IET Wireless Sensor Systems

Review Article

IET Journals
The Institution of Engineering and Technology

Trust enforcement in vehicular networks: challenges and opportunities

ISSN 2043-6386
Received on 14th November 2018
Revised 27th February 2019
Accepted on 27th March 2019
E-First on 20th May 2019
doi: 10.1049/iet-wss.2018.5211
www.ietdl.org

Hesham El-Sayed[1] ✉, Moumena Chaqfeh[1], Hadeel El-Kassabi[1], Mohamed Adel Serhani[1], Henry Alexander[1]

[1]*College of Information Technology, UAE University, Al Ain, UAE*

✉ *E-mail: helsayed@uaeu.ac.ae*

Abstract: A major objective of vehicular networking is to improve road safety and travel convenience. The experience of individual vehicles on traffic conditions and travel situations can be shared with other vehicles for improving their route planning and driving decisions. Nevertheless, the frequent occurrence of adversary vehicles in the network is unavoidable. These vehicles may engage in various malicious activities affecting the overall network performance. To control and monitor effectively security threats in vehicular networks, an efficient trust management system should be employed to identify the trustworthiness of individual vehicles and detect malicious drivers. This study provides a review of the research efforts aimed at enabling trust in vehicular environments. The major challenges are highlighted, and an edge-based architecture is proposed as a supportive platform. Furthermore, existing models proposed for trust evaluation, aggregation, propagation and decision making are reviewed. Finally, the current directions to enforce trust in vehicular environments are highlighted.

1 Introduction

Rapid urbanisation has increased the dependency on on-road vehicles [1, 2]. It is estimated that globally, there are currently ∼1.2 billion vehicles [3], and transportation systems face challenges such as traffic congestion [4], accidents and safety-related problems [5], long commuting time [6], environmental impact and increased energy consumption [7–9]. Accordingly, vehicular networking environments are proposed as promising solutions for urban transportation problems.

A major objective of vehicular networking is to improve road safety and travel convenience. The experience of individual vehicles on traffic conditions and travel situations can be shared with other vehicles for improving their route planning and driving decisions. Nevertheless, the frequent occurrence of adversary vehicles in the network is unavoidable. These vehicles may engage in various malicious activities that affect overall network performance.

Existing solutions for such security problems mainly employ cryptography, digital signatures, certification, pseudonym schemes and public key infrastructures. These solutions demand high resource utilisation owing to their computational complexity. For example, cryptography can provide confidentiality, integrity, availability, authentication and non-repudiation. However, it cannot address real-time threats in vehicular networks such as false message injection. Additionally, its potential to determine the trustworthiness of the received messages is limited.

Trust management (TM) systems can provide access control, reliability, accurate trustworthy computation and high-quality services. However, their implementation in a vehicular environment is challenging owing to rapid network disconnections, dynamic mobility patterns and limited computing and communication capabilities. In this study, these challenges are reviewed in a comprehensive survey that emphasises different hierarchal levels of trust dynamics. The survey highlights specific trust properties for vehicular networks and provides a classification of existing trust models and evaluation techniques. Moreover, current research directions are discussed in this context.

Existing review studies [10–12] do not comprehensively explain the complex representation of the trust models designed for vehicular environments. In addition, they often assume a fully decentralised self-organising infrastructure. For example, in [10], the authors review existing trust models proposed in different domains and address the key issues for application in vehicular *ad-hoc* networks. Trust models proposed for vehicular networks are surveyed in [11]. In [12], the authors provide an adversary-oriented survey for existing vehicular trust models by considering when trust is preferable over cryptography and vice-versa. In contrast, the present survey aims at drawing attention to TM in next-generation vehicular environments. In future smart cities, complex infrastructures may enhance vehicular networks with computational resources and prior trust data, in addition to central and semi-central services.

The remaining of the paper is organised as follows: Section 2 provides background on trust and highlights existing challenges for enabling trust in vehicular networks. Section 3 proposes an edge computing (EC) architecture as a trust enforcement platform. Section 4 classifies and reviews existing trust evaluation models, whereas Section 5 reviews trust propagation, aggregation and decision-making models. Section 6 highlights current opportunities for enabling trust in vehicular environments. The last section concludes the paper.

2 Background

Trust is commonly defined as a relationship between two or more entities. To ensure data precision and accuracy, trust often certifies the data from every entity for reliability and credibility. Using trust as an inception model, a rational relationship of dependence and reliance between entities may be established. Also, the trust holds credibility over predictability, value exchange, delayed reciprocity, similarity and dependability. Owing to its flexible nature, trust can be incorporated in various domains to function as a decision-making process. In general, trust is the integration of different characteristics including belief, confidence, faith, reliability, integrity, ability, timeliness, reliance, dependence and expectation. The functionality of these characteristics is largely domain-specific [13–15]. In vehicular networks, trust enforcement is a challenging issue owing to the dynamic nature of these environments. In this section, the importance of trust realisation in different domains is highlighted in general and in vehicular networks in particular; furthermore, the challenges of vehicular networking environments affecting trust-based systems are described.

Table 1 Main trust terminologies

Term	Definition
trustor (TR)	Entity that trusts another entity. It refers to the willingness or intention to depend on another person.
trustee (TE)	Entity that shows benevolence, integrity, competence and predictability. Trustor behaviourally depends on the trustee in making decisions.
trustworthiness (TW)	Cognitive measure that is a level of belief between entities.
reputation (RE)	Collective measure of trustworthiness that is estimated by the trust the others hold for a certain entity.
trust metric (Tm)	Numerical value derived used to estimate the trustworthiness of an entity.
trust list (TL)	List that stores the collection of trusted entities for future reference
trust channel (TC)	Trusted path where all the participating nodes in an event are authorised and authenticated prior to participation.

2.1 Significance of trust

The importance of trust is acknowledged in various fields involving multidimensional and multifaceted perception. In sociology, trust is perceived as a social reality that controls and monitors confidence and power in human relationships. In [16], trust is defined as a basic fact of social life that plays a vital role in every decision-making process. The accuracy and integrity of trust entirely depend on its impact from past and present activity; furthermore, the complexity and uncertainty metrics for every event can be monitored in terms of the trust. In psychology, trust is attributed to security, optimism and reliance. It also preludes to subjective well-being and fosters personality traits. In [17], trust is defined as the confidence that one will find what is desired from another rather than what is feared, thereby it is one of the most conceptualised cognitive processes in the development of a relationship. In philosophy, trust is comprehended as a type of dependence and belief on other people, underpinned on a certain demeanour.

The attitude that builds trust may vary. It can be expressed as a simple belief that a person would act appropriately for the right reasons, or as anticipation that a person would do what others expect him/her to do. In philosophy, trust can be flexible and compromised up to a certain level, but the critical point derivation is based on experience and recommendations. In [18], it is explained that the trustor can accept some level of risk or vulnerability over the trustee, and trust will aggregate before one starts to monitor the actions of the others. In economics, trust has a great impact on the instantaneous distribution between peers. In [19], it is claimed that higher trust propagation in society would yield higher economic development and prosperity.

In computer science, trust is implemented in all layers of system architecture. In [20], trust is defined as the assertion that functions separately verify and authorise an entity. Both the trustor and trustee should be validated equally to enhance the contextual factor of expectancy. In wireless networks, trust models are used to enhance the credentials between the entity relationships and the leverage between information resources. Different trust terminologies are interchangeably used in miscellaneous domains. The main common terminologies are mentioned in Table 1.

In vehicular networks, trust is a major challenge owing to the dynamicity, mobility and heterogeneity of the entities involved, including drivers, providers and brokers. TM in vehicular environments consists of four main hierarchically structured components, as shown in Fig. 1: trust evaluation, propagation, aggregation and decision making. Trust components use the 'trust value' to provide reliable services. This can be computed by evaluating the sending entity and/or analysing the content of the

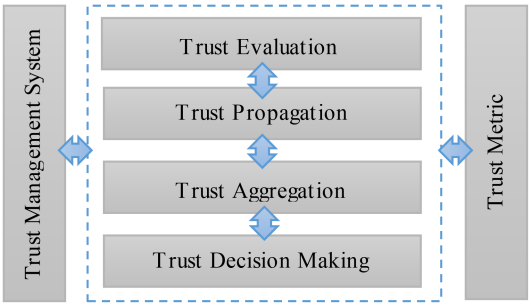

Fig. 1 *Hierarchical TM components*

received messages. This value can be represented as a point of uncertainty taking values in the interval [0, 1].

