Trust in VANET: A Survey of Current Solutions and Future Research Opportunities

Rasheed Hussain, *Senior Member, IEEE*, Jooyoung Lee, and Sherali Zeadally

***Abstract*— Security and privacy will play a pivotal role in the commercialization of Vehicular Ad-hoc NETworks (VANETs). Traditionally, both cryptographic and non-cryptographic approaches have been used by researchers to address security and privacy issues and achieve secure Intelligent Transportation System (ITS) applications. However, some security goals such as trust and reputation, are still hard to achieve through conventional cryptographic approaches. Trust is the degree of certainty with which the received information is accepted and acted upon. Historically trust has been computed for both the content generator and the content itself with former known as entity trust and the latter known as data trust. Both entity and content trust are equally important to support trustworthy communication in VANET. We review, analyze, and compare some of the recently proposed trust establishment and management mechanisms (from 2014 to 2019) in vehicular networks. Furthermore, we also discuss the weaknesses and inadequacies of existing trust establishment and management approaches when deployed in a VANET environment. Finally, we discuss some future challenges that will need to be addressed for trustworthy communications in vehicular networks.**

***Index Terms*— Privacy, reputation, security, trust, vehicular networks.**

I. Introduction

CONNECTED car technology which is enabled by Vehicular Ad-hoc NETworks (VANETs) is on the verge of deployment as a result of tremendous research efforts from both academia and industry. VANET is a special type of Mobile Ad-hoc NETwork (MANET) where vehicles communicate with each other opportunistically in an ad-hoc manner without any infrastructure. Vehicles also communicate with the roadside infrastructure (for instance, Road Side Units (RSUs)) to support different types of applications that fall into two broad categories namely, safety and non-safety. The non-safety category includes infotainment (information and entertainment) applications which have relaxed requirements for communication delays as compared to the safety category which includes safety- and warnings-related applications (for instance accident warnings, black ice on the road, and other critical incident related notifications and warnings). There are numerous other applications such as personalized interest information, Internet on the move, news, vehicular diagnostics, maintenance, and so on that are supported by VANET technology. It is also worth mentioning that most VANET applications are based on cooperative data and information exchange among vehicular nodes and with the roadside infrastructure. Cooperative traffic information dissemination system is the best example of such cooperation among nodes, where vehicular nodes share their location information (such as current location, speed, direction, and control information such as brake status and steering wheel angle) with their neighbors and with the infrastructure for cooperative awareness [1]. This data is structured into a special format referred to as Cooperative Awareness Message (CAM) or beacons. The IEEE 802.11p standard recommends that the frequency of CAM exchange should be in the order of milliseconds [2]. Recipients of such information on the other hand, use the CAMs for constructing traffic views as well as for other applications such as location-based services and warning messages [3]. Thus, vehicles in VANET act both as providers and consumers at the same time and therefore, efficient data dissemination for the successful realization of VANET applications is of paramount importance. The performance of data dissemination-related VANET application is affected by many factors such as cooperation among nodes, security of data, user privacy, health of exchanged information, authenticity, and so on. Among the aforementioned factors, authenticity of the information source and the information itself are key factors to consider for the acceptance or rejection of the received information from neighbors. In other words, the quality (trustworthiness) of the received information should be checked before taking any action based on that information.

Today's high-end vehicles are hosts to numerous computation and communication resources that include arrays of sensors, actuators, communication interfaces, microprocessors, and storage [4]. These high-end vehicles can also communicate with other components within the car as well as with other entities outside of the car. Dedicated Short Range Communication (DSRC) and Wireless Access in Vehicular Environment (WAVE) (or IEEE 802.11p) are the standards that are used in VANET and specialized hardware referred to as On-Board Unit (OBU) is used as VANET module in cars for both *vehicle-to-vehicle* and *vehicle-to-anything* communications [5]. Besides, other communication technologies and standards such as WiFi, 3G/LTE, WiMax, and Bluetooth are also used in high-end cars and 5G is being explored for vehicular communications [6]. These different types of

Manuscript received April 22, 2019; revised October 7, 2019 and December 16, 2019; accepted February 5, 2020. The Associate Editor for this article was S. Kong. *(Corresponding author: Rasheed Hussain.)*

Rasheed Hussain is with the Networks and Blockchain Lab, Institute of Information Security and Cyber-Physical Systems, Innopolis University, 420500 Innopolis, Russia (e-mail: r.hussain@innopolis.ru).

Jooyoung Lee is with the College of Engineering and Computer Science, The Australian National University, Canberra, ACT 0200, Australia (e-mail: jooyoung.lee@anu.edu.au).

Sherali Zeadally is with the College of Communication and Information, University of Kentucky, Lexington, KY 40506 USA (e-mail: szeadally@uky.edu).

Digital Object Identifier 10.1109/TITS.2020.2973715

communication technologies on one hand, provide better connectivity among vehicles and with the infrastructure, but on the other hand, they also require complex network models, seamless protocol definitions, quality of service provisions, efficient data dissemination, security, and privacy.

Despite the extensive research efforts that have been invested into VANET research, it has not been fully commercialized yet, partially because of the afore-mentioned challenges that still need to be addressed. Among the various challenges in VANET, practical security and privacy are two of the most important requirements that must be met cost-effectively. To date, different security aspects such as authentication, confidentiality, privacy, trust and reputation, misbehavior detection, attack detection and mitigation, and access control have been extensively investigated in VANET [7]–[10]. Although these security aspects need different mechanisms to mitigate the possible attacks in VANET, some of these aspects are either directly or indirectly related to each other. For instance, authentication, trust and reputation, and misbehavior detection are related to each other. Trust refers to a mechanism that determines whether to accept the information from an arbitrary sender with a degree of certainty. When a node receives some data and/or information, it needs to check: a) whether the sender of the message is legitimate and trustworthy, b) whether the content of the message is trustworthy. The former requirement is addressed through authentication and node trust, whereas the latter requirement is addressed through content trust. Several mechanisms have been proposed in the literature to deal with both entity and node trust in VANET [10]–[12] that leverages different characteristics such as mobility, frequent communication patterns, and behavioral information (e.g., degree of node trust and reputation) of the vehicular network, to name a few. Furthermore, different techniques have been used to propose mechanisms to calculate the trust and reputation values of both nodes and the content in vehicular networks. These techniques include cryptographic, non-cryptographic, consensus, game theory, recommendation, and fuzzy logic-based techniques [10], [13]–[16]. To provide the readers with a comprehensive review of the available trust management solutions in VANET, it is imperative to systematically review these solutions and analyze them in a holistic fashion. In this context, we conduct a systematic review of the trust management solutions in VANET and discuss different attacks mitigated through these solutions. The contribution of this paper is outlined below.

A. Existing Surveys

To date, many researchers have addressed trust management issues in VANET. A rich literature already exists that addresses trust issues on various aspects of vehicular communications. However, to the best of our knowledge, and based on our detailed search through different well-known databases, we could not find dedicated surveys that cover trust management in VANET in a holistic way. In this section, we outline the existing surveys that cover different trust establishment and management solutions in vehicular networks. Table I summarizes the existing surveys on trust management in VANET and also discusses the enhancements in our paper. The table contains topics that are covered by the existing surveys and the enhancements done in our survey. We divide these surveys into the following classes: security issues in VANET including trust, trust issues in enabling technologies for VANET, and survey on trust-based services in VANET.

From Table I, we note that most of the existing surveys are either old (we searched the papers from 2010 onward), or they do not fully address all aspects of trust management in VANET. Past surveys in the literature have covered trust management in general ad-hoc networks [17] and, to some extent, in vehicular networks [18]–[21]. However, these surveys covered trust management schemes that target different applications in VANET. For instance, the authors of [19] focused on the adversary-oriented trust management in vehicular networks. El-sayed *et al.* discussed current trust-based challenges in vehicular networks and proposed an edge-based trust management scheme [20]. Similarly, Souissi *et al.* [21] surveyed trust management solutions in vehicular networks from application and performance perspectives. In a nutshell, there is no comprehensive survey in the literature that covers all aspects of trust management in VANET. To address this deficiency, in this work, we have surveyed the recent literature on trust management in vehicular networks that encompasses different types of solutions.

B. Main Contributions of This Paper

In this work, we present a comprehensive review of the recent state-of-the-art solutions on trust management in vehicular networks. In contrast to past trust management surveys that have been published in the literature, we present a survey of recently proposed trust management schemes for VANETs from 2014 to 2019 (at the time of writing this paper). Furthermore, we describe the attacks that can be mitigated by recently proposed trust management mechanisms based on the underlying techniques for trust establishment and management. The main contributions of this work are summarized below.

1) We present a comprehensive review of trust management solutions in VANET that includes both traditional approaches (covered in recent papers) and emerging trust management techniques.
2) We describe different solutions that have been proposed in the last six years (2014 to 2019) to establish and manage trust in vehicular networks. We classify different solutions for trust establishment and management in VANETs based on the specific methodology used which includes cryptography, recommendation, fuzzy logic, game theory, infrastructure, and consensus-based trust management. Moreover, we also cover trust-based services, blockchain-based trust and trust in emerging technologies integrated with VANET.
3) We identify several outstanding research challenges that still need to be addressed by the VANET research community to ensure trust in the vehicular environment.

In a nutshell, this paper presents an extensive review on recent advances in the area of trust management in VANET

TABLE I
EXISTING SURVEYS ON TRUST MANAGEMENT IN VEHICULAR NETWORKS

Year	Paper	Topic(s) of the survey	Related content in our paper	Enhancements in our paper
2010	[22]	Short survey on trust in MANET, wireless sensors networks, cognitive radio networks, and vehicular networks	Section IV	An in-depth and detailed survey of trust management in VANET encompassing almost all the aspects of trust
2011	[23]	Survey on authentication, location privacy, and a brief discussion on trust management in VANET	Section IV	Coverage of recent state-of-the-art trust management solutions in VANET
2011	[17]	Survey of social trust management in resource-constrained MANET	Section II	Recent trust management schemes, their classification, and relisience against attacks in VANET
2012	[24]	Survey of trust management in VANET before 2011 and proving their inadequacy in VANET	Section IV	Review of recent advances in trust management in VANET and future challenges
2013	[25]	Applications, features, security issues, attacks and trust management in vehicular networks	Section I	Focuses on VANET and its enabling technologies and review of existing trust management solutions with future research directions
2015	[26]	Survey of authentication, access control, routing, privacy, and trust in vehicular networks along with an architecture proposal	Section III	Detailed survey of recent trust management solutions in VANET and its enabling technologies
2015	[18]	Survey on trust in vehicular networks covering works prior to 2014 and focuses only on the management classification without taking security requirements for trust into account	Section IV	Covers recent state-of-the-art regarding trust management in VANETs and their ability to mitigate different kinds of attacks
2016	[19]	Adversary-oriented approaches for trust management in VANET and how trust management could help mitigating different attacks in VANET	Section IV	Classification of trust management schemes in VANET based on security requirements and current state-of-the-art solutions for both VANET and enabling technologies
2016	[27]	Trust management schemes in MANET and their classification metrics and a comparison of trust-enabling solutions	Section II	Focuses on vehicular networks with trust management solutions, keeping in mind the salient features of VANET
2018	[28]	Overview of trust management schemes for routing in vehicular networks	Section IV-C	Covers almost all aspects of trust management solutions in vehicular networks in a holistic way
2019	[20]	Trust management schemes for malicious vehicle detection and architecture of an edge-based solution to support the trust platform in vehicular networks	Section IV-C	Focuses on the current state-of-the-art in trust management solutions for VANET and its enabling technologies in a holistic way
2019	[10]	Survey on security services in VANET, anonymous authentication, location privacy, and various trust management solutions	Section I	Comprehensive survey of the current state-of-the-art in trust management solutions for vehicular networks with future research directions
2019	[21]	Application-oriented approach for trust management in VANET and focuses on application performance for trust management	Section IV	Comprehensive survey of the security requirements of VANET and coverage of the current state-of-the-art trust management solutions

and bridges the gap between current solutions and the way forward. Figure 1 presents a pictorial representation of the scope and taxonomy of this survey.

The rest of the paper is organized as follows. In section III, we discuss the importance of trust in vehicular networks. Section II presents current trust management schemes in general ad-hoc networks and how they are related to vehicular networks. In section IV, we present current state-of-the-art techniques on trust management in vehicular networks. We discuss future research challenges on trust management in section V. Section VI concludes the paper.

