A survey of trust management in the Internet of Vehicles

Amal Hbaieb, Samiha Ayed, Lamia Chaari

A Survey of Trust Management in the Internet of Vehicles

Amal HBAIEB[a,b,c], Samiha AYED[a], Lamia CHAARI[c]

[a] *University of Technology of Troyes, LIST3N-ERA, Troyes, France*
[b] *National School of Electronics and Telecommunications of Sfax, Sfax, Tunisia*
[c] *CRNS-SM@RTS (Laboratory of Signals, systeMs, aRtificial Intelligence and neTworkS), Sfax, Tunisia*

Abstract

In recent years, the emergence of the Internet of Vehicles (IoV) aims to enhance the users' quality of experience through proposing more sophisticated services ranging from guaranteeing the user safety to improving his comfort. The IoV ecosystem is complex, heterogeneous, and evolving. Many entities participate to compose its architecture (such as vehicles, humans, roadside units, ITS). Moreover, different communication types co-exist to ensure the IoV connectivity and continuity. This diversity leads to new security requirements that seem more complex to take into account and enlarge the attack surface of such ecosystem. Many security mechanisms should be considered to enforce the security of IoV environment at many levels: data, entities, communications, storage, etc.. Trust management is one of the potential security mechanisms that aims to increase the reliability within the IoV environment. The topic has been widely explored within the vehicular ad hoc networks (VANETs). However, the VANET represents only one component of the IoV ecosystem. Thus, the approaches proposed for the VANET should be adapted to be applied for the IoV. Moreover, the advent of the emerging technologies like Blockchain, Cloud, SDN as well as artificial intelligence bring new opportunities to propose more relevant approaches within the trust management mechanisms within the IoV context.

Email addresses: amal.hbaieb@utt.fr (Amal HBAIEB), samiha.ayed@utt.fr (Samiha AYED), lamiachaari1@gmail.com (Lamia CHAARI)

Accordingly, this survey deals with the literature about the trust management topic in vehicular environments. The scope considers the IoV environment as well as the relevant approaches proposed for the VANET context since it is one of the important component of the IoV ecosystem. We start by quickly reviewing the existing surveys about security of the vehicular environments. Then, we give a general overview about trust concepts. Afterwards, we present the security and trust challenges and attacks in the vehicular context. Later, we classify and compare the most relevant approaches related to the trust management for the IoV proposing a new taxonomy. We complete this survey by highlighting the open future directions and perspectives for research.

Keywords: Vehicular networks, VANET, IoV, V2X, Trust management, Security, Blockchain

1. Introduction

The transition to connected and automated driving is accelerated by cross-sectors synergies with enablers such as IoT (Internet of Things), HPC (High Performance Computers), AI (Artificial Intelligence), 5G/6G, data driven engineering, as well as robotics. In this mobility context, the IoV paradigm brings new services and usages that reinforce the transformation towards automation. The adoption of these technologies aims mainly to make driving more secure and enhance the users' quality of experience. However, the deployment of multiple technologies that interact with each other brings out big security and privacy challenges. Indeed, it enlarges the attack vectors and surface (LiDAR, hotspot, OBD port, ECU, cameras, TPMs, GPS, etc.). In the IoV ecosystem, cybersecurity issues can be driven from the security of communication links, security of devices, identity and liability, access control, privacy of drivers and vehicles and overall information systems security. It is obvious that the protection of the IoV systems against the cyber attacks that compromise their operation is mandatory to ensure the safety of their users. For that, many security mechanisms could be applied to reinforce the IoV security. One of the largely explored

mechanisms is the trust management. Many research works exist in literature to bring innovative approaches of integrating the trust management within vehicular environment. This survey focus on these works to help the reader having an easy entry point to the topic and be updated with the last innovations about the use of artificial intelligence and emerging technologies for deploying the trust management within a vehicular context. In the following, we introduce the IoV context, the trust management concept, as well as our survey contributions and methodology.

1.1. From ITS to autonomous vehicles

The automotive industry is a significant component of economic benefits. In recent years, transportation systems are growing quickly, and there is always a strong motivation for more proficient transport systems. The cooperation with the Information and Communication Technologies (ICT) sector has created a propelled digital transformation in the automotive domain; towards more Intelligent Transportation Systems (ITS). Initially, the VANET represents an adhoc network defined between a set of vehicles. The VANET nodes may join or leave the network depending on their position and connectivity. The definition of VANET is mainly related to the vehicles representing the topology nodes. The VANET applications are mainly focusing on traffic management and congestion monitoring based on a communication between the vehicles and the road side units. Later on, the advent of the IoT, consisting on different devices and technologies, leads to evolving from the VANET to the IoV. Indeed, the IoT paradigm [1][2], with the help of big data, Cloud computing as well as artificial intelligence [3] promotes the proliferation of , among others, smart cities, intelligent transportation and e-health domains. In addition to the vehicle's networking aspect already existing in the VANET, the IoV focuses on the vehicle's intelligence. The IoV [4] extends the safety-related applications, already proposed by the VANET, to more sophisticated applications such as payment services, advanced infotainment services, crash prevention, traffic and crash response, etc.. For that, the IoV integrates the communications between vehicles,

infrastructures, the internet and people. These communications are known as Vehicle-to-everything (V2X) communications. The term V2X is used to refer in general Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Road (V2R), Vehicle-to-Human (V2H), Vehicle-to-Sensor (V2S), Vehicle-to-Cellular (V2C), and V2-Internet data exchange [5]. To facilitate the deployment of IoV applications, different standardization bodies have devoted efforts into specifying wireless technologies with extensive enhancements that detail new opportunities of IoV and V2X-enabled vehicles (e.g., WAVE-DSRC and cellular V2X technologies)[6][7]. The IoV applications need in many cases real time responses like in the case of crash response or payment services. To enhance the connectivity and to ensure prompt data exchange among the IoV ecosystem, many efforts have been proposed. As example, the Institute of Electrical and Electronics Engineers (IEEE) has proposed, specified and developed the WAVE (Wireless Access in Vehicular Environments) standard within the IEEE 1609 family of standards. Many working groups are focusing on different levels of the WAVE standard : architecture and services of WAVE devices (IEEE 1609.0-2013, [8]), security (IEEE 1609.2b-2019, [9]), MAC and physical layers access (IEEE 1609.4-2016, [10]). Besides, the dedicated short-range communications (DSRC) standard [11] has been proposed as a technology to be used for the V2V communications and for the communications between vehicles and the roadside units. This standard is widely deployed in many country like the USA. The layered architecture for DSRC communication is mainly based on IEEE (IEEE 1609.2, IEEE 1609.3, IEEE 1609.4, IEEE 802.2, IEEE 802.11p) and SAE (J2735, J2945.1) standards. Other recent projects proposed enhancement concerning the communication technologies within the IoV ecosystem. For example, the 3GPP project (3rd Generation Partnership Project) [12] proposed new technical specifications and requirements of Cellular V2X based on a 4G-LTE network. Despite of the increasing evolution of the IoV paradigm, the research and industry domains are also interested on evolving the autonomous driving domain based on vehicles that are able to guide themselves across different driving situations without human intervention. With this innovation

comes the responsibility of having giant capabilities that imitate human reflexes and behaviour [13]-[16]. We break this into three main features: massive amount of data perception, purposeful decisions planning, and intended tasks control. Connected and autonomous vehicles are getting more consumers allure and providing an important business opportunity for players in the auto industry. Accordingly, automotive stakeholders and technology service providers are ramping their product segments from design needs, consumers views, and customized offerings, to maintain the pole position with best success prospects in this trend market and make these services as much as widespread and affordable for consumers in innovative ways. Actually, many projects are ongoing on autonomous connected vehicles and are resulting in several new scenarios like the European project EU LSPAUTOPILOT [17]. Figure 1 shows IoV underlying system architecture and contributing technologies towards V2X. Table 1 lists acronyms used throughout this paper.

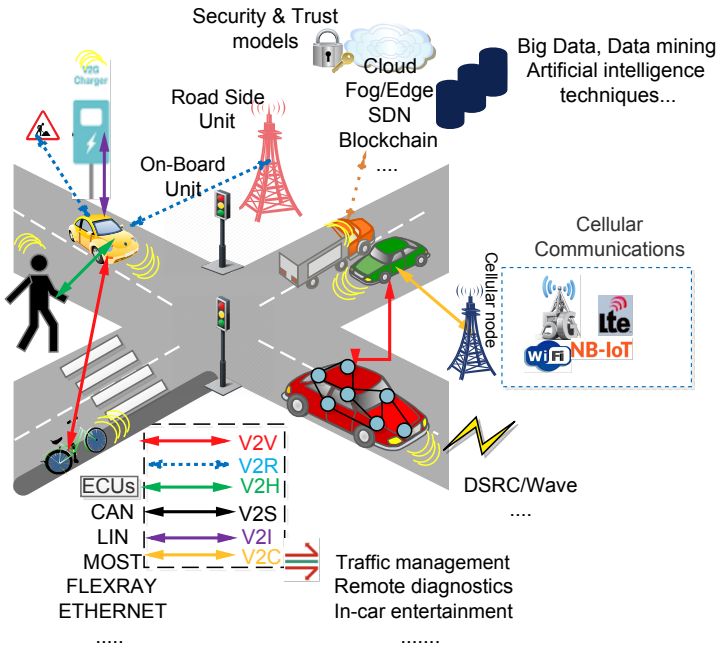

Figure 1: Overall IoV communication system architecture

Table 1: *List of acronyms*

Acronym	Full-form
ICT	Information and Communication Technologies
IoT	Internet of Things
IoV	Internet of Vehicles
VANET	Vehicular Ad-Hoc Network
V2X	Vehicle-to-X
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2R	Vehicle-to-Road
V2S	Vehicle-to-Sensor
V2H	Vehicle-to-Human
V2C	Vehicle-to-Cellular
ECU	Electronic Control Unit
CAN	Controller Area Network
LIN	Local Interconnect Network
MOST	Media Oriented Systems Transport
ADAS	Advanced Driver Assistance Systems
WAVE	Wireless Access in Vehicular Environments
DSRC	Dedicated Short Range Communication
QoS	Quality of Service
PKI	Public Key Infrastructure
SDN	Software-Defined Networking
DST	Dempster Shafer Theory
SVM	Support Vector Machine
NDN	Named Data Networking

