IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 1, 2016, accepted December 20, 2016, date of publication December 26, 2016,
date of current version January 27, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2645452

Trust Management for Vehicular Networks: An Adversary-Oriented Overview

CHAKER ABDELAZIZ KERRACHE[1], CARLOS T. CALAFATE[2], JUAN-CARLOS CANO[2], NASREDDINE LAGRAA[1], AND PIETRO MANZONI[2], (Member, IEEE)
[1]Informatics and Mathematics Laboratory, University of Laghouat, BP 37G, route de Ghardaia, Laghouat, Algeria
[2]Department of Computer Engineering, Polytechnic University of Valencia, Camino de Vera, S/N, Valencia, Spain

Corresponding author: C. A. Kerrache (a.kerrache@mail.lagh-univ.dz)

This work was supported by the Ministerio de Economía y Competitividad, Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad, Proyectos I+D+I 2014, Spain, under Grant TEC2014-52690-R.

ABSTRACT Cooperative Intelligent Transportation Systems, mainly represented by vehicular ad hoc networks (VANETs), are among the key components contributing to the Smart City and Smart World paradigms. Based on the continuous exchange of both periodic and event triggered messages, smart vehicles can enhance road safety, while also providing support for comfort applications. In addition to the different communication protocols, securing such communications and establishing a certain trustiness among vehicles are among the main challenges to address, since the presence of dishonest peers can lead to unwanted situations. To this end, existing security solutions are typically divided into two main categories, cryptography and trust, where trust appeared as a complement to cryptography on some specific adversary models and environments where the latter was not enough to mitigate all possible attacks. In this paper, we provide an adversary-oriented survey of the existing trust models for VANETs. We also show when trust is preferable to cryptography, and the opposite. In addition, we show how trust models are usually evaluated in VANET contexts, and finally, we point out some critical scenarios that existing trust models cannot handle, together with some possible solutions.

INDEX TERMS VANETs, trust management, attacker models.

I. INTRODUCTION

Ensuring secure and trusted communications within Vehicular Ad hoc NETworks (VANETs) is a complex task due to the different threats to be addressed [1], where the most dangerous ones are those targeting safety alert services.

Tremendous efforts have been made by researchers at both academia and industry to provide security solutions for all kinds of networks including VANETs. Most of the existing security solutions for VANETs inherit cryptography efficiency in terms of secure and confidential communication, and they use different software and hardware components to reach their goals such as certificates [2], signatures [3], Public Key Infrastructures (PKIs) [4], intrusion detection systems [5], and trusted third parties [6].

On the other hand, in some critical cases like high mobility scenarios in the absence of infrastructures, cryptography solutions cannot perform as well as expected. In addition, if an authorized and authenticated user becomes malicious, or is under the control of an attacker, classical cryptography solutions are easily overtaken. Hence, to fill the gap of cryptography against inside attackers, trust management is usually adopted. Trust models were inspired by economic science [7], [8], and can be used for different networks and applications. Trust can be defined as a subjective belief of a peer about other peers belonging to the same society or geographical zone [9].

For the VANET case, trust establishment is based on the evaluation of direct historical interactions, as well as on the indirect recommendations among vehicles that are gathered. Thus, trust evaluation is mostly based on the recent history regarding data exchanges, and it does not have any negative impact on message treatment and transmission delays.

Existing trust models for VANETs are generally classified into entity-oriented, data-oriented, and hybrid trust models depending of the revocation target, which can be either dishonest entities, malicious messages, or both of them [10].

As mentioned above, in the scope of VANETs, trust mostly addresses inside attackers as cryptography has already showed its efficiency in handling outside unauthorized attack attempts. In other words, trust mainly deals with inside attackers in those situations where cryptography completely fails, also contributing to enhance cryptography in case of delay-sensitive infrastructureless environments, which is the case of VANETs.

In this paper we clearly point out when and where trust is a better choice than, or a complement of cryptography, and the opposite. We also explain the main features, differences, advantages and drawbacks of both trust and cryptography. In addition, an adversary-oriented survey of the existing trust establishment solutions is also provided. We show some specific attacks trying to bypass both cryptography and trust solutions, and how the latter can be enhanced to detect such threats. Finally, we show how the existing trust models for VANETs are usually evaluated.

The rest of this paper is organized as follows: in section II we acknowledge the exiting survey papers addressing either cryptography or trust management solutions for VANETs. In section III we point out the main security requirements and countermeasures for a secure vehicular network. Section IV details the features and differences between trust and cryptography, together with a survey of the existing trust models for VANETs. Then, in section V, we provide a performance evaluation-oriented study of existing trust models. Later, learned lessons and future directions for trust management in VANETs are discussed in section VI, which also highlights those security threats able to bypass the existing trust models, along with possible solutions to mitigate those threats. Finally, section VII concludes the paper.

II. RELATED WORKS

Differently from existing surveys, where works are classified based on the revocation target (entities, data, and both), in this work we also emphasize the studied adversary models, in addition to clarifying the main differences between trust-based and cryptography-based solutions, highlighting the advantages and drawbacks of the proposed solutions in each category, and defining a security model able to combine both strategies.

In the literature we can find several surveys on this topic [11]–[14], although most of them solely tackle cryptography-based solutions when dealing with the different VANET threats.

However, most of the exiting works focus on the security aspects without taking VANET application requirements into account in terms of cooperation level among vehicles and delay sensitivity issues.

The work in [15] offers a summary about state-of-the-art solutions for VANETs, in addition to VANETs' security challenges and associated cryptographic solutions. Works [16], [17] are the newest surveys in this category. Karn and Gupta [17] refer only a few VANET threats, and focus mainly on the Sybil attack and its probable solutions, whereas [16] focuses on techniques and technologies used to secure vehicular networks in a general way, but without actually describing any kind of adversary model.

On the other hand, only a few surveys [10], [18], [19] deal with trust management for VANETs. In [10] and [18] authors adopt the same classical categorization depending on the revocation target as follows: entity-oriented, data-oriented, and hybrid trust models. Moreover, while showing the main steps for building a good trust system, both works handle trust management in a separated manner, without acknowledging where and when it is better to use trust instead of cryptography, and the opposite. Instead, [19] provides a systematic and quantitative review about how many papers addressing these topics exist, along with information about their keywords and publishers.

Differently from existing surveys, in this work we provide the reader with an adversary-oriented survey of the trust-based solutions for VANETs, detailing when and where trust is a better choice than cryptography for enhancing VANET security. We also show the studied adversary models, and discuss the limits of trust-based solutions. At the end, we point out those threats able to bypass both cryptography and trust, together with some possible solutions to these threats. An evaluation of methods regarding the existing trust-based solutions is also provided.

III. VANET SECURITY REQUIREMENTS AND THREATS

Same as all kinds of networks, VANET security requirements are divided into five main axes in addition to the privacy concerns: availability, authenticity, confidentiality, integrity, and non-repudiation [20]. However, in VANET environments, attacks addressing availability are the most dangerous since they directly affect safety-critical situations. In the following sections we describe the different VANET security requirements, and we then classify the main existing threats.

A. VANET SECURITY REQUIREMENTS

Securing vehicular communications is a complex issue, with plenty of challenges to be addressed which can be grouped in six different requirements.

1) *Availability:* it is the most important factor to account for in VANETs since it is directly related to all safety applications. Maintaining the network's functionality is an availability issue, and so a security framework should ensure the presence of the required information or service, as well as the communications bandwidth, at any time. Hence, the most dangerous attacks taking place in VANETs address availability more than any other security aspect. Both trust-based and cryptography-based approaches allow securing the network in the presence of an infrastructure, although trust-based approaches are better options for fully distributed scenarios.
2) *Authenticity:* it is also among the major security aspects to account for. It includes identification, authentication, and access control. By adopting security certificates and signatures, it represents the first line of defense against any external danger. Vehicle authenticity can be achieved by using cryptographic solutions alone.

3) *Confidentiality:* Through the use of certificates and the shared public keys all exchanged messages can be encrypted and, hence, all peer-to-peer communications can become confidential (illegible) for all intermediate vehicles. However, in a VANET context, safety messages and neighboring discovery messages (beacons) should remain clear and readable by all receiving vehicles. Also notice that confidentiality is ensured through cryptographic solutions, but not by trust-based solutions.
4) *Integrity:* Data integrity and trustiness is about ensuring that messages have not been modifiedor reduced by an intermediate node. Achieving these requirements is a difficult task in any distributed system. In the specific case of VANETs, it can be ensured through the public key infrastructure and cryptography revocation mechanisms. However, for fully distributed cases, even trust management can be used when choosing the most trusted packet relay, thereby avoiding nodes trying to drop, modify, or inject new messages.
5) *Non-repudiation:* This service matches the vehicles' real identity with their actions. Hence, it can be used when a certain node tries to deny that it was sending specific messages. Signatures are the main technique used to avoid this kind of attack. Hence, only cryptography approaches can satisfy this particular requirement.
6) *Privacy:* Vehicle privacy is an important issue in VANETs, as it includes both position and identity privacy. Pseudonym changing techniques are the main solution adopted to provide this security service.