When two vehicles communicate for the first time, the receiving vehicle can compute the trustworthiness of the sender by collecting recommendations from its neighbours. The received recommendations can then be aggregated to determine the trustworthiness of the sender for improving trust decisions.

The challenges in vehicular networking environments have prompted the proposal of various solutions for trust computation and evaluation. These challenges will be discussed in the next section.

2.2 Challenges of vehicular networks

The characteristics of vehicular networking environment pose various challenges in the modelling, implementation and management of different types of communication systems [21] and applications. The high mobility that characterises vehicular networks usually causes frequent disconnections and short-living communication links. Vehicular mobility is affected by network density, as higher densities would certainly result in lower average speeds. In addition to mobility, network connectivity is also affected by density. Obviously, connectivity improves as density increases because vehicles may stay in the communication range of their neighbours for longer periods when they travel at lower speeds. In this section, the effect of density, mobility and connectivity on TM systems is discussed in the context of vehicular environments.

2.2.1 Density: Network density often refers to the number of vehicles on the road. The common speed–density relationship is often used to describe driver behaviour, and implies that the average speed declines as density increases. The characteristic driver reaction to higher densities is to slow down, and this is reflected in modern urban traffic flow models. By contrast, uninterrupted flow occurs primarily on freeways, where there are no intersections, traffic signals, or stop signs. In that case, the characteristics of the traffic stream are based on the interactions between vehicles and the surrounding environment. Under high-density scenarios, more interactions are anticipated for data collection and dissemination. These interactions can enrich TM systems with direct experiences, indirect recommendations and reliable multi-hop data propagation. However, higher densities may lead to serious scalability-related problems, such as broadcast storms, data redundancy, communication overhead and networking delays.

2.2.2 Mobility: The high mobility that characterises vehicular networks enables individual vehicles to collect data about the surrounding environment from multiple sources through vehicle-to-vehicle (V2V) and/or V2I communication. Therefore, vehicles can receive different trust opinions and recommendations on entities and data as they travel, depending on the density of the network. Under low-density scenarios, vehicles may not receive sufficient data to make trust decisions. Also, the received opinions may present considerable variations, and thus the vehicle trustworthiness evaluation may be affected by the uncertainty factor, resulting in unreliable trust decisions. Generally, even though mobility allows data propagation to relatively long

distances, it may decrease data delivery ratios owing to frequent disconnections.

A major challenge in vehicular *ad-hoc* networks (VANETs) is the construction of a mobility model that is characterised by high accuracy and realistic mobility description. In [22], the authors proposed a framework with guidelines for the construction of vehicular mobility models. In addition, they explained the different approaches used for the development of these models and their interaction with networking simulators. According to [22], mobility models can be classified as synthetic-based, survey-based, trace-based and traffic-simulator-based. Examples of synthetic-based models include stochastic, traffic stream, queueing and car-following models.

2.2.3 Connectivity: In self-organising VANETs [23, 24], connectivity is affected by mobility and density. Under high-density scenarios, mobility decreases; therefore, communication efficiency increases and data can be more reliably disseminated. However, extremely high densities may easily lead to the broadcast storm problem, where traffic data may be lost owing to collisions. Moreover, the communication overhead is increased owing to data redundancy. By contrast, low densities result in high mobility, sparsely connected networks, frequent disconnections and error-prone communication links. However, the connectivity of vehicular networks can be effectively improved by VANETs with fixed infrastructural units. Each unit provides connectivity to the vehicles within its communication range. Thereby, the influence of mobility and density on network availability is controlled. In the next section, the potential architectures for vehicular networks are reviewed. It is proposed that TM be enabled in the context of an EC architecture, which would have a great impact on addressing the challenging features of vehicular networking environments in future smart cities [25].

3 Trust architecture: from VANETs to the edge

In vehicular environments, the experience of individual vehicles on traffic conditions and travel situations can be shared with others for improving their route planning and driving decisions. To avoid making inappropriate decisions, it is essential to ensure the trustworthiness of other vehicles that may behave maliciously to gain more benefits compared to other vehicles. Such malicious behaviours include injecting false information in the network or refusing to participate in message dissemination. An efficient TM system should accurately identify the trustworthiness of individual vehicles and detect malicious drivers. In this section, a background on existing architectures to support vehicular TM solutions is provided. Then, an EC platform consisting of three layers is proposed. Finally, an evaluation scenario for smart city environment is provided.

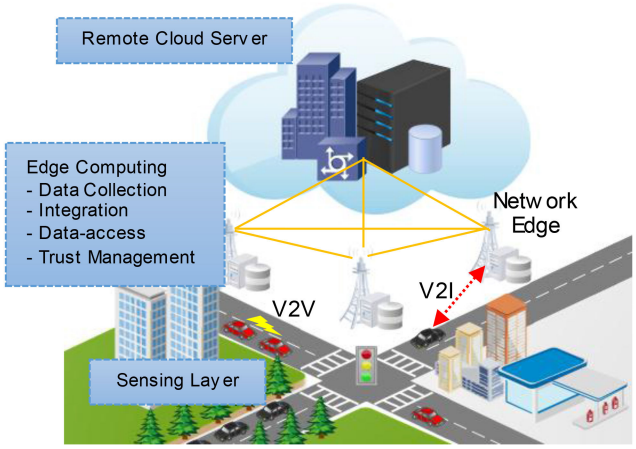

Fig. 2 *Edge-based TM architecture*

3.1 Background

Existing TM solutions in the context of vehicular environments usually consider either the V2V approach in a fully decentralised VANET [26] or the centralised cloud-based architecture [27]. Enabling trust in VANETs remains challenging mainly owing to the high mobility of vehicles, which causes frequent disconnections, as discussed in the previous section. Thus, vehicles may not be able to collect sufficient data for trust evaluation, particularly under low traffic conditions. As connectivity improves under high traffic flow rates, traffic data may be lost owing to packet collisions. In addition, TM poses a serious communication overhead in VANETs that may accidentally prohibit the retrieval of time-critical safety data.

To take advantage of cloud computing in vehicular networks, vehicular cloud computing (VCC) was recently introduced [28]. Current application taxonomy and key management issues of VCC can be found in [27]. The main objective of integrating cloud computing in vehicular environments is to provide dynamic applications that can predict traffic events and adapt to environmental changes. However, the fully centralised environment provided by VCC has various drawbacks in terms of user privacy and control. For instance, personal data and social activities may be released to various centralised services such as search engines and rating services. This aspect of pulling the control from the user to the cloud eliminates the opportunities for exploiting the capabilities of modern personal devices. Moreover, even though VCC has greatly improved resource utilisation and computation performance in vehicular environments, transmission delays are considered serious issues, particularly when the cloud servers are far from travelling vehicles.

To push the cloud services of the radio network closer to mobile endpoints, mobile EC (MEC) has been recently introduced [29]. MEC provides low latency responses, high bandwidth and real-time access to network information via applications and services. These characteristics enable MEC to offer an ideal platform for vehicular networks, which are highly dynamic environments that essentially require real-time data support. An EC architecture can overcome the limitations of both VANETs and VCC by providing low latency, high scalability and efficient data access services. Despite its essential role, TM research in the context of EC is quite limited, mostly because it is a recent paradigm, and its infrastructure is not standardised yet [30].

3.2 Proposed platform

Two networking paradigms can be considered for the integration of EC in vehicular environments: 5G [31] and software-defined networking (SDN) [32]. 5G can offer better response time, greater coverage and more efficient signalling, whereas SDN provides flexibility, scalability and programmability by separating the data plane from the control plane for simplified network development, deployment and management [33]. The required communication components for enabling TM in an edge-based vehicular environment are an SDN global controller, a 5G base station (BS), SDN roadside units (RSUs) and SDN wireless nodes.

An EC architecture is proposed for TM in future vehicular environments consisting of three layers: The traffic sensing, the MEC and the cloud server layers, as shown in Fig. 2. The traffic sensing layer combines two types of entities in a hierarchical architecture: a large number of mobile vehicles with limited computation and communication capabilities, and a set of network edges. Passive data, namely, the number of vehicles and license plate numbers, is collected by edges, whereas vehicles act as a source of active data, namely, speed, direction and location information [34], through their on-board units. It is worth noting that smartphones have received considerable attention to support portable vehicular urban sensing, as they are equipped with a variety of environmental sensors and wireless interfaces [35].