1.2. Trust management in vehicular networks

The V2X paradigm brings more security concerns that arise from its specific characteristics (e.g., high mobility, highly dynamic topology, environment density, QoS constraints, etc.) and may lead to serious road hazards (e.g., accident, incident, or congestion). The use of this new generation of ITS framework remains cautious and suspicious as vehicular networks become a further open access environment that gets more exposed to attackers. Indeed, four measurements in which attackers can be categorized: (1) Insider/outsider attackers, (2) malicious/rational attackers, (3) local/extended attackers, and (4) active/passive attackers. In addition vehicular networks users dread infringement of their protection and revelation of their data. Besides, it is of paramount

importance for users to make sure of received data (further data source) reliability before using it. However, traditional security mechanisms may not tackle all these issues and provide comprehensive protection in current IoV scenarios (e.g., anonymous authentication with, data quality assessment, sender credibility verification, dishonest node revocation, attacks detection, etc.). For instance, cryptographic-based approaches cannot serve for credibility assessment. In a nutshell, we remind conventional security requirements to be looked upon, such as integrity, confidentiality, availability, authentication, and non-repudiation. Certain other specifications might be also appended, depending on IoV requirements in a given context, like auditing in terms of services tracking and control, and trustworthiness since non-trustworthy entity may rise malice actions. Noting that trustworthiness is required particularly within autonomous driving context (as a concrete example, within cooperative perception scenario [18]). It is therefore of paramount importance to organize trust in such environment and distinguish dishonest entity from trustworthy. Accordingly, trust-based schemes are additionally needed to assist in effective vehicular network deployment. It is further worth noting that intra-vehicle communications security must also be handled [19]. Trust management refers to a set of steps where a node trying to assign a trust degree to another node during their interaction. In other words, the trust factor is a characteristic measured by a trustor node as a quantified belief, and a trustee node (i.e., host node), in order to mitigate the bad effects of malicious and selfish nodes actions. We need to consider misbehaving and selfish nodes jointly. Yet, the segregation between the meaning of these two terms is nevertheless helpful and beneficial. The node which generally aims at intentionally leaving other entities' ordinary behaviour is known as a misbehaving node. It consists usually in the willingness to spread disperse and inject falsified, malicious or fake data, or reach a deny services, while transmission. Whereas, a node is termed selfish once it seeks to attempt one's proper interest and looks at obtaining a benefit that can be served at the expense of other nodes. From the intuitive segregation of definitions, we could draw that a malicious node is considered selfish, for instance, once its behaviour refers to benefit a rise mu-

tual resources utilization (e.g., bandwidth coverage) while declining sharing its owns (referred rather a greedy node), or its actions are uttered, for example, in prevailing the higher communication quality (called also strategic node). Other behaviour that corresponds to seek harm is considered malicious. In addition, we can refer some trust related attacks like bad-mouthing attack (entity attack), on-off attack (service attack), and black hole attack (route attack). Moreover, the trust factor can be used as a by-product to improve vehicular networks services like routing [20], relay selection and information dissemination [21][22]. Hence, trust management is a significant pillar in vehicular security services, and thus a formidable challenge encountered by vehicular networks. Having briefly defined related trust notions, we point out also the importance of its overall properties (generally defined in regard to used metrics (subsection 2.1)). The trust proprieties can be summarized in direct vs. indirect trust, local vs. global trust, dynamic trust, asymmetric trust, subjective vs. objective trust, history-based trust, and context-based trust. Over the past few years, extensive research efforts have been put to build trust in general ad-hoc networks. Yet, effective trust-based approaches for vehicular networks context require ongoing research, mainly within V2X environment and autonomous driving vehicles context, where it is necessary, while designing, to accommodate related imperatives (e.g., QoS satisfaction). In fact, different QoS-related performances aspects and requirements like robustness, dynamicity, scalability, autonomy (e.g., auto-configuration, and auto-optimization), complexity, communication overhead, and resource constraints (e.g., energy consumption) should be more considered in trust-based vehicular networks realization. The main intent is to reach better secure Quality-of-Experience for V2X services users.

1.3. Contribution and survey organization

This article is meant mainly to serve as a brief survey on trust management in vehicular networks. Despite the grow interest in this topic, dedicated surveys are somewhat limited. In fact, we could not find different related surveys that address trust management in vehicular networks in a holistic way. In

contrast to published past surveys, we highlight in this paper the types of the proposed solutions for managing trust in vehicular networks. Hence, we provide our classification for these approaches based on used tools which include artificial intelligence-enabling techniques and emerging technologies. Our paper exposes first an overall view about basic trust notions and phases. Then, it provides recent vehicular networks dedicated survey papers. Next, the paper presents major security and trust management challenges in the realm of vehicular communications. Thereafter, the paper reviews some trust management approaches within vehicular networks. The contribution of this survey consists of a new taxonomy of approaches taxonomy, according to used tools. The paper expands a little by discussing in short the efficiency of surveyed solutions, and giving future directions for trust management in vehicular networks. In sum, the paper covers the following points: (1) Introduction of main concepts for trust establishment, (2) Exposition of recent existing surveys on vehicular networks, (3) Identification of major security and trust challenges in vehicular networks, along with some related possible attacks, (4) New classification of recent trust management approaches in vehicular networks, (5) Discussion of the reviewed approaches efficiency, and (6) Overview of IoV trust management future directions. The article organizational structure is presented in Figure 2 with a top-down layout. To define the paper context and the key driving motivations behind this work, we describe at the beginning the evolution of the automotive communication systems from ITS toward autonomous driving technology, then, we exhibit the importance of security in this field, where we outline the requirement of building trust for V2X. Also, we discuss the research methodology in this paper. Section 2 presents an overview of basic trust concepts. Section 3 provides recent existing surveys on vehicular networks. Section 4 emphasizes on major security and trust challenges for IoV as well as their potential attacks. Section 5 introduces our taxonomy for the recent proposed trust management approaches in vehicular networks. Section 6 discusses briefly reviewed approaches. Section 7 presents some future directions for trust management in IoV. Finally, Section 8 concludes the survey.

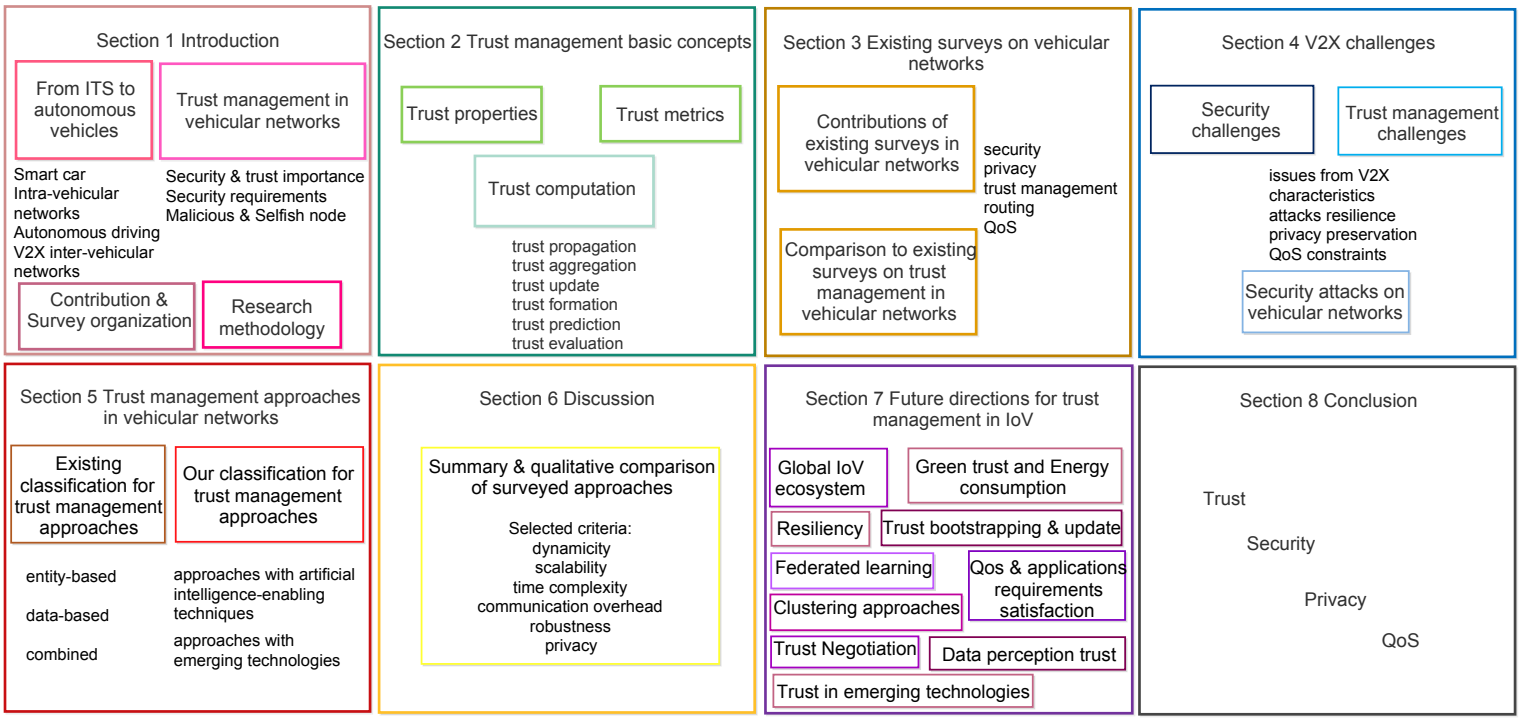

Figure 2: Survey paper organization

1.4. Research methodology

The main objective of this article is to identify, classify, analyze, and synthesis the research papers on the security and particularly the trust management in vehicular networks, to provide a summary of the works done in this field. First, we establish a strategy for selecting the relevant papers. Accordingly, we present in this subsection the methodology adopted to conduct the selection of the works to be included in our survey. Our literature search comprises the definition of search strings, source bases, and inclusion and exclusion criteria. Furthermore, defining the research questions is significant in reflecting the purpose of the survey and the importance of the papers to be chosen. The research questions to be answered for our study are the following:

- What are the common concepts for the trust management in the litera-

ture?

- What are the metrics used to assess the trust?
- What are the adopted tools in trust management?
- How we can classify the trust approaches based on the used tools to later interpret their efficiency?

We considered different search criteria as exclusion criteria in the activity of papers selection. Hence, the papers not related to the defined research questions, and did not present scientific contributions on security aspect in vehicular networks context were excluded. The selected search criteria correspond mainly to the year of publication, the citations number.

1.4.1. Search string & source bases

The relevant selection of keywords is crucial to ensure the identification of the vital papers useful to answer the defined research questions. We started by applying the main search terms to extract the preferred results. Initially, we proceeded a broad search for papers on Google Scholar and IEEE Xplore Digital Library using "Trust" + "VANET"+ "vehicular networks" as keywords. We received an excellent coverage of related papers. The amount of obtained papers was about 415 on IEEE Xplore Digital Library. The search results denoted also that "reputation" represents a main term related with "trust". However, to treat the massive results and find vital new articles, we reformulated the keywords to be "trust management" + "internet of vehicles" + "vanet" + "reputation". This served to provide us enough relevant papers. The second set of keywords focused on the adopted tools in trust management within the vehicular context. We used the following search queries:

- "trust" + "vehicular network" + "internet of vehicles" + "reputation" + {"machine learning" or "Cloud" or "Edge" or "Fog" or "SDN" or "Blockchain"}

1.4.2. Inclusion and exclusion criteria

As previously mentioned, inclusion and exclusion criteria serve as an important way to extract relevant papers to our survey. The main conditions to select exhibited papers correspond to the year of publication and the number of citations. The use of demographics filter was to realize and assess the evolution of the trust management concept over time, as well as to include the recent papers in case of multiple works introducing very similar schemes. The rational behind considering the number of citations was that we believe that papers having high citations have more impact and pertinent scientific potential. Nevertheless, for papers published from 2018, this criteria was not necessarily applied, since these works are considered recent. We raised also some questions related to conducted experiments to further decide the papers' quality (e.g., the experiments were properly explained?, Does experiments support the suggested idea in the paper?). With these criteria, we selected the papers having acceptable number of citations (with an average of 5 citations per paper) in different relevant databases, from 2008 to present.