To satisfy all the aforementioned requirements, cryptography and trust have been combined together in many approaches [21]–[23]. In fact, they are also used together in secure key distribution contexts [24], [25] and privacy-preserving communications [26], [27].

B. VANET THREATS

Same as any open network using a shared medium, VANETs suffer from a variety of vulnerabilities. In fact, the damage associated to some security attacks can withhold the different applications from performing correctly. Even if the target is a specific service, for sure other related services will be affected as well. Since VANET applications can be classified into safety, security, and infotainment, below we provide an application-oriented classification of the main VANET threats. In particular, this classification shows in which kind of applications the impact of each type of attack is high. Anyway, we should keep in mind that every attack has a negative impact on all kinds of applications, and not only in one of them. Figure 1 summarizes the main existing threats, and which applications are affected the most according to the three categories defined below:

- Attacks addressing secure communications,
- Attacks addressing safety applications,
- Attacks addressing infotainment applications,

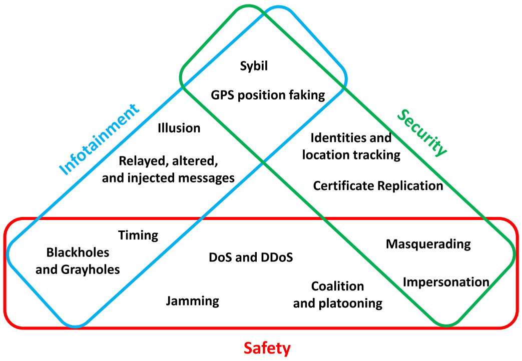


FIGURE 1. **Application-oriented VANET security threats.**

1) ATTACKS ADDRESSING SECURE COMMUNICATIONS

Achieving secure and confidential communications is a main concern on all networks, also including safety and infotainment. Thus, VANET security suffers from many threats including, but not limited to, the certificate replication attack, the eavesdropping attack, and identity/location privacy attacks.

- *Certificate Replication Attack:* In this attack a dishonest node uses a certain number of replicated certificates at the same time to avoid being traced/tracked by the authorities, or by other vehicles. Dishonest vehicles can also behave smartly by discarding any detected certificate to avoid being black-listed or identified using this detected certificate (see Figure 2 (J)).
- *Eavesdropping Attack:* Recently known as APT for Advanced Persistent Threat [28], [29], eavesdropping attacks occur when a dishonest vehicle with a valid certificate behaves as a spy, therefore gathering all possible information. Notice that the impact of such a passive behaviour on the network is not instantaneous or very evident, but it can nevertheless be the cause of many attacks on privacy, confidentiality and cyber security [30], [31].
- *Attacks on Privacy:* Vehicles/Driver identities/location privacy should always be ensured. Various kinds of attacks can be launched against privacy-preserving systems, including both tracking systems and the advanced persistent threat described above. Similarly to eavesdropping attacks, the impact of attacks addressing privacy appear in a delayed manner, meaning that an attacker can use its target identity, location, or certificate to launch another attack without being detected.

2) ATTACKS THAT ENDANGER SAFETY APPLICATIONS

Safety applications are the main aim of cooperative ITS. Since all safety applications are based on multi-hop and delay-sensitive information exchange. Attacks belonging to this category are mostly related to the channel occupation.

- *Denial of Service Attacks:* This famous type of attack, known as DoS, occurs when a set of dishonest vehicles send a high rate of messages, effectively blocking all possible actions by the target. This attack can be

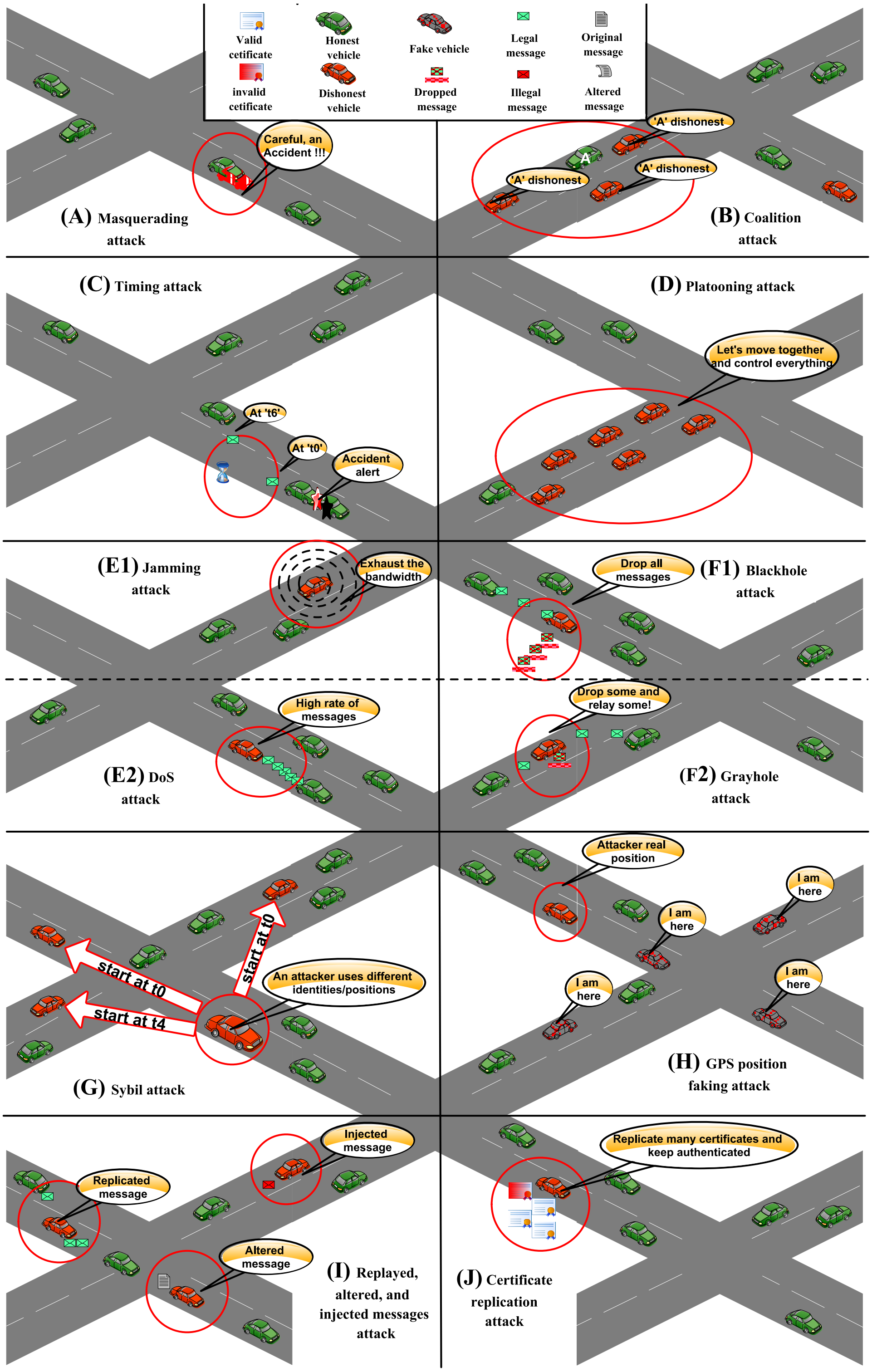


FIGURE 2. Main VANET security attacks.

launched in a distributed manner by many attackers simultaneously, hence becoming a distributed DoS (DDoS), which is similar to the coalition attack with a target/time synchronization [32](See Figure 2 (E2)).

- *Jamming Attack:* As shown in Figure 2 (E1), this attack is similar to the DoS attack, but now the target is the shared bandwidth. It occurs when a dishonest vehicle tries to hold channel access continuously through

different strategies including beacons, frequency changing, medium access backoff cheating, and alert injection. This is among the most dangerous attacks for safety applications since it avoids that valid safety alerts are disseminated.
- *Coalition and Platooning Attack:* This attack occurs when a group of dishonest vehicles situated in the same geographical area or moving together collaborate for malicious purposes such as excluding honest nodes from network operations, malicious bandwidth usage, or service consumption in the case of vehicular clouds. Figures 2 (B) and (D) illustrate these types of attacks.
- *Betrayal Attack:* Similar to the masquerading attack, the betrayal attack occurs when a honest vehicle suddenly turns into a malicious node, starting to send malicious messages or fake alerts.

3) ATTACKS ON INFOTAINMENT APPLICATIONS

Infotainment applications are all those related to passengers' comfort, and most of them are based on relay selection strategies for message exchanges. Bellow we list the most dangerous attacks on infotainment applications.

- *Replayed, Altered, and Injected Messages Attack:* As illustrated in Figure 2 (I), dishonest vehicles can replicate many copies of the same message, modify the message, or create and inject new messages in the system while acting as a relay node for inter-vehicular communication. These attacks can clearly reduce the performance of all network applications, as well as the exchanged data trustiness.
- *Illusion Attack:* This attack is mostly related to hardware components, and it occurs when an authenticated attacker implements some vulnerabilities at the sensing level. Hence, generated information is not valid.