II. TRUST IN AD-HOC NETWORKS

Ad-hoc networking refers to the spontaneous formation of a network of nodes without the help of any infrastructure, usually through wireless communication channels [29]. VANET is a specialized type of ad-hoc networks where the nodes are highly mobile [30]. In this context, it is imperative to discuss trust management in ad hoc networks and then explore how it can be adapted to VANET. There are many trust management solutions that have been proposed for general ad-hoc networks [27], [31]–[34]. Trust and reputation-based approaches strengthen security and decision making processes at node levels. Network security techniques aim to protect and manage access to networks and mitigate threats and possible attacks preventing the attackers from infiltrating the networks. In this context, network security techniques could be classified as hard requirements. Trust and reputation management techniques complement network security by encouraging good behaviors and penalizing bad behaviors. Good trust and reputation schemes penalize the users with malicious behaviors and promote good behaviors in a way that it is beneficial for both the user and the network. First we focus on the trust management in generic ad hoc networks.

A. Current Trust Management Approaches in Ad-Hoc Networks

Traditional methods to prevent network attacks become vulnerable when networks become decentralized and when attacks come from within the networks. Decentralized networks need to implement decision making processes at the node level where every node must take part in the computation of trust and reputation in ad-hoc networks. According to [35], there are 4 factors that establish trust and they include bootstrapping, trust evidence, trust computation, and

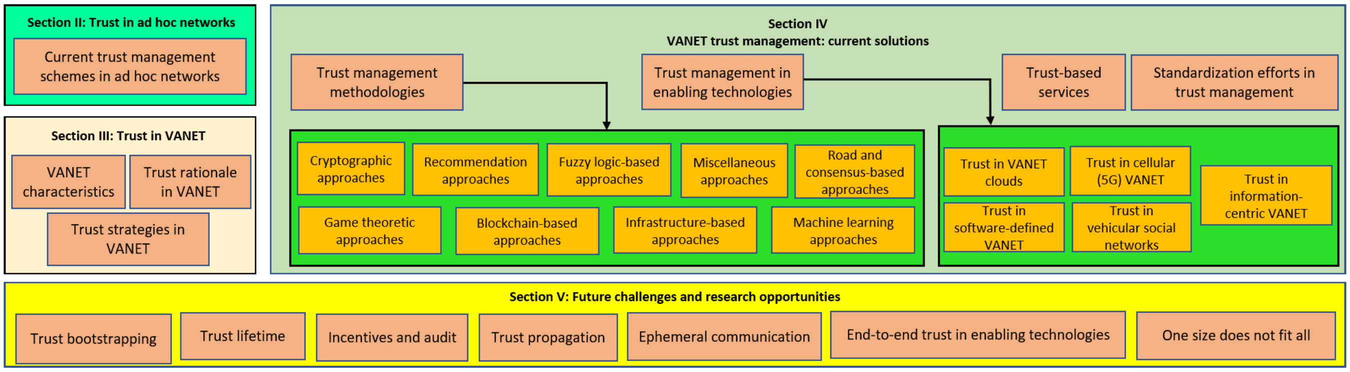
Section II: Trust in ad hoc networks
Current trust management schemes in ad hoc networks
Section III: Trust in VANET
VANET characteristics
Trust rationale in VANET
Trust strategies in VANET
Section IV
VANET trust management: current solutions
Trust management methodologies
Trust management in enabling technologies
Trust-based services
Standardization efforts in trust management
Cryptographic approaches
Recommendation approaches
Fuzzy logic-based approaches
Miscellaneous approaches
Road and consensus-based approaches
Game theoretic approaches
Blockchain-based approaches
Infrastructure-based approaches
Machine learning approaches
Trust in VANET clouds
Trust in cellular (5G) VANET
Trust in information-centric VANET
Trust in software-defined VANET
Trust in vehicular social networks
Section V: Future challenges and research opportunities
Trust bootstrapping
Trust lifetime
Incentives and audit
Trust propagation
Ephemeral communication
End-to-end trust in enabling technologies
One size does not fit all

Fig. 1. Taxonomy of this survey.

decision making. Bootstrapping methods handle uncertainties when two entities interact for the first time. Most of the trust management methods prefer neutral trust to high or low trust initially. In [36], the authors proposed a similarity-based bootstrapping method which enables flexible assignment of initial trust score to the neighbors or the entities involved in interaction. Abstractly, there are three ways how trust is established: direct trust, indirect trust and hybrid trust. Direct trust collects evidences from direct experiences while indirect trust collects evidences via hearsay. Most trust management systems combine both pieces of evidence and use hybrid methods [37], [38]. To compute trust in general ad-hoc networks, existing systems deploy various algorithms based on neural network [39], [40], probability [41], Bayesian [42], [43], and entropy-based mechanisms [31], [44]–[47].

Bayesian based approaches [48] apply the theory of Bayes to infer trust among users in a network. Therefore, a series of prior events need to be defined to compute the posterior probability of trust. Game theoretic tools are also often used in many trust computation schemes. However, since game theory itself is not a predictive model, game theoretic analysis is used to model the convergence of behaviors of the entities [49]. Though not popular, some neural network based models also exist. For example, [50] introduced a neural network model which uses factors such as user profiles to find relationships between trust level and adoption decisions.

The trust management schemes mentioned above are used in VANET as well. However, VANET has expanded its scope from simple V2V communication to V2X communication which encompasses other enabling technologies thereby requiring a re-evaluation of the existing trust management models. Furthermore, the incorporation of new emerging technologies such as blockchain and cellular networks also require trust management solutions in vehicular networks to be revisited.

III. Trust in Vehicular Networks

A. Characteristics of VANET

Despite the fact that there are several trust management approaches that can evaluate the trustworthiness of users in ad-hoc networks, specific characteristics of VANET require more efficient, robust, and scalable trust management solutions. Next, we summarize the salient characteristics of VANET:

- **Speed**: Unlike many other traditional networks including MANET, VANET nodes move with different speeds. This implies that the formation of a certain topology constantly changes and there are no permanent neighbors. Therefore, most of the time, reputation values are computed only at the first encounter with the neighbor instead of being frequently updated. Hence, the importance of trust bootstrapping is much higher in VANET environment.
- **Directed**: Vehicles must follow traffic regulations and therefore their mobility is limited by the road topology.
- **Opportunistic**: Within a VANET, vehicles can communicate with each other and with the road-side infrastructure. In other words, vehicles can interact only when they belong to the same VANET at the same time.
- **Intermittent network of vehicles in VANET**: Vehicles constantly set up a network. In other words, VANETs exist continuously but the vehicular nodes of each network frequently change. Therefore, technically speaking, VANETs are intermittent because they continuously appear and disappear all the time. The opportunistic characteristic (i.e., vehicular nodes encounter each other opportunistically without any prior plan for that, making VANET an opportunistic network) makes it difficult to deploy a traditional trust mechanism (initially designed for general ad-hoc networks) in VANETs. Since these characteristics of VANETs imply that interactions with unknown neighbors are much more likely, a strong motivation exists for vehicular nodes to cooperate with each other and behave honestly.
- **Resource availability**: Each vehicle is equipped with computing resources such as computing power, storage, and so on.
- **Automatic connectivity to other vehicular nodes**: This specific characteristic distinguishes VANETs from other networks. While individuals need to join or register with a network to be considered as a member, VANETs are automatically created based on the communication radius (range) of each vehicle. Consequently, vehicular nodes lack the motivation to build trust with other nodes in VANET unlike other networks.

As the above features demonstrate, VANETs are formed dynamically and automatically with a restricted topology. Due to short and frequent interaction cycles, it is crucial in VANET environments to accurately infer the level of trust quickly (almost instantly). Unlike other network environments where individuals can accumulate interaction information to estimate the trust of the other entities, in VANET, it is difficult to wait for enough interactions before one can infer some level of trust. Furthermore, the inclusion of different enabling technologies such as cellular, clouds, social networks, and so on, also necessitate new trust management solutions. Therefore, trust bootstrapping and trust propagation mechanisms need to be well integrated into trust management.

B. Rationale for Trust Management in VANET

To date, many attacks (both theoretical and practical) on VANET have been discussed in the literature that could hinder the normal functionality of VANET [8], [51]–[54]. These attacks include, but not limited to, Distributed Denial of Service (DDoS), identity theft, sybil attack, forging, message suppression, hacking, and blackhole attacks. As a result, the receiver must be sure about the quality of the received data before it can be used for future accurate and timely decisions. Trust in VANET is of paramount importance because of several reasons. For instance, although cryptography is the first line of defense for most of the security attacks in networks, every security problem cannot be solved through cryptographic solutions alone. In other words, cryptography cannot detect security-related problems such as *fake messages* and *dishonest users*. Therefore, mutual trust among nodes and the trust of received data will determine the effectiveness of the underlying trust management mechanism. Consider a VANET safety-critical application where the application recommends to apply the emergency brake as a result of an accident or some obstruction along the road ahead of the current node. In this case, the warning message can be either legitimate in which case the driver must take an action and apply the brake immediately, or it could be generated by a malicious node for selfish reasons. In order to make a timely decision on the received information, the vehicle should take into consideration both the trustworthiness of the sender as well as the trustworthiness of the data. After the vehicle evaluates these values, it can provide accurate information to the VANET application in order to determine whether to apply the brakes or disregard the message and report the sender to another security system such as a Misbehavior Detection System (MDS) [55]–[57]. It is worth noting that such a situation is difficult to handle with current security mechanisms for VANET. Similarly, non-safety applications also need trust and reputation information about communicating nodes and the content they share. In the case of non-safety applications such as location-based services, any fake or false information can have severe consequences on the application performance and may abuse the privacy of the nodes.[1] For example, a node receives a recommendation about sale at a mall, an offer for music share, or an interesting application. This could be either bogus information where the service quality will be impaired or the music, video, and applications could have malicious code that could jeopardize the security of the vehicular node. Therefore, accepting such information is always subject to the trustworthiness of the sender. Thus, it is essential to assess the trustworthiness of nodes and their shared information prior to any decision based on such information.

C. Trust Management Strategies

Two major steps are required for organizing trust among nodes and the trust of data/information, i.e., trust establishment and trust management. Trust establishment or trust computation refers to a set of steps that are performed to obtain the trust value of either a node or data for the first time. Once the trust value is computed locally for a node, it is managed for the duration of the interaction with that node. This is referred to as trust management. There are many trust computation and trust management mechanisms devised for vehicular networks that use different techniques such as direct techniques by exchanging messages and calculating a trust value for the immediate or intermediate nodes and indirect techniques that use recommendation, reputation, and voting from either neighbors or infrastructure [58], [59]. Trust computation and management techniques can be broadly divided into following categories: recommendation, data analytics, reputation, fuzzy logic, game theoretic, probabilistic, and entropy-based solutions. The aforementioned mechanisms use different underlying techniques such as cryptography, machine learning, neural networks, weightage, and priorities to manage entity trust in VANET. Apart from these techniques, punishment and rewards, and consensus-based solutions are also employed to establish and manage trust among vehicular nodes. When trust is computed for data, its immediate use is to take a decision based on the computed trust value for that data. Usually the decision is binary where either the received data is accepted or rejected with further action against the sender (such as degradation in reputation and reporting it to the authorities). In contrast, trust management is a continuous process where the trust value is updated for every node based on the underlying trust management mechanism which can be any of the previously mentioned techniques (such as recommendation, data analytics, reputation, and so on). When data is received from a node, its trust value is updated locally and future communication with this node is subject to a trust value greater than an acceptance threshold. Figure 2 presents a general classification of the trust management and trust establishment techniques in vehicular networks from an application perspective.

There are three main categories in the classification of trust management techniques, i.e., subject trust, trust-based services, and the origin of trust. Subject trust describes either entity or content trust. Entity trust leverages different tools such as cryptography, game theory, fuzzy logic, social networking, and machine learning whereas data analytics, plausibility, watermarking, and evidence-based approaches are used for content trust establishment. On the other hand,

[1] We have used the terms ”node”, ”vehicular nodes”, and ”vehicles” interchangeably in the paper.