2. Trust management basic concepts

Trust management mechanisms are widely deployed to secure network environments. However, this concept has been initially defined in other contexts. To understand the trust management approaches presented in this survey, we start by giving a simple definition of the trust concept. First of all, trust is different from trustworthiness that consists on the quality of being reliable. Moreover, trust can also be confused with reputation. It is important to note that in the network environments, the reputation of a specific node is the opinion that can be built on that node based on the recommendations of other network nodes (direct or indirect neighbours). These recommendations are mainly deduced based on previous exchanges with the node and considered as a feedback about the node behavior during the past. Concerning the trust concept, it is closely related to its application domain and the associated discipline. Considering the

sociology domain, the trust meaning is associated to persons and represents one of the values to build the social relationships. From another point of view, in the psychology discipline, the trust concept represents a relation between two persons the trustor and the trustee. The trustor will believe that the trustee will do exactly what is expected. The trust relationship leads to a security and optimism feeling if it succeeds, otherwise, it leads to insecurity and mistrust feelings. In psychology, trust can be impacted by the life experiences and it cannot be regained if lost. The trust concept has also been so attractive to secure networks within the computer science domain. In this context, the trust is associated to the network entities or nodes. It represents the probability of a node to be honest. When this probability is lower than a threshold, then the node could be considered malicious. This subjective probability can vary from 0 when the node is completely distrusted to 1 when the node is completely trusted. When considering the IoV ecosystem, the trust concept is applied to all the entities composing the IoV environment (vehicles, devices, humans, infrastructure entities)

2.1. Trust properties

The trust may have many properties. To deal with them, we consider that the trust is a relationship between the two entities: a trustor and a trustee. The trustor is the entity that has trust on the trustee. The trustee is the entity that is considered as trustworthy. The properties of trust can be defined as follows:

- Direct: when the trust value is calculated based on the direct relationship between the trustor and the trustee.
- Indirect: when the trust value is calculated based on the recommendations propagated from different neighbours to the trustor.
- Subjective: when the trust is calculated based on a personal opinion of the trustor.
- Objective: when the trust is calculated based on well known parameters about the trustee entity.

- Local: when the trust value is only available for the trustee and the trustor. The value can not be propagated across the network.
- Global: each entity within the network has a unique trust value known by all network entities.
- Asymmetric: when an entity x give trust on an entity y, nevertheless, y does not give trust on x.
- History-dependent: when the trust is determined based on past behaviors.
- Context-dependent: the trust value is related to some contextual conditions (related to the network environment for example) or events.
- Composite: when the trust value is based on different parameters such as security, honesty, etc.
- Dynamic: when the trust value can be updated with time if any change occurs on the parameters (for example the network topology). used to calculate the initial trust value.

2.2. Trust metrics

A holistic view on the proposed trust management approaches shows that different metrics are applied (rather in different ways) for trust measurement and evaluation. According to the related state-of-the-art, trust computation includes the following typical metrics:

- Reputation-based metrics: in this case the trust value is based on the recommendations given about a specific node within the network. The network nodes may share the same opinion about a node that is propagated within the network. In this case, we are considering a major opinion or a global feedback about that node.
- Knowledge-based metrics: the trust value is calculated based on a direct or a past experience that a node has or got with a specific node. These

metrics can be useful for example to detect the selfish nodes within the network.

- Expectation-based metrics: in this case the node will calculate the trust of another node based on how it is expecting that node behavior. Its expectation may rely on its history with that node, on received recommendations or only on an initial prediction when no previous communication exists with that node.

- Node properties-based metrics: in this case, the trust formula is mainly based on a set of node properties like speed, direction, resource availability, etc.

- Proximity-based metrics: in this case, the trust calculation uses the main parameters of proximity with the considered node such as the time, the location as well as the distance.

- Environment factors-based metrics: in this case, the trust formula includes some environment parameters or properties like the network density, the considered network area, or the network topology (for example the presence of cluster heads), when dealing with an IoV network.

We remind that major trust metrics inherit its properties. From reviewed literature, we notice that reputation, knowledge, and proximity-based factors are the most employed metrics. However, trust metrics are often properly selected based on approach design purpose (or rather according to different criteria, such as accuracy, dynamicity, and required time and resource for computation). We can also give classes to trust metrics, as in [23] which identified (1) trust scale class (i.e., trust described by continuous, or discrete values), (2) trust facets class (e.g., trust described by pair, or triplet values), and (3) trust logics class (i.e., trust described by probability, fuzzy values). Besides, trust can be distinguished in different types like blind trust, conditional trust, or unconditional trust.

2.3. Trust computation

Trust computation includes different components (see Figure 3). Common considered modules are briefly explained below. Once trust is established it is managed for the duration of target nodes interactions.

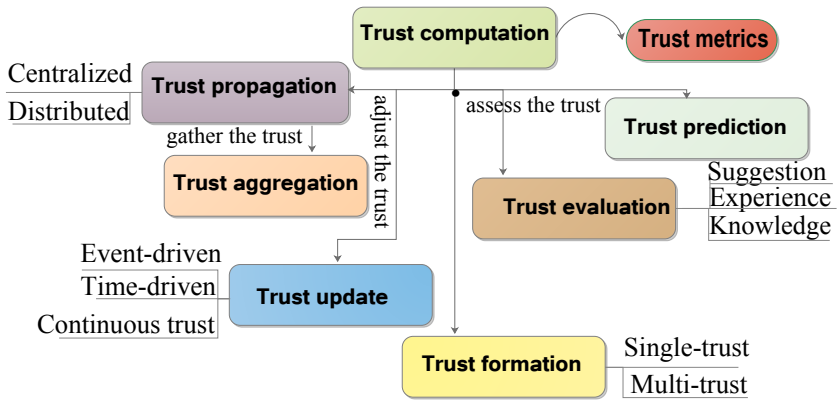

Figure 3: General modules in trust computation

- Trust Propagation: Trust propagation module refers to the principle of deriving trust among different communication system nodes, based on generated relationships and pre-existing trustworthiness values while collaboration (e.g., recommendations). Trust propagation is noted as centralized approach where trust is propagated to entities through centralized node or technique, and distributed scheme where propagation do not requires central agent [24]. Trust transitivity property and also trust fusion are the core factors of trust propagation. Such module provides key benefits. Resources computation cost might be mitigated when measured trust value is propagated over the network, instead of determining each individual entity trust. Moreover, users who are globally trustworthy may command better influence for services.

- Trust Aggregation: diverse versions about the trust value of a node can be propagated through different network paths. When receiving different

trust values about a node, the aggregation module aims to define one single value based on an aggregation of received values. Fuzzy logic, weighted sum approaches, and Bayesian model are the major applied techniques for aggregation. Trust aggregation is the principle of composing trust based on a trust path of the different received values.

- Trust Update: Trust update refers to updating trust value, which is a very significant aspect. There are three schemes in trust update. (1) Event-driven trust: node trust value get adjusted after an event occurrence or while transaction making, for instance, when a node is entering, or hereupon a feedback on the quality of a provided service is transmitted for trust aggregation operation. (2) Time-driven trust: concerns when node trust value is applied for adjustment within a determined time period using the aggregation scheme. (3) Continuous trust update: this serves to control one specific node tasks, and consists mainly of protecting integrity.

- Trust prediction: Trust prediction module aims to potentially predict trust relationships among entities based on chosen metrics. In other words, it refers to guess whether a truster node will trust another.

- Trust evaluation: Trust evaluation module includes generally experience (direct; local knowledge), suggestion, and global knowledge parts (indirect and direct trust). Experience is forwardly computed by requesting node neighbours and gets upgraded at regular intervals in the table of trust, then it will be transmitted as a recommendation trust piece. The evaluated trust value is then joined to the global knowledge part. These segments can serve for efficient trustworthiness assessment.

- Trust Formation: this module defines the trust formula. To define how the trust will be calculated, we should define the set of trust properties and metrics that should be considered for the trust formula. For that, the trust formula can be simple or composed. Thus, two trust categories can be defined for the formation module:

1. Single trust: in this case the trust formula is almost simple, it is considering only one specific property like direct (when we only consider the previous direct exchanges with the node) , indirect (when we consider the different recommendations built about the node), etc. (see section 2.1). Also, for the single trust, only one metric is almost used for the evaluation. For example, when we consider the direct property, we can use the knowledge-based metrics for evaluating the trust. For the indirect property, the reputation-based metrics are suitable to evaluate the trust.
2. Multi-trust: when the trust formula satisfies more than one property and is evaluated based on more than one metrics type then, we are dealing with multi trust category. Indeed, the multi-trust serves to optimize the trust value and it minimizes the error rate about the calculated value. Considering many metrics helps to get more accurate and reliable trust values.

3. Existing surveys on vehicular networks

This section refers some recent existing reviews and survey papers that are written in the context of vehicular networks (from 2017 to the time of writing this paper). We summarize the contributions of these papers in Table 2 and Table 3. Indeed, we organize these works according to their main scopes that refer to the following aspects: security issues, privacy issues, trust management issues, routing and QoS issues. We remark that a limited number of papers have highlighted IoV communications, more specifically trust management-focused works. The cited surveys covering the works on vehicular networks, especially from security and privacy perspectives could bring more comprehension to our survey content, since we will discuss in short the major IoV security challenges in the next section.

Table 2: *Recent surveys on vehicular networks*

Topic	Ref Year	Basic content	Related content
Security	[25] 2019	security attacks in VANET	subsection 4.1 subsection 4.3
	[26] 2019	security, attacks, and applications in VANET	subsection 4.1 subsection 4.3
	[27] 2019	security attacks and protection schemes of intelligent connected vehicles	subsection 4.1 subsection 4.3
	[28] 2020	security issues and challenges in V2X	subsection 4.1 subsection 4.3
	[29] 2019	security issues and solutions for V2X	subsection 4.1 subsection 4.3
	[30] 2018	security standards and issues in V2X	subsection 4.1 subsection 4.3
	[31] 2019	security issues in V2X	subsection 4.1 subsection 4.3
	[32] 2018	security issues and research directions for C-V2X	subsection 4.1 subsection 4.3
	[33] 2019	security assessment of 5G V2X	not considered
	[34] 2018	authentication issues for cellular-assisted V2X	not considered
	[35] 2017	authentication issues in V2X	not considered
	[36] 2017	security challenges, authentication, and trust models for VANET	subsection 4.1 subsection 4.3 section 5
Privacy	[37] 2019	privacy regulations and attacks in vehicular systems	not considered
	[38] 2019	local differential privacy for securing IoV	not considered
	[39] 2019	privacy issues in IoV	not considered
	[40] 2019	authentication and privacy for VANET	not considered

Topic	Ref Year	Basic content	Related content
Privacy	[41] 2019	location privacy techniques in VANET	not considered
	[42] 2019	privacy challenges in vehicular systems	not considered
Trust management	[43] 2020	trust management current trends and future research directions in IoV	section 5 section 7
	[44] 2020	trust management solutions in VANET and future research directions	section 5 section 7
	[45] 2019	trust management challenges, Blockchain, and Fog solutions in social IoV	subsection 4.2 subsection 4.3
	[46] 2019	trust management solutions in VANET	section 5
	[47] 2019	trust management risk-based decision making solutions in VANET	not considered
	[48] 2018	trust management solutions in VANET	section 5
	[49] 2018	trust management for secure routing in VANET	section 5
	[36] 2017	security challenges, authentication, and trust models for VANET	subsection 4.1 subsection 4.3 section 5
Routing	[50] 2020	location-based routing protocols in VANET	not considered
	[51] 2019	routing protocols solutions in IoV	not considered
	[52] 2019	optimization solutions for routing protocols, and trends in VANET	not considered
	[53] 2019	multimetrics-based routing protocols in VANET	not considered
	[54] 2019	link efficiency and link stability-based routing protocols in VANET	not considered
	[55] 2018	node trust-based routing protocols for VANET	section 5
	[56] 2018	routing protocols solutions in VANET	not considered

Topic	Ref Year	Basic content	Related content
Routing	[57] 2018	routing protocols solutions in VANET	not considered
	[58] 2018	geographic routing protocols for VANET	not considered
	[59] 2018	topology and position-based routing protocols in VANET	not considered
QoS	[60] 2019	QoS issues in IoV	not considered
	[61] 2019	QoS in SDN-IoV	not considered
	[62] 2018	QoS issues in VANET	not considered
	[63] 2018	QoE/QoS models for video streaming in VANET	not considered
	[64] 2017	QoS aware broadcasting techniques in VANET	not considered

3.1. Contributions of existing surveys in vehicular networks

As shown in Table 2, most existing surveys on vehicular networks studied security issue and routing protocols. The surveys addressing the security covered related issues and requirements, and exposed suggested solutions against possible attacks, following different taxonomies and nomenclatures e.g., [25]-[27]. Other surveys on security studied the threats for vehicular applications enabling technologies, e.g., [30]-[32]. Besides, the impact of trending standardizations on security was highlighted such in [33]. Surveys on privacy challenges that are encountered for vehicular applications deployment were provided in [[37]-[42]]. For example, in [41], the authors introduced further a privacy factor and indicated that vehicle location, speed, and steering wheel angle consist of the riskiest sensors regarding privacy. Study [38] stated that the local differential privacy can protect the privacy in IoV scenarios. Also, the combination of the local differential privacy with emerging techniques e.g., machine learning can provide potential solutions to guarantee the privacy. Surveys [50]-[59] presented

the state-of-the-art of vehicular routing, following various taxonomies. We can conclude that the SDN has the potential to enhance the routing schemes [51]. Moreover, position, density, and speed are the most promising parameters in routing within vehicular networks, and QoS routing protocols are mostly based on stability [54]. Additionally, QoS becomes more challenging when deploying multimedia vehicular applications [60]. Table 3 lists the pros and the cons of the referred surveys.