4) COMMON ATTACKS AGAINST BOTH SECURE COMMUNICATIONS AND SAFETY APPLICATIONS

In addition to the aforementioned attacks, security and safety applications also share some common vulnerabilities including the following:

- *Masquerading Attack:* the adversary in this attack is a dishonest vehicle that uses a valid identity/certificate called mask to take advantage of network resources. Hence, it can perform maliciously without being detected (See Figure 2 (A)).
- *Impersonation Attack:* This attack occurs when a vehicle provides its valid identity to an attacker. This way, the latter can launch attacks able to bypass the authentication process.

5) COMMON ATTACKS AGAINST BOTH SECURE COMMUNICATIONS AND INFOTAINMENT APPLICATIONS

Some attacks have almost the same severity level on both security and infotainment applications; the main attacks in this category are the Sybil and the GPS position faking attacks.

- *Sybil Attack:* This attack is similar to the botnet attack where an attacker is able to manage a certain number of controlled/penetrated vehicles (real/virtual identities in real/virtual positions), and so it can launch attacks using these vehicles as shown in Figure 2 (G). Hence, the attackers can be either honest vehicles that lack security measures, or dishonest vehicles.
- *GPS Position Faking Attack:* The second attack in this category is illustrated in Figure 2 (H), and it occurs when an attacker broadcasts fake positioning information which can punish certain applications based on geographical routing, or even nodes located at that same falsified position.

6) COMMON ATTACKS AGAINST BOTH SAFETY AND INFOTAINMENT APPLICATIONS

Last but not least, some attacks are dangerous for both safety and infotainment applications. These attacks are mainly timing attacks, blackholes, and grayholes attacks.

- *Timing Attack:* the delay in the packet delivery process can be even more dangerous than actually dropping these packets. The principle of this attack is that the dishonest vehicles store the transmitted packets for a certain period of time before sending them again, which can cause plenty of problems to both safety and infotainment applications. This case is illustrated in Figure 2 (C).
- *Blackhole Attack:* Massive packet dropping is also among the known attacks. It consist of discarding absolutely all received packets, as illustrated in Figure 2 (F1).
- *Grayhole Attack:* Finally, the last attack, which is also known as selective forwarding, occurs when a dishonest vehicle randomly selects some packets to forward while dropping the others to avoid being detected. This principle is illustrated in Figure 2 (F2).

Besides the application-oriented classification, Table 1 shows what are the security services targeted by every attack. It also shows in which category these attacks are better handled by either trust or cryptography

C. DISTINGUISHING CRYPTOGRAPHY FROM TRUST

Trust management can be seen as an additional security level to address the shortcomings of classical cryptography solutions, being typically required against inside attackers in possession of valid certificates (see Figure 3).

From a security perspective, both trust and cryptography can be used against a group or a single attacker within the network. However, differently from trust-based solutions, cryptography cannot handle inside attackers. Both techniques can detect rational (the attacker uses a predefined strategy in order to reach a defined benefit, and the attack stops once the aim is reached) and irrational (a suicide bombing attack, for instance) attacks.

Notice that both techniques handle active attackers alone. Thus, passive attackers remain mostly undetected since they

TABLE 1. Security threats target and solutions category.

Type of attack	Targeted service	Trust-based solutions	Cryptography-based solutions
Certificate Replication attack	Authenticity	-	X
Eavesdropping attack	Confidentiality, Privacy	X	X
Tracking/Tracing attacks	Privacy	-	X
Denial of Service attack	Availability	X	X
Jamming attack	Availability	X	X
Coalition and platooning attack	Availability, Privacy	X	-
Betrayal attack	Authenticity, Availability, Integrity	X	-
Replayed, altered, and injected messages attack	Authenticity, Availability, Integrity	X	X
Illusion attack	Integrity	X	-
Masquerading attack	Authenticity	X	-
Impersonation attack	Authenticity, Non-repudiation	X	X
Sybil attack	Authenticity, Non-repudiation	X	X
GPS position faking attack	Availability, Non-repudiation	X	-
Timing attack	Availability	X	X
Blackhole attack	Availability	X	X
Grayhole attack	Availability	X	X

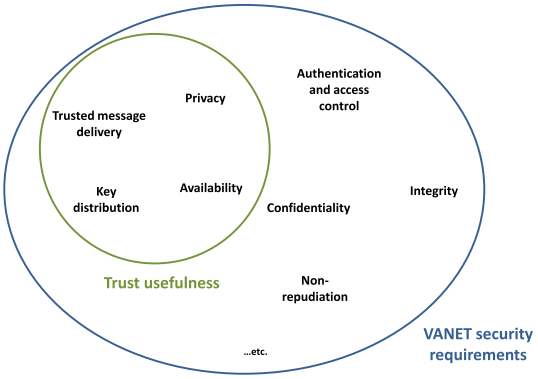


FIGURE 3. Inside and outside attackers in VANETs.

TABLE 2. Features of Trust-based and Cryptography-based solutions.

	Trust-based solutions	Cryptography-based solutions
Adversary model	Single and group	Single and group
	Insider	Insider and Outsider
	Rational and irrational	Rational and irrational
	Active	Active
Architecture	Distributed and semi-centralized	semi-centralized an centralized
Traffic	Delay sensitive and delay tolerant	Delay tolerant
Network topology	Stable and high dynamic	Stable or quasi stable
Accuracy	Medium	Accurate

do not perform any malicious action. Notice that the aim of such passive attacks is to gather as much information as possible in order to prepare for another more dangerous attack. Advanced-persistent-threat (APT) attacks are the main example of such passive, hard to detect, and dangerous behaviour [29], [33], [34]. In addition, it is worth highlighting that cryptography-based solutions have a higher detection accuracy compared to trust-based solutions.

From a network perspective, trust management solutions are mostly dedicated to distributed and semi-centralized computing since they can be effective independently of the exchanged traffic, and despite network mobility. On the contrary, cryptography-based solutions can achieve high performance levels, especially in the case of centralized computing and delay-tolerant traffic.

Table 2 summarizes the main differences between cryptography-based and trust-based solutions for improving VANET security.

Taking both cryptography and trust features into account, Figure 4 summarizes VANET security requirements together with trust management use cases. It shows that cryptography can be used for all authentication/authorization cases, confidential communication, and both non-repudiation and data integrity. Differently from it, trust is instead applicable to privacy preservation, availability, distributed key distribution, and message delivery.

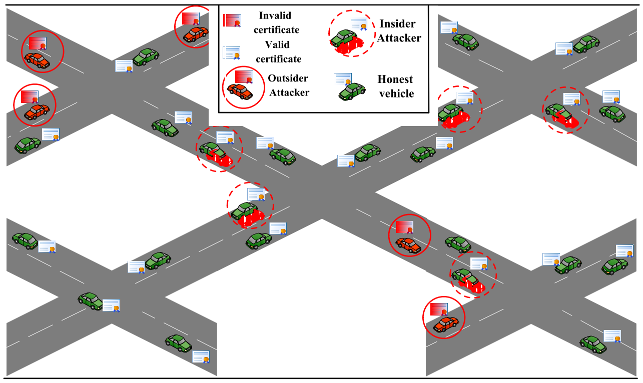


FIGURE 4. VANET security requirements and trust management use cases.

IV. TRUST MANAGEMENT FOR VANETs

Despite their many advantages, we find that all cryptography-based approaches are prone to introduce excessive delays in order to accomplish all the required checks since the computation power of an On Board Unit (OBU) is limited. Also, the verification of messages coming from unknown vehicles involves exchanging public certificates, which leads to a high message overhead. Notice that, even though we translate the verification tasks to a nearby RSU, the huge number of messages sent in a small time period does not allow reducing this delay, which becomes critical especially in safety-related scenarios [35]. Thus, most of the existing protocols focus on vehicle-to-infrastructure communication, and try to perform a quick batch verification of the exchanged messages [36]–[38].

Since in this work we focus solely on trust-based solutions, we refer the reader to the previous survey papers, including

TABLE 3. Main trust-based solutions.

	Topology				Purpose			Additional parameters			Revocation target		
	Organization		*Architecture (Use of RSU)*		*Privacy*	*Safety*	*Infotainment*	*Role of vehicles*	*Trusted third party*	*Message analysis*	*Dishonest entities*	*Malicious messages*	*Both*
	Flat	Clustered	Centralized	Distributed									
Golle et al. [46]	X				X		X					X	
Dotzer et al. [47]	X			X		X				X			X
Raya et al. [42]	X			X			X	X				X	
Gerlach [48]	X			X			X		X		X		
Tajeddine et al. [49]		X		X	X		X		X		X		
Ding et al. [41]		X		X			X					X	
Gazdar et al. [50]	X			X		X							X
Sahoo et al. [51]		X	X				X				X		
Zhang et al. [44]		X		X			X	X	X				X
Marmol et al. [52]	X		X									X	
Yang [40]	X		X			X		X	X			X	
Haddadou et al. [39]	X			X			X						X
Li et al. [53]				X			X		X				X
Chen and Wei [54]	X			X	X					X		X	
Gurung et al. [43]	X			X		X				X		X	
Kumar and Chilamkurti [45]	X			X			X						X
Shaikh and Alzahrani [55]	X			X		X							X
Kerrache et al. [56]	X			X		X	X	X		X			X
Sedjelmaci and Senouci [21]		X	X		X		X		X				X
Kerrache et al. [57]	X			X			X	X			X		
Jesudoss et al. [58]		X			X	X					X		
Khan et al. [59]		X	X		X		X	X			X		
Rostamzadeh et al. [60]	X			X		X	X		X	X			X
Haddadou et al. [61]	X			X			X			X			X
Kerrache et al. [62]	X		X	X		X	X	X	X	X			X

but not limited to [15] and [17], for a detailed description about cryptography-based solutions.