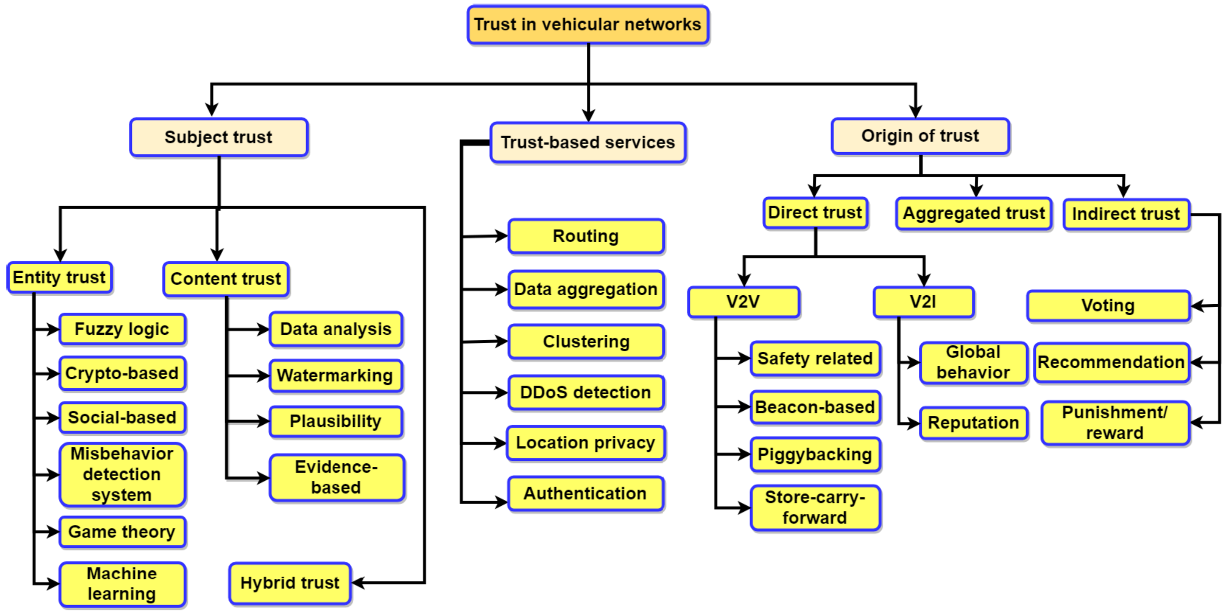

Fig. 2. Classification of trust establishment mechanisms in vehicular networks.

trust-based services refer to the services that are aided by trust establishment. Such services include trust-based routing, trust-based relay selection in vehicular networks, trust-based information dissemination, and so on. The origin of trust is also divided into three categories namely, direct trust, indirect trust, and aggregated trust. In direct trust, vehicular nodes communicate directly with each other and/or with the infrastructure through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. In indirect trust, usually voting or recommendation-based approaches are used by the vehicles. In other words, vehicles request opinions and/or recommendations about a neighbor (let us assume v_i) from other neighbors who have already evaluated the trust level of v_i. In the aggregated trust, both direct and indirect trust are evaluated together.

IV. VANET Trust Management: Current Solutions

In this section, we discuss the recent advances on trust management mechanisms for vehicular networks and its enabling technologies such as cellular networks, Software-Defined Networks (SDN), Named Data Networking (NDN), and so on. In a generic trust establishment and management, each node first computes the trust of its neighbors based on either direct communication with the neighbor or indirectly through recommendations, voting, or reputation via some infrastructure. Recently, several trust establishment mechanisms that, 1) mitigate the malicious behavior of vehicles [57], [60]–[65] and 2) are used to limit false data dissemination in the network [11], [61], [66]–[68]. In this paper, we broadly focus on cryptographic and non-cryptographic approaches, where non-cryptographic approaches can be further classified into game theory-based, fuzzy logic-based, misbehavior detection, blockchain-based approaches, machine learning-based approaches, and social-based approaches that use different communication paradigms and methodologies. We organize the trust management solutions for VANET into the following categories: a) trust management methodologies in VANET, b) trust management in enabling technologies for VANET, c) trust-based services, and d) standardization efforts for trust in VANET.

A. Trust Management Methodologies in Vehicular Networks

In its essence, trust is a multidimensional attribute associated with an entity and is used to decide with a certainty whether to accept information from a node or not [69], [70]. This attribute can be associated with content as well as when different notions of the same features are used. In order to calculate/compute trust for both entity and content, several methodologies have been used in the literature [71]–[75]. In this paper, we focus on the recent and most frequently used methods in the literature to establish and manage trust among entities and content trust in vehicular networks. The trust establishment mechanism requires two operations namely, the selection of the trust establishment path and the selection of the underlying methodology. The trust establishment path could be either direct or indirect (in some cases combination of these two) whereas based on the selection of the approach, different methods of trust establishments can be used. Next, we present trust establishment mechanisms in the vehicular network environment.

1) Cryptographic Approaches: Although trust computation is considered to be a computationally cheaper alternative to cryptography, however, many recent works [15], [54], [61], [76], [77] have used cryptography to help trust establishment in vehicular networks. Hu *et al.* [61] proposed a mechanism called reliable trust-based platoon service recommendation (also referred to as REPLACE) to compute the trust score of a candidate for the platoon head in a platooning application. The platoon head is then used to provide a platooning service to the vehicles. REPLACE uses a centralized approach for trust computation instead of a distributed mechanism where a central authority and/or server is employed to perform trust computation and evaluation. The ultimate goal of REPLACE is to recommend a trustworthy platoon head for the platooning service. A central server accumulates the feedbacks from user vehicles through RSUs to evaluate the trust value of the head of the platoon. Furthermore, because of the possibility that the feedback itself could be polluted, the trust management mechanism incorporates iterative filtering of the malicious feedbacks. The security of this scheme is based on establishing a secure session key between the RSU and the vehicular node using public key cryptography and certificates. The use of the established non-interactive session key prevents malicious nodes from launching attacks. It is worth noting that in most of such centralized trust management mechanisms, the cryptographic primitives are constructed and then distributed by the trusted authorities which may become overloaded as well. As a result, trust values are iteratively updated by the server and then distributed either on demand or periodically whenever the platoon head must be elected/selected. In [76], Biswas *et al.* studied the possibility of long-term vehicular trust. The rationale behind long-term trust is to reduce the computational overhead incurred by re-computing the trust value of neighbors who might be neighbors at some point, but may have been disconnected and then connected again. In such cases, it would be more efficient to retrieve that neighbor's trust value rather than computing it again. Furthermore, a centralized system is more suitable for long-term trust values because there must be enough storage to store the trust values for all the nodes of the network. This solution used PKI and certificates to exchange the trust evaluation message among different entities. However, the certificates are used only during bootstrapping phase to decrease the communication and computation overheads. This scheme also leverages RSU for trust propagation, and the movement of vehicles between different RSUs does not require the downloading of certificates from CAs. The movement between different RSUs, however, require the vehicles to download the list of neighbor RSU's public key certificates and to validate themselves to the current RSU. Once the current RSU validates the authenticity of the certificate issued to the vehicle by the previous RSU, the current RSU issues a trust value. The scheme lacks a practical implementation and a full performance evaluation.

Similarly, several other recent papers have used cryptographic approaches for evaluating and managing trust in vehicular networks [19], [61], [76], [78]–[80]. Kerrache *et al.* [80] proposed a social-driven trust management scheme for Internet of Vehicles (IoV). They use chaotic maps-based PKI for establishing trust among communicating nodes. More precisely, they use the movement history of the vehicles and measure their honesty in providing such information. The cryptographic primitives used in this scheme are reported to be more energy-efficient than RSA and ECC-based schemes.

From another perspective, trust has been considered as an alternative to cryptography to achieve different security goals such as authentication, integrity, non-repudiation, and misbehavior detection. The fact that cryptography alone does not include every aspect of security, trust computation is used to fill this void. Nevertheless, it depends on the application, context, and type of attacker (attack space, attacker resources, and type of resources the attacker has) to decide where to use trust and cryptography. We note that, from the literature, both trust and cryptography can be used simultaneously [19]. Kerrache *et al.* [19] describe the pros and cons of both cryptography and trust in networks and analyzed the use of cryptography and trust in network security. This study concluded that both trust and cryptography must be used for VANET security based on the context of the application.

2) Recommendation-Based Approaches: Recommendation-based trust management is achieved through indirect communication among the vehicular nodes. More precisely, both vehicular nodes and the stationary infrastructure share their communication experience with other nodes in the form of recommendation. This recommendation could be active where let say a node v_1 requests the trust value of another node v_2 from its neighbors. v_1's neighbors respond with their experience of communication with v_2. This scenario could also be applied to RSUs where vehicular nodes can query nearby RSUs about the trust value of particular nodes. RSUs may gather the individual trust values about nodes from the cars on the road and construct recommendations accordingly and then share it with the moving cars (either actively or passively). Moreover, in some cases when nodes share useful information with the neighbors, the neighbors may vouch for the sending node in terms of recommendation that will eventually increase the sender's trust. Furthermore, peer evaluations are also used for recommendation and trust propagation in vehicular networks. Several research efforts have used recommendation techniques for trust management and propagation in VANETs [11], [12], [61], [81].

Kerrache *et al.* [12] proposed a direct and indirect trust management mechanism in vehicular networks namely T-VNets by using beacon messages and neighbors' behaviors. The beacon-based trust is computed locally and subsequent recommendation is broadcasted automatically to one-hop neighbors. Furthermore, the behavior of the neighbors are also shared with nearby RSUs. In another work, Ahmed *et al.* [11] combined existing trust management mechanisms that include data-centric trust, entity trust and recommendation trust to identify any potential malicious nodes in the current VANETs. In essence, this mechanism combines direct and indirect trust by computing the local trust and analyzing recommendations from other neighbors. In another work, Kerrache *et al.* [81] proposed a hierarchical trust establishment mechanism through a static infrastructure (RSUs and trusted authorities) and through mobile vehicles. After accumulating individual trust values from the vehicles, the trusted authorities construct a global view of the trust values and share subsequent recommendations with vehicles on the road. The aforementioned schemes address both direct and indirect trust management issues in vehicular networks.

3) Fuzzy Logic-Based Approaches: Plausibility checking has been used in many security-enhancing mechanisms to alleviate the problem of uncertainty about the quality of information [63]. In essence, it is more related to content trust than node trust where plausibility checks are applied to the received information. Different filters (such as Kalman filter [82]) exist to enable plausibility checks. Trust, by definition, is measured through approximation rather than through discrete values. Thus, fuzzy logic can be a suitable approach to calculate the accuracy of information and the source of information. Soleymani *et al.* [83] used fuzzy logic to compute node trust in vehicular networks. This approach is layered wherein at the first layer, node authentication is performed to guarantee that the node is authentic. The authentication process filters out the outsiders. Next, the trust management system checks for the freshness of the information. If the received information is in the range of the accepting threshold time, then location accuracy is checked to verify the location of the node that generated the information. Moreover, at the core, this approach is also based on the direct trust establishment where every node maintains its past experience with the neighbors and use it in the trust evaluation process through fuzzy logic. It is worth noting that the core trust establishment mechanism is based on direct trust where each node computes the trust value from direct interaction with the neighbors. However, the trust computation mechanism itself employs fuzzy logic.

4) Game Theory-Based Approaches: Game theory has been used for both security and other services in vehicular networks such as clustering, routing, incentives as a result of cooperative contribution to the network (such as forwarding information to neighbors), and so on [84]. Game theory is used as a compute-efficient alternative for security in networks. Similarly, in VANET game theory has been used to establish and manage trust among nodes. As mentioned in the previous sections, behavior analysis is the pinnacle of the trust establishment. In this context, game theory is one of the best tools to formulate behavior analysis among nodes and authorities in a network. Shivshankar *et al.* [85] developed a game theoretic approach to evaluate the cooperation among nodes in a vehicular network. This scheme takes into account the individual node behaviors and the networking properties to fully achieve the cooperation mechanism which is essential for almost every VANET application. Similarly cluster-based cooperation has been studied by Chen *et al.* [86] by using game theoretic approach. This study focused on intra-cluster cooperation instead of cooperation among individual nodes. Therefore, it can be applied to platooning applications to study the behavioral aspects of such applications. As we have mentioned before, node behavior is also essential in trust establishment among nodes and has been frequently used in social networks [87]. Another game theory-based trust establishment mechanism was proposed by Mehdi *et al.* [13] for vehicular networks. In their approach, they establish trust among nodes based on three parameters, i.e., the majority opinion, betweenness, and node density. In principle, the authors have used game theory to combine both entity and content trust where they consider information verification to distinguish between trusted and malicious nodes. From the majority opinion (such as about the exchange of routing information and the exchange of frequent beacon information among neighbors) among nodes, the proposed scheme calculates the trust level of a node. Betweenness measures the importance of a node among its neighbors. In other words, betweenness records the frequency with which a particular node is selected as a relay or as an intermediate node during the shortest path calculation. The third parameter for the game theory is the node density which aids in forming a homogeneous cluster of nodes that have the same speed and direction. By combining all three parameters, a game theory is developed to establish Nash Equilibrium where attackers and defenders are evaluated against these criteria (i.e., majority opinion, betweenness, and node density) and consequently helps in the eviction of non-trusted nodes from the network.