3.2. Comparison of our survey to existing surveys on trust management in vehicular networks

Although there are a significant number of publications regarding the trust management in vehicular network context, there is so far few comprehensive surveys that cover all the various aspects of trust. For example, surveys [46][48] covered the main aspects of the trust in vehicular networks. The existing trust approaches were divided in [46] as follows: reputation based, reputation and similarity-based, reputation and utility-based, behaviour and similarity-based. The concept of trust management, along with relevant trust approaches were not presented in [36]. In [48], the trust approaches were reviewed without providing a detailed classification. Besides, the emerging technologies-based trust works (e.g SDN-based, Fog-based, and Blockchain-based) were not studied in these two papers. The recent proposals for trust management in VANET from the year 2014 to 2019 were reviewed, classified, and synthesized in [44]. The paper covered more research works. The authors introduced a detailed taxonomy of trust solutions in VANET based upon significant factors. They provided a comprehensive comparison and discussion. Compared to the previous surveys, this paper is much more complete and meaningful, however more details about trust management concept, involved modules, and possible related attacks are needed. Besides, the paper does not include the trust in vehicular networks at large scale (i.e., considering the trust approaches in the IoV context). Authors in [43] discussed the trust management in both VANET and IoV, yet the different procedures consisting the trust management process were not intro-

duced. Furthermore, for example the survey [45] provided a review in social IoV. Nevertheless, a clear classification of studied approaches would be appreciated to help in evaluating their efficiency. Compared to the previous cited surveys, our survey focuses on reviewing, classifying, and comparing the different trust-based proposals, while covering the various aspects of trust (trust modules, trust metrics, trust attacks, trust and security challenges, related open directions) (see Table 4). Our survey applies a complete taxonomy of trust approaches in vehicular networks especially from the aspect of used tools, hence it includes the various solutions for vehicular trust; we conduct an analysis on two dimensions. The first dimension comprises the application of classical trust models (entity-based, data-based, and hybrid models). The second dimension covers the emerging trust schemes. This will help to pick out the advantages and the disadvantages of each adopted tool for trust management.

4. V2X challenges

The major challenges of vehicular communications are discussed in this section. Particularly, we present V2X issues in terms of security and trust management, and we expose some trust-related attacks.

4.1. V2X security challenges

The development of full potential V2X applications puts many requirements to tackle primary communication system security challenges. Security issues can come with network technologies heterogeneity, security policies, bootstrapping, or network scalability regarding varied security solutions features designs, and also large network control along with security techniques. The high V2X framework mobility, and hereupon the dynamic network topology nature and the communication latency factor impose adapting proposed security schemes features to the connection quality. Indeed, due to the fast vehicular nodes speed, communication system parties establish short duration communication links, or may frequently have connections breakage; mostly vehicles when moving in opposite lines, which requires to address communication latency resulting issues

Table 3: *Pros and cons of referred surveys*

Ref Year	Pros	Cons
[25] 2019	-Introduction of security challenges and privacy in VANET, along with possible attacks definition -Review of security approaches in VANET: cryptography-based approaches, trust-based approaches, and identity-based approaches -Discussion of Cloud-based VANET effectiveness, with identification of related privacy and security issues -Examination of VANET layers protocols with possible attacks identification -Presentation of some emerging issues in VANET	-The survey could elaborate comprehensive evaluation of Cloud-based (e.g., based on security metrics with QoS management)
[26] 2019	-Exploration of VANET from architectural view, standards, characteristics, and security services -Identification of attacks in VANET -Review of works on VANET security -Review of proposed authentication approaches in VANET: cryptography-based approaches and signature-based approaches -Discussion of simulation tools in VANET (mobility simulators, network simulators, and comprehensive simulation) -Identification of open challenges in VANET, regarding security and routing aspects	-The survey does not explore Blockchain-based approaches)

Ref Year	Pros	Cons
[27] 2019	-Identification of the major attack in vehicular system -Introduction of the key security methods	-The survey could discuss further the impact of the introduced methods on QoS performance
[28] 2020	-Discussion of applications and communication technologies for V2X -Introduction of security challenges and requirements in V2X -Comparative study of V2X attacks -Review of security schemes in V2X: symmetric Key cryptography-based approaches, privacy preservation based approaches, and message authentication based approaches -Identification of future directions of V2X from a security perspective	-The survey does not explore the adopted architectures in V2X (e.g., Blockchain-based approaches)
[29] 2019	-Introduction of VANET from architectural view, enabling technologies and application domains -Exploration of V2X security challenges, and analysis of threats for V2X enabling technologies (IEEE802.11p and LTE-V2X) -Review of security approaches in V2X: cryptography-based approaches, trust-based approaches, and identity-based approaches -Comparative study of security approaches in V2X considering attack type (internal, external attack), message type, latency limit and model structure	-The survey does not explore the adopted architectures in V2X (e.g., Blockchain-based approaches)

Ref Year	Pros	Cons
[29] 2019	-Identification of future directions of V2X from security and QoS	
[30] 2018	-Introduction of base standards for security in V2X (ISO, ITU, IEEE, and ETSI) -Discussion of V2X security issues	-The survey does not provide the future directions for V2X standardizations (e.g, implication of 5G from a security perspective)
[31] 2019	-Presentation of VANET details -Exploration of V2X standardizations (802.11-OCB mode, IETF IPWAVE, IEEE 1609 and ETSI ITS, and Cellular-based: LTE/ 5G) -Presentation of similarities and differences between V2X standardizations	-There is no threats analysis -The survey does not provide possible future directions of V2X
[32] 2018	-Analysis of the 3GPP security requirements for C-V2X -Exploration of trends for C-V2X (e.g., machine learning, Fog, and Cloud)	-The proposed works to mitigate C-V2X attacks are not provided
[33] 2019	-Exploration of V2X standardizations (IEEE 802.11p and cellular technologies) -Introduction of security requirements for ITS applications -Discussion of the impact of 5G NR introduction in V2X	-The survey does not provide other possible future directions of V2X
[34] 2018	-Introduction of VANET standards and characteristics -The survey highlights the possible attacks in LTE-enabled V2X -Authors have introduced the corresponding counter measures	-Only two evaluation parameters are considered: computational cost and communication overhead

Ref Year	Pros	Cons
[34] 2018	-Exploration of cellular-based V2X features -Review of authentication in LTE based V2X -Comparative analysis of the defence methods in LTE-V2X -Identification of future trends for securing LTE-enabled V2X	
[35] 2017	-The survey emphasizes the integrated sensors for in-car authentication -Review of deployed multi-factor authentication solutions in V2X, along with future of multi-factor authentication for V2X -Proposition of a MFA system that relies on reversed Lagrange polynomial to allow flexible in-car authentication -Improvement of the proposal considering possible metrics' static behaviour	-Authors could present a use case for the evaluation phase
[36] 2017	-Identification of security challenges and possible solutions in VANET -Review of authentication schemes in VANET -Introduction of some trust-based approaches in VANET	-The survey does not provide the comparison of the authentication schemes -Details about trust management concept are missing -The survey does not provide the related open directions
[37] 2019	-Introduction of automotive privacy regulations -Review of privacy attacks according to three factors: driver fingerprinting, location inferencing,	-The survey does not provide the solutions against the reviewed attacks

Ref Year	Pros	Cons
[37] 2019	and driving-behavior -Introduction of a privacy score for risk assessment	
[38] 2019	-An overview of autonomous driving technology -Survey of works on local differential privacy in the IoV, with comparative analysis -Evaluation of the surveyed schemes: identification of associated limitations	-Authors could add criteria to evaluate the surveyed models
[39] 2019	-Review of privacy models in the IoV: differential privacy, distributional privacy, crowd-blending privacy, and randomized response model	-Authors could add criteria to evaluate the surveyed models -The survey does not provide related future directions
[40] 2019	-Classification of several authentication and privacy schemes -The surveyed schemes are classified according to the adopted mechanisms (e.g., pseudonymous-based, group based, identity, and hybrid anonymous-based) -Evaluation of the surveyed schemes: identification of associated limitations	-The survey does not provide related future directions
[41] 2019	-Overview of VANET -The survey focuses on location privacy in vehicular networks -Review of group-based authentication approaches, mix groups-based authentication approaches, and obfuscation-based approaches -Comparative analysis of the discussed techniques	-Related Future directions are not provided

Ref Year	Pros	Cons
[42] 2019	-Introduction of characteristics of connected and autonomous vehicles -Categorization of privacy challenges for connected and autonomous vehicles, according to vehicle tasks -Classification of privacy preserving approaches into: anonymity-based, perturbation-based, and cryptography-based -Qualitative analysis of reviewed approaches -Identification of privacy open issues in vehicular systems	-Authors could explore privacy persevering with QoS management
[43] 2020	Trust management is discussed in both VANET and IoV -Taxonomy of reviewed trust approaches in VANET and IoV -The survey provides the trends in trust management within VANET and IoV and the open directions	-Details about trust management procedures are missing
[44] 2020	-Overview of VANET -Taxonomy of trust approaches in VANET according to adopted methodologies -Comparative analysis of reviewed works -Identification of open directions for trust in VANET	-Details about trust management procedures are missing -The survey does not provide a detailed information of trust related attacks -The survey does not explore the trust in vehicular networks at large scale (i.e., considering the IoV context)
[45] 2019	-The survey explores the trust management in social IoV -Presentation of social IoV details -The survey explains the trust metrics -Identification of trust management	-Authors could analyze the proposed trust approaches following a clear classification to more understand the related benefits and drawbacks

Ref Year	Pros	Cons
[45] 2019	challenges in social IoV, along with trust-related attacks discussion -Authors have provided the trends for trust management in social IoV (e.g, Blockchain, and Fog)	
[46] 2019	-Overview of security requirements -Classification of threats in VANET considering the attacker type and the attack goal -Classification of trust schemes in VANET according to adopted methodologies -Identification of future directions for trust in VANET -Classification of trust metrics into vehicle trust-based, message trust-based, and common metrics-based -Comparison of the reviewed approaches according to used trust model, methodology, addressed attacks and domains of application	-The survey does not discuss the recent solutions for managing trust in vehicular networks (e.g, Blockchain-based) -Details about trust management procedures are missing -The survey does not explore the trust in vehicular networks at large scale (i.e., considering the IoV context)
[47] 2019	-Survey of the trust approaches having incorporated the risk factor in VANET -Analysis of the considered factors -Identification of related open directions	-The survey does not explore the trust in vehicular networks at large scale (i.e., considering the IoV context)
[48] 2018	-Overview of security issues in VANET -The survey highlights fuzzy logic-based trust approaches	-Authors could study the proposals following a clear classification to help in interpreting the related benefits and drawbacks -The survey does not provide a detailed information of trust related attacks