The EC layer provides integration, localisation, traffic data processing, traffic condition detection and data access services. Edges can be represented by RSUs equipped with processing units and EC servers. Vehicles are assumed to directly communicate with nearby network edges for service provision and data

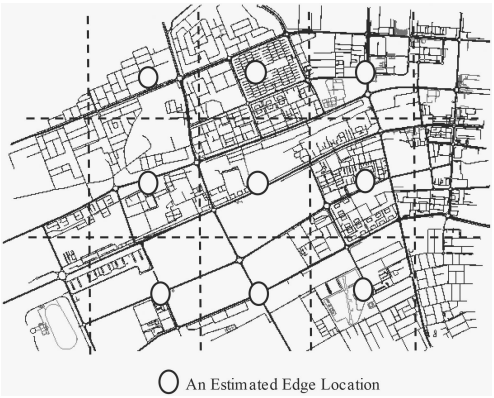

Fig. 3 *Al Ain city map with estimated edge locations*

collection. For enhanced privacy, vehicular data are consumed locally and anonymously without the need for cloud storage. High computational power and storage capabilities are provided by the cloud server layer, which is accessed by edges on an on-demand basis.

3.3 Evaluation scenario

To demonstrate the advantages of employing an edge-based TM architecture, trust data dissemination is selected as a representative smart city scenario. Specifically, the performance of two existing protocols is evaluated in a simulation-based environment. In general, data dissemination in vehicular environments aims to support real-time interactions for improving traffic safety and convenience. It is expected that the edges can improve global data coverage, decrease the total dissemination overhead, and minimise the dissemination delay. This is due to improved connectivity and the potential of using traffic condition information in controlling multi-hop broadcast. Traffic condition detection with the proposed architecture is characterised by its high accuracy owing to the global or semi-global network knowledge that is offered by edges. In contrast, the VANET environment can provide only an estimated traffic condition for individual vehicles based on local data, which is sometimes misleading owing to rapid changes in the urban environment.

Two representative protocols from the literature are considered for performance comparison. Each protocol is simulated in the VANET environment and then in an edge-based architecture for comprehensive analysis. Performance metrics include data delivery ratio, dissemination overhead, and dissemination delay. The first protocol is the enhanced slotted 1-persistance (ES1P), which is an enhanced version of the well-known slotted 1-persistance method [36]. The enhancement is achieved by integrating a broadcast control mechanism to accommodate urban vehicular environment. ES1P-EC enhances the performance of ES1P using edges. The second protocol is TURBO, which is a representative example of recent VANET protocols [37]. Similarly, TURBO-EC enhances the performance of TURBO using an EC architecture.

The implementation is carried out in the OMNET++ [38] simulation environment. Traffic flows are generated using the SUMO [39] traffic simulator. The Veins [40] framework, which models vehicular communication, was extended to integrate network edges. Specifically, a set of edges, which are assumed to collect traffic data, were included. At the end of a predefined time cycle, each edge estimates the traffic conditions within its coverage. These conditions are used to control data dissemination in the vehicular network. The Al Ain city map was selected for an urban road network representation. Fig. 3 shows the Al Ain map with estimated edge locations, which generate and disseminate safety messages to nearby vehicles. Receiving vehicles continue data dissemination in a multi-hop manner via VANET. To set the physical and the MAC layer, the implementation of IEEE 802.11p available in Veins was employed. Four traffic flow generation rates were used to represent different traffic scenarios, ranging from low to high density.

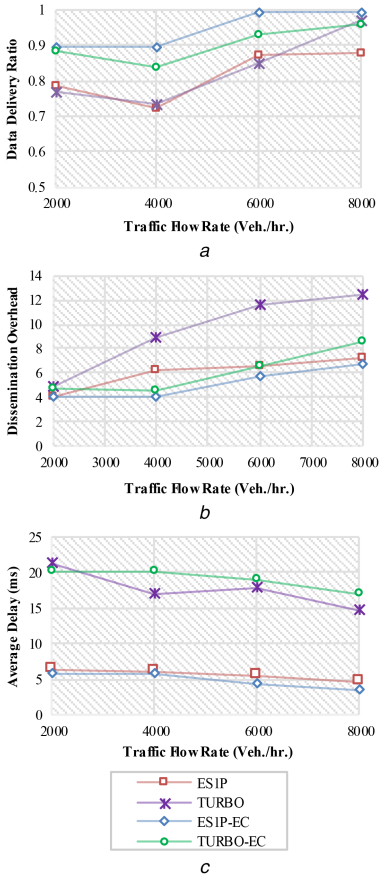

Fig. 4 *Performance evaluation of trust data dissemination in a smart city environment*

(a) Data delivery ratio, ***(b)*** Dissemination overhead, ***(c)*** Average dissemination delay

The simulation results are shown in Fig. 4, where it can be seen that under EC architecture, both protocols exhibit significant improvement in terms of data delivery. In terms of dissemination overhead, a noticeable improvement by 40% is observed in TURBO-EC compared to the original version of TURBO (Fig. 4*b*). This is due to the role of the edge in initiating the data dissemination process on behalf of individual vehicles. Thus, vehicles do not receive redundant data at the first hop where data is excessively disseminated.

Fig. 4*c* shows the average dissemination delay values under different flow rates. Both protocols present average delay values in the EC environment that are very close to those in VANET. Therefore, it can be concluded that an EC architecture would not negatively affect the minimised dissemination delays of VANETs, but could significantly reduce existing dissemination delays of cloud-based infrastructures, as expected.

4 Trust evaluation models for vehicular networks

Trust evaluation in vehicular networks aims at enabling trust between entities. Based on an estimated trust value, a trust relationship can be established between two vehicles. This value can be computed based on direct communication experience and/or collected recommendations. In this section, existing trust evaluation schemes for vehicular environments are reviewed and discussed. They are classified into direct, indirect and hybrid trust models.

4.1 Direct trust model

In this model, the TM system relies on direct communication to compute the trustworthiness of vehicles and/or messages. Existing schemes that follow the direct trust model can be classified into ‘entity-oriented’ and ‘data-oriented’ schemes. In the following, examples for each scheme are reviewed and discussed.

4.1.1 Entity-oriented trust: This scheme enables updating the trustworthiness of individual vehicles dynamically based on one or more attributes. According to [41], if a node B provides reliable advice for node A, then A increases the trust value of B as follows:

$$T_A(B) \leftarrow \begin{cases} T_A(B) + \alpha(1 - T_A(B)) & \text{if } T_A(B) \geq 0 \\ T_A(B) + \alpha(1 + T_A(B)) & \text{if } T_A(B) < 0 \end{cases} \quad (1)$$

otherwise, the trust value of B is decreased as follows:

$$T_A(B) \leftarrow \begin{cases} T_A(B) + \beta(1 - T_A(B)) & \text{if } T_A(B) \geq 0 \\ T_A(B) + \beta(1 + T_A(B)) & \text{if } T_A(B) < 0 \end{cases} \quad (2)$$

where α is a positive increment factor that ranges from 0 to 1, and β is a negative decrement factor that ranges from −1 to 0.

In another example [42], when a trustor receives a message from a potential trustee, the current trust value $\mathrm{TR}_{\mathrm{cur}}$ is calculated as

$$\mathrm{ST}_n^{\mathrm{T}} = \gamma \times \mathrm{ST}_{\mathrm{cur}} + (1 - \gamma) \times \mathrm{ST}_{n-1}^{\mathrm{T}}, \quad \mathrm{ST}_0^{\mathrm{T}} = 0.5 \quad (3)$$

where $\mathrm{TR}_{\mathrm{cur}} = \mathrm{ST}_n^{\mathrm{T}}$. The satisfaction level ST is defined using the number of successful operations N_{suc} and the number of failed operations N_{fail} during multiple packet delivery as follows:

$$\mathrm{ST} = \frac{N_{\mathrm{suc}} + 1}{N_{\mathrm{fail}} + N_{\mathrm{suc}} + 2'} \quad (4)$$

A direct trust evaluation strategy that is inspired by the job market signalling model is proposed in [43], where the sender transmits a signal with its message to ensure the truthfulness of that message for the receiving vehicles. To use the signal, the sender is charged, and the cost depends on the value of the signal and its own behaviour. The signalling cost is negatively correlated with the productivity of the signaller, i.e. the bad behaviour of the signaller implies high cost. Because the signalling cost is low for highly productive entities, a high signal value is used. Furthermore, less productive entities are prevented from cheating by establishing a high signalling cost for them.