Trust management was mainly conceived to decide whether to believe or disbelieve information asserted by other peers. This belief should only take into account statements coming from trustworthy peers. Existing Trust-based solutions for VANETs are usually classified into entity-based [39]–[41], data-based [42], [43], and hybrid trust models, depending on the revocation target, which can be dishonest entities, malicious messages, or both of them [21], [44], [45].

Existing works have chosen different architectures; some of them are RSU-based, others are fully distributed, and yet others deal with privacy issues. Moreover, many works consider official vehicles (e.g. police cars, ambulances, etc.) as fully trustable, thus having a positive impact on securing communication among vehicles.

It is also worth pointing out that most works deal with all kinds of messages and applications, while only a few ones are specific to event-related and alert dissemination situations.

Table 3 summarizes the main existing works in chronological order:

Existing trust models can be classified according to the topology and vehicles organization strategy adopted as follows: (i) inter-cluster communication where a chosen vehicle makes the messages relay decision according to its cluster member opinions; (ii) flat communication where all vehicles behave autonomously; or (iii) when vehicles are within the range of an RSU, the latter plays the role of a sink handling all communications.

Overall, we find that most of the existing trust models focus on routing, path disruption, and resource exhaustion attacks, including blackholes and bogus messages' injection. In the following, we survey and classify the main existing works depending on their adversary models.

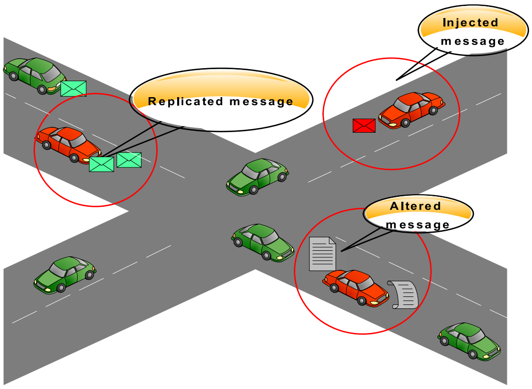


FIGURE 5. Replayed, altered, and injected messages attacks.

1) *Trust-based solutions against replayed, altered, and injected messages:* This kind of attacks, illustrated in Figure 5, can cause huge damage, especially in safety-related contexts. Hence, most of the existing works fall under this category.

The *entity-oriented trust models:* presented in [39] and [40] try to revoke nodes by sending falsified messages and fake information, respectively, using different techniques. Haddadou et al. [39] chose to associate a credit value to each neighbor vehicle. This credit will increase or decrease depending on the concerned neighbor's messages trustiness. Hence, this credit will be quickly decreased when replaying or injecting new messages. Concerning Yang's solution [40], it uses the Euclidean distance to compute the similarity between nodes in terms of reported events, deleting redundant or inadequate messages. Unfortunately, the first solution does not differentiate between direct and indirect trust, while the second one faces a huge problem in the case of simultaneous events.

The work in [47] represents a distributed reputation system called VARS. In this proposal, peers can generate opinions about a message based on the aggregated opinions of other nodes and the evaluation of direct interactions with the sender. In order to give more importance to the opinions coming from the closest nodes to the reported event, Dotzer et al. distinguish three areas: event, decision, and distribution. The main disadvantage of this scheme is the overhead added to messages by including the other trusted nodes' opinions. In addition, the case where a malicious node is the first to report about other nodes is not well investigated, as its opinion will affect all the opinions that follow.

The detection of attacks related to message quality is a process that is usually based on messages themselves, which explains why some of the existing works within this category are *Data-oriented trust models* [43], [46]. Golle et al. [46] have adapted a signature-based technique where every received message is compared to a typical model of legal VANET messages. The problem with this solution is that it is not feasible to actually build such a global model; in addition, all new legal messages will be dropped as well. Unlike [46], Gurung et al. [43] use three main metrics to classify received messages into either legal or malicious messages; these metrics are content similarity, content conflict, and routing path similarity. However, in addition to its high time complexity, this solution does not take into account the high level of mobility associated to VANETs, nor the case of node sparsity.

A distinguished reputation scheme for VANETs based on a fuzzy computational model is developed in [41]. In this work, nodes are classified regarding their closeness to the events as follows: event reporter (ER), event observer (EO) and event participant (EP). Moreover, using the messages' timestamp, they define six degrees of message honesty representing the combination of the three previous classes and the freshness of information. Nevertheless, this event-based scheme is very limited, and it cannot preserve a good message quality because, except for safety messages, the other kinds of messages are not related to a specific event.

Some *Hybrid trust models* have been also proposed in this same context. In particular, Zhang et al. [44] propose a semi-distributed trust framework for message propagation and evaluation; in their approach, the clusterheads are responsible for broadcasting and then gathering opinions about the broadcasted messages. Afterward, they decide either to drop untrustworthy messages or relay legal messages with the aggregated opinions to the next cluster in order to continue with the dissemination process. Similarly to other cluster-based techniques, the clusterhead election and the probability of malicious nodes becoming clusterheads are the main problems of this solution. Differently from the aforementioned work, Mármol and Pérez [52] prefer associating a confidence value to exchanged messages, in addition to the gathered recommendations from both RSU and nearby vehicles, to build three fuzzy sets (no trust, +/−trust, trust). The message will be dropped if it belongs to the first set, accepted but not forwarded for the second set's case, and both accepted and forwarded for the trusted messages set. The number of recommendations and their trustworthiness remain as the pending problems of this solution.

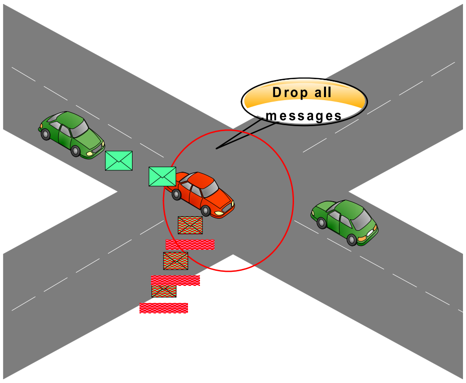


FIGURE 6. Blackhole attack.

2) *Trust-based solutions against blackholes:* Inter-vehicular communication is the enabling process supporting ITS over VANETs. Hence, forcing nodes to be collaborative is an indispensable task. Solutions falling under this category try to detect selfish nodes acting as blackholes (see Figure 6) in order to ensure a more efficient forwarding process for both safety and data messages.

The *Entity-oriented trust model* proposed by Khan et al. [59] proposes computing a distrust level for every neighbor acting as a blackhole through a watchdog technique. This distrust level will be sent to the clusterhead, and in turn delivered to a third trusted party that revokes the attacker certificate. Unfortunately, authors did not detail the different communication steps involved, nor the overhead associated to the cluster-based implementation. Our previous work, called *TROUVE* [57], differs from this one by taking advantage of existing CAM messages, which are periodically exchanged according to the ETSI-ITS European standard [63], in order to estimate the distribution of the selfish nodes within the network and, hence, select the most trusted path avoiding these blackholes. However, this solution only addresses unicast data traffic in urban environments.

To deal with blackholes and the selective forwarding (greyholes) procedure, some *Hybrid trust models* are also available [21], [61]. The first solution, proposed by Sedjelmaci et al., is a two-level intrusion detection system, the first one being based on a collaborative in-cluster detection, and the second one on a global detection processed by the RSU. The main weaknesses of this solution are the excessive time associated to clusterhead election, and the assumption of having stable clusters around fixed RSUs.

The work of Haddadou et al. [61], called DTM^2, proposes forcing nodes to be cooperative by establishing a communication cost. The latter is higher for selfish nodes, decreasing alongside with in-network collaborativity. How to choose the initial cost, and how to differentiate between selfish behavior and packet losses due to propagation issues, are the mains questionable points of this work.

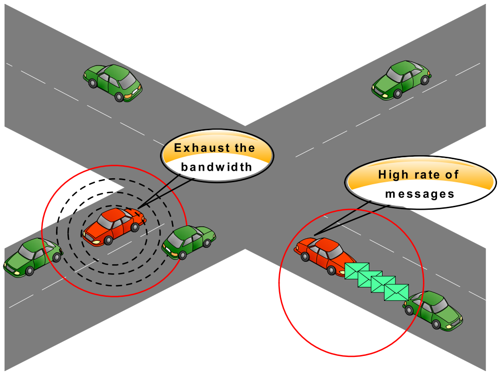


FIGURE 7. Jamming and denial of service (DoS) attacks.

3) *Trust-based solutions against jamming and denial of service (DoS) attacks:* Similarly to blackholes, jamming and DoS attacks can also prevent important information from being delivered on time, thereby disturbing VANET functionality (see Figure 7).