Ref Year	Pros	Cons
[48] 2018		-Details about trust management procedures are missing -The survey does not discuss the recent solutions for managing trust in vehicular networks (e.g, Blockchain-based) -The survey does not give future directions for trust in VANET
[49] 2018	-Identification of trust management challenges in VANET -Analysis of the algorithms adopted by routing schemes according to QoS performance and used methodologies -Discussion of some related open directions	-Authors could provide a clear classification for the reviewed works to help in distinguishing their efficiency -Details about trust management procedures are missing -Authors could discuss the efficiency of VANET emerging architecture to build trusted routing
[50] 2020	-Exploration of VANET routing standards -The survey highlights locations-based routing protocols -Extensive review and classification of proposed solutions against location-based routing issues into four sub-categories: repair strategy-based, optimum forwarder selection, broadcasting overhead-based, and accurate positioning-based -Comparison of reviewed solutions using different criteria -Examination of challenges associated with hybrid communication technology (WAVE/LTE) -Identification of future directions for	The survey does not explore architectures in routing

Ref Year	Pros	Cons
[50] 2020	-secure routing in VANET and IoV	
[51] 2019	-Classification of proposed solutions for routing in the IoV according to used methods: swarm intelligence based, Bio inspired-based -The classification extends from security aspect, including key management, intrusion detection, and trust strategies -Comparison of reviewed protocols using a set of criteria -Discussion of two network architectures in vehicular networks: traditional architecture-based and SDN architecture-based -Details of routing criteria and SDN architecture' impact on routing performances of vehicular applications	-Authors could present in the trends the different optimization strategies for vehicular routing
[52] 2019	-Review of different taxonomies and various nomenclatures for routing protocols in VANET -Authors have emphasis on geographical protocols -Exposition of optimization methods for enhancing routing protocols in VANET: bio-inspired, computational intelligence, SDN, Cloud and Fog -Identification of open challenges for developing robust routing in the IoV	-Authors could give a comparative evaluation of the introduced optimization methods (e.g, regarding QoS management)
[53] 2019	-Overview of VANET -The survey focuses on multimetrics-	-It would be interesting to compare routing and dissemination approaches

Ref Year	Pros	Cons
[53] 2019	based routing protocols -Authors have explained the utility of designing metrics in routing -Classification of multimetric-routing proposals for VANET -Discussion of dissemination algorithms in VANET	
[54] 2019	-The survey emphasizes the significance of QoS-based routing protocols in VANET -Authors have highlighted the routing protocols considering link efficiency and link stability parameters -A sub classification for the reviewed proposals according to their used methods would be appreciated to more clarify the impact on the Qos	-The survey does not provide possible future directions for the QoS-based routing protocols
[55] 2018	-The survey focuses on discussing secure trust-based routing in VANET	-The introduction of basic trust concepts is missing -The survey does not emphasis the techniques and the trust metrics that were applied to establish the trust in the reviewed proposals -The survey does not provide possible future directions for the trusted routing in vehicular networks
[56] 2018	-Overview of VANET and its simulation environment -Discussion of the strengths and the weakness in the existing routing protocols for VANET -Identification of routing challenges in VANET	-The paper does not give the possible trends to build robust routing in VANET

Ref Year	Pros	Cons
[57] 2018	-Overview of VANET deployment challenges -Comparison between reactive routing protocols and proactive routing protocols	-The survey discusses only the topology and the position based protocols -Future directions are missing
[58] 2018	-Introduction of the challenges in the design of position based for VANET -Review of the geographic-based upon the routing in VANET -Discussion of related deserves and demerits -Identification of future directions for geographic-based routing in VANET	-Trends in optimization methods are missing
[59] 2018	-Presentation of VANET details -Identification and categorization of VANET issues into technical challenges and security challenges -Examination of the topology and the position-based upon the routing in VANET, following related advantages and disadvantages	-Future directions and possible optimization methods for routing in VANET are not given
[60] 2019	-Identification of QoS significance and challenges in the IoV -Classification of QoS specifications (QOS metrics and QOS policy) -Discussion of the measurement parameters that could impact the performance of the IoV	-The survey does not explore architectures and answer QoS satisfaction
[61] 2019	-The survey focuses on the QoS in SDN-IoV environment	-Authors could provide more comprehensive analysis of the reviewed works
[62] 2018	-Review of the proposed approaches for QoS maintaining: RSU-based, Cloud-based, machine-to-machine	-The survey does not explore architectures and answer QoS satisfaction

Ref Year	Pros	Cons
[62] 2018	communication-based, and mobile agent-based -Discussion of routing protocols designed with keeping in mind QoS considerations: exploration of their applicability in different scenarios	
[63] 2018	-Review of QoE/QoS correlation models for transmission in VANET -Presentation of QoE applications in video streaming -Analysis of influence factors of QoE in video streaming -Identification of related challenges and open issues	-More extensive analysis of QoE influencing factors in vehicular networks would be appreciated
[64] 2017	-Presentation of the details of VANET -Review of dissemination strategies and broadcast protocol -The survey focuses on QoS aware broadcasting -Identification of broadcasting issues in VANET -Specification of QoS requirements in VANET -Classification and comparative study of QoS aware broadcasting protocols in VANET (according to used techniques) -Identification of related challenges and future trends	-The survey does not explore architectures and answer QoS satisfaction

Table 4: *Comparison with existing surveys*

Comparison aspects		Ref [43]	Ref [44]	Ref [45]	Ref [46]	Ref [47]	Ref [48]	Ref [49]	Ref [36]	Our survey
Coverage of main concepts	trust modules	no	no	no	no	no	no	no	no	yes
	trust metrics	yes	yes	yes	yes	yes	no	no	no	yes
	trust challenges	yes	no	yes	yes	yes	no	yes	no	yes
	trust attacks	yes	no	yes	yes	yes	no	no	no	yes
	open directions	yes	yes	yes	yes	yes	no	yes	no	yes
Works taxonomy		yes	yes	no	yes	no	yes	yes	yes	yes
Comparative analysis	evaluation criteria	no	yes	no	yes	yes	yes	yes	yes	yes
	simulation setup	no	no	no	no	no	no	no	no	yes
Domain/scenario	VANET	yes	yes	no	yes	yes	yes	yes	yes	yes
	IoV/V2X	yes	no	yes	no	no	no	no	no	yes

such as defining target messages for exchange or filtering. This fact makes the network system more sensitive to threats (e.g., very limited time for suspicious nodes identification). It may accordingly result out of certain messages priority, buffering and queuing issues. Vehicular cyber physical systems require evidently maximum immune to dangerous attacks. Assaults on system and its participating users can disturb the whole V2X communication. Exchanged messages can be falsified and filled by dummy information. Attackers also get access to the system to delete, or intercept forwarded data. Furthermore, examples of attackers who steal other device identity (i.e., Sybil attack, more specifically e.g., sensor impersonation attack), and seek to prohibit the use of system communications channels (e.g., channel jamming attack) need to be prevented. Inaccurate traffic messages, and forgeries; false warnings and bogus misconduct reports might be generated, which increases safety services threats and consist of causing many risks like vehicular nodes crashes, traffic collision, and immaculate drivers sanction. Privacy is further an exposed challenge. This aspect is well related to trust issues. Research works on security in vehicular cyber physical systems comprise generally cryptography-based techniques

(e.g., asymmetric cryptography, and symmetric cryptography), and identity-based techniques (e.g., pseudonym-based, geographic proximity, id-based signature, and certificate-based authentication). Other security schemes utilize privacy preservation techniques. In addition, we remind standard security measures like IEEE P1609.2, and LTE-V2X, and also intrusion detection system tools. The effectiveness of used techniques is evaluated with regard to intended performances criteria to be met (e.g., addressed attacks).

4.2. V2X trust management challenges

Many challenges can weaken the trust management schemes while developed in V2X environment. The major challenges that we intend to mention are, likewise general security models threats, related to the safeguard against most correlated attacks and QoS trust (see Figure 4). V2X users look for trustworthiness in derived relationships while cooperation. Thus, trust-based approaches are concerned with malicious and selfish nodes. Examples of malicious attacks are black hole attack, message replay attack and malicious code attack. For instance, a malicious node receives packet and discards it instead of relaying it to the destination, in black hole attack. Secure routing schemes are efficient against such attack. Further, we point reputation-based malicious attacks. Bad mouthing is a well-known form of reputation-based attacks. It can ruin the good trust reputation of nodes through providing bad recommendations. Another example of malicious node behaviour is on-off attack. This attack consists to launch malignant service, and behave well alternatively, so as to evade bad trust reputation. The selfish node behaviour comprises kind of prevalent attacks like repudiation attack, where a greedy node seeks to deny communication and causes the loss of nodes' actions tracking and events logging. Other instances of malicious attacks consist of movement tracking attack, traffic packets extraction and analysis, and transmitted message sniffing. These attacks can be mitigated with the use of privacy preservation mechanisms. In this context, we remind the privacy concern in V2X. Good trade-off in terms of trust and privacy is still claimed, since portion of critical personal data that can reveal connected

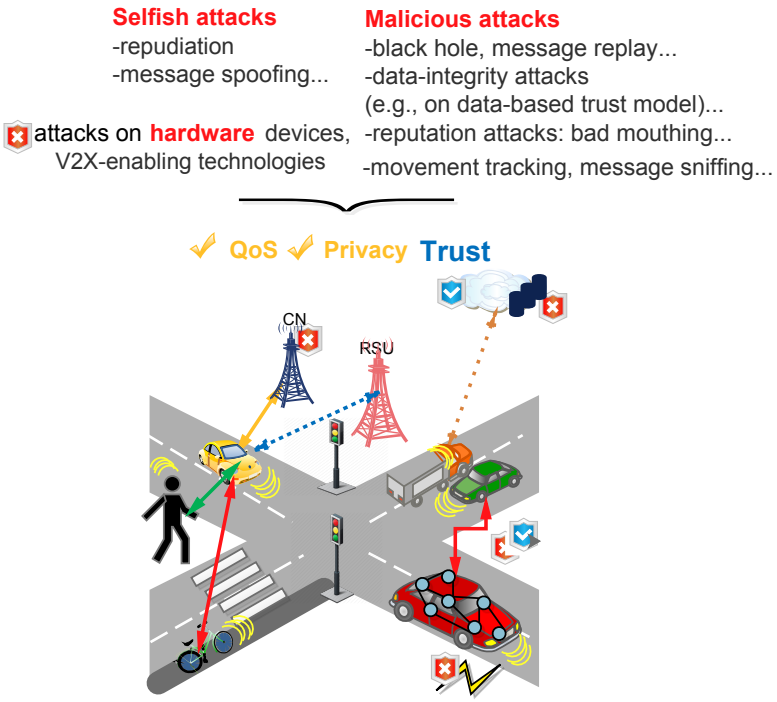

Figure 4: V2X trust management challenges

parties identities are shared (e.g., vehicle identity revealing attack), in other words, node identity disclosure affects trust relationships, and hence the communication process. Trust models threats can be also the outcome of malicious attacks on data integrity (e.g., on data-based trust model), hardware devices, or V2X-enabling technologies.

4.3. Security attacks on vehicular networks

Due to the vulnerabilities that characterize the vehicular environments, many attacks can occur on these networks. In literature, many efforts have been proposed to classify and define taxonomies for these attacks. Many surveys were also dedicated to deal with attacks in vehicular environments [65]. In this subsection, we give in Table 5 a succinct introduction to these attacks and provide to the reader relevant references about some related solutions.