In general, an entity-oriented trust evaluation in vehicular networks occurs when vehicles receive messages. These messages can hold data about traffic events (such as safety or congestion conditions), or trust data to recommend to other potential trustees. In both cases, vehicles evaluate data senders based primarily on the data included in the received messages. Other behavioural attributes may contribute to the trust evaluation process, often with smaller weighting factors. As data is the basic factor for entity-oriented evaluation in vehicular networks, some of the existing models follow the data-oriented scheme for direct trust evaluation. Examples are given in the next section.

4.1.2 Data-oriented trust: Unlike the entity-oriented scheme, that data-oriented scheme enables individual vehicles to evaluate the trustworthiness of the received messages themselves, without evaluating the senders. In [44], a data-oriented trust model called RMCV is proposed. RMCV uses the following attributes: content similarity support Support(c), maximum distance of the content between two messages in the same cluster, number of messages, content conflict con_c, path similarity and number of messages in the cluster. The trust value of content c is calculated as

$$\mathrm{Trust}(c) = \frac{\left(e^{\xi} e^{\xi con_c}\right)\mathrm{Support}(c)}{e^{\xi} - 1} \quad (5)$$

where ξ is a positive number used to adjust the importance of conflicting values.

Another set of attributes are used for direct data-oriented trust computation in [45], namely, confidence, location closeness, time closeness, location verification and a total number of sending vehicles.

In general, all direct trust schemes in vehicular networks (including entity-oriented and data-oriented schemes) rely on the communication experience for trust evaluation. Even though shared data is thereby validated, it is neither efficient nor feasible to solely rely on the evaluation of the data and neglect the evaluation of its source. Thus, data-oriented trust schemes should be supported by an entity-based evaluation.

Owing to the high mobility in vehicular networks, a certain vehicle may not have the chance to communicate with another certain vehicle again. Therefore, the benefit of direct experience may be limited, particularly when vehicles are sparsely connected. As collaborative approaches form the core of V2V communication, trust evaluation can significantly benefit from the experience of nearby vehicles to recommend a newly connected entity. This recommendation-based evaluation is often referred to as indirect trust evaluation. In the following, the existing indirect approaches for trust evaluation in vehicular networks are discussed.

4.2 Indirect trust models

Trust can be recommended and observed from third parties. Indirect trust uses recommendations from multi-hop vehicles across referral groups. Indirect trust follows a transitive path based on the trust metric, experience and cluster. Using indirect trust modelling, a vehicle can create a trust relationship between faraway nodes and evaluate messages using various recommendations.

Roadside aided trust evaluation is a robust indirect trust model [46] that relies on observation and feedback factors. Upon the detection of an event, a vehicle generates an observation factor, which reflects the recently reported frequency of the evidence along with the confidence of the observer on that evidence as well as the weight corresponding to the reporter's identity. The model uses the following attributes: observation factor, distance from the vehicle to the event, the maximum range of the event, number of sensors in the vehicle and feedback factor. An RSU collects data from the reporting vehicles and calculates trust values.

Similarity plays a significant role in making trust decisions from different recommendations. The commonly used similarity values are computed based on location, time and historical trust values from different recommendations. An example framework can be found in [47], where a receiver i can compute the trust value $C_{i,j}$ for node j from different recommendations as follows:

$$C_{ij} = \frac{\sum k = 1, \ldots, n, \quad K \neq i\left(W_{i,k}^{u} \times R_{i,k} \times R_{k,j}\right)}{\sum k = 1, \ldots, n, \quad K \neq i\left(W_{i,k}^{u} \times R_{i,k}\right)} \quad (6)$$

where k denotes the neighbouring nodes, n denotes the number of recommenders, and R_i represents the reputation evaluations of node k given by node i. Further, R_k is the value of the direct experience of node j given by node k and W represents a similarity weight.

Modern trust evaluation approaches tend to combine both direct and models for increased efficiency and controlled uncertainty. These models are known as *Hybrid Trust Models*, and are reviewed below.

4.3 Hybrid trust models

In these models, both direct experiences and indirect recommendations are considered in the computation of the trustworthiness of individual vehicles. In [48], the trust value is computed based on three types of messages generated in the system: sender messages, trust opinions and aggregated messages. The sender message *SM* is characterised by event, confidence, time and location. Trust opinion messages are provided by nearby vehicles based on their experiences in a particular event. The opinion factor is represented by two parameters: confidence and reaction. Confidence C is the level of trust and takes values in the interval [0, 1], whereas reaction is represented by $r \in \{trust, trust\}$. An aggregate message is computed from the combination of the correlated sender message and trust opinion messages from n direct peers. Assuming that A is a message to be sent, s is the original

sender peer, p is the opinion of '*trust*' and p' is the opinion of '*-trust*', then the aggregate trustworthiness of A is computed as

$$T_A = \frac{C_S + \sum_{i \in p} C_i - \sum_{i \in p'} C_i}{1 + |P| + |P'|} \tag{7}$$

where C_S denotes the sender confidence and C_i is the trust opinion given by peer i. If $T_A = 1$, the message obtains full trust, but when $T_A = -1$, the message obtains full distrust.

In addition to the neighbourhood recommendations, a hybrid trust evaluation scheme called TRIP also uses infrastructural recommendations [49]. In TRIP, a vehicle V_i computes the trust value of V_j as follows:

$$\mathrm{REP}_{ij}^{t} = \mathrm{REP}_{ij}^{t-1} + \beta_i + \sum_{k=1}^{n^t} \omega^k \mathrm{REP}_{kj} + \mathrm{REP}_{\mathrm{RSU}j} \tag{8}$$

where REP_{ij}^{t-1} represents the reputation score given by node V_i to node V_j at time t, REC_{kj} represents the indirect recommendation of node V_k about node V_j and $\mathrm{REC}_{\mathrm{RSU}j}$ is the score provided by the RSU about node V_j.

In high-density networks, cluster-based strategies can improve networking performance in terms of redundancy overhead because messages are mainly disseminated via cluster heads once clusters have been formed. An example is provided in [50], where vehicles are grouped into multiple clusters, and a trust opinion on a certain message is exchanged between the cluster nodes. Such an opinion is computed as

$$T_A = \frac{C_S + \sum_{i \in p} C_i - \sum_{i \in p'} C_i}{1 + P + P'} \tag{9}$$

where C_S represents the sender's confidence, C_i denotes the trust opinion of node i, P denotes the number of peers of a 'trust' opinion and P' denotes the number of peers with 'distrust' opinion. Because the TM system is potentially subject to malicious vehicles that may provide untrustworthy opinions, the authors in [51] proposed an iterative filtering algorithm to exclude these opinions.

In general, cluster-based approaches may lead to additional networking delays during the formation process. Also, even though they can effectively reduce the redundancy overhead, they pose a communication overhead during cluster-head and member selection. In the recent study [52], the authors introduced a timer to reduce the control traffic during this process by eliminating the cluster-head competition among nodes. Instead of a static trust function, they proposed an adaptive function to assess the data trust among vehicles according to the reported event severity requirement. Another recent clustering approach for vehicular networks can be found in [53].

Beacons may also be used in trust models, as proposed in [50, 54, 55], where trust is computed from cross-checking the plausibility of event messages and beacon messages. In [50], multiple attributes are used in trust computation, namely, similarity, location, direction, velocity, distance and delay.

In addition to direct experience and indirect recommendations, trust score computation can use a global reputation value, as proposed in [56, 57]. In [56], trust scores determine trustworthy vehicles (which are classified as white vehicles), and selfish vehicles (which are classified as grey vehicles). The trust score (i, j) at time t_{k+1} is computed by

$$\mathrm{TS}_{ij}^{t_{k+1}} = \alpha_i \cdot \mathrm{GREP}_i^{tk} + \beta_i \cdot ltru_{ij}^{t_{k+1}} + \gamma_i \cdot \sum_{i \in B} \omega_l \cdot ltru_{ij}^{t_{k+1}} \tag{10}$$

where GREP is the global reputation value of node j obtained from the neighbourhood, *ltru* is the direct previous experience of vehicle i about j, ω_l is the normalised recommendation value from the nearby vehicles $l \varepsilon \mathscr{B}$, and $\alpha_i = \mathrm{e}^{-(tk+1-tk)}$ and β_i, γ_i are substitute values satisfying $\alpha_i + \beta_i + \gamma_i = 1$.