5) Infrastructure-Based Approaches: Vehicular networks employ RSI (RSUs) to support communication between vehicles and management authorities as well as to help to realize VANET applications and services. RSUs cover larger areas through a higher transmission range than normal vehicles and therefore have access to a large number of vehicles in the areas with their range. To this end, vehicles broadcast beacon messages to their one-hop neighbors and share this data as well as other event information with RSUs. Therefore, RSUs are capable of analyzing this data and use it for different purposes. Similarly, RSUs also evaluate the trust of vehicles through either direct interaction with them or through aggregated trust values computed by other vehicles. The use of the computed trust for a node by an RSU depends on the underlying strategy. For instance, when a vehicle requests for the trust and reputation value of a particular node from an RSU, the RSU can provide that data to the requesting vehicle. On the other hand, an RSU can periodically broadcast the current trust values of the moving vehicles to their neighbors. Kerrache *et al.* [12] used the existing communication architecture for vehicular networks and modeled a trust establishment mechanism that uses beacon messages. Vehicles use a direct trust mechanism to compute neighbors' trust and RSUs are used as oversight entities to manage historical behavior of the nodes which may be shared with other vehicles later. Furthermore, this RSU-based mechanism uses hybrid approach where direct trust, indirect trust, recommendation, and reputation are all used to encompass every aspect of the trust in vehicular networks. Kerrache *et al.* [81] used another similar mechanism for trust evaluation in VANET. In order to calculate the long-term trust values, Biswas *et al.* [76] used RSUs to serve as intermediate nodes between vehicles on the road and the back-end servers (maintained by either the service provider or the government) that store the long-term trust values for the vehicles.

Besides RSUs, central authorities can also be leveraged to compute and manage trust for vehicular nodes by using a centralized approach. Liao *et al.* [88] proposed an infrastructure-based reputation mechanism that uses both direct and indirect communication paradigms for trust establishment. The proposed scheme considers event reports and the receivers of such reports determine the trust level of the nodes that send these reports. It is worth mentioning that the trust score is computed by the central authority for all the originators and the forwarders of the event report via vehicle-to-infrastructure communication. Whenever a vehicle receives such an incident report, it can request the central authority for the trust level of the originators and the forwarders.

6) Road- and Consensus-Based Approaches: Most of the trust establishment mechanisms in VANET have focused either on entity trust or data trust [89] as the discussions above have shown. However, recently a new perspective of trust establishment in vehicular network has been introduced by Rostamzadeh *et al.* [90]. The authors proposed a Framework for Application-oriented Context-aware Trust-based communication (FACT) for vehicular networks. Instead of computing trust for a node or data, FACT computes trust for a road segment. In essence, FACT applies plausibility checks to the received messages before forwarding it to the downstream. In essence, three conditions are checked, 1) whether the message originated from a trusted road segment, 2) whether the message's integrity was intact throughout its journey in the network, and 3) whether the message suffered from any potential attacks. FACT maintains a database of road segments and their associated trust values. When a trust value is assigned to a road segment instead of vehicles, then it can be assumed that the vehicles in the road segment with higher trust values will be trustworthy and vice versa. This different perspective about trust management is comparable to the original entity trust in some aspects: for instance, whenever a node behaves maliciously in a road segment, the overall reputation of that road segment will be decreased and any kind of messages originating from such segments will not be given the desired trust level and thus not given importance.

In [57] and [91], the authors proposed a MDS which is used to detect and possibly evict malicious and misbehaving nodes in vehicular networks. Most of the uses of an MDS in vehicular networks are based on the mutual cooperation and collaboration among vehicular nodes with help from the infrastructure. However, this cooperation needs to be trustworthy to alleviate the possibility of collusion among malicious nodes. Thus, trust management of the cooperation is essential for the successful operation of MDS. Krishna *et al.* [66] proposed a mechanism to assess the trustworthiness of the collaborating nodes in MDS applications. Krishna *et al.*'s scheme can be divided into two parts namely, MDS and trust evaluation. MDS is employed in vehicular networks and in order to effectively identify the misbehaving nodes, the developed trust management algorithms are used to assess the trust values of the collaborators. Vehicles share their MDS values with each other to have a better perspective of any misbehavior in the system. The proposed system is based on two main approaches. In the first approach, every vehicle calculates the trust value based on its local MDS and then shares it with the neighbors whereas in the second approach, vehicles share only MDS values and then calculate the trust value based on the majority opinion and consensus. Apart from these trust management mechanisms, social-based techniques have also been used in vehicular networks to evaluate the trust of nodes [37]. For instance, Huang *et al.* [92] discussed email-based trust mechanism, and they proposed situation-aware trust in [93], and Hussain *et al.* [37] proposed hybrid trust mechanism for vehicular social networks. In the email-based trust, a trust query is used where each user maintains the trust of its neighbors based on its email interaction with them. It is important to note that the user ranks the neighbors based on the node's interaction with these neighbors through email. Similarly, in the hybrid trust management system, a combined trust based on email and other social interaction among the nodes is proposed. In the recent literature, punishment-based and reward-based approaches are also key enablers to guarantee trustworthiness among nodes in vehicular networks [94]–[96]. In addition to managing trust among cooperating nodes in vehicular networks, the aforementioned punishment-, incentive-, and reward-based approaches also encourage the active cooperation of nodes in vehicular networks. We summarize the existing trust management solutions in vehicular networks in Table II.

7) Blockchain-Based Trust Management in Vehicular Networks: The last few years have witnessed unprecedented development in blockchain technologies and the services provided by blockchain are applicable to many aspects of our lives such as business, finance, engineering, health, food, governance, and so on. In this context, computer networks and cybersecurity are no exception and blockchain is also being explored to solve some of the challenges in these areas. In our context, blockchain technology has been leveraged for trust establishment in vehicular networks. Here we discuss the blockchain-based trust mechanisms in vehicular networks.

Yang *et al.* [97] used blockchain for ensuring data credibility in vehicular networks. Data credibility employs a reputation system that uses the ratings from certain data receivers and then stores these reputations into blockchain blocks. A vehicle is chosen from the crowd that rates the received message and stores it into a block. The selected vehicle then broadcasts the block to the neighbors and the neighbors validate the rating using their local knowledge. If the majority of neighbors agree, then the block is added to the blockchain. Similarly, Yang *et al.* [16] proposed event trust and a reputation system through blockchain that ensures the correctness of shared event information. They proposed a 'proof-of-event' consensus where the roadside infrastructure collects the data which is verified by the vehicles passing by. In essence, the Road-Side Units (RSUs) collect information about a (possible) event on the road and initiate consensus among vehicles about the authenticity of the event. If there is a consensus among the vehicles, then the event information is stored in the blockchain and is shared publicly. Lu *et al.* [54], [98] worked on a privacy-aware anonymous reputation system in vehicular networks using blockchain. In the proposed scheme, anonymous certificate are issued to the vehicles and the actions of the Certification Authority (CA) are recorded in a blockchain. Furthermore, node reputation is calculated using legacy techniques (direct trust and opinions) and the recorded event messages from the senders are stored in a blockchain which are then used by the authorities for misbehavior detection.

Similarly, Yang *et al.* [99] used blockchain technology to establish trust among vehicles. The vehicles use a Bayesian inference model for the received messages and based on the validation results from the model, the receiving vehicle assigns a rating value to the sender and sends it to the nearby RSU. The RSU calculates the trust value based on the received ratings. Then the RSUs collectively and cooperatively embed

TABLE II
COMPARISON OF RECENT TRUST MANAGEMENT SCHEMES IN VANET

Scheme	V2V	V2I	Classification	Type of trust	Approach	Withstanding Attacks
Replace [61]	✓	✓	Cryptographic-based reputation, recommendation	Entity trust	Server-based reputation calculation	False feedback attack, collusion attack
LTT [76]	×	✓	Cryptography-based and Infrastructure(RSU)-based approach	Entity trust	Long-term PKI-based and server-based trust propagation	Malicious collusion and deceit attack
AOT [19]	✓	✓	Cryptographic-based and non-cryptographic-based approach	Entity and content trust	Trust and reputation management	Replay, black-hole, jamming, DoS, and timing attacks
T-VNets [12]	✓	✓	Infrastructure-based inter-vehicle trust and RSU-vehicle trust	Entity trust	Beacons-driven and RSU-aided trust management, dishonest nodes identification and eviction	DoS, jamming, black-hole and collusion attacks
NTF [11]	✓	×	Recommendation propagation and trust evaluation	Entity and content trust	Event messages are used to evaluate trust and nodes can recommend their neighbors	Malicious nodes, recommendation, and false information attacks
HTE [81]	✓	✓	Infrastructure-based non-cryptographic recommendation propagation	Entity trust	hierarchical trust, local trust through V2V and global trust through V2I communications	Not available
STMFL [83]	✓	×	Location verification, past experience and security checks	Entity and content trust	Fuzzy logic-based and fog node-based, using the correctness of information based on security and plausibility check	Malicious nodes and faulty node attack
PGG [85]	✓	×	Network-based cooperation evaluation using evolutionary game theory	Entity trust	Game theory	Not available
GTTM [13]	✓	✓	Direct and indirect trust from vehicles, RSUs, and infrastructure	Entity trust and misbehavior detection	Game theory, attacker-defender game to identify malicious nodes. Majority opinion, betweenness centrality, and node density are considered as game strategies	Collusion attack
ART [89]	✓	×	Trustworthiness of nodes evaluated through malicious behavior detection and data trust evaluated through analytics	Node and entity trust	Functional trust of a node depends on its operation and on how other nodes recommend the node	Compromise nodes, badmouth, and zig-zag attacks
FACT [90]	✓	×	Non-cryptographic spatial trust	Road segment and neighborhood trust	Trust computation for a road segment. Admission process checks if the message came from a trusted location and dissemination selects the trustworthy forwarder	Good mouthing and bad mouthing attacks
CAT [66]	✓	×	Consensus-based MDS-equipped collaborators trust	MDS and node trust	Individual vehicles calculate MDS values for neighbors and share computed values with neighbors. CAT identifies malicious collaborators	Illusion and collusion attacks
HTM [37]	✓	×	Social-based trust propagation	Entity trust	Email-based communication and entity recommendation used to evaluate trust	Not available
PPS [94]	✓	×	Recommendation-based and approval-based	Entity trust	Payment and punishment, trust-based cluster head selection	Not available
DTM^2 [96]	✓	×	Credit-based approach	Entity trust	Tamper-proof device for incentives and punishment	Tampering attack

the trust data into blocks and based on the collective consensus (proof-of-work), store the block in the blockchain. In this scheme, RSUs help maintain trust among the vehicles. The authors also proposed a new consensus algorithm where the RSUs compete for updating the trust values. Khelifi *et al.* [100] addressed the cache management problem in Named Data Networking (NDN)-driven VANET by using a reputation-based blockchain mechanism. The aim is to establish trust among the data consumers and the cache stores in NDN-based VANET. The preceding discussion shows that blockchain has the potential for enabling trust among different entities in vehicular networks.

8) Machine Learning-Based Trust Management in Vehicular Networks: Recently, machine learning-based approaches for secure communications in VANET have emerged. Oubabas *et al.* [101] proposed a clustering algorithm which discovers a community for a given node (vehicle) and assigns a role to the node, either as a member or as a head, based on the similarity of mobility among members of the cluster. Then, the authors proposed a trust update scheme for both data and entity trust. In contrast, Fan *et al.* [102] used a fuzzy C-means clustering algorithm to group the exchanged messages into two clusters, true and false.

Zhang *et al.* [103] proposed a deep reinforcement learning algorithm to find optimal routing paths for packet forwarding in VANET. The algorithm learns the optimal path based on computed trust values of vehicles by maximizing the path trust value. Shams *et al.* [104] designed a trust-aware intrusion detection system which includes a Support Vector Machine (SVM) module to detect malicious behaviors.

This approach, as with [103], utilizes supervised machine learning techniques and needs training before its use which can worsen bootstrapping issues.

9) Miscellaneous Trust Management Techniques in Vehicular Networks: In addition to the techniques mentioned above, there are some other miscellaneous trust management techniques used in VANET. For instance, a privacy-aware data trust mechanism has been proposed by Yeung *et al.* [105]. The scheme is based on popularity counting of an event and the authors used pseudo-identities to preserve the privacy of the event reports. However, the privacy is conditional and the pseudo-identities are subject to revocation in case of any misbehavior. Similarly, Xiao *et al.* [106] used implicit Web of Trust (WoT) to establish trust among communicating nodes in VANET. This trust is then used to select a trustworthy node for cooperation. The use of WoT in VANET was inspired by the webpage ranking algorithm [106]. Based on the ranking algorithm, the authors proposed two algorithms, BayesTrust and VehicleRank. BayesTrust is used to derive the local trust whereas VehicleRank is used to establish global trust for a vehicle. In essence, the number of interactions among vehicles determine the trust level of the neighboring vehicles. Similarly, Sohail *et al.* [107] used three-valued subjective logic to establish trust in a multi-hop communication environment in VANET.

B. Trust Management in Enabling Technologies for Vehicular Networks

Recently, various other enabling technologies such as cloud computing, Software-Defined Network (SDN), social networks, cellular networks, and Device-to-Device (D2D) communication are being integrated with VANET. As a result, new networking paradigms such as Vehicular Clouds (VC), Vehicular Social Network (VSN), Vehicular SDN (VSDN), and cellular-driven VANET have emerged. Here we review the trust management solutions associated with these enabling technologies.

1) Trust in Cloud-Based VANET: Vehicular cloud is an emerging form of vehicular networks where cloud features are leveraged for enhanced applications and services. Trust among different entities is essential and more challenging than traditional VANET [108]. Tang *et al.* [109] designed a trust establishment mechanism for security-related cooperation in vehicular clouds. The trust mechanism leverages two kinds of boards, i.e., a public board that is used for indirect trust among the participating nodes and a private board that is used for maintaining direct trust among nodes. Based on the information from these boards, a trusted path is established that consists of trusted nodes and then cooperative tasks can be performed among the participating nodes. It is worth mentioning that the proposed techniques extend the traditional trust management techniques to vehicular clouds. Similarly, Huang *et al.* [110] focused on the security of computations carried out in the cloud component of vehicular clouds. For this purpose, they proposed a trust management framework to evaluate the trust of the nodes interested in forming vehicular clouds. They also proposed a computation verification mechanism through trust management in vehicular clouds. The trust evaluation mechanism is direct and the vehicles evaluate each other's trust through direct interactions. On the other hand, Alishev *et al.* [36] used social interactions and Analytic Hierarchy Process (AHP) to bootstrap trust among vehicular nodes in both VANET and vehicular clouds. While calculating trust, they consider different factors such as total distance driven and user behavior.

2) Trust in Cellular-Based (5G) VANET: Due to the increasing number of applications and services in VANET and the emergence of autonomous cars, 5G technology is considered to be a suitable candidate for both connected and autonomous vehicles [6], [111]. Here we only focus on trust management in 5G-based VANET. Ortega *et al.* [112] envisioned the integration of Content-Centric Networking (CCN) and permissioned blockchain to establish trust relationship among participating nodes in 5G-based VANET. On the other hand, Cui *et al.* [113] addressed the problem of fast and lightweight authentication in 5G-based VANET. They proposed a reputation system-based approach for message authentication in VANET where high frequency Cooperative Awareness Messages (CAMs) are authenticated based on the reputation of the sender. The trust management solution is centralized wherein a trusted CA is in-charge of the reputation management. Nodes below a certain reputation level cannot get the credentials from the trusted authority for authentication.

It is also worth mentioning that the current cellular networks do not have any concrete mechanism to avoid the fake base station attack due to lack of an authentication mechanism between the User Equipment (UE) and the base station. This lack of authentication is exploited by the attackers to deploy a fake base station and then launch various attacks on the network. A fake base station will have severe consequences in 5G-based VANET. In this context, Hussain *et al.* [114] proposed a trust-aware authentication mechanism in 5G network. This solution complements the security solution already implemented in 5G to secure International Mobile Subscriber Identities (IMSIs)/ International Mobile Station Equipment Identity (IEMIs) through encryption with the network provider's public key. The network service provider is trusted and thus the current solution is built on top of the already established trust. We believe that the same trusted mechanism can be applied to 5G-based VANET as well after taking the VANET characteristics into account. Similarly, Han *et al.* [115] developed a Trust Zone (TZ) for 5G network at the edge cloud where authentication, authorization, and accounting include a trust evaluation mechanism. Moreover, the old trust assumptions in the cellular networks will not be applicable in 5G because technological changes in the 5G network architecture not only introduce network virtualization, but also enable the stakeholders to rent resources. This new development requires new trust solutions in 5G-based VANET. To discuss the need for new trust management mechanisms in 5G, Surridge *et al.* [116] discussed the outcomes of the 5G-ENSURE project that focused on the trust evaluation in a multi-stakeholder system. The outcome of the 5G-ENSURE project includes a tool called it Trust Builder that identifies the security threats to the assets of the system and triggers necessary countermeasures. In the context of 5G-VANET, we believe that multi-stakeholder trust is essential.

3) Trust in Software-Defined and Device-to-Device Communication-Enabled Vehicular Networks: Device-to-Device communication (D2D) and Software-Defined Network (SDN) are two of the cornerstone enabling technologies in 5G networking. The D2D communication feature of the 5G network increases the spectral efficiency and enables V2V communication without any infrastructure whereas SDN enables the separation of control and data planes that enhances the vehicular networks applications. It is, therefore, imperative to enable trust-aware communication among the vehicles in 5G-enabled VANET. In this subsection, we discuss the trust management solutions for the 5G enabling technologies mentioned above which can then be used in VANET. Although D2D provide an efficient communication mechanism for vehicles to communicate without any infrastructure through 5G network, but the selfish and misbehaving nodes must be identified in the network. In this context, Yan *et al.* [117] proposed a trust-oriented peer selection mechanism for D2D communications. The main goal is to avoid non-cooperative nodes in D2D communication scenarios which is the essence in vehicular networks. Yan *et al.* considered three dimensions for trust management, i.e., cognition, emotion, and behavior. In this solution, the authors model cognitive trust, emotion trust, and behavior trust between the message originator and the cooperative users. Using the Naive Bayes technique, the cooperative users are divided into reliable, observed and unreliable users. Similarly, Canepa *et al.* [118] introduced the concept of stereotype where qualities and attributes associated with people are grouped together and people are classified based on those attributes. In this context, the nodes communicating in the D2D environment are also classified into stereotypes and trust values are assigned to them. However, to avoid sharing profiles of the stereotypes among communicating nodes and to avoid a security breach as a result of sharing profiles, the attributes from the profiles are used to generate an encryption key by using attribute-based encryption. This key is later used for secure communication between communicating nodes in D2D communications.

Wang *et al.* [119] used social relationships among nodes to establish and manage trust in D2D environment. One of the salient features of D2D is to provide a relay mechanism for the peer devices. In this context, the selection of right and trustworthy peer is crucial to secure D2D communication. In the presence of social outcasts in the D2D nodes, it is challenging to select the right peers for cooperative communication in D2D environment. Wang *et al.* proposed a physical layer communication-based security approach (using heuristic techniques) to mitigate such threats. In principle, trusted jamming partners are selected in D2D communication to hamper the threats from malicious jammers. We note that such a scenario is naturally true for vehicular communication where the vehicular nodes rely on the cooperation of neighbors in close proximity, and therefore trust among them should be developed and evaluated for secure communication. Similarly, Militano *et al.* [120] also leveraged social-aware trust establishment among communicating nodes in D2D communication for uploading content-based services. The authors developed a coalition formation game among the D2D nodes that are willing to upload content to the base station. The game is played among the uploading nodes with the aim to evict misbehaving nodes and the social interactions of the D2D nodes are taken into account. It is also worth noting that content uploading and downloading is also a normal service in vehicular networks and therefore developing trust relationships in vehicular D2D environment could benefit the secure realization of such applications. A more detailed discussion on trust management in the D2D environment for different applications and services can be found in [121].

Software-Defined VANET (SDVANET) is another area of traditional vehicular networks where scalability, programmability, and flexibility features are applied. As with other vehicular network paradigms, security and trust are essential in SDVANET. Here, we summarize the current research efforts for trust management in SDVANET. In [122], Zhang *et al.* implemented a trust management framework in SDVANET with a frequently used routing protocol, i.e., Ad hoc On-Demand Vector routing (AODV). To establish trust, the authors considered node trust and forwarding ratio. Forwarding ratio is the number of received packets (from an arbitrary sender) to the number of packets forwarded by a node. These packets could be both data and control packets. The authors used variable weights to adjust the trust evaluation mechanism. In the same context, Vasudev *et al.* [123] proposed a trust management mechanism for secure routing in SDVANET. The proposed scheme is the same as that of Zhang *et al.*'s, but the trust verification is carried out by the RSU rather than locally by the node. In contrast, in [124], the authors used blockchain for trust management in SDVANET. In this solution, the authors considered local temporary miners to carry out computations for the blockchain transactions and the miner selection is based on trust evaluation. Trust evaluation takes into account parameters such as link quality, connectivity degree, and the rank of the node. Nodes with higher link quality, increased connectivity, and higher rank are assigned higher trust values and are selected as miners in the blockchain-based SDVANET. In addition to traditional trust management solutions, machine learning-inspired trust management solutions have also recently been proposed for vehicular networks. Zhang *et al.* [125] used a deep learning approach to establish a trusted routing path among the communicating nodes in SDVANET. The authors used Deep Reinforcement Learning (DRL) algorithm through Deep Neural Network (DNN) in the SDN controller to select a trusted routing path. Thus the DL-based method offers both flexibility and trust in selecting the right neighbor for relaying information in SDNVANET. Mahmood *et al.* [126] conducted a short review of trust management schemes in SDNVANET.

4) Trust in Vehicular Social Networks: VSN is a mobile communication system where entities can communicate by exploiting social features inherited from overlaying social structures. Many applications have been developed for users of VSN to share safety information or entertainment related messages. Unlike VANET, VSN is not equipped with hard security measures such as access control and authentication and, therefore, thorough consideration of trust issues in VSN is essential. Since VSN is a form of an Online Social Network (OSN), it is common to adopt trust mechanisms applied in OSN reflecting unique features of VSN such as spatiotemporal mobility of the network.

Yang *et al.* [127] discussed about applying the trust mechanisms from OSN to VSN. They also pointed out some challenges in deploying the models to VSN such as resource-aware information discrimination and efficiency in computing trust. In [128], the authors proposed a trust model based on the three-valued subjective logic trust model (3VSL). 3VSL is popularly adopted to model trust among nodes because it explicitly captures the uncertainty and source trust. The authors then used the OpinionWalk algorithm [129] to compute trust levels of nodes in the network. Iqbal *et al.* [130] surveyed the existing solutions for trust management which can potentially be deployed in VSN including Blockchain-based and fog computing-based trust solutions. The authors described many features (such as context, social relationship, environment, and timeliness) which affect trust levels and thus should be included when designing a trust mechanism in VSN.

5) Trust Management in NDN-Based VANET: Recently, Named Data Networking (NDN) has been leveraged to realize content-centric vehicular networks where content in the vehicular network is given more importance than the source of the content [131]. In this context, trust in the data must be guaranteed in NDN-based VANET. Here we discuss the trust management schemes proposed for NDN-based VANET. It is worth mentioning that trust management in NDN-based vehicular networks is still in its infancy but there are a couple of trust management schemes proposed for NDN-based VANET. Khelifi *et al.* [100] proposed a reputation-based blockchain mechanism for secure caching in vehicular NDN. Their aim is to increase the trust between the content consumers and cache store in vehicular NDN. More precisely, only trusted content is stored in the intermediate node's cache store and the consumers accept only trusted content. The trust values are maintained on a blockchain network. Similarly, Barka *et al.* [132] proposed a trusted communication mechanism for flying ad hoc networks. The underlying principle for trusted communication is the same as in traditional vehicular networks where inter-node trust is established by leveraging historical communication and then the data producer's trust is evaluated. The producer trust is driven by a probabilistic authenticity verification where a fraction of the data producers are authenticated randomly and a trust value is then established for them. We believe that this mechanism can be adapted in NDN-based vehicular networks as well. We also note that some existing papers [133]–[135] have already identified trust issues in NDN which have been already inherited by VANET.

C. Trust-Based Services

In trust-based VANET services, the established trust is used as a by-product to enhance other VANET applications and services such as secure routing, efficient relay selection for message spraying, and information dissemination [64], [90], [136]–[139]. These applications and services use the trust score of the nodes to select suitable relay nodes and routes for information dissemination in VANET. Other such services include trust-based anonymous authentication [113], [140], credential revocation [141], clustering [142], DoS identification [143], and location privacy [144]. Next, we briefly discuss these trust-based services in VANET.

Rostamzadeh *et al.* [90] leveraged trust values to find a shorter and trusted route for information dissemination in VANET. In the proposed solution, the nodes forward the message only to their trusted neighbors and keep the message, otherwise. Whenever a node receives a message, it performs a series of plausibility checks and then based on a locally computed trust value, the message is forwarded to trusted nodes only. The authors reported that the proposed scheme outperforms the traditional routing algorithms in vehicular networks. Similarly, Dahmane *et al.* [136] addressed the relay-selection mechanism in vehicular networks by leveraging trust management. More precisely, they proposed a probabilistic trust mechanism to select relay nodes for information dissemination. They considered multiple parameters such as distance among nodes, stability of the link among nodes, and message reception probability and then the most suitable and trusted nodes are selected as relayers. Furthermore, Kerrache *et al.* [64] proposed a trust-based data delivery framework that also helps in mitigating DoS attacks in VANET. The proposed framework is a hybrid approach which leverages both entity trust and data trust. Similar to Dahmane *et al.*'s scheme, this solution also takes the context of the messages into account. The context information is used to calculate trust for both nodes and the data.

In the same context, Crine *et al.* [137] proposed a trustworthy routing mechanism in VANET. In essence, each routing message is authenticated using symmetric cryptography to stop attackers from manipulating the routing messages. The proposed scheme does not directly use trust establishment, but it assumes the trustworthiness of the components of the system responsible for distributing credentials. Xia *et al.* [139] also designed a trust-driven routing protocol in VANET where two prominent attributes of trust, i.e., subjective trust and recommendation trust are used to determine the trust level of a vehicle. In this protocol design, the authors also used trust-based handoff, and trusted relay selection which further complement the secure routing.

Trust management is also leveraged for authentication among different entities in VANET. Paranjothi *et al.* [138] developed a social trust-based authentication mechanism in VANET. The proposed authentication mechanism is designed for the urban scenario where the probability of communication with neighboring vehicles through social media is higher. More precisely, the trustworthiness of a vehicle's user is assessed through its social media interaction and it is then included in the vehicle's authentication wherein more connected users through social media means higher trustworthiness. Tolba *et al.* [140] and Cui *et al.* [113] also proposed trust-based authentication mechanisms in VANET. Tolba *et al.* used a global server for trust history and vehicle behavior to derive a trust value for a vehicle which is then used in authenticating the vehicle. The authentication mechanism helps in mitigating attacks on the networks. Trust management has also been leveraged for credential revocation [141]. DJamaludin *et al.* used social confidence and a peer evaluation scheme for credential revocation. The current scheme is analogous to the trust mechanism of Pretty Good Privacy (PGP). Similarly, Tian *et al.* [143] proposed an incentive-driven reputation mechanism in vehicular networks to identify DoS attacks, where each vehicle holds an initial capital (incentive) which updates after reporting traffic events. If the event is legitimate, then the vehicle can increase its capital and RSUs assess the legitimacy of the reports otherwise, the vehicle loses the capital. Another similar incentive-driven trust-based location privacy preservation scheme has been proposed by Ying *et al.* [144] where vehicles get incentives to cooperate and change their pseudonyms when operating in a mix-zone. Based on the vehicle's reputation, the other vehicles in the vicinity decide whether to change their pseudonyms for location privacy. In a nutshell, there are many trust-based services in vehicular networks that include most of the vehicular networks' operational requirements.

D. Standardization Efforts for Trust Management in Vehicular Networks

Due to the commercialization of vehicular networks and enabling technologies as well as the availability of 5G networks, the standardization bodies are working toward security and trust management standards. In this context, both the Institute of Electrical and Electronic Engineers (IEEE) and European ETSI have defined a comprehensive set of standards that cover many security aspects in vehicular communications. Hussain *et al.* [111] discussed the existing security standards in VANET in detail. Here, we only focus on the standardization efforts for trust management in VANET. There are two main standards defined by ETSI that define trust-related functions and procedures as follows. *ETSI TS 102 941*[2] is the standard that describes trust management in vehicular network in detail. There are two versions of this standard, i.e., version 1.1.1 (2012-06) and the latest version 1.2.1 (2018-05). This standard defines the relationship among different entities in an ITS network and the trust establishment requirements for ITS. Furthermore, it also defines the maintenance of identities and cryptographic information required for providing security services in ITS. This standard is based on the security architecture defined in *ETSI TS 102 940.*[3] According to this standard, multiple root CAs collaborate together within the same trust model. Proper procedures are defined for different trust management-related functions in ITS along with the required cryptographic primitives in this standard.

V. Future Challenges and Research Opportunities for Trust in VANET

Despite noteworthy progress and research results obtained to date in the trust and reputation management areas for vehicular networks, there are several challenges that still need to be addressed in the future. In this section, we discuss some of these challenges and outline future research directions for the trust establishment and management in VANET.

A. Trust Bootstrapping

Recently proposed trust management solutions assume an arbitrary initial trust value when a node is encountered. There are mainly two trends in the literature. Some schemes assume that upon the first encounter, the recipient node will assign 0 trust to the encountered node while others assume that the first trust value should be 0.5 (assuming that the trust value can be between 0 and 1). However, this assumption does not match the real trust value of the encountered node. The actual trust value might be different from the assumed value based on the node's history. Therefore, it is necessary to compute the real initial trust value of the node. At the moment, some researchers came up with the idea of long-term trust where the long-term trust value is stored at the back-end servers for each node of the network and when a node encounters a new neighbor, in order to obtain its real trust value, the encountering node can query the server about the trust value of the encountered neighbor. Recently another social-based trust bootstrapping mechanism was proposed by Alishev *et al.* [36] where they used Analytical Hierarchy Process (AHP) to calculate the initial trust value. However, more research is needed to compute the precise initial trust value for newly encountered nodes. One possible solution to address this issue could be a hybrid mechanism wherein social-based factors, past history, and cooperation among nodes could be leveraged to bootstrap the trust value for new neighbors.

B. Lifetime of Trust Value/Decay

The lifetime of trust values for neighbors as maintained by every node is another important challenge in vehicular networks. Owing to the characteristics of VANET, vehicles during operation may encounter many other vehicles depending on the duration of its operation. As a result, it will be impossible for them to store the trust values for all encountered nodes in the past. It will require a lot of storage which is not a viable option for vehicles at present. Therefore, an efficient lifetime definition is essential for the neighbors' trust values. In other words, each trust value stored by a particular node must be subject to decay after a specific time period. Here, the characteristics of vehicular networks could be used to decide on the lifetime of the trust value stored locally in the vehicle. For example, the vehicle's movement direction, speed, area of interest, and the frequency of encounters could be used to develop an efficient policy for trust lifetime.

C. Incentives and Audit

Most of the existing trust establishment and management schemes compute trust (local trust through direct interaction and global trust through recommendation) by relying on the cooperation among nodes and/or with the authorities. For such mechanisms to work properly, the nodes must guarantee to avoid freeloaders in the network who do not participate in

[2] https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf

[3] https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

the cooperation process but use the services offered by other benign nodes. In other words, some malicious and selfish nodes may not provide or provide wrong recommendation for their neighbors. Therefore, an audit mechanism is essential to address this issue. Furthermore, efficient incentive mechanisms are needed to stimulate nodes in the network to participate in the combined trust evaluation service [26], [145]–[147]. Incentives mechanisms have been successfully designed for other networks for data ferrying [148] and similar applications. However, because of the non-deterministic characteristics of vehicular networks, current incentive mechanisms will need to be tweaked or new mechanisms should be developed.

D. Reputation Propagation

One of the interesting characteristics of reputation in many online social networks is that it propagates through the network [149]. Similar to the real world where reputation spreads through hearsay, reputation propagates in online networks through connected links. Therefore, it is essential to online users to behave strategically to keep good reputation. For example, since one has limited resources to interact with (or help) others, it is strategically better if one keeps a good relationship with neighbors who have many connected links rather than caring for someone with less connections. However, this strategy is challenging in VANETs because the number of direct connections does not depend on one's ability to be social (or to maintain friendships) but only on opportunistic encounters with passersby. Therefore, in VANETs, we need to develop reputation management mechanisms that motivate members of a network to maintain good reputation.

E. Ephemeral Communications

Vehicular nodes communicate with nodes and with the infrastructure opportunistically which makes VANET communications highly ephemeral. The interconnection time among nodes is unpredictable and this characteristic has a strong impact on trust computation and management. With an ephemeral network such as VANET, the nodes usually interact with a large number of nodes and often for very short periods of time. Therefore, in order to manage an accurate record of trust for a particular node, it is required to spend enough time interacting with that node in the neighborhood. This issue is also indirectly related to the information decay and reputation propagation. In ephemeral networks, the nodes need to have enough storage to store the trust value of all of their neighbors. Furthermore, bootstrapping, and updating, adding, and removing trust value from the storage will incur additional overhead. One possible solution to address this issue could be the implementation of lightweight and scalable data structures such as bloom filters. In addition, the ephemeral nature of VANETs on trust management need further research.

F. End-to-End Trust Management in Enabling Technologies

VANET is integrating with other enabling technologies such as cloud computing, cellular networks, blockchain, IoT, and social networks. Therefore, this integration will not only inherit the security issues and attacks in these technologies but will also introduce new security issues. In this context, Hussain *et al.* [111] identified the security issues faced by the integration of VANET and 5G. Similarly, the integration of VANET with enabling technology will require efficient, intelligent, and effective security and trust management mechanisms that take into account the underlying technologies. We note that trust management is handled differently in different environments. For instance, in VANET both node and data trust are considered, whereas, in resource-constrained environments such as IoT wherein lightweight or centralized trust management solutions are employed, they may not be suitable in a VANET environment. Similar challenges could be faced by cellular networks as well. Therefore, end-to-end trust management mechanisms must be designed to enable the integration of emerging technologies with VANET.

G. Heterogeneity: One Size Does Not Fit All

The integration of enabling technologies with the traditional VANET brings along heterogeneity issues at different levels including architecture, protocols, communication paradigms, and resources. This heterogeneity calls for an adaptive trust management mechanism in different types of VANETs. A single static trust management solution will not work for all types of VANETs. A possible solution could be the inclusion of context information into trust management mechanisms. A context-aware trust management mechanism would invoke the respective trust evaluation with the desired parameters in a particular environment (i.e., clouds, IoT, 5G, and so on). Furthermore, the context information could be extended to the application layer as well where different applications measure trust at different levels.

VI. Conclusion

Trust is one of the pillars of secure communication for the reliable information exchange among entities in networks. In this paper, we have presented a comprehensive review of recently proposed trust establishment and management schemes in VANET. After modeling the taxonomy for trust in VANET, we discussed current trust management mechanisms from different perspectives which include entity-centric, data-centric, aggregation, direct, indirect, game theoretic, and fuzzy logic-based mechanisms. Our review of the current trust management schemes concluded that over the last 5 years, no *new* trust management schemes for vehicular networks have been proposed in the literature. Instead, different variations and combinations of existing approaches have been used. As Internet of Vehicles, Intelligent Transportation Systems, Autonomous vehicles emerge, high quality, trustworthy data becomes even more important for many real-time decisions in the vehicular environment. Research areas of trust management that require further research investigation include the consideration of space-centric trust instead of only entity-centric or data-centric trust management as well as bootstrapping of trust management.

Acknowledgment

The authors would like to thank the reviewers for their valuable comments which helped us to improve the content and presentation of this paper.

References

[1] M. Chaqfeh, A. Lakas, and I. Jawhar, "A survey on data dissemination in vehicular ad hoc networks," *Veh. Commun.*, vol. 1, no. 4, pp. 214–225, Oct. 2014.

[2] H. P. Luong, M. Panda, H. L. Vu, and B. Q. Vo, "Beacon rate optimization for vehicular safety applications in highway scenarios," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 524–536, Jan. 2018.

[3] R. Hussain, S. Kim, and H. Oh, "Traffic information dissemination system: Extending cooperative awareness among smart vehicles with only single-hop beacons in VANET," *Wireless Pers Commun*, vol. 88, no. 2, pp. 151–172, May 2016.

[4] J. Guerrero-Ibáñez, S. Zeadally, and J. Contreras-Castillo, "Sensor technologies for intelligent transportation systems," *Sensors*, vol. 18, no. 4, p. 1212, Apr. 2018.

[5] X. Huang, D. Zhao, and H. Peng, "Empirical study of DSRC performance based on safety pilot model deployment data," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2619–2628, Oct. 2017.

[6] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 111–117, Jan. 2018.

[7] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[8] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Commun.*, vol. 4, no. 7, pp. 894–903, Apr. 2010.

[9] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[10] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[11] S. Ahmed, S. Al-Rubeaai, and K. Tepe, "Novel trust framework for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9498–9511, Oct. 2017.

[12] 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.

[13] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for vehicular Ad hoc networks (VANETs)," *Comput. Netw.*, vol. 121, pp. 152–172, Jul. 2017.

[14] M. A. Javed, S. Zeadally, and Z. Hamid, "Trust-based security adaptation mechanism for vehicular sensor networks," *Comput. Netw.*, vol. 137, pp. 27–36, Jun. 2018.

[15] T. N. D. Pham and C. K. Yeo, "Adaptive trust and privacy management framework for vehicular networks," *Veh. Commun.*, vol. 13, pp. 1–12, Jul. 2018.

[16] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[17] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

[18] S. A. Soleymani *et al.*, "Trust management in vehicular ad hoc network: A systematic review," *J. Wireless Comput. Netw.*, vol. 2015, no. 1, p. 146, Dec. 2015.

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

[20] H. El-Sayed, M. Chaqfeh, H. El-Kassabi, M. A. Serhani, and H. Alexander, "Trust enforcement in vehicular networks: Challenges and opportunities," *IET Wireless Sensor Syst.*, vol. 9, no. 5, pp. 237–246, Oct. 2019.

[21] I. Souissi, "Trust management in vehicular ad hoc networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 31, no. 4, pp. 230–243, 2019.

[22] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proc. IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.

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

[24] J. Zhang, "Trust management for VANETs: Challenges, desired properties and future directions," *Int. J. Distrib. Syst. technol.*, vol. 3, no. 1, pp. 48–62, Jan. 2012.

[25] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2013, pp. 1–6.

[26] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: A survey," *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1812–1827, Jun. 2015.

[27] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287–1309, 2nd Quart., 2016.

[28] M. Gillani, A. Ullah, and H. A. Niaz, "Trust management schemes for secure routing in VANETs—A survey," in *Proc. 12th Int. Conf. Math., Actuarial Sci., Comput. Sci. Statist. (MACS)*, Nov. 2018, pp. 1–6.

[29] L. Eschenauer, V. D. Gligor, and J. Baras, *On Trust Establishment Mobile Ad-Hoc Networks*. Berlin, Germany: Springer, 2004, pp. 47–66.

[30] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012, doi: 10.1007/s11235-010-9400-5.

[31] Y. Wang *et al.*, "CATrust: Context-aware trust management for service-oriented ad hoc networks," *IEEE Trans. Services Comput.*, vol. 11, no. 6, pp. 908–921, Nov. 2018.

[32] S. Tan, X. Li, and Q. Dong, "A trust management system for securing data plane of ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7579–7592, Sep. 2016.

[33] Y. Wang, I.-R. Chen, J.-H. Cho, A. Swami, and K. S. Chan, "Trust-based service composition and binding with multiple objective optimization in service-oriented mobile ad hoc networks," *IEEE Trans. Services Comput.*, vol. 10, no. 4, pp. 660–672, Jul. 2017.

[34] H.-C. Chen, "TCABRP: A trust-based cooperation authentication bit-map routing protocol against insider security threats in wireless ad hoc networks," *IEEE Syst. J.*, vol. 11, no. 2, pp. 449–459, Jun. 2017.

[35] A. Ahmed, K. Abu Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," *Front. Comput. Sci.*, vol. 9, no. 2, pp. 280–296, Apr. 2015.

[36] D. Alishev, R. Hussain, W. Nawaz, and J. Lee, "Social-aware bootstrapping and trust establishing mechanism for vehicular social networks," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.

[37] R. Hussain, W. Nawaz, J. Lee, J. Son, and J. T. Seo, *A Hybrid Trust Management Framework for Vehicular Social Networks*. Cham, Switzerland: Springer, 2016, pp. 214–225.

[38] J. Lee and J. C. Oh, *A Node-Centric Reputation Computation Algorithm on Online Social Networks*. Cham, Switzerland: Springer, 2015, pp. 1–22.

[39] Y. Trofimova, A. M. Moucha, and P. Tvrdik, "Application of neural networks for decision making and evaluation of trust in ad-hoc networks," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 371–377.

[40] W. Song and V. V. Phoha, "Neural network-based reputation model in a distributed system," in *Proc. IEEE Int. Conf. e-Commerce Technol. (CEC)*, 2004, pp. 321–324.

[41] W. Alnumay, U. Ghosh, and P. Chatterjee, "A trust-based predictive model for mobile ad hoc network in Internet of Things," *Sensors*, vol. 19, no. 6, p. 1467, Mar. 2019.

[42] C. T. Nguyen, O. Camp, and S. Loiseau, "A Bayesian network based trust model for improving collaboration in mobile ad hoc networks," in *Proc. IEEE Int. Conf. Res., Innov. Vis. Future*, Mar. 2007, pp. 144–151.

[43] Z. Wei, H. Tang, F. R. Yu, and P. Mason, "Trust establishment based on Bayesian networks for threat mitigation in mobile ad hoc networks," in *Proc. IEEE Military Commun. Conf.*, Oct. 2014, pp. 171–177.

[44] Y. Lindsay Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[45] K. Thirunarayan, P. Anantharam, C. Henson, and A. Sheth, "Comparative trust management with applications: Bayesian approaches emphasis," *Future Gener. Comput. Syst.*, vol. 31, pp. 182–199, Feb. 2014.

[46] M. Yin, J. Feng, and Y. Tang, "An overview on node behavior trust evaluation in ad hoc network," in *Proc. Adv. Wireless Sensor Netw.*, R. Wang and F. Xiao, Eds. Berlin, Germany: Springer, 2013, pp. 631–641.

[47] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Trust modeling and evaluation in ad hoc networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, vol. 3, 2005, p. 6.

[48] A. Jøsang, *Bayesian Reputation Systems*. Cham, Switzerland: Springer, 2016, pp. 289–302.

[49] J. Lee and J. C. Oh, "Convergence of true cooperations in Bayesian reputation game," in *Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Sep. 2014, pp. 487–494.

[50] C. Mao and R. Lin, "QoS trust rate prediction for Web services using PSO-based neural network," in *Proc. Int. Conf. Adv. Cloud Big Data (CBD)*, Aug. 2016, pp. 68–74.

[51] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. M. Gerdes, "Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures," 2019, *arXiv:1903.01541*. [Online]. Available: https://arxiv.org/abs/1903.01541

[52] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[53] R. Hussain and H. Oh, "On secure and privacy-aware sybil attack detection in vehicular communications," *Wireless Pers. Commun.*, vol. 77, no. 4, pp. 2649–2673, Aug. 2014.

[54] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[55] R. Hussain, S. Kim, and H. Oh, "Privacy-aware VANET security: Putting data-centric misbehavior and sybil attack detection schemes into practice," in *Information Security Applications*, D. H. Lee and M. Yung, Eds. Berlin, Germany: Springer, 2012, pp. 296–311.

[56] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7929–7937, Dec. 2015.

[57] S. Ahmed and K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.

[58] 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.

[59] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei, and F. Yang, "A security authentication method based on trust evaluation in VANETs," *J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 59, Dec. 2015.

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

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

[62] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: A lightweight self-organized trust model in VANETs," *Mobile Inf. Syst.*, vol. 2016, Dec. 2016, Art. no. 7628231.

[63] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. 2017.

[64] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs," *Veh. Commun.*, vol. 9, pp. 254–267, Jul. 2017.

[65] C. A. Kerrache, A. Lakas, N. Lagraa, and E. Barka, "UAV-assisted technique for the detection of malicious and selfish nodes in VANETs," *Veh. Commun.*, vol. 11, pp. 1–11, Jan. 2018.

[66] T. R. V. Krishna, R. P. Barnwal, and S. K. Ghosh, "CAT: Consensus-assisted trust estimation of MDS-equipped collaborators in vehicular ad-hoc network," *Veh. Commun.*, vol. 2, no. 3, pp. 150–157, Jul. 2015.

[67] X. Chen and L. Wang, "Exploring trusted data dissemination in a vehicular social network with a formal compositional approach," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jun. 2016, pp. 616–617.

[68] R. S. Bali and N. Kumar, "Secure clustering for efficient data dissemination in vehicular cyber–physical systems," *Future Gener. Comput. Syst.*, vol. 56, pp. 476–492, Mar. 2016.

[69] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Comput. Surv.*, vol. 48, no. 2, pp. 1–40, Oct. 2015.

[70] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in Internet of Things systems," *Comput. Commun.*, vol. 97, pp. 1–14, Jan. 2017.

[71] J. W. Zhang and X. Gu, "Research on trust computation models in wireless sensor networks," in *Manufacturing Technology, Electronics, Computer and Information Technology Applications* (Applied Mechanics and Materials), vol. 687. Zürich, Switzerland: Trans Tech Publications, Dec. 2014, pp. 3007–3010.

[72] U. Jayasinghe, N. B. Truong, G. M. Lee, and T. Um, "RpR: A trust computation model for social Internet of Things," in *Proc. Int. IEEE Conf. Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Jul. 2016, pp. 930–937.

[73] I. T. Javed, K. Toumi, and N. Crespi, "TrustCall: A trust computation model for Web conversational services," *IEEE Access*, vol. 5, pp. 24376–24388, 2017.

[74] J. Guo and I.-R. Chen, "A classification of trust computation models for service-oriented Internet of Things systems," in *Proc. IEEE Int. Conf. Services Comput.*, Jun. 2015, pp. 324–331.

[75] V. B. Reddy, A. Negi, and S. Venkataraman, "Trust computation model using hysteresis curve for wireless sensor networks," in *Proc. IEEE SENSORS*, Oct. 2018, pp. 1–4.

[76] T. Biswas, A. Sanzgiri, and S. Upadhyaya, "Building long term trust in vehicular networks," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.

[77] J. Son, D. Kim, H. Oh, D. Ha, and W. Lee, "Toward VANET Utopia: A new privacy preserving trustworthiness management scheme for VANET," in *Proc. IEEE Int. Conferences Big Data Cloud Computing (BDCloud), Social Comput. Netw. (SocialCom), Sustain. Comput. Commun. (SustainCom) (BDCloud-SocialCom-SustainCom)*, Oct. 2016, pp. 301–308.

[78] B. Koirala, S. S. Tangade, and S. S. Manvi, "Trust management based on node stay time in VANET," in *Proc. Int. Conf. Adv. Comput., Commun. Inf. (ICACCI)*, Sep. 2018, pp. 242–248.

[79] S. Tangade and S. S. Manvi, "CBTM: Cryptography based trust management scheme for secure vehicular communications," in *Proc. 15th Int. Conf. Control, Autom., Robot. Vis. (ICARCV)*, Nov. 2018, pp. 325–330.

[80] C. A. Kerrache *et al.*, "TACASHI: Trust-aware communication architecture for social Internet of Vehicles," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5870–5877, Aug. 2019.

[81] C. A. Kerrache, C. T. Calafate, N. Lagraa, J.-C. Cano, and P. Manzoni, "Hierarchical adaptive trust establishment solution for vehicular networks," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.

[82] N. Bismeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2012, pp. 78–85.

[83] S. A. Soleymani *et al.*, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[84] F. Chiti, R. Fantacci, E. Dei, and Z. Han, "Context aware clustering in VANETs: A game theoretic perspective," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 6584–6588.

[85] S. Shivshankar and A. Jamalipour, "An evolutionary game theory-based approach to cooperation in VANETs under different network conditions," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 2015–2022, May 2015.

[86] Y. Chen, S. Weng, W. Guo, and N. Xiong, "A game theory algorithm for intra-cluster data aggregation in a vehicular ad hoc network," *Sensors*, vol. 16, no. 2, p. 245, Feb. 2016.

[87] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and Q. Han, "A game theory-based trust measurement model for social networks," *Comput. Social Netw.*, vol. 3, no. 1, p. 2, Dec. 2016.

[88] C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, "A trust model for vehicular network-based incident reports," in *Proc. IEEE 5th Int. Symp. Wireless Veh. Commun. (WiVeC)*, Jun. 2013, pp. 1–5.

[89] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[90] 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.

[91] A. Singh and H. C. S. Fhom, "Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection," *Int. J. Inf. Secur.*, vol. 16, no. 2, pp. 195–211, Apr. 2017.

[92] D. Huang, Z. Zhou, X. Hong, and M. Gerla, "Establishing email-based social network trust for vehicular networks," in *Proc. 7th IEEE Consum. Commun. Netw. Conf.*, Jan. 2010, pp. 1–5.

[93] D. Huang, X. Hong, and M. Gerla, "Situation-aware trust architecture for vehicular networks," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 128–135, Nov. 2010.

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

[95] 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.

[96] 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.

[97] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun.(PIMRC)*, Oct. 2017, pp. 1–5.

[98] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 98–103.

[99] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[100] H. Khelifi, S. Luo, B. Nour, H. Moungla, and S. H. Ahmed, "Reputation-based blockchain for secure NDN caching in vehicular networks," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–6.

[101] S. Oubabas, R. Aoudjit, J. J. P. C. Rodrigues, and S. Talbi, "Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme," *Veh. Commun.*, vol. 13, pp. 128–138, Jul. 2018.

[102] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101740.

[103] D. Zhang, F. R. Yu, and R. Yang, "A machine learning approach for software-defined vehicular ad hoc networks with trust management," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[104] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks," *Comput. Secur.*, vol. 78, pp. 245–254, Sep. 2018.

[105] C. Y. Yeung, L. C. K. Hui, T. W. Chim, S.-M. Yiu, G. Zeng, and J. Chen, "Anonymous counting problem in trust level warning system for VANET," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 34–48, Jan. 2019.

[106] Y. Xiao and Y. Liu, "BayesTrust and VehicleRank: Constructing an implicit Web of trust in VANET," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2850–2864, Mar. 2019.

[107] M. Sohail, L. Wang, S. Jiang, S. Zaineldeen, and R. U. Ashraf, "Multi-hop interpersonal trust assessment in vehicular ad-hoc networks using three-valued subjective logic," *IET Inf. Secur.*, vol. 13, no. 3, pp. 223–230, May 2019.

[108] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 284–294, Mar. 2013.

[109] Z. Tang, A. Liu, Z. Li, Y.-J. Choi, H. Sekiya, and J. Li, "A trust-based model for security cooperating in vehicular cloud computing," *Mobile Inf. Syst.*, vol. 2016, pp. 1–22, Oct. 2016.

[110] C. Huang, R. Lu, H. Zhu, H. Hu, and X. Lin, "PTVC: Achieving privacy-preserving trust-based verifiable vehicular cloud computing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[111] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G Security: A review of design and implementation issues," *Future Generation Comput. Syst.*, vol. 101, pp. 843–864, Dec. 2019.

[112] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.

[113] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6417–6428, Aug. 2019.

[114] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "Insecure connection bootstrapping in cellular networks: The root of all evil," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*. New York, NY, USA: ACM, 2019, pp. 1–11.

[115] B. Han, S. Wong, C. Mannweiler, M. Dohler, and H. D. Schotten, "Security trust zone in 5G networks," in *Proc. 24th Int. Conf. Telecommun. (ICT)*, May 2017, pp. 1–5.

[116] M. Surridge *et al.*, "Trust modelling in 5G mobile networks," in *Proc. Workshop Secur. Softwarized Netw., Prospects Challenges (SecSoN)*. New York, NY, USA: ACM, 2018, pp. 14–19.

[117] J. Yan, D. Wu, S. Sanyal, and R. Wang, "Trust-oriented partner selection in D2D cooperative communications," *IEEE Access*, vol. 5, pp. 3444–3453, 2017.

[118] G. Huerta-Canepa, "An encryption scheme based on trust for device-to-device communication on 5G," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2015, pp. 360–362.

[119] L. Wang, H. Wu, L. Liu, M. Song, and Y. Cheng, "Secrecy-oriented partner selection based on social trust in device-to-device communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7275–7279.

[120] L. Militano, A. Orsino, G. Araniti, M. Nitti, L. Atzori, and A. Iera, "Trust-based and social-aware coalition formation game for multihop data uploading in 5G systems," *Comput. Netw.*, vol. 111, pp. 141–151, Dec. 2016.

[121] M. Nitti, G. Stelea, V. Popescu, and M. Fadda, "When social networks meet D2D communications: A survey," *Sensors*, vol. 19, no. 2, p. 396, Jan. 2019.

[122] D. Zhang, F. R. Yu, Z. Wei, and A. Boukerche, "Software-defined vehicular ad hoc networks with trust management," in *Proc. 6th ACM Symp. Develop. Anal. Intell. Veh. Netw. Appl. (DIVANet)*. New York, NY, USA: ACM, 2016, pp. 41–49.

[123] H. Vasudev and D. Das, "A trust based secure communication for software defined VANETs," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2018, pp. 316–321.

[124] Y. Yahiatene and A. Rachedi, "Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–7.

[125] D. Zhang, F. R. Yu, R. Yang, and H. Tang, "A deep reinforcement learning-based trust management scheme for software-defined vehicular networks," in *Proc. 8th ACM Symp. Design Anal. Intell. Veh. Netw. Appl. (DIVANet)*. New York, NY, USA: ACM, 2018, pp. 1–7.

[126] A. Mahmood, W. E. Zhang, Q. Z. Sheng, S. A. Siddiqui, and A. Aljubairy, *Trust ManagementTrust Management for Software-Defined Heterogeneous Vehicular Ad Hoc NetworksVehicular Ad hoc Networks*. Cham, Switzerland: Springer, 2019, pp. 203–226.

[127] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 42–47, Aug. 2015.

[128] T. Cheng, G. Liu, Q. Yang, and J. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 652–663, Mar. 2019.

[129] G. Liu, Q. Chen, Q. Yang, B. Zhu, H. Wang, and W. Wang, "OpinionWalk: An efficient solution to massive trust assessment in online social networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, May 2017, pp. 1–9.

[130] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social Internet of Vehicles: Factors, challenges, blockchain, and fog solutions," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, 2019, Art. no. 1550147719825820.

[131] H. Khelifi *et al.*, "Named data networking in vehicular ad hoc networks: State-of-the-art and challenges," *IEEE Commun. Surveys Tuts.*, to be published.

[132] E. Barka, C. Kerrache, R. Hussain, N. Lagraa, A. Lakas, and S. Bouk, "A trusted lightweight communication strategy for flying named data networking," *Sensors*, vol. 18, no. 8, p. 2683, Aug. 2018.

[133] H. Khelifi, S. Luo, B. Nour, and S. C. Shah, "Security and privacy issues in vehicular named data networks: An overview," *Mobile Inf. Syst.*, vol. 2018, pp. 1–11, Sep. 2018.

[134] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 566–600, 1st Quart., 2018.

[135] E. G. Abdallah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1441–1454, 3rd Quart., 2015.

[136] S. Dahmane, C. A. Kerrache, N. Lagraa, and P. Lorenz, "WeiSTARS: A weighted trust-aware relay selection scheme for VANET," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[137] P. Cirne, A. Zquete, and S. Sargento, "TROPHY: Trustworthy VANET routing with group authentication keys," *Ad Hoc Netw.*, vol. 71, pp. 45–67, Mar. 2018.

[138] A. Paranjothi, M. S. Khan, S. Zeadally, A. Pawar, and D. Hicks, "GSTR: Secure multi-hop message dissemination in connected vehicles using social trust model," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100071.

[139] H. Xia, S.-S. Zhang, Y. Li, Z.-K. Pan, X. Peng, and X.-Z. Cheng, "An attack-resistant trust inference model for securing routing in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7108–7120, Jul. 2019.

[140] A. M. R. Tolba, "Trust-based distributed authentication method for collision attack avoidance in VANETs," *IEEE Access*, vol. 6, pp. 62747–62755, 2018.

[141] C. I. Djamaludin, E. Foo, S. Camtepe, and P. Corke, "Revocation and update of trust in autonomous delay tolerant networks," *Comput. Secur.*, vol. 60, pp. 15–36, Jul. 2016.

[142] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, "Trust-based secure clustering in WSN-based intelligent transportation systems," *Comput. Netw.*, vol. 146, pp. 151–158, Dec. 2018.

[143] Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: A novel reputation framework for identifying denial of traffic service in Internet of Connected vehicles," 2019, *arXiv:1902.03994*. [Online]. Available: http://arxiv.org/abs/1902.03994

[144] B. Ying and D. Makrakis, "Reputation-based pseudonym change for location privacy in vehicular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7041–7046.

[145] A. Mislin, L. V. Williams, and B. A. Shaughnessy, "Motivating trust: Can mood and incentives increase interpersonal trust?" *J. Behav. Experim. Econ.*, vol. 58, pp. 11–19, Oct. 2015.

[146] H. Mousa, S. B. Mokhtar, O. Hasan, O. Younes, M. Hadhoud, and L. Brunie, "Trust management and reputation systems in mobile participatory sensing applications: A survey," *Comput. Netw.*, vol. 90, pp. 49–73, Oct. 2015.

[147] Q. Xu, Z. Su, S. Yu, and Y. Wang, "Trust based incentive scheme to allocate big data tasks with mobile social cloud," *IEEE Trans. Big Data*, to be published.

[148] T. Ning, Y. Liu, Z. Yang, and H. Wu, "Incentive mechanisms for data dissemination in autonomous mobile social networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3084–3099, Nov. 2017.

[149] G. Haralabopoulos, I. Anagnostopoulos, and S. Zeadally, "Lifespan and propagation of information in on-line social networks: A case study based on Reddit," *J. Netw. Comput. Appl.*, vol. 56, pp. 88–100, Oct. 2015.

Rasheed Hussain (Senior Member, IEEE) is currently working as an Associate Professor and also the Director of the Institute of Information Security and Cyber-Physical Systems, Innopolis University, Innopolis, Russia. He is also the Director of the Networks and Blockchain Lab, Innopolis University. His research interests include information security and privacy, vehicular ad hoc networks (VANETs), vehicular clouds, and vehicular social networking, applied cryptography, the Internet of Things, content-centric networking (CCN), cloud computing, blockchain, and machine learning in cybersecurity. He is an ACM Distinguished Speaker, a member of ACM, and a Certified Trainer for the Instructional Skills Workshop (ISW).

Jooyoung Lee received the Ph.D. degree from Syracuse University in 2014. She was also a Visiting Scholar with the Korea Advanced Institute of Science and Technology (KAIST) and also with the Polytechnic University of Milan (PoliMi). She was with Innopolis University, Russia. She is currently a Lecturer with the Research School of Computer Science, The Australian National University. Her recent research interests include quantifying online social movements, predicting outcomes of online engagements, trust/reputation management, and vehicular ad-hoc networks.

Sherali Zeadally received the bachelor's degree in computer science from the University of Cambridge, U.K., and the Ph.D. degree in computer science from the University of Buckingham, U.K. He is currently an Associate Professor with the College of Communication and Information, University of Kentucky. His research interests include cybersecurity, privacy, the Internet of Things, computer networks, and energy-efficient networking. He is a fellow of the British Computer Society and the Institution of Engineering Technology, U.K.