Table 5: *Attacks samples in vehicular networks*

Attack	Description	Conditions	Solutions
Sybil attack	The node within the network propagates more than one identity. The attacker can propagate across the network erroneous information based on false identities	Sybil attack can be more probable within networks using geographical routing. It facilitates falsifying the position for the attacker	[66]-[70]
Denial of Service attack (DoS)	Impact the network availability (the network established by the RSU for example) through sending a huge number of requests	The attacker can exploit vulnerabilities of end-to-end congestion control protocols in order to deteriorate network performances. The attack is also facilitated when many attackers collaborate from different locations to perform it (it is called DDOS)	[71]-[75]
Blackhole attack	It is a kind of denial of service (DoS) where the attacker drops all the data packets. All the information and packets are redirected to a malicious vehicle claiming that it is an optimum routing path after the broadcast of a false routing information	The attacker exploits the freshness feature of route to hide the true paths from the other nodes, it can broadcast false routing information and entice others to route across itself, claiming that his path is the best one.	[76]-[79]
Wormhole attack	Two or more malicious vehicles linked by a low latency communication	The attacker can collude with other malicious nodes	[80]-[81]

Attack	Description	Conditions	Solutions
Wormhole attack	channel form a tunnel to transfer packets. Attackers announce that the tunnels are of high quality towards the destination for neighboring cars that use them in their paths. Therefore, the sent data will be under the control of the attackers	to misguide victims by exploiting routing protocols. Attackers will place themselves in the most vital position to form a tunnel and advert the other nodes that they are in the best position to forward the packets (shortest route)	
Bogus information attack	The attacks propagate false information across the network (for example, false positive information)	The attacker has a good knowledge about the network and can change from a cluster to another to not be detected	[82]-[84]
Replay attack	It consists of replaying the transmission of old valid messages and injecting them in the network. The malicious node can save transmitted data from the network and then reuses them to deceive legitimate vehicles. It entraps the network using expired messages	When injecting back the messages to the network, the location table of the node gets poisoned by the replayed contents. Besides the messages replays causes the increasing of the network bandwidth cost. This can lead to the discard of priority messages	[85]-[88]
Passive eavesdrop-ping attack	It threatens confidentiality in VANET aiming to get unauthorized access to confidential VANET information	The attacker gathers the confidential data of nodes. It observe silently the behaviour and the current location of the victim node	[89]-[92]

Attack	Description	Conditions	Solutions
Passive eavesdropping attack	(i.e. vehicles location, public and private keys, etc.). An attacker can stock information of the normal vehicles and profit of it to damage the network	The identification of such malicious node is very difficult as it behaves in a normal way and it is limited to intercept the communication	

5. Trust management approaches in vehicular networks

Trust management approaches are usually categorized into the following popular classes: (1) entity-based approaches, (2) data-based approaches, and (3) combined approaches, (based on the solution revocation target). On the one hand, we can further divide these classes in general in terms of reputation and knowledge, similarity, and utility. On the other hand, these approaches can rely on miscellaneous tools (e.g., enabling techniques, and network-advanced architectures) to take their merits for more efficient trust management strategy. Accordingly, we review in the following section some classical examples (e.g., simply inspired by probabilistic logic) of trust management solutions for vehicular communications in each aforementioned class. Next, we present our taxonomy for the recent related approaches, which is based on used tools. We broadly focus on artificial intelligence and advanced technologies tools. Here, our taxonomy can be viewed as a sub-classification of above existing classes. Shortly, Figure 5 draws the contribution of this survey, which consists of presenting our taxonomy for trust management approaches in vehicular networks, along with resume tables of the surveyed approaches (Tables 6-7, 8-9, 10-11) in subsection 5.2) containing related used trust metrics, applied tools, simulation experiments, and comparative criteria. Figure 5 summarizes also the existing trust-approaches in vehicular networks (entity, data and hybrid based). We remind that we classify the proposed approaches into two categories: (1) artificial intelligence-based approaches that apply clustering, reinforcement learning,

fuzzy logic, and game theory techniques, and (2) emerging technologies-based approaches that apply Cloud, Fog, Edge, Blockchain, and SDN.

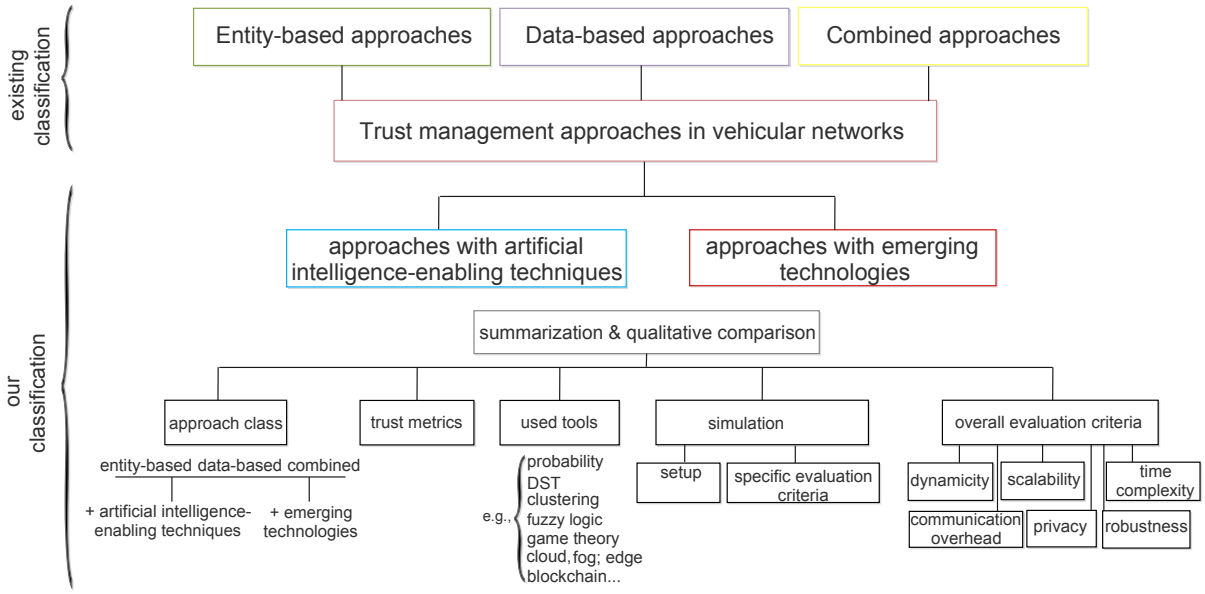

Figure 5: Contribution of this survey

5.1. Existing classification for trust management approaches

The entity oriented approaches consider that the trust concept is associated to the network nodes. These approaches aim to evaluate the trustworthiness of the nodes participating in the data forwarding and data exchanges within the network. Then, based on the evaluation of their trust level, the malicious nodes may be excluded from the network or isolated. A part of the existing entity-based approaches in literature are inheriting from the social trust dimension. These approaches are mainly considering reputation-based metrics. Thus, to calculate the trust value of a trustee node, the trust formula is mostly based on past knowledge-related metrics such as the node experience about the perceived behavior and activities over time as well as on the exchanged recommendations

among the different entities. Other works are considering a multifaceted trust. Indeed, in addition to the reputation-based metrics, they consider the similarity factor. This latter refers to entities having the same properties. For example, within an IoT network, a vehicle belonging to a specific cluster may consider that the vehicles belonging to the same cluster are more trustworthy than those belonging to other clusters. For this example, we can be based on the proximity of the node to assign a better trust value to the trustee node.

In data-based approaches, trust is linked to the produced message content, which means that these solutions require data authenticity instead entity legitimacy evaluation. Utility is an important aspect to evaluate the data content's trustworthiness. The utility is introduced to refer a specific beneficial act, a worth or usefulness of produced event, in comparison with other actions in same context. Data utility assessment uses often such trust factors: proximity, time, vehicular node role, and occurred event type. Hence, data-based approaches can be distinguished into information oriented methods and event oriented methods. Similarity aspect has been also introduced to assess data trust value. Initially, similarity refers to exchanged data contents coincidence, regarding some parameters like time and closeness. This fact helps in reducing disseminated data amount and ensuring that only useful contents are spread. Nevertheless, we can not reach typically the assessment of trustworthiness of each exchanged messages part with this model. Moreover, data sparsity represents the major issue for this class. Combined trust management approaches are based on the trustworthiness of both entity and exchanged data, for better efficient trust computation. Entity trustworthiness assists in data trust value assessment [93]; The data content that has been evaluated to be reliable by many trusted entities is suggested as trustworthy to other nodes.

5.1.1. Entity-based trust management approaches

In [94], authors proposed a reputation infrastructure-based approach that aims to identify selfish and misbehaving entities. The approach relies on three trust metrics to assess the reputation value of every single vehicle: (1) past

and direct entity experiences, (2) surrounding vehicles recommendations, and (3) recommendations from the infrastructure (through available RSUs). Likewise, the proposal considers trust levels (Not trust, +/- Trust, and Trust), and severity levels (high, medium, and low) to be assigned, respectively, to each vehicle and transmitted message, in order to determinate the received content acceptance. This task is performed through probability rules. The content with 'high' severity level is accepted if its issuer reputation score belongs to 'Trust' level, while other contents with lower severity level are accepted from entities placed in '+/- Trust' or 'Trust' level. An example of similarity-based approach was presented in [95] to cope with the injection of false information within VANET safety-related events reports. The similarity rating is derived through periodic beacons that carry location and speed information. Authors relied also on an echo protocol to achieve trust rating and validate produced reports i.e., supervising the ordinary and anticipated behaviour of neighbour vehicles in regard to their reported event. Another multifaceted-agents trust modeling solution for VANET environment was referenced in [96]. The trust computation procedure core comprises agents trust maintaining part which is priority notion-based (combines role and experience metrics), and majority opinion-based trusted agents feedback aggregation part. More specifically, the process of trust computation consists of forming a selected agents list, ordered based on priority metrics, for advice asking/ report. When receiving responses, the requester entity proceeds to majority-based trust calculation. The feedback is followed once majority response consensus is reached otherwise the requester entity follows the advice of highest trust rate list agent, then it evaluates the reliability of the advice (with highlight on location/time event factors), and finally updates agents' value trust. Similarly, authors in [97] designed a multifaceted trust scheme for agents in VANET. The trust values of honest nodes are maintained to demand their related feedback. The authors consider the role, the experience, the majority opinion, and the priority metrics to determine the trustworthiness and ask the proper advisors. Accordingly, when an advice is sought, the proposal scheme proceeds to require multi agents, receive

the replies and then proceeds the majority-based trust calculation. The nodes are considered having : (1) authority role , (2) expert role , (3) seniority role, and (4) ordinary role, and the number of interactions is taken into account to measure the experience factor. In addition, a forgetting factor is introduced to deal with the behavior changes. In [98] the reputation of VANET nodes is modeled to assess node trust. Each node shares its trust with other entities by transmitting trust messages to an authentic infrastructure. This later consists of reputation management center collecting nodes' trust. The trust messages are filtered by the authentic infrastructure on the basis of statistical regularity. Every node can acquire updated trust data from the reputation center. The reputation is determined through historical trust and authentic center recommendation. The highway platooning scenario was addressed in [99]. The reputation metric is employed to rank the platoon head vehicles. The system model includes a server to evaluate the head vehicles' trust. The reputation values are computed by the collection of feedbacks from user vehicles. The system applies an iterative filtering to exclude the feedbacks of the malicious user vehicles. The reliable platoon head vehicle is then recommended by the server node. The authors of the work [100] elaborated an attack-resistant trust inference scheme for VANET, which was able to cope with black/grey hole attacks by quantifying subjective trust and recommendation trust. Specially, the subjective trust is derived from historical interactions, whereas the recommendation trust is gained based on neighbours opinions. Subsequently, the authors demonstrated a trust-aware multicast routing protocol. Reference [101] highlighted the authentication based on trust assessment in VANET.The authentication process comprises the evaluation of direct trust; computed from behaviour trusts, and the estimation of the indirect trust based on the given recommendations. Behaviour trusts are maintained by authority units. The indirect trust is adopted to allow all the vehicles in the network to validate the new accessing node. The method uses correlation coefficient to identify the malicious vehicles and remove their recommendations. Then, the average of recommendation trusts is calculated to obtain the final recommended trust. Likewise, a reputation-based message

authentication for 5G-enabled vehicular was developed in [102]. In this model, a trusted authority node is in charge of reputation management in order to decide whether the vehicle node can access the network. A vehicle with a low reputation value cannot obtain the credit reference from the trusted authority node to participate in the communication.

5.1.2. Data-based trust management approaches

Authors in [103] were the first to assume that entity-based trust assessment is not enough. Accordingly, they introduced an establishment of data trust suitable for VANET context. Each type of node has a predefined trustworthiness value. Reports by each node type on each kind of events are evaluated using default trustworthiness ranking and other trust metrics derived from security status value (which denotes node trust level), as well as dynamic nodes attributes such time proximity and location closeness; regarding that the reporter is more likely to have accurate messages as it is close to the generated event location, or further has the most recent report. The reports containing the same event are combined, then reports validity is inferred using a decision logic scheme. Authors in [104] presented a scheme for detecting rogue node in VANET through messages similarity. The main idea consists of checking close vehicles self-reported and received messages similarity. Within a moving window, each vehicle can calculate its own flow value based on speed and density parameters correlation, using the Greenshields traffic model. When receiving message (i.e., flow value), the vehicle compares it with its estimated flow measurement. Afterward, the vehicle can accept the received content if it matches with the traffic model and its own calculations (i.e., other close vehicles flow values are similar to its own computed value), otherwise the sender is singled out and reported. Authors in [105] introduced an intrusion-aware trust solution for VANET. In this approach, the data trust assessment requires the computation of confidence and trust values for every received content about particular event. To perform confidence measurement, receiver vehicles rely on location closeness, data freshness, location correctness, and time information verification

parameters. In a second step, the method proceeds to trust value measurement on the basis of sender vehicles number and their confidence values. After that, the receiver needs to decide the message acceptance according to highest trust and acceptable threshold values. The trust on information in VANET was considered also in work [106], where the RSU node is employed to execute the trustworthiness establishment, along with the use of ant colony optimization algorithm. This infrastructure-based approach aimed to attenuate the CFD attack through the filtration ability in RSU. The ant colony optimization algorithm integrates observation with feedback information to measure the data trust. The observation factor is defined using the distance from the reported event and the detection range of the vehicle. The RSU, as an intermediator node, gathers and transforms vehicles' reports into evidences to disseminate the trust. A RSU and beacon based trust scheme was further highlighted in [107]. The vehicles, with the cooperation of RSUs, build, use and disseminate the trust values by verifying the plausibility of the beacons and the reported events with the tanimoto coefficient.The trust building for VANET in [108] was completed through location proximity, time closeness, and location verification. The receiver node measures its confidence on each message reported from unique senders about a specific event. The trust value is determined for each unique message reporting the same event. Then, the proposed method sorts the computed trust values to make the decision in favour of the particular message. The message validation-based approach in [109] consisted to assign the trust according to message similarity, message conflict and route similarity. The routing path parameter is involved to alleviate the fact that the probability of reporting similar tampered messages increases as more the senders share common nodes.

5.1.3. Combined trust management approaches

Authors in [93] established for location privacy enhancement in VANET aimed to distinguish trustworthy messages by treating beacon messages to compute entity trust, and verifying event messages and beacon messages plausibility to construct data trust. Cosine similarity is used to assess the trust of beacon

sender entity (based on position, velocity, and drive direction values). The proposed mechanism also takes into account the historical trust information of surrounding vehicles beacons. Data trust is evaluated in two dimensions, i.e., direct trust (beacons and direct received events), and recommendation trust. Direct event message trustworthiness is determined through verifying vehicle position and movement information; by using tanimoto coefficient additionally to the cosine similarity. Indirect event information trust is evaluated based on vehicles recommendations. In next step, event reputation value is computed to obtain the overall message trustworthiness. In addition, the Dempster-Shafer Theory (DST) is applied to combine transmitted opinions trustworthiness. The acceptance decision will be taken according to a trust degree threshold. Reference [110] studied a scheme that addresses VANET traffic data trustworthiness as well as vehicle nodes, by behaviour assessment and similarity rating. The scheme proposed DST-based data analysis as an evidences combination phase, serving for trust evaluation. The trustworthiness of data is measured through reported traffic information similarity. Nodes trustworthiness is described using functional trust which denotes how likely the vehicle can conduct appropriate behaviour (the scheme assigns for each node a function of misbehaviours observed by neighbouring nodes), and collaborative filtering-based recommendation trust. Cosine similarity is applied to help the evaluation of recommendations credibility. Specially, trust rate formation, trusted neighbour selection, and predicted trust rate computation are carried to help define the recommendation trust. Another trust-method that combines behaviour and similarity factors is proposed in [111], for VANET traffic signal control-applications. The approach enables the detection of the malicious data that are injected by Sybil attack. The trust values are assigned through the verification of the similarity between the expected and the real behaviour (i.e., driver reaction face to traffic signals) of a vehicle, and the similarity of neighbour vehicles generated messages. In a different work, authors in [112] integrated the particle filters to carry out the plausibility check and estimate the trust of neighbour nodes. They performed the aggregation of the different data in one particle filter per neighboring node to

avoid the duplication. The separate particle filter aims to achieve a local consistency verification of location-related data in each vehicle. The assessment of the trustworthiness relies on the trust value of the analyzed message and the sender confidence (history-based). The integration of Perron Frobenius theorem was studied in [113] to execute trust management in VANET and deal with the absence of the majority of direct trust metrics. The estimation of trustworthiness takes into consideration the types of received messages, the direct interactions and the recommendations from vehicles, and the content of the messages. The problem of information cascading and oversampling in VANET was studied in [114]. A voting scheme is proposed to decide the opinions of nodes based on the received messages. Each vehicle has different opinion weight according to its closeness from the reported event. Higher weights are given to vehicles which are situated close to the event. To address traffic message plausibility in VANET, an event-based reputation system was elaborated in [115]. The main functions supported in this system are event management, reputation adaptation, event reputation collection, and event confidence list collection. The event reputation score defines the intensity level of a traffic event. The reputation of the vehicle is increased by one once this vehicle detects the traffic event. The confidence score indicates the reliability degree of the traffic event. Considering these factors, the event intensity and the event reliability are evaluated at the same time. The approach presented in [116] used context to filter bogus messages. The trust computation is conducted by the analysis of the different messages that report the same event, considering previous knowledge and majority consensus. Thus, each message has to be validated by many vehicles before the event is regarded as true. The database that maintains the trust values is cleaned periodically by discarding faulty messages. The objective of work [117] is to make adaptive decision to improve the efficiency of the trust management in VANET. The decision making scheme will trigger when the time delay exceeds the defined threshold, or in case where the number of received messages overrides the specific threshold. The decision is made according to the trust degree computed through reporting events.

5.2. Our classification of trust management approaches

To date, there are different techniques devised for managing trust when deploying vehicular networks. The conceived approaches include broadly both artificial intelligence-enabling conventional schemes such as fuzzy logic and game theory variants, and current machine learning-based schemes. More recently, various advanced technologies have been leveraged to assist in vehicular trust management such as Cloud, Fog, Edge computing, Software Defined Networking (SDN), as well as Blockchain technologies. We can point out, in this context, trust modeling within 5G-based network architecture [118][119]. Differently, some works leveraged other tools, such [120] which adapted Web of Trust for VANET trust management. In this section, we classify the recently presented solutions into the two following categories: (1) trust management in artificial intelligence-enabling techniques for vehicular networks, and (2) trust management in emerging technologies for vehicular networks.

5.2.1. Trust management in artificial intelligence-enabling techniques

Machine learning has recently emerged in security enhancing mechanisms. Different underlying methods have been employed in developing the trust-based vehicular networks models, such as clustering (is the key element), as well as reinforcement learning and other heuristic algorithms.

- Clustering & Reinforcement learning-based approaches

Clustering based approaches consist to group similar objects, in which a center cluster denoted as cluster head is responsible for the coordination of the data exchange between all nodes within its cluster (intra-cluster communications), and other clusters (inter-cluster communications), and all other management tasks, including trust assessment. In vehicular cluster formation-based trust model, the scheme elects the node with highest trust value as a cluster head among all entities group for receiving other data requests. This fact can help in enhancing resources system utilization; e.g., by means of service priority-based allocation by the elected head. In this context, the scheme in [121] used a composite

metric that encompasses assigned vehicles trustworthiness values and related available resources. Each node possesses a trust score assigned by its neighbouring vehicles (behaviour-based). The available resource computation takes into account nodes link capacity and remaining power factor, for later determining nodes acceptable resources requirement. The selection of the cluster head and its proxy is then held through highest composite value (e.g., whenever a new better composite metric value node is added or the elected node trust score starts to fall, the selection of the head cluster is held by random). Another trust management-based clustering algorithm and stability was suggested for VANET in [122]. Trust management is event specific which is defined by trust data and trust communication metrics. Stability refers to vehicle mobility similarity factor. Three phases were required to define nodes cluster role (i.e., cluster head or cluster member). These phases consist of (1) neighborhood discovery (considers only neighbours with the same direction), (2) cluster head election, using a backoff timer solution (trust score calculation is based on reputation, and mobility and direction similarity), and (3) cluster stability maintenance. Two main phases were defined for global trust value assessment (trust data and trust communication). The first step consists in supervising vehicles behaviour; regarding cooperation with other nodes (Beta reputation system-based) and information reliability in terms of exchanged messages legitimacy (event reputation-based), and data-trust determination (severity metric-based). VANET nodes can provide opinions about whether the data can be trusted based on a combination of role and experience metrics in [123]. The approach extended a cluster-based routing scheme by incorporating an identity-based aggregation mechanism for the aggregation and the propagation of the trust. Besides, the relay control scheme is included to serve as a filter of malicious messages during the propagation module. The proposed framework in [124] relied on a bio-inspired and trust-based clustering approach to deal with the high overhead problem in WSN based ITS. The trust is associated with two levels. In the node level (normal node and cluster head node), the cluster head computes trust values of its cluster members. Each cluster member measures trust value for its one hop neighbor.

Then, the cluster head aggregates the trust value computed by its cluster members to find their final trust value. In the base station level, the node sends the estimated trusts to the nearest base station to aggregate them and find the final trust. The Bat optimization algorithm is applied to select the cluster head based on the residual energy, the trust value, and the number of neighbours. Some other recent methods are presented to support the trust management upon the clustering algorithm for unmanned aerial vehicle-assisted VANET such in [125]. The paper incorporated unmanned aerial vehicles to assist in routing and dishonest vehicles identification (e.g., when roads are disconnected, unmanned aerial vehicles can help to relink communications). Two routing ways are introduced: (1) routing data among vehicles with the help of unmanned aerial vehicles to reduce delay and overhead, and (2) routing data among unmanned aerial vehicles. The cluster heads are selected by the unmanned aerial vehicles based on the speed, the position and the trust parameters. The ant colony optimization algorithm is applied to improve routing process, and the trust score is knowledge and recommendation-based. A noteworthy classification-based trust solution was also introduced in [126] to alleviate the adversarial effects of misbehaving nodes in IoV. Reinforcement learning-inspired trust management solutions are used in general to adjust the evaluation (i.e., decision-making) strategy, and help entities to get maximal reward [127][128][129]. Other heuristic algorithms-based trust proposals such Support Vector Machine (SVM) and neural network can be found in [130][131]. Finally, collaborative intrusion detection system for VANET was studied in [132] using ensemble learning and shared knowledge. In this proposal, each vehicle elaborates a set of weighted random forest classifiers, for which aggregation takes place by means of a voting scheme. Each vehicle trains the local classifiers and shares its knowledge on-demand. The shared classifiers are considered as trust factor.

- Fuzzy logic-based approaches

As trust is determined through approximation (i.e., exchanged data might be inaccurate, incomplete, imprecise), some existing works elaborated their methods

by mean of plausibility checking as a suitable solution for tackling uncertainty, and measuring data and source accuracy [133][134]. For example, authors in [133] conducted the trust management through fuzzy logic-based method. Every node adds a unique encrypted ID to its submitted messages. By this way, receiver node can verify the message source node. Hereafter, three behaviour aspects were presented to conduct the trust estimation: cooperativeness, honesty, and responsibility. These metrics are assessed for each neighbour, and are jointly considered in fuzzy logic, where they will be converted to fuzzy values, and applied to fuzzy rules and defuzzification step for final trust level computation (a high value means that the node has a good cooperation behaviour). The honesty metric refers to honest forwarded packets percent. The responsibility corresponds to trustee node work regarding event reports detection.

- Game theory-based approaches

Game theory is likewise appealing for trust management in vehicular networks, since it represents an effective tool for nodes behaviour analysis (e.g., by means of clustering and cooperation incentives) [[134]-[141]]. Reference [134] established an approach to help vehicles define the trust of other entities (reputation-based) for better messages legitimacy assessment. The work applies the certainty factor theory to quantify vehicle trust. Direct reputation data are gathered and stored in a history communication table, as usual from direct interactions, and indirect reputation is build through neighbours feedback (experience-based trust rate) and RSUs reported recommendations. fuzzy C-means clustering method is also applied in indirect-reputation establishment to distinguish trustworthy reported messages. Then the uncertain deductive theory is employed to combine both computed scores. Moreover, the evaluation of the received contents legitimacy is achieved through attribute-weighted K-means algorithm. The received message is discarded once its sender has a reputation score lower than the defined threshold, otherwise the content is forwarded as its sender is recognized as a trustworthy node. Achieving nodes cooperative behaviours is also a main goal of the work. At this end, authors developed an

evolutionary game theory-based incentive scheme. The game model comprises nodes clusters (normal, selfish, and malicious), nodes adopted strategies (i.e., willingness for receiving, forwarding, or releasing data), and payoff computation (based on reputation value). Similarly, based on evolutionary game theory, the authors of [135] addressed trust within IoV system. The idea is to simulate the dynamical protection process within a reputation-based trust running example, under an evolutionary game framework, by modeling misbehaving nodes attacking strategies, to define its effectiveness. Reputation scores are assigned for both vehicles and traffic related event messages. In terms of trust computation, a punitive reduction ensued on reputation values (e.g., values will be decreased by one unit) when receiving false reports, or removing sent messages. One important factor that was taken into consideration when deploying the trust game model is the deception intensity, which refers to node deceptive behaviour and defines the false reports sending strength. Every malicious node decision is influenced by others. The strategy of these nodes is the deception intensity (related to node's proper utility). Obviously, dishonest nodes will make a heuristic change in the decisions distribution to converge to the optimal choice (i.e., the best negative system impact on the communication system), according to the reputation scheme feedback. The evolution in this trust mechanism is reflected with selection process (malicious node eviction) and reproduction process (nodes joining/rejoining). Reference [136] presented a scheme for IoV securing communications, using cooperative game theory. The proposal adopts the hedonic coalitional model for the vehicular trustworthy coalitions formation. (i.e., forming coalition or modeling vehicle collaboration by means of vehicles trust integration to build trust relationship preference that help in confidence decision making, i.e., coalition joining intention). Vehicle trust is established through Bayesian inference method based on experience assessment from direct interactions. The trust evaluation process goes as follows: whenever a vehicle receives an event message from another, the content of this message is compared to the real event state, which enables the vehicle to update the sender trustworthiness score using incomplete beta function. The process applies the

punishing strategy for newcomer vehicles once the absence of its previous interactions. In next step, the coalition formation algorithm is executed periodically to capture trust scores changes variation and derive new coalitions. The algorithm utilizes vehicles trustworthiness and preference relation parameters to form the final coalition. Each vehicle makes its decision for moving between coalitions according to its utility, by applying the shifting rule. An attacker and defender trust game approach was conducted in [137], where it comes with three main parameters measurement for each node and Nash equilibrium application, to help set vehicles trustworthiness and find the win-win strategy. The first parameter betweenness centrality refers to the number of times the node is crossed during a shortest communication route between nodes pair; the node is more central when it is frequently accessed. Such factors as hops count, nodes distance, intermediate node number, and connections number are related with betweenness measure. The second parameter majority opinion corresponds to nodes trustworthiness levels measure, which relies on events trustworthiness and nodes type trustworthiness correlation that enables defender to establish opinion on certain misbehaving nodes. The hop distance factor could also affect this parameter. The last important parameter is node density. It helps determining the number of neighbouring nodes with similar velocity and direction. The computation of the three considered parameters is supported with communications log. Obviously, the outcome of these parameters values differ for a defender and attacker situation. The Nash equilibrium implementation goes through the game matrix (payoff matrix), e.g., having good trust, centrality, and node density values, is the attacker desirable scenario, as it will initially behaves as a benign node before launching attacks. Authors in [138] provided a signaling game-based trust management solution. They adapted the Spence's model to VANET context to filter out malicious nodes and obtain a collaborative network. Markov chains was also used to validate this proposed heuristic. The idea behind reproducing this concept, is that asymmetric information are spread in vehicular environment, which makes the build of truthful relationships difficult. To deal with this, signal values (credits) are allocated to each

node according to its behaviour and used as node trustworthiness guarantee for receivers during data sending. These signals are observable by others nodes. Furthermore, inciting rewards are proposed to improve selfish nodes cooperation. The eviction of misbehaving nodes depends on credit count exhaustion (e.g., node's resources). The sender node selects a signaling value attached to its content and sends both of them to a trusted platform module to manage its credit count (the platform performs also cryptography functions). The signal value is then returned to its source. Once, this latter send its content, the receiver node asks the platform module to check transmitted signal value signature for content legitimacy evaluation. The message assessment is made also on the basis of sender reputation value (directly monitored behaviour as referred above). A reported refusal message is sent to the message source if the receiver node refuses the content. The sender credit count is raised by a reward when it obtains a majority recipients' positive returns. An incentive model was also proposed in [139] in order to tackle selfish nodes in VANET. The credits functions are implemented to handle nodes' accounts according to their behaviors. Each node keeps a signal to establish a reference of its actions in the communication system, and upon credit verification, it can receive reward. The credit is dependent on the reputation metric. Finally, If the node runs out of signals, it is considered as misbehaving node. Authors in [140] presented a game theory based multi layered intrusion detection scheme for VANET, along with a distributed cluster head selection algorithm. They employed a lightweight neural network based classifier to recognize the malicious nodes. Also, they used a Vickrey-Clarke-Groves-based incentive structure to promote the vehicles' participation in the head election procedure. In addition, reputation scores are maintained by the RSUS nodes to assess the trustworthiness of the cluster head (behaviour-based).

5.2.2. Trust management in emerging technologies

We introduce in this subsection some of the recent trust management approaches for vehicular networks that leverage advanced technologies such as

Cloud, Fog, Edge, Blockchain and SDN.

- Cloud computing-based approaches

Cloud computing technology features have been exploited in recent research to support the solve of trust issue and its deployment. The merits of Cloud in the design of trust management schemes for vehicular networks are available in literatures [[142]-[147]]. As for instance, research in [142] built a three-layer Cloud-based trust management framework for a vehicular social networks scenario. The network architecture includes (1) a central Cloud layer (server clusters group), (2) a road-side Cloud layer as a trust manager, and (3) a vehicular Cloud layer to support vehicles resources utilization. Accordingly, trust is managed at three levels: (1) the global trust manager, linked with the central Cloud layer, where all vehicles profiles are recorded (e.g., communications history trust list), (2) the domain trust manager, linked with the road-side Cloud layer; this level maintains vehicles trust evaluation requests service and conducts trust degrees computation (through neighbouring nodes trust, friends trust, and history trust values), and (3) the overall trust degree evaluation level, which is associated with the vehicular Cloud layer. Hence, the trust management procedure is summarized as follow: the vehicle sends a request to vehicular virtual machine (created from road-side servers) to get sender message trust. The virtual machine undertakes, first, neighbours and friends trustworthiness calculation. Second, the history trust is got from central servers. Thereafter, the overall trust degree will be sent to the requester vehicle and the central severs for updating. Authors in [143] suggested an interdependent strategic trust approach for autonomous vehicles within a Cloud-based environment. The presented framework is composed of three layers. In the Cloud layer, the Cloud services security are threatened by attackers and maintained by network administrators. The interactions at Cloud services are captured using a flipit game [144]. The communication layer depicts the interaction between the Cloud and the device which decides the Cloud services trustworthiness, through the use of signaling game (reputation and knowledge based trust). The physical layer

consists of the control performance which quantifies the utility of the device, the attacker, and the defender for the signaling game. The decision making in this design is based on the players strategies at the Cloud layer, and the physical layer performance. The work in [145] addressed the trust computation in VANET-Cloud trust management approach. The process of the trust establishment comprises three phases. The first step is DST-based data preprocessing phase. The second step consists of fuzzy analyzer phase to decide the level of trusted and untrusted vehicles (based on direct and indirect trust values). The third phase applies an algorithm to give rewards or penalty for messages senders. Whenever a vehicle needs neighbouring vehicle trust score, the cloud can be queried to get the trust information within time limit. In [146], the authors presented an agent based intelligent architecture which can build trust within vehicular Clouds. The method consists of mobile and static agents working in coordination to estimate the trust on both Cloud service provider and Cloud service user. The calculation of the cumulative trust is performed using the direct and the indirect trust values. The direct trust refers to the accounts past transactions. The indirect trust computation is done by a mobile agent which aggregates the trust factors in vehicular Cloud and Cloud service providers.

- Fog/Edge computing-based approaches

As within vehicular Cloud, some ideas were elaborated for trust management in vehicular Fog computing environment to take advantage of computing capacity extending and offload computation from Cloud to Edge nodes [[148]-[151]][133]. For instance, the work [148] relied on bidding price-based approach for guaranteeing trusted Fog service transaction in rural area: The registration to infrastructure-based Fog node is required for each vehicle client to conduct Fog service transaction (through certificates). During registration, vehicle client deposits digital currency for bidding. After being accepted, vehicle client may make activities within the uncovered area, as a result, the Fog computing service is extended by exploiting infrastructure-based Fog node resources. This is where

the need to build trust comes in. The trust computation takes into consideration transaction on rural area (based on node type, bidding number, and transaction record) and global transaction (i.e., transaction with infrastructure-based Fog node). Lastly, according to computed scores, malicious activity may lead to actors bidding, and accordingly trust loss and victim compensation (redeem point gain). Reference [149] suggested to ensure trust in the implementation of an Edge-based vehicular environment, wherein Edge computing servers undertakes the work of executing local reputation management requests. To summarize, local authorities nodes (assumed trusted) schedule Edge servers to promote trust building responsibility consisting of reputation value's query, calculation, and manifestation. Each vehicle uploads reputation segments (behavior-based) of its one-hop neighbours to the nearest local authority. Aggregated reputation segments are then weighted (based on familiarity, similarity, and freshness) for timely update. These values are also stored simultaneously in a global reputation base. Vehicle can query newly passing vehicle reputation before cooperating with. Hence, the local authority exhibits the intended reputation score. The research proposed, as well, the concept of reputation-assