ad hoc network (Springer, Lille, 2016), pp. 279–293
33. C. Sommer, R. German, F. Dressler, Bidirectionally coupled network and road traffic simulation for improved IVC analysis. IEEE Trans. Mob. Comput. **10**(1), 3–15 (2011). https://doi.org/10.1109/TMC.2010.133
34. F. G. Mármol, G. M. Pérez, Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. J. Netw. Comput. Appl. **35**(3), 934–941 (2012)
35. Z. Li, C. Chigan, in *IEEE International Conference on Communications (ICC)*. Joint privacy and reputation assurance for VANETs (IEEE, Ottawa, 2012), pp. 560–565
36. Q. Ding, X. Li, M. Jiang, X. Zhou, in *International Conference on Multimedia Technology (ICMT)*. Reputation management in vehicular ad hoc networks (IEEE, Ningbo, 2010), pp. 1–5
37. N.-W. Lo, H.-C. Tsai, A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP J. Wirel. Commun. Netw. **2009**(1), 1 (2009)
38. E.-J. Lee, I.-H. Bae, in *International Conference on Testbeds and Research Infrastructures*. A reputation-based adaptive trust management system for vehicular clouds (Springer, Guangzhou, 2014), pp. 77–86

Publisher's Note