Recent hybrid models use existing architectures for better computational and storage resource utilisation in vehicular networks. Examples can be found in [58, 59]. In [58], unmanned vehicles were used to facilitate trust-aware crowd sensing, which handles trip requirements and security challenges. In another example [59], the authors used a cloud-based infrastructure for trust evaluation, and proposed and evaluated a trust algorithm in the context of their infrastructural framework.

4.4 Discussion

In Table 2, the surveyed trust models are compared in terms of modelling scheme, detection approach and limitations (including computation complexity, scalability, communication overhead and delay). As the table shows, recent trust models proposed in the context of vehicular networks tend to be hybrid. In general, entity-oriented trust models are behaviour-aware, whereas data-oriented models tend to detect intrusions by filtering messages based on the trustworthiness of their contents.

Most trust models suffer from communication delay and/or overhead. Additional communication delays may cause serious problems in time-critical safety applications, where vehicles should immediately respond to events such as accidents. Even though some models are not evaluated in terms of delay, a conclusion on their delay performance can be drawn from their communication scheme.

For example, the direct trust model proposed in [41] follows the request–reply model, which is often used in delay-tolerant applications. These applications may include travel convenience services such as congestion detection or travel-time estimation. However, safety-related data are time-critical in most cases where additional delays cannot be tolerated. According to [41], a receiving vehicle should send a trust request and wait for a reply to be received before deciding to take appropriate action. Such a communication delay may easily result in more complex safety conditions, and therefore it is not acceptable. A similar concept of trust can be found in the hybrid model proposed in [48].

The overhead limitation in trust evaluation is mainly caused by computation complexity or the use of beacons [50, 54, 55]. Beacons with a fixed period affect networking performance by wasting bandwidth and increasing congestion. For example, when vehicles send a beacon of size 200 bytes every 100 ms, the channel would be 80% loaded at a range of 300 m [61].

In general, any of the previously mentioned limitations may result in poor scalability. In vehicular networks, scalability often refers to performance sustainability under different levels of traffic density, including data delivery ratio, communication overhead and delay. Several of the reviewed models suffer from scalability issues owing to poor performance under high-density scenarios in terms of overhead and/or delay. In some scalable models, other issues arise owing to computational complexity. For example, the model proposed in [48] is claimed to be scalable owing to cluster-based data propagation. Nevertheless, the computation complexity of cluster formation may not be practical under safety conditions.

5 Trust propagation, aggregation and decision making

In the previous section, existing models for computing trust scores were discussed for evaluating the trustworthiness of individual vehicles. In TM systems designed for vehicular environments, trust scores are often propagated across the network to provide recommendations on making trust and/or driving decisions. In this section, trust data propagation, aggregation and decision making are discussed in the context of vehicular environments.

5.1 Trust propagation

Similarity metrics can play a significant role in trust data propagation. In [56], the similarity is computed based on the maximum speed and vehicle brand as follows:

$$\Gamma(X, Y) = \frac{\sum_{i=1}^{m} \Phi(\tau_x(\alpha_i))_i, \quad \tau y(\alpha_i)}{m} \tag{11}$$

where m denotes the total number of similarity attributes, α_i is the ith attribute of a particular node and Φ denotes the similarity degree between the ith attribute of vehicles X and Y. If vehicle X decides to propagate data to vehicle Z via Y, the trust values of all intermediate downstream nodes are also verified by the similarity metric.

A beacon-based propagation scheme is proposed in [55], where message propagation is validated based on the majority opinions. A message is propagated only if it is trusted by the majority of participating vehicles. Vehicles are clustered, and a leader is selected for each individual cluster. When a message is to be propagated, the trustworthiness of the message is computed by the cluster head using the opinions of the participating cluster peers. Assuming that p is the set of peers that trust the message, and p' is the set of peers that do not trust it, the cluster head computes the majority opinion as follows:

$$W_{trust} = \sum_{I \in P} C_i T_i, \quad W_{\neg trust} = \sum_{I \in P'} C_i T_i \tag{12}$$

where T_i is the threshold set by cluster head and $C_i \in [0, 1]$ represents the confidence value given by peer i. From this opinion, the trustworthiness of a message is computed as

$$\frac{W_{trust}}{W_{trust} + W_{\neg trust}} > 1 - \in \tag{13}$$

A forwarding decision is made only when the computed trust score is greater than $(1 - \varepsilon)$, where ε is the maximum allowed error rate. The decision-making process considers the following real-time factors: the maximum propagation distance, the longest time to live, the distance between the vehicle's location and the event location, and the time duration of trust score computations.

5.2 Trust aggregation

Trust aggregation is used to evaluate the quality of the data shared among different peers in the network. It combines different trust opinions and/or recommendations from different sources in a single trust value. This value can be used to draw a trust conclusion on entities and/or data, thus supporting decision making. Various approaches have been adopted for meaningful data aggregation in TM systems designed for vehicular environments.

Cluster-based trust aggregation is presented in [48]. In this scheme, an aggregated message (A) is computed by combining a sender message M and a list of trust opinions O from direct peers. Initially, the nodes are geographically grouped into n clusters C_i, …, C_n and a cluster leader is randomly selected for each cluster. When message propagation is initiated, the cluster leader C_i performs aggregation to reduce the number of exchanged messages. The obtained message A is then shared with the next-hop cluster leaders $C_{2, \ldots, 1}$. Upon receiving the aggregated message, each cluster leader computes a newly aggregated message A' from its own observations and share it with the next-hop cluster leaders.

Another aggregation model is presented in [62] and implements a data fusion technique based on fuzzy logic to combine the consolidated trust values in a single aggregated value. The computed trust is mapped to one of the following levels: low, medium and high. In addition to fuzzy logic and data fusion techniques, trust aggregation may employ signature algorithms. Examples can be found in [63, 64].

In [63], a trust aggregation scheme employing multiple signatures over a group of vehicles is proposed. When an event occurs, each informed vehicle constructs a message with a time stamp and a signature, and then broadcasts it to its neighbours. Existing vehicles may receive several messages from different sources about the same event. To reduce data redundancy, the signatures of these messages are aggregated into a single signature before propagation. An extended scheme exhibits improved signature redundancy performance by using an identity-based signature aggregation algorithm [64].

5.3 Decision making

In a smart city environment, the physical world can be monitored in real time to provide intelligent control systems that make appropriate decisions according to different types of events and actions. In a recent study [65], various smart city applications were proposed considering miscellaneous security and privacy challenges. A representative application is traffic management, where decisions are made in real time to reduce traffic congestion. In [66], traffic congestion in smart cities is studied by using the Internet of Things and *ad-hoc* networks. In another recent study [67], the authors proposed traffic lights management using a vehicular priority estimation and route discovery method. Because data collection is an essential component in smart city applications, the development of data collection and dissemination methods has attracted considerable attention. These methods should carefully make decisions on what data to accept or ignore. In [68], an

Table 2 Comparison of trust evaluation models for vehicular networks

Ref.	Year	Trust model			Detection scheme				Limitations			
		Direct		Indirect	Hybrid	Behaviour-aware	Intrusion-aware	Delay	Overhead	Complexity	Scalability	
		Entity-oriented	Data-oriented									
[46]	2011			√			√	√				
[41]	2011	√				√		√			√	
[49]	2012				√	√					√	
[55]	2012				√	√			√		√	
[54]	2013				√	√			√		√	
[47]	2013			√		√	√	√		√	√	
[43]	2013	√				√				√		
[44]	2013		√				√	√		√		
[45]	2013		√			√		√		√		
[48]	2013				√	√		√		√		
[57]	2013				√	√			√		√	
[56]	2015				√	√			√		√	
[42]	2015	√				√		√				
[60]	2016				√		√		√		√	
[59]	2017				√	√		√		√		
[52]	2018				√	√		√	√		√	
[58]	2018				√	√			√		√	

optimised data collection scheme is proposed to effectively collect data with opportunistic communication.

In TM systems, decision making consists in determining 'whom' or 'what' to trust based on a trust evaluation process. Traditionally, trust is established among entities based on a sequence of interactions in a long-term relationship [69]. Thereby, each entity determines whom to trust in advance, so that it can directly accept the data generated by those trusted entities, or determine the optimal partner to cooperate with [70, 71]. In a vehicular environment, the inherent high mobility makes it challenging to establish trust relationships among the entities themselves in a fully distributed manner. The situation does not significantly change when connectivity improves under high-density circumstances because prior knowledge about nearby vehicles cannot be ensured. Upon the retrieval of time-critical safety data, vehicles should make immediate trust decisions on these data, so that they can determine appropriate actions without additional delays.

In [69], the authors proposed a data-oriented trust framework that, in addition to the number and the type of data statements, considered dynamic factors of the environment such as location and time to derive trust relationships. These relationships are derived from multiple pieces of evidence that are weighted based on well-established rules and metrics. Each piece of data along with its corresponding weight serve as inputs to a decision-making component that outputs the level of trust on data and reported events. Data reports are evaluated using Dempster–Shafer theory, and trust relationships are re-established frequently according to environmental changes.

The author in [47] relies on the evaluation of both the trustworthiness of received messages and the reputation of senders to make decisions on the trustworthiness of event messages in vehicular environments. A reputation evaluation algorithm is employed for evaluating the reputation of a communicating vehicle based on similarity theory. The similarities are received from different recommenders, and are used as weights for reputation computation. Trust and reputation are updated based on the validation of message content. Trusted messages are rebroadcasted, whereas untrusted messages are discarded.

An event-based trust system is proposed in [72] to determine whether a traffic event exists or not, and how long it lasts in the former case. To validate the trustworthiness of a message, the decision-making process computes the reputation and the confidence of the event data carried by the message by comparing it with a benchmark value. As in [47], a traffic event will be broadcasted by an involved vehicle only if it has accumulated sufficient reputation credit. Thereby, false warning messages can be successfully filtered out for improved road safety and convenience.

In [45], the decision-making process totally ignores the identity of the vehicles by assuming an identity-anonymous environment. The trustworthiness of a message is computed from the confidence and trust values. Initially, the confidence value is evaluated from the location of the sender and the sending time, whereas the trust value is computed from the recommendations and the confidence. Eventually, the decision-making process employs a two-step filtering method to determine a trusted message. In the first step, only high-value messages are selected and forwarded to the second step, in which messages are considered as trusted only if the computed trust value is greater than a minimum threshold.

6 Current research directions

Information security is a highly important issue in vehicular environments that is still under investigation [73]. It aims at protecting data confidentiality and integrity, as well as ensuring its availability. In this section, the current directions for enabling trust in vehicular networks are highlighted.

6.1 Trust enforcement in future vehicular networks

Existing TM solutions in the context of vehicular environments follow either the centralised cloud-based approach or the fully decentralised VANET approach [29], and each approach has its own drawbacks. As proposed in this study, the integration of the recent EC paradigm in vehicular networks can overcome the limitations of both approaches by providing low latency, high scalability and efficient data access services. As the necessary technologies exist, these characteristics would enable EC to be integrated into future smart cities. The essential role of TM in the context of EC would prompt further research in this direction, particularly when the architecture of EC is standardised.

6.2 Trustworthy vehicular social networks (VSNs)

A considerable number of individuals in crowded cities around the world drive every day between their homes and workplaces. In several cases, the same people travel along the same route at the same time. This allows the formation of VSNs, which were first introduced in [74], and would enable the provision of TM solutions in the context of social networks. VSNs can be employed in fully decentralised VANETs, centralised cloud-based vehicular networks and controlled edge-based networks [75]. A related taxonomy can be found in [76], and recent proposals can be found in [77, 78].

In [79], a directed graph trust computing methodology in the context of social networks is proposed. Another directed trust graph is implemented in the context of the semantic web [80], where the relationships among vehicles are weighted for trust evaluation. In [81], a generalised framework for enabling trustworthy VSN in VANETs is discussed. New research opportunities exist in trustworthy VSNs, including construction protocols, trust information discrimination, direct and indirect trust computation and evaluation, and simulation platform proposal.

6.3 Smart attackers detection

In vehicular networks, vehicles are often assumed to behave cooperatively. However, the selfish behaviour of adversary vehicles is generally unavoidable. These vehicles may engage in various malicious activities affecting the overall network performance and safety. Moreover, they may attempt to evade detection. For effectively monitoring and controlling these security threats, an efficient TM system should identify the trustworthiness of individual vehicles and detect malicious drivers.

New trust models are required to detect smart attackers [12]. Game theory seems to provide promising approaches for enhancing intrusion detection with smaller resource utilisation and more balanced risk. A coalitional game approach with an incentive mechanism for vehicular networks is proposed in [82]. This approach is extended in [83] to adopt cooperative data dissemination. Another game theoretic approach for addressing security issues in vehicular environments is proposed in [84].

Moreover, the concept of trust in the literature of multi-agent systems effectively represents trust in human interactions [10]. The major benefit of integrating multi-agent modelling in vehicular networks is to enable individual vehicles to interact cooperatively in response to environmental changes without forcing them to follow a predefined policy. Accordingly, individual vehicles have the choice to cooperate based on their own perception of the trustworthiness of the others [85].

6.4 Handling uncertainty

In a vehicular environment, it cannot be ensured that two vehicles that have already communicated will further communicate [10]. Even though VSNs [74] can provide long-term relationships, it is not always possible to rely on the existence of a VSN. If vehicles collect recommendations from other vehicles, it is less likely to receive sufficient information on the trustworthiness of a certain vehicle in sparsely connected networks. Therefore, there is a certain level of uncertainty in deciding whom and what to trust.

Fuzzy logic has been widely used to enable trust in peer-to-peer systems. Examples can be found in [86, 87]. Moreover, heuristic evaluation techniques can reduce uncertainty in trust propagation and aggregation and thus improve driving decisions. A heuristic algorithm that predicts trust-based optimal paths for social networks is proposed in [88]. Another trust-aware resource management system based on a heuristic algorithm is proposed in

[89]. In conclusion, fuzzy logic systems and heuristic algorithms are promising for handling uncertainty in vehicular trust services.

7 Conclusion

TM in vehicular systems can be associated with rapidly evolving communication technologies. In this study, current challenges and opportunities for enabling trust in vehicular environments were comprehensibly explored. The focus was on potential architectures ranging from fully distributed VANETs to cloud-based and edge-enabled networks. Various modelling proposals for handling the components of TM were discussed, including evaluation, propagation, aggregation and decision making. Finally, current research directions were highlighted in this context.

8 Acknowledgment

This research was supported by the Roadway, Transportation, and Traffic Safety Research Center (RTTSRC) of the United Arab Emirates University (grant no. 31R116).

9 References

[1] Buhaug, H., Urdal, H.: 'An urbanization bomb? Population growth and social disorder in cities', *Glob. Environ. Change*, 2013, **23**, (1), pp. 1–10
[2] Small, K.: '*Urban transportation economics*', vol. **4**, (Taylor & Francis, Abingdon, 2013)
[3] Shepard, S., Jerram, L.: 'Transportation forecast: light duty vehicles, navigant research', 2014
[4] Vipin, J., Sharma, A., Subramanian, L.: 'Road traffic congestion in the developing world'. Proc. of the 2nd ACM Symp. on Computing for Development, 2012
[5] World Health Organization: 'Violence, injury prevention'. Global status report on road safety: supporting a decade of action', 2013
[6] Buchanan, C.: '*Traffic in towns: a study of the long term problems of traffic in urban areas*' (Routledge, Abingdon, 2015)
[7] Kai, Z., Batterman, S.: 'Air pollution and health risks due to vehicle traffic', *Sci. Total Environ.*, 2013, **450**, pp. 307–316
[8] Wolch, J.R., Byrne, J., Newell, J.P.: 'Urban green space, public health, and environmental justice: the challenge of making cities 'just green enough', *Landsc. Urban Plann.*, 2014, **125**, pp. 234–244
[9] Zhang, S., Wu, Y., Liu, H., *et al.*: 'Real-world fuel consumption and CO_2 (carbon dioxide) emissions by driving conditions for light-duty passenger vehicles in China', *Energy*, 2014, **69**, pp. 247–257
[10] Zhang, J.: 'A survey on trust management for VANETs'. 2011 IEEE Int. Conf. on Advanced Information Networking and Applications (AINA), 22 March 2011, pp. 105–112
[11] Soleymani, S.A., Abdullah, A.H., Hassan, W.H., *et al.*: 'Trust management in vehicular *ad hoc* network: a systematic review', *EURASIP J. Wirel. Commun. Netw.*, 2015, **1**, p. 146
[12] Kerrache, C.A., Calafate, C.T., Cano, J.C., *et al.*: 'Trust management for vehicular networks: an adversary-oriented overview', *IEEE Access*, 2016, **4**, pp. 9293–9307
[13] Uddin, M.G., Zulkernine, M., Ahamed, S.I.: 'CAT: a context-aware trust model for open and dynamic systems'. Proc. of the 2008 ACM Symp. on Applied Computing, 16 March 2008, pp. 2024–2029
[14] Zhou, M., Mei, H., Zhang, L.: 'A multi-property trust model for reconfiguring component software'. Fifth Int. Conf. on Quality Software, 2005, 19 September 2005, pp. 142–149
[15] Wu, J.J., Tsang, A.S.: 'Factors affecting members' trust belief and behaviour intention in virtual communities', *Behav. Inf. Technol.*, 2008, **27**, (2), pp. 115–125
[16] Luhmann, N.: '*Trust and power*' (John Wiley & Sons, Hoboken, 1979)
[17] Deutsch, M.: '*The resolution of conflict*' (Yale University Press, New Haven, 1973)
[18] Becker, L.C.: 'Trust as noncognitive security about motives', *Ethics*, 1996, **107**, (1), pp. 43–61
[19] Morgan, R., Hunt, S.: 'The commitment-trust theory of relationship marketing', *J. Mark.*, 1994, **58**, (3), pp. 20–38
[20] Grandison, T., Morris, S.: 'A survey of trust in internet applications', *IEEE Commun. Surv. Tutor.*, 2000, **3**, (4), p. 216
[21] Bhoi, S.K., Khilar, P.M.: 'Vehicular communication: a survey', *IET Netw.*, 2014, **3**, (3), pp. 204–217
[22] Harri, J., Filali, F., Bonnet, C.: 'Mobility models for vehicular *ad hoc* networks: a survey and taxonomy', *IEEE Commun. Surv. Tutor.*, 2009, **11**, (4), pp. 19–41
[23] Karagiannis, G., Altintas, O., Ekici, E., *et al.*: 'Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions', *IEEE Commun. Surv. Tutor.*, 2011, **13**, (4), pp. 584–616
[24] Zeadally, S., Hunt, R., Chen, Y.S., *et al.*: 'Vehicular *ad hoc* networks (VANETS): status, results, and challenges', *Telecommun. Syst.*, 2012, **50**, (4), pp. 217–241
[25] Lu, N., Cheng, N., Zhang, N., *et al.*: 'Connected vehicles: solutions and challenges', *IEEE Internet Things J.*, 2014, **1**, (4), pp. 289–299
[26] Anwer, M.S., Guy, C.: 'A survey of VANET technologies', *J. Emerg. Trends Comput. Inf. Sci.*, 2014, **5**, pp. 661–671
[27] Whaiduzzaman, M., Sookhak, M., Gani, A., *et al.*: 'A survey on vehicular cloud computing', *J. Netw. Comput. Appl.*, 2014, **40**, pp. 325–344
[28] Gerla, M.: 'Vehicular cloud computing'. 2012 Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Ayia Napa, Cyprus, 2012, pp. 152–155
[29] Ahmed, A., Ahmed, E.: 'A survey on mobile edge computing'. 2016 10th Int. Conf. Intelligent Systems and Control (ISCO), Coimbatore, India, 2016, pp. 1–8
[30] Roman, R., Lopez, J., Mambo, M.: 'Mobile edge computing, fog *et al.*: a survey and analysis of security threats and challenges', *Future Gener. Comput. Syst.*, 2018, **78**, pp. 680–698
[31] Liu, J., Wan, J., Jia, D., *et al.*: 'High-efficiency urban traffic management in context-aware computing and 5G communication', *IEEE Commun. Mag.*, 2017, **55**, (1), pp. 34–40
[32] Salahuddin, M.A., Al-Fuqaha, A., Guizani, M.: 'Software-defined networking for RSU clouds in support of the internet of vehicles', *IEEE Internet Things J.*, 2015, **2**, (2), pp. 133–144
[33] Truong, N.B., Lee, G.M., Ghamri-Doudane, Y.: 'Software defined networking-based vehicular *ad hoc* network with fog computing'. 2015 IFIP/IEEE, Int. Symp. Integrated Network Management (IM), 2015, pp. 1202–1207
[34] Heidari, E., Gladisch, A., Moshiri, B., *et al.*: 'Survey on location information services for vehicular communication networks', *Wirel. Netw.*, 2014, **20**, (5), pp. 1085–1105
[35] Uichin, L., Gerla, M.: 'A survey of urban vehicular sensing platforms', *Comput. Netw.*, 2010, **54**, (4), pp. 527–544
[36] Wisitpongphan, N., Tonguz, O.K., Parikh, J.S., *et al.*: 'Broadcast storm mitigation techniques in vehicular *ad hoc* networks', *IEEE Wirel. Commun.*, 2007, **14**, (6), pp. 84–94
[37] Akabane, A.T., Villas, L.A., Madeira, E.R.M.: 'An adaptive solution for data dissemination under diverse road traffic conditions in urban scenarios'. 2015 IEEE Wireless Communications and Networking Conf. (WCNC), Shanghai, China, 2015, pp. 1654–1659
[38] Varga, A.: 'The OMNeT++ discrete event simulation system'. Proc. of the European Simulation Multiconference (ESM'2001), 2001, vol. 9, no. S 185, p. 65
[39] Behrisch, M., Bieker, L., Erdmann, J., *et al.*: 'SUMO–simulation of urban mobility: an overview'. Third Int. Conf. on Advances in System Simulation (SIMUL 2011), Barcelona, Spain, 2011, pp. 55–60
[40] Sommer, C., German, R., Dressler, F.: 'Bidirectionally coupled network and road traffic simulation for improved IVC analysis', *IEEE Trans. Mob. Comput.*, 2011, **10**, (1), pp. 3–15
[41] Minhas, U.F., Zhang, J., Tran, T., *et al.*: 'A multifaceted approach to modeling node trust for effective communication in the application of mobile *ad hoc* vehicular networks', *IEEE Trans. Syst. Man Cybern.*, 2011, **41**, (3), pp. 407–420
[42] Rostamzadeh, K., Nicanfar, H., Torabi, N., *et al.*: 'A context-aware trust-based information dissemination framework for vehicular networks', *IEEE Internet Things J.*, 2015, **2**, (2), pp. 121–132
[43] Haddadou, N., Rachedi, A.: 'DTM^2: adapting job market signaling for distributed trust management in vehicular *ad hoc* networks'. IEEE Int. Conf. on Communications, Budapest, Hungary, 2013, pp. 1827–1832
[44] Gurung, S., Lin, D., Squicciarini, A., *et al.*: '*Information-oriented trustworthiness evaluation in vehicular ad-hoc networks*' (Springer, Berlin, 2013), pp. 94–108
[45] Shaikh, R.A., Alzahrani, A.S.: 'Intrusion-aware trust model for vehicular ad-hoc networks', *Secur. Commun. Netw.*, 2013, **9**, (8), pp. 5989–6007
[46] Wu, A., Ma, J., Zhang, S.: 'RATE: a RSU-aided scheme for data-centric trust establishment in VANETs'. IEEE in Wireless Communications, Networking and Mobile Computing (WiCOM), Wuhan, China, 2011, pp. 1–6
[47] Yang, N.: 'A similarity based trust and reputation management framework for VANETs', *Int. J. Fut. Gener. Commun. Netw.*, 2013, **6**, (2), pp. 25–34
[48] Zhang, J., Chen, C., Cohen, R.: 'Trust modeling for message relay control and local action decision making in VANETs', *Secur. Commun. Netw.*, 2013, **6**, (1), pp. 1–14
[49] Mármol, F.G., Pérez, G.M.: 'TRIP, a trust and reputation infrastructure-based proposal for vehicular *ad hoc* networks', *J. Netw. Comput. Appl.*, 2012, **35**, (3), pp. 934–941
[50] Chen, C., Zhang, J., Cohen, R.: 'A trust modeling framework for message propagation and evaluation in VANETs'. IEEE Information Technology Convergence and Services (ITCS), Cebu, Philippines, 2010, pp. 1–8
[51] Hu, H., Lu, R., Zhang, Z., *et al.*: 'REPLACE: a reliable trust-based platoon service recommendation scheme in VANET', *IEEE Trans. Veh. Technol.*, 2017, **66**, (2), pp. 1786–1797
[52] Oubabas, S., Aoudjit, R., Rodrigues, J.J., *et al.*: 'Secure and stable vehicular *ad hoc* network clustering algorithm based on hybrid mobility similarities and trust management scheme', *Veh. Commun.*, 2018, **13**, pp. 128–138
[53] Wang, J., Wang, Y., Gu, X., *et al.*: 'Clusterrep: a cluster-based reputation framework for balancing privacy and trust in vehicular participatory sensing', *Int. J. Distrib. Sens. Netw.*, 2018, **14**, (9), p. 1550147718803299
[54] Chen, Y.M., Wei, Y.C.: 'A beacon-based trust management system for enhancing user centric location privacy in VANETs', *J. Commun. Netw.*, 2013, **15**, (2), pp. 153–163
[55] Wei, Y.C., Chen, Y.M.: 'An efficient trust management system for balancing the safety and location privacy in VANETs'. 2012 IEEE 11th Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, 25 June 2012, pp. 393–400
[56] Hu, H., Lu, R., Zhang, Z.: 'VTrust: a robust trust framework for relay selection in hybrid vehicular communications'. IEEE Global Communications Conf., San Diego, USA, 2015, pp. 1–6

[57] Saraswat, D., Chaurasia, B.J.: 'AHP based trust model in VANETs'. 2013 5th Int. Conf. Computational Intelligence and Communication Networks (CICN), Mathura, India, 2013, pp. 391–393

[58] Barka, E., Kerrache, C.A., Lagraa, N., *et al.*: 'Behavior-aware UAV-assisted crowd sensing technique for urban vehicular environments'. 2018 15th IEEE Annual Consumer Communications & Networking Conf. (CCNC), Las Vegas, USA, 2018, pp. 1–7

[59] Chen, X., Wang, L.: 'A cloud-based trust management framework for vehicular social networks', *IEEE Access*, 2017, **5**, pp. 2967–2980

[60] Kerrache, C.A., Calafate, C.T., Lagraa, N., *et al.*: 'RITA: risk-aware trust-based architecture for collaborative multi-hop vehicular communications', *Secur. Commun. Netw.*, 2016, **9**, (17), pp. 4428–4442

[61] Yousefi, S., Fathy, M.: 'Metrics for performance evaluation of safety applications In vehicular *ad hoc* networks', *Transport*, 2018, **23**, (4), pp. 291–298

[62] Dietzel, S., Schoch, E., Konings, B.: 'Resilient secure aggregation for vehicular networks', *IEEE Netw.*, 2010, **24**, (1), pp. 26–31

[63] Viejo, A., Sebé, F., Domingo-Ferrer, J.: 'Aggregation of trustworthy announcement messages in vehicular *ad hoc* networks'. IEEE in Vehicular Technology Conf., Barcelona, Spain, 2009, pp. 1–5

[64] Chen, C., Zhang, J., Cohen, R.: 'Secure and efficient trust opinion aggregation for vehicular ad-hoc networks'. IEEE in Vehicular Technology Conf. Fall (VTC 2010-Fall), Ottawa, Canada, 2010, pp. 1–5

[65] Zhang, K., Ni, J., Yang, K., *et al.*: 'Security and privacy in smart city applications: challenges and solutions', *IEEE Commun. Mag.*, 2017, **55**, (1), pp. 122–129

[66] Sharif, A., Li, J.P., Saleem, M.A.: 'Internet of things enabled vehicular and *ad hoc* networks for smart city traffic monitoring and controlling: a review', *Int. J. Adv. Netw. Appl.*, 2018, **10**, (3), pp. 3833–3842

[67] Ilyas, M., Zokarkar, V.: 'Optimizing city traffic light management for improving traffic system in smart cities', *Int. J. Comput. Appl.*, 2016, **133**, (14), pp. 23–28

[68] Xu, Y., Chen, X., Liu, A., *et al.*: 'A latency and coverage optimized data collection scheme for smart cities based on vehicular ad-hoc networks', *Sensors*, 2017, **17**, (4), p. 888

[69] Raya, M., Papadimitratos, P., Gligor, V. D., *et al.*: 'On data-centric trust establishment in ephemeral *ad hoc* networks'. IEEE, INFOCOM Conf. on Computer Communications, Phoenix, USA, 2008, pp. 1912–1920

[70] Samek, J., Malačka, O., Zbořil, F.: 'Decision making and partner selection based on trust in multi-context environment'. Int. Conf. on Intelligent Systems Design and Applications, Girona, Spain, 2014, pp. 19–24

[71] Burnett, C., Norman, T.J., Sycara, K.: 'Supporting trust assessment and decision making in coalitions', *IEEE Intell. Syst.*, 2014, **29**, (4), pp. 8–24

[72] Lo, N.W., Tsai, H.C.: 'A reputation system for traffic safety event on vehicular *ad hoc* networks, EURASIP', *J. Wirel. Commun. Netw.*, 2009, **2009**, pp. 1–9

[73] Lu, Z., Qu, G., Liu, Z.: 'A survey on recent advances in vehicular network security, trust, and privacy', *IEEE Trans. Intell. Transp. Syst.*, 2018, **20**, (2), pp. 760–776

[74] Smaldone, S., Han, L., Shankar, P., *et al.*: 'Roadspeak: enabling voice chat on roadways using vehicular social networks'. Proc. of the 1st ACM Workshop on Social Network Systems, Glasgow, UK, 2008, pp. 43–48

[75] Zheng, K., Zheng, Q., Chatzimisios, P., *et al.*: 'Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions', *IEEE Commun. Surv. Tutor.*, 2015, **17**, (4), pp. 2377–2396

[76] Mezghani, F., Dhaou, R., Nogueira, M., *et al.*: 'Content dissemination in vehicular social networks: taxonomy and user satisfaction', *IEEE Commun. Mag.*, 2014, **52**, (12), pp. 34–40

[77] Hossain, M., Hasan, R., Zawoad, S.: 'Trust-IoV: a trustworthy forensic investigation framework for the internet of vehicles (IoV)'. IEEE Int. Congress on Internet of Things (ICIOT), Honolulu, Hawaii, USA, 2017, pp. 25–32

[78] Gai, F., Zhang, J., Zhu, P., *et al.*: 'Trust on the ratee: a trust management system for social internet of vehicles', *Wirel. Commun. Mob. Comput.*, 2017, **2017**, pp. 1–10

[79] Golbeck, J.A.: 'Computing and applying trust in web-based social networks', 2005

[80] Ziegler, C.N., Lausen, G: 'Spreading activation models for trust propagation'. IEEE Int. Conf. on e-Technology, eCommerce, 2004, pp. 83–97

[81] Yang, Q., Wang, H.: 'Toward trustworthy vehicular social networks', *IEEE Commun. Mag.*, 2015, **53**, (8), pp. 42–47

[82] Chen, T., Wu, L., Wu, F., *et al.*: 'Stimulating cooperation in vehicular *ad hoc* networks: a coalitional game theoretic approach', *IEEE Trans. Veh. Technol.*, 2011, **60**, (2), pp. 566–579

[83] Li, Y., Ying, K., Cheng, P., *et al.*: 'Cooperative data dissemination in cellular-VANET heterogeneous wireless networks'. IEEE in High Speed Intelligent Communication Forum (HSIC), Nanjing, China, 2012, pp. 1–4

[84] Prabhakar, M., Singh, J.N., Mahadevan, G.: 'Nash equilibrium and Markov chains to enhance game theoretic approach for VANET security'. Proc. of Int. Conf. on Advances in Computing, Bengaluru, India, 2013, pp. 191–199

[85] Seymour, R., Peterson, G.L.: 'A trust-based multiagent system'. Int. IEEE Conf. Computational Science and Engineering. CSE'09, 2009, vol. 3, pp. 109–116

[86] Song, S., Hwang, K., Zhou, R., *et al.*: 'Trusted P2P transactions with fuzzy reputation aggregation', *IEEE Internet Comput.*, 2005, **9**, (6), pp. 24–34

[87] Griffiths, N., Chao, K.M., Younas, M.: 'Fuzzy trust for peer-to-peer systems'. 26th IEEE Int. Conf. on Distributed Computing Systems Workshops, Lisbon, Portugal, 2006, pp. 73–73

[88] Liu, G., Wang, Y., Orgun, M.A., *et al.*: 'A heuristic algorithm for trust-oriented service provider selection in complex social networks'. IEEE Int. Conf. on Services Computing (SCC), Miami, USA, 2010, pp. 130–137

[89] Azzedin, F., Maheswaran, M.: 'Towards trust-aware resource management in grid computing systems'. IEEE Cluster Computing and the Grid, Miami, USA, 2002, pp. 452–452