Raya et al. [42] propose a *Data-oriented trust model* for Ad-hoc ephemeral networks. This model uses different trust metrics, in addition to the *a priory* fixed entities trust (e.g. $Trust(Police\ vehicles = 1; ordinary\ vehicles = 0.5)$), in order to detect whether the reported events are real, or if it is just an attempt to jam bandwidth. They also propose evaluating the evidences related to the reported events using Dempster-Shafer theory and Bayesian inference. The problems of their solution are the fixed entities trust and the required training phase, which cannot be ensured in practice.

In a previous work [56], we proposed a hybrid trust model in order to enhance the message relaying procedure and to detect DoS attacks in a fast manner through the use of an intrusion detection module. The latter takes advantage of the access categories of 802.11p, in the context of dedicated short-range communications (DSRC), to classify the received messages at an early stage and, hence, accelerate the intrusion detection process. Same as all existing solutions, this approach assumes that the adversary has a malicious behaviour that remains stable throughout time, thus not being a valid solution under nodes having an intelligent dishonest behaviour.

In addition to the Denial of Service and message dropping attacks, our previous work also addressed the coalition and platooning attacks. Taking advantage of the standardized messaging services of ETSI ITS, our solution called T-VNets [62] could estimate the traffic as well as the attackers distribution within the network. By achieving high detection ratios and a low overhead, the T-VNets proposal is the only trust architecture that uses and acknowledges the standardization efforts.

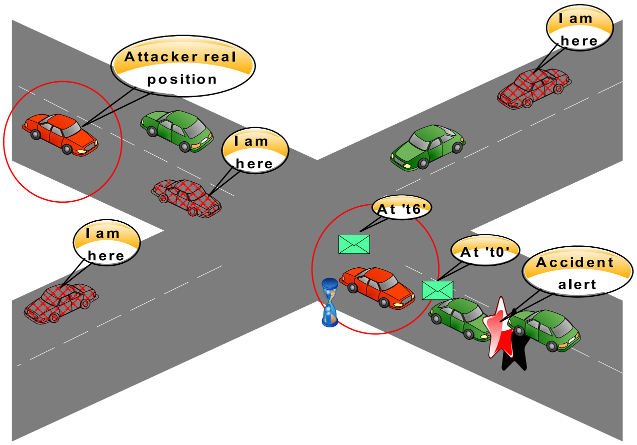


FIGURE 8. Fake location and timing attacks.

4) *Trust-based solutions against fake location and timing attacks:* Figure 8 illustrates the fake location and timing attacks.

The *Data-oriented trust model* proposed by Shaikh and Alzahrani [55] is an intrusion-aware trust model that differs from other works by being capable of detecting fake location and timing values generated either by the event's reporter or the message forwarder. In this event-related solution, authors propose the computation of a confidence value for each message coming from a unique source. In addition, for all messages describing a same event, a trust value is calculated using the previously computed confidence information. Finally, accepting or rejecting an event message depends on its trust value. Despite the high accuracy of this approach, we find that it introduces a high delay, which is not acceptable when targeting VANET safety applications.

5) *Trust-based solutions with unspecified adversarial model:* In addition to the aforementioned trust models, in some works authors do not specify an adversarial model, nor the types of attack they support. Instead, they only address trust establishment over the inter-vehicular communication link.

The only *Entity-oriented trust model* falling under this category was proposed by Jesudoss et al. [58]. In particular, authors propose a clustering technique to reduce the communication overhead and assign a reputation weight to all nodes participating in the clusterhead election and network control tasks by sharing their reports about exchanged traffic. Unfortunately, this scheme does not embrace reference trust metrics such as direct and indirect trust. Moreover, high mobility levels can cause this scheme's performance to decrease considerably.

Works [45], [53], [54], [60] are examples of *Hybrid trust approaches*.

Li et al. [53] propose a reputation-based trust establishment scheme for VANETs where the messages and their senders are evaluated based on the direct trust, indirect trust and node reputations. The main drawback of this scheme is its centralized trust computing procedure through the use of an additional infrastructure Called RMC (Reputation Management Center). This RMC is responsible for all revocation decisions.

Under the assumption that all application messages are encrypted, Chen et al. [54] propose a beacon-based trust model for enhancing users' location privacy in VANETs. The proposed system can secure the VANET while maintaining privacy by using two kinds of messages: beacons and event-based messages. The main idea is crosschecking the plausibility of these two types of messages to decide if other messages are trusted or not. Despite preserving the privacy of far-away vehicles (at more than one hop), this scheme cannot efficiently evaluate all kinds of messages, nor can it detect attacks occurring at upper layers (routing, application, etc.). In addition, whenever an obstacle appears between two neighboring vehicles, this scheme causes those two vehicles to judge each other as being a liar and malicious.

In [48] authors propose constructing a trust system based on node reputation to secure communications and preserve the location privacy of vehicles. In this solution, a belief-based trust is calculated using three metrics: the situational trust, the event-based trust, and the dispositional trust. However, there is no description of how different metrics are combined, neither the exchanged traffic and adversary model.

To ensure the privacy of nodes within dynamic groups, a trust model is proposed [49]. In this scheme, only the cluster-heads are in charge of exchanging information or disseminating it to group members. Despite being able to preserve privacy, this scheme has two main shortcomings: first, a security weakness is detected when the group leader is compromised or malicious nodes launch a distributed denial of service (DDoS) attack. Second, it is hard to see how groups can be formed based on heterogeneous entities because group formation is often related to the presence of vehicles in a specific geographical area. A model similar to [49] using ant colony routing is proposed in [51]. The clusters are formed around the RSUs, or around the slowest and most trusted vehicles. For each message sent by a node, the clusterhead gathers the members' opinions about that node and generates a decision about the message. The ant colony algorithm is used to choose the best path between different clusters using boundary nodes. The main weaknesses of this work are the use of a static clusterhead and the slow forwarding decision due to the opinion gathering process.

In another work [50], authors propose a trust model based on the formalization of the trust metrics' variation using a Markovian chain; this way, each vehicle has to evaluate and assign a trust weight to its neighbors based on the formalized model. Evidently, the decision process about the identities' honesty and the messages' validity is purely local, a process authors denote as 'monitoring process', meaning that each monitored vehicle will have its trust value increased, decreased, or unchanged in the monitoring registry. The main limitation of this model is the limited local knowledge of vehicles, which is easy to overcome through a betrayal behavior and different DOS attacks, especially due to the re-execution of the markovian process for each received message.

T-CLAIDS [45] is another work providing a trust-aware intrusion detection solution for VANETs. This solution takes into account the number of vehicles, their mobility, and their motion direction to perform an action. It also maintains a probability matrix of all actions which is updated in the iterations that follow until convergence to a particular value is achieved. This way, it offers an approximate representation of a global knowledge about the environment. Unfortunately, even if this solution shows good results in the general case where malicious behaviors are stable throughout time, it looks questionable in the case of unpredictable events or attacks. Also, convergence time may be very long in sparse cases since it will be hard to gather all the information required to have a global view.

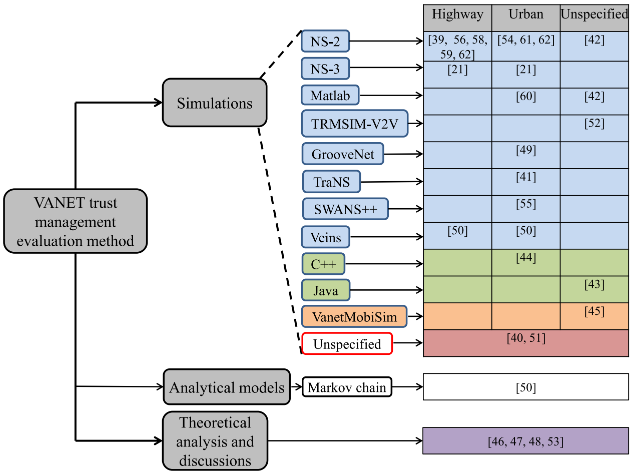
Last but not least, Rostamzadeh et al. [60] try to divide the map into different areas, and the traffic into three categories: safety, infotainment, and third party services, such as inter-transportation vehicular communication. In this solution, called "FACT," the message source should be known by piggybacking the identities of all vehicles participating in the routing process. Meanwhile, an admission module is responsible for analyzing the messages using the traffic category and the piggybacked identities' trust. If the degree of satisfaction is high, a trusted path is selected for the message. Unfortunately, this solution adds a considerable overhead and processing delay. Moreover, authors do not provide information about its security performance.

V. VANET TRUST MODELS' EVALUATION METHODS

The evaluation part of existing trust models for VANETs is mostly done through simulations. In particular, most of these proposals have used the NS-2 simulator [64]. Moreover, some proposals have adopted other existing simulation tools such as NS-3 [65], Matlab [66], TRMSIM-V2V [67], GrooveNet [68], TraNS [69], SWANS++ [70], and Veins [71]. In addition, in some works, authors have chosen to develop their own simulator instead of using the existing simulators relying on either C++ or Java programming languages.

It is worth pointing out that in [51] authors did not specify which tool they used, whereas the authors of [45] mention that they used VanetMobisim [72] as a simulator, when the latter is in fact a mobility trace generator. Hence, further details about how authors modified this tool to consider all simulation patterns should be provided.

Besides the simulation experiments, other works only offer a theoretical analysis and discussion of their proposals. We also noticed that only one work has used Markov chains as an analytical validation method.


VANET trust management evaluation method
Simulations
Analytical models
Markov chain
Theoretical analysis and discussions

	Highway	Urban	Unspecified
NS-2	[39, 56, 58, 59, 62]	[54, 61, 62]	[42]
NS-3	[21]	[21]	
Matlab		[60]	[42]
TRMSIM-V2V			[52]
GrooveNet		[49]	
TraNS		[41]	
SWANS++		[55]	
Veins	[50]	[50]	
C++		[44]	
Java			[43]
VanetMobiSim			[45]
Unspecified		[40, 51]	
Markov chain		[50]	
Theoretical analysis and discussions		[46, 47, 48, 53]	

FIGURE 9. Evaluation tools of existing trust models for VANETs.

Figure 9 summarizes the existing trust models evaluation methods together with the selected simulators and environments.

We should also mention that there is no real testbed implementation of any of the existing trust models. Hence, implementing and testing either existing or new proposals is highly recommended.

A drawback found in most of the available solutions is that they do not mention which propagation models are used for inter-vehicular communications. Thus, it does not matter which environment is simulated (highway, freeway, or urban) if we do not use realistic propagation and mobility models that take into account all relevant factors, including: signal attenuation, multi-path fading, obstacles, etc. The absence of such realistic models clearly affects any studied performance metrics.

Many works have studied and clarified the impact of the propagation models in inter-vehicular communication including [73], [74]. The obtained results show that the end-to-end delay and packet delivery ratio were clearly affected when varying the attenuation scheme with obstacles, and using a real map layout, compared to those when varying the attenuation scheme without obstacles and using a Manhattan layout. Both results also differ from those obtained when using the realistic attenuation scheme and varying the visibility/layout schemes.

Similarly to radio propagation models, mobility models have clearly a direct impact on network performance. For instance, the work in [75] highlighted the relevance of mobility patterns when aiming at realistic vehicular mobility for VANET simulations.

Table 4 summarizes the simulated solutions, together with the evaluated metrics and the used propagation and mobility models (if specified).

VI. OPEN RESEARCH ISSUES

Security is always considered as a continuously open research field. Moreover, when focusing on safety applications affecting human lives, as the case of VANETs, it becomes even more so, attracting both research and industry interests.

Because of the wide range of security threats seeking different network and security services, finding a single security scheme able to deal with all parameters of interest is a hard and quasi impossible task. Hence, towards this objective, we believe that all proposals should follow and enhance the major standards, projects and consortia including 3GPP/oneM2M/WAVE, 1609.2 [82], and ETSI ITS [83] security models.

Besides, handling both location and identities privacy, while ensuring efficient and reliable safety messages' dissemination, is one of the open issues of existing trust models. In addition, dealing with smart attackers is an issue that remains mostly untackled in terms of VANET trust models since all existing models assume that their adversary has a stable and continuous malicious behaviour, which facilitates the detection process.

As mentioned is section I, trust can be defined as the evaluation of the historical interactions among peers. The fact that trust is based on these historical interactions may affect its robustness and make it susceptible to some attacks, such as the On-Off and the Newcomer attacks. In these kinds of attacks, attackers behave smartly to avoid being detected. Hence, they either alternate between legal and illegal behaviours (i.e. Betrayal and tracking-based attacks), stopping all network activity until meeting new nodes that have no previous knowledge about their behaviour (i.e. On-Off and Newcomer attacks), control a certain number of nodes having lack of security measurements and launch attacks using their identities (i.e. Sybil attack), or keep within a coalition or a platoon of attackers, assuring this way that only positive recommendations about each other are disseminated (i.e. Bad-mouthing, coalition, and platooning attacks).

Figure 10 summarizes the main VANET threats, together with those attacks that most of the existing trust models cannot overcome.

Despite the rule that a good trust strategy is the one were trust is hard to get but can be easily lost, when an inside attacker becomes aware of the game rules, both cryptography

TABLE 4. Simulation tools and performance evaluation metrics.

Proposal	Simulator	Trust and security performance metrics	Network performance metrics	Additional remarks	
				Propagation model	*Mobility model*
Golle et al. [46]	-	-	-	-	-
Dotzer et al. [47]	-	-	-	-	-
Raya et al. [42]	Matlab [66] and NS-2 [64]	-Decision correctness (correct reports and false reports)		Unspecified	Unspecified
Gerlach [48]	-	-	-	-	-
Tajeddine et al. [49]	GrooveNet [68]	-Trust values variation		Unspecified	Sight Seeing Trip
Ding et al. [41]	TraNS [69]	-Reported event correctness -Fuzzy logic enhancements		Unspecified	Random Waypoint [76]
Gazdar et al. [50]	Veins [71]	-Trust values variation	-Average number of vehicle-to-vehicle interactions -Duration of vehicle-to-vehicle interactions	Unspecified	SUMO [77]
Sahoo et al. [51]	Unspecified		-Clusters creation time -Clusterheads selection time -Message delivery probability -Routing overhead	Unspecified	Unspecified
Zhang et al. [44]	C++	-Spam's propagation distance -Average number of undetected spams -Average number of wrong decisions	-Number of delivered messages -Overall delivery probability	Unspecified	Unspecified
Marmol et al. [52]	TRMSIM-V2V [67]	-Percentage of selection of trusted vehicles (autonomous attackers) -Percentage of selection of trusted vehicles (attackers in collusion)		Unspecified	Unspecified
Yang [40]	Unspecified	-Trust values variation		Unspecified	Unspecified
Haddadou et al. [39]	NS-2 [64]	-Attackers detection ratio -Corrupted data ratio	-Data delivery ratio	Unspecified	VanetMobisim [72]
Li et al. [53]	-	-	-	-	-
Chen and Wei [54]	NS-2 [64]	-Attackers detection ratio -Attackers detection with location privacy -Attackers detection delay		TwoRayGround	Random Trip [78]
Gurung et al. [43]	Java	-Trust values variation	-Processing time	Unspecified	Unspecified
Kumar and Chilamkurti [45]	VanetMobisim [72]	-Attackers detection ratio	-Processing time -Number of successfully delivered packets	Unspecified	VanetMobisim [72]
Shaikh and Alzahrani [55]	SWANS++ [70]	-Attackers detection accuracy -False positive rate		Free space	STreet RAndom Waypoint [79]
Kerrache et al. [56]	NS-2 [64]	-Attackers detection ratio -Attackers detection speed -False positive and false negative rates		TwoRayGround	IMPORTANT
Sedjelmaci and Senouci [21]	NS-3 [65]	-Attackers detection ratio -False positive rate -Detection time	-Communication overhead	Unspecified	SUMO [77]
Kerrache et al. [57]	NS-2 [64]	-Packet loss causes	-Packet delivery ratio -Average end-to-end delay	TwoRayGround	VanetMobisim [72]
Jesudoss et al. [58]	NS-2 [64]	-Trust values variation -Attackers detection probability -False negative rate	-Average number of hops for data delivery -Clusters stability	Unspecified	VanetMobisim [72]
Khan et al. [59]	NS-2 [64]		-Average throughput -Packet delivery ratio -End-to-end delay	Unspecified	Unspecified
Rostamzadeh et al. [60]	Matlab [66]		-Packet delivery delay -Average number of packet retransmissions -Packet delivery ratio	Rician fading with shadowing [80]	Real traffic traces
Haddadou et al. [61]	NS-2 [64]	-Attackers detection ratio and required delay -Detection of false positives -False Message Diffusion		Unspecified	VanetMobisim [72]
Kerrache et al. [62]	NS-2 [64]	-Attackers detection ratio -Generated false positives -Trust metrics impact on the detection process	-Average end-to-end delay -Packet delivery ratio -Communication overhead	RAV [74]	Krauss [81]

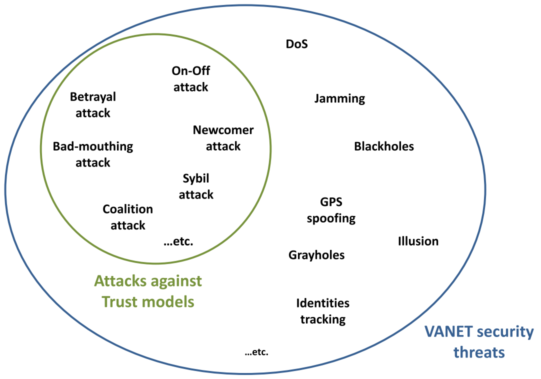


FIGURE 10. VANET security threats and attacks against trust management.

and trust are easily bypassed. Figure 11 shows an example of a smart attacker behaviour to avoid being detected.

Therefore, new trust models for VANETs should be able to cope with smart attackers. To this end, many techniques can be used such as the adaptive detection threshold and behaviour variation estimation. For instance, our recent work [84] is the first approach that attempts to address such smart dishonest behavior. In particular, it evaluates the vehicles' honesty instead of the whole experiments. Afterward, a risk metric representing the trust variation during the different time slots is obtained in order to detect smart attackers.

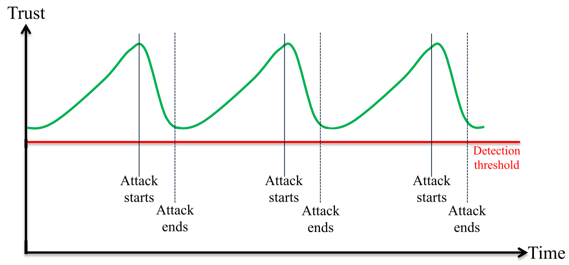


FIGURE 11. Intelligent dishonest behavior.

However, this solution requires a minimum number of interactions (minimum density) to run.

Also, the last trust evaluation can be used for the next re-keying/re-certification phases and, hence, smart attackers will be dismissed from all network operations directly after their initial attack attempt. Evaluating trust for separated time intervals can also help in detecting dishonest nodes attempting to avoid being detected.

More important than performing extensive simulations, there is a clear need to deploy real testbeds to assess the effectiveness of the different trust-based proposals in real scenarios. We also noticed that most existing solutions belong to the application layer, which means they are software-based and do not require specialized hardware or extra components. Thus, the use of smartphones seems like the easiest and less costly way to implement and test existing solutions.

In fact, different researchers have already developed some prototypes supporting vehicular communications using smartphones [85]–[87].

Among the main open issues for VANET security and trust is the human factor (i.e., the drivers' degree of honesty or selfishness). Since human honesty can clearly enhance both security and safety in VANETs, this information can be extracted from online social networks through trusted third parties, as the latter are usually the only authorities able to match the vehicle identity with the driver identity, and to gather the driver's Online Social Network (OSN) profile based on the identity. To our knowledge, there is no trust-based system for VANETs that has taken the human factor into account the way we are suggesting. Furthermore, the use of the social dimension for VANET purposes is already existing in comfort applications like user preference estimations [88]–[90] and leader selection [91].

Moreover, advanced persistent threats in the VANET context are also among the worthwhile research issues to take into account in trust management for VANETs.

Finally, there has been efforts for integrating Content Centric Network (CCN) and Named Data Networking (NDN) in VANETs [92], [93]. Hence, future trust management solutions should be able to cope with these future internet challenges [94].

VII. CONCLUSION

Various security threats and different adversaries are expectable when attempting to secure vehicular communications. In addition, other influential parameters in VANETs should be taken into account by any security system, including high mobility, open wireless medium, and the absence of trusted infrastructures in some cases, like rural environments. In this review paper we first clarified the main threats and adversary models handled by the existing trust-based solutions. Secondly, we reviewed the main existing trust establishment approaches in an adversary-oriented way. The third point was dedicated to the trust management evaluation strategies and their limits. Finally, we pointed out the main open challenges for researchers willing to contribute to this research area. We conclude that a robust security system should include both cryptography and trust strategies to face all kind of threats. Such a desirable system should have the ability to alternate between cryptography and trust, depending on the context and the probable adversary in that context.

REFERENCES

[1] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw.*, Nov. 2005, pp. 11–21.

[2] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for VANET," in *Proc. 5th ACM Int. Workshop Veh. Inter-Netw.*, Sep. 2008, pp. 88–89.

[3] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," *Mobile Netw. Veh. Environ.*, vol. 2007, pp. 103–108, May 2007.

[4] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 22–28, Oct. 2010.

[5] T. Leinmüller, A. Held, G. Schäfer, and A. Wolisz, "Intrusion detection in VANETs," in *Proc. 12th IEEE Int. Conf. Netw. Protocols (ICNP)*, 2004, pp. 1–2.

[6] Y.-C. Hu and K. P. Laberteaux, "Strong VANET security on a budget," in *Proc. Workshop Embedded Secur. Cars (ESCAR)*, vol. 6. Nov. 2006, pp. 1–9.

[7] J. K. Butler, "Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory," *J. Manage.*, vol. 17, no. 3, pp. 643–663, 1991.

[8] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Acad. Manage. Rev.*, vol. 20, no. 3, pp. 709–734, 1995.

[9] S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Trust Management*. Paris, France: Springer, 2005, pp. 77–92.

[10] J. Zhang, "A survey on trust management for VANETs," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2011, pp. 105–112.

[11] B. Mishra, P. Nayak, S. Behera, and D. Jena, "Security in vehicular adhoc networks: A survey," in *Proc. Int. Conf. Commun., Comput. Secur.*, Feb. 2011, pp. 590–595.

[12] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proc. 6th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2012, pp. 1–9.

[13] R. G. Engoulou and M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[14] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for dos attacks in VANET," *Int. J. Comput. Appl.*, vol. 66, no. 22, p. 45, Mar. 2013.

[15] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014.

[16] N. Kaur and S. Kad, "A review on security related aspects in vehicular adhoc networks," *Procedia Comput. Sci.*, vol. 78, pp. 387–394, Apr. 2016.

[17] C. K. Karn and C. P. Gupta, "A survey on VANETs security attacks and sybil attack detection," *Int. J. Sensors Wireless Commun. Control*, vol. 6, no. 1, pp. 45–62, 2016.

[18] Q. Alriyami, A. Adnane, and A. K. Smith, "Evaluation criterias for trust management in vehicular ad-hoc networks (VANETs)," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Nov. 2014, pp. 118–123.

[19] S. A. Soleymani *et al.*, "Trust management in vehicular ad hoc network: A systematic review," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, pp. 1–22, 2015.

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

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

[22] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Proc. 7th Int. Conf. Telecommun. (ITS)*, Jun. 2007, pp. 1–6.

[23] I. A. Sumra and H. B. Hasbullah, "Using trusted platform module (TPM) to secure business communciation (SBC) in vehicular ad hoc network (VANET)," *Safety*, vol. 5, pp. 28–33, Jan. 2016.

[24] C.-Y. Yeun, "Security protocol model for ubiquitous networks," U.S. Patent Appl. 11 533 728, Sep. 20, 2006.

[25] Y. Wu, F. Meng, G. Wang, and P. Yi, "A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Aug. 2015, pp. 1–7.

[26] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks," *Ad Hoc Netw.*, vol. 37, pp. 122–132, Feb. 2016.

[27] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs," *Int. J. Distrib. Sensor Netw.*, vol. 2016, 2016, Art. no. 6138251.

[28] M. K. Daly, "Advanced persistent threat," in *Proc. Usenix*, vol. 4. Nov 2009.

[29] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Netw. Secur.*, vol. 2011, no. 8, pp. 16–19, 2011.

[30] I. Woon, G.-W. Tan, and R. Low, "A protection motivation theory approach to home wireless security," in *Proc. ICIS*, 2005, pp. 367–380.

[31] E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in *Proc. VDE Kongress*, vol. 116. 2004, pp. 213–218.

[32] L. Buttyan and J.-P. Hubaux, *Security Cooperation Wireless Networks: Thwarting Malicious Selfish Behavior Age Ubiquitous Computing*. Cambridge, U.K.: Cambridge Univ. Press, 2007.

[33] A. K. Sood and R. J. Enbody, "Targeted cyberattacks: A superset of advanced persistent threats," *IEEE Secur. Privacy*, vol. 11, no. 1, pp. 54–61, Jan./Feb. 2013.

[34] R. Brewer, "Advanced persistent threats: Minimising the damage," *Netw. Secur.*, vol. 2014, no. 4, pp. 5–9, Apr. 2014.

[35] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): Challenges and perspectives," in *Proc. 6th Int. Conf. ITS Telecommun.*, Jun. 2006, pp. 761–766.

[36] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient rsu-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2008, pp. 1451–1457.

[37] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. 27th Conf. Comput. Commun. IEEE (INFOCOM)*, Apr. 2008, pp. 816–824.

[38] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, 2011.

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

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

[41] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation management in vehicular ad hoc networks," in *Proc. Int. Conf. Multimedia Technol. (ICMT)*, Oct. 2010, pp. 1–5.

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

[43] S. Gurung, D. Lin, A. C. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. NSS*, 2013, pp. 94–108.

[44] J. Zhang, C. Chen, and R. Cohen, "Trust modeling for message relay control and local action decision making in VANETs," *Secur. Commun. Netw.*, vol. 6, no. 1, pp. 1–14, Jan. 2013.

[45] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Comput. Elect. Eng.*, vol. 40, no. 6, pp. 1981–1996, 2014.

[46] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, Oct. 2004, pp. 29–37.

[47] F. Dotzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad-hoc network reputation system," in *Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, Jun. 2005, pp. 454–456.

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

[49] A. Tajeddine, A. Kayssi, and A. Chehab, "A privacy-preserving trust model for VANETs," in *Proc. IEEE 10th Int. Conf. Comput. Inf. Technol. (CIT)*, Jun. 2010, pp. 832–837.

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

[51] R. R. Sahoo, R. Panda, D. K. Behera, and M. K. Naskar, "A trust based clustering with ant colony routing in VANET," in *Proc. 3rd Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2012, pp. 1–8.

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

[53] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst. (INCoS)*, Sep. 2013, pp. 210–214.

[54] Y. Chen and Y. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *J. Commun. Netw.*, vol. 15, no. 2, pp. 153–163, Apr. 2013.

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

[56] K. C. Abdelaziz, N. Lagraa, and A. Lakas, "Trust model with delayed verification for message relay in VANETs," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2014, pp. 700–705.

[57] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TROUVE: A trusted routing protocol for urban vehicular environments," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 260–267.

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

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

[60] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 121–132, Apr. 2015.

[61] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3657–3674, Aug. 2015.

[62] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, "T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS," *Comput. Commun.*, vol. 93, pp. 68–83, Nov. 2016.

[63] *ETSI Eurpean Standard, EN 302 637-2—V1.3.1, (2014–09)*, Eur. Telecommun. Standards Inst., Sophia Antipolis, France, 2014.

[64] *Network Simulator (ns-2)*, accessed on Jan. 2016. [Online]. Available: http://www.isi.edu/nsnam/ns/

[65] *Network Simulator (ns-3)*, accessed on Jan. 2016. [Online]. Available: http://www.nsnam.org

[66] *MATLAB—Mathworks*, accessed on Jan. 2016. [Online]. Available: www.mathworks.com/products/matlab/

[67] F. G. Mármol and G. M. Pérez, "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2009, pp. 1–5.

[68] R. Mangharam, D. Weller, R. Rajkumar, P. Mudalige, and F. Bai, "GrooveNet: A hybrid simulator for vehicle-to-vehicle networks," in *Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst., Netw. Services*, Jul. 2006, pp. 1–8.

[69] M. Piórkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J.-P. Hubaux, "TraNS: Realistic joint traffic and network simulator for VANETs," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 12, no. 1, pp. 31–33, Jan. 2008.

[70] *Swans++ Extensions to the Scalable Wireless Ad-Hoc Network Simulator*, accessed on Apr. 2016. [Online]. Available: http://www.aqualab.cs.northwestern.edu/projects

[71] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3–15, Jan. 2011.

[72] J. Härri, M. Fiore, F. Filali, and C. Bonnet, "Vehicular mobility simulation for VANETs," in *Proc. 40th Annu. Simulation Symp. (ANSS)*, Mar. 2009, pp. 301–309.

[73] F. J. Martinez, C.-K. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Realistic radio propagation models (RPMs) for VANET simulations," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2009, pp. 1–6.

[74] F. J. Martinez, M. Fogue, M. Coll, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Assessing the impact of a realistic radio propagation model on VANET scenarios using real maps," in *Proc. 9th IEEE Int. Symp. Netw. Comput. Appl. (NCA)*, Jul. 2010, pp. 132–139.

[75] P. Manzoni, M. Fiore, S. Uppoor, and F. J. M. Domínguez, C. T. Calafate, and J. C. C. Escriba, "Mobility models for vehicular communications," in *Vehicular Ad Hoc Networks*. London, U.K.: Springer, 2015, pp. 309–333.

[76] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful," in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. IEEE Soc. (INFOCOM)*, vol. 2. Mar. 2003, pp. 1312–1321.

[77] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO—Simulation of Urban MObility: An overview," in *Proc. 3rd Int. Conf. Adv. Syst. Simulation (SIMUL)*, Barcelona, Spain, 2011, pp. 3–20

[78] J.-Y. Le Boudec and M. Vojnovic, "The random trip model: Stability, stationary regime, and perfect simulation," *IEEE/ACM Trans. Netw. (TON)*, vol. 14, no. 6, pp. 1153–1166, Dec. 2006.

[79] D. R. Choffnes and F. E. Bustamante, "An integrated mobility and traffic model for vehicular wireless networks," in *Proc. 2nd ACM Int. Workshop Veh. Ad Hoc Netw.*, Sep. 2005, pp. 69–78.

[80] R. Prasad and A. Kegel, "Effects of Rician faded and log-normal shadowed signals on spectrum efficiency in microcellular radio," *IEEE Trans. Veh. Technol.*, vol. 42, no. 3, pp. 274–281, Aug. 1993.

[81] D. Krajzewicz, G. Hertkorn, and C. Rössel, and P. Wagner, "SUMO (Simulation of Urban MObility)—An open-source traffic simulation," in *Proc. 4th Middle East Symp. Simulation Modelling (MESM)*, 2002, pp. 183–187.

[82] *IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages*. Standard 1609.2-2016, Mar. 2016 , doi: 10.1109/IEEESTD.2016.7426684.

[83] *Intelligent Transport Systems (Its); Security; Its Communications Security Architecture and Security Management (2012–06)*, document TS 102 940 v1.1.1, ETSI, 2012.

[84] C. A. Kerrache, C. T. Calafate, N. Lagraa, J.-C. Cano, and P. Manzoni, "RITA: RIsk-aware Trust-based Architecture for collaborative multihop vehicular communications," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4428–4442, Nov. 2016.

[85] S. M. Tornell, S. Patra, C. T. Calafate, J.-C. Cano, and P. Manzoni, "Grcbox: Extending smartphone connectivity in vehicular networks," *Int. J. Distrib. Sensor Netw.*, vol. 2015, p. 5, 2015.

[86] W.-L. Jin, C. Kwan, Z. Sun, H. Yang, and G. Qijian, "SPIVC: Smartphone-based intervehicle communication system," in *Proc. Transp. Res. Board Annu. Meeting*, 2012, pp. 1–12.

[87] J. Zaldivar, C. T. Calafate, J. C. Cano, and P. Manzoni, " Providing accident detection in vehicular networks through OBD-II devices and Android-based smartphones," in *Proc. IEEE 36th Conf. Local Comput. Netw. (LCN)*, Oct. 2011, pp. 813–819.

[88] A. A. Penilla and A. S. Penilla, "Systems for learning user preferences and generating recommendations to make settings at connected vehicles and interfacing with cloud systems," U.S. Patent 9 288 270, Mar. 15, 2016.

[89] Y. Liu, X. Chen, C. Chen, and X. Guan, "Traffic big data analysis supporting vehicular network access recommendation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[90] Q. N. Nguyen, T. M. Hoang, L. Q. T. Ta, C. Van Ta, and P. M. Hoang, "User preferences elicitation and exploitation in a push-delivery mobile recommender system," in *Proc. Int. Conf. Context-Aware Syst. Appl.*. Ho Chi Minh City, Vietnam: Springer, 2012, pp. 201–211.

[91] F. Mezghani, R. Dhaou, M. Nogueira, and A.-L. Beylot, "Offloading cellular networks through V2V communications—How to select the seed-vehicles? (regular paper)," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lampur, Malaysia, 2016, pp. 1–6.

[92] S. H. Ahmed, S. H. Bouk, and D. Kim, "RUFS: Robust forwarder selection in vehicular content-centric networks," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1616–1619, Sep. 2015.

[93] S. H. Ahmed, S. H. Bouk, M. A. Yaqub, D. Kim, H. Song, and J. Lloret, "CODIE: Controlled data and interest evaluation in vehicular named data networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3954–3963, Jun. 2016.

[94] S. H. Bouk, S. H. Ahmed, and D. Kim, "Vehicular content centric network (VCCN): A survey and research challenges," in *Proc. 30th Annu. ACM Symp. Appl. Comput.*, Apr. 2015, pp. 695–700.

CHAKER ABDELAZIZ KERRACHE received the M.Sc. degree in computer science from the University of Laghouat, Algeria, in 2012. He is currently pursuing the Ph.D. degree in computer science. In 2013, he was with the Informatics and Mathematics Laboratory, as a Research Assistant and the Computer Networks Group as a Visiting Ph.D. Student, in 2015. His research interests include trust and risk management, secure multi-hop communications, and vehicular networks.

CARLOS T. CALAFATE received the Degree (Hons.) in electrical and computer engineering from the University of Porto, Portugal, in 2001, and the Ph.D. degree in informatics from the Polytechnic University of Valencia, Spain, in 2006. He has been with the Polytechnic University of Valencia, since 2002, where he is currently an Associate Professor with the Department of Computer Engineering. His research interests include ad-hoc and vehicular networks, mobile applications, QoS, network protocols, video streaming, and network security.

JUAN-CARLOS CANO received the M.Sc. and Ph.D. degrees in computer science from the Polytechnic University of Valencia (UPV), Spain, in 1994 and 2002, respectively. From 1995–1997 he was a Programming Analyst with IBM's Manufacturing Division, Valencia. He is currently a Full Professor with the Department of Computer Engineering, UPV. His current research interests include wireless communications, vehicular networks, mobile ad hoc networks, and pervasive computing.

NASREDDINE LAGRAA received the M.Sc. and Ph.D. degrees in automatic control engineering from École Nationale Polytechnique, Algeria, in 2000 and 2008, respectively. He is currently a Professor with the Department of Mathematics and Computer Science, University of Laghouat, where he is also the Head of Informatics and Mathematics Laboratory. His current research interests include computer security and reliability, cloud computing, Internet of Things, and vehicular networks.

PIETRO MANZONI (M'00) received the M.S. degree in computer science from the Università degli Studi di Milano, Italy, in 1989, and the Ph.D. degree in computer science from the Politecnico di Milano, Italy, in 1995. He is currently a Full Professor of Computer Science with the Polytechnic University of Valencia, Spain. His research interests include mobile wireless data systems design, modeling, and implementation, particularly oriented to intelligent transport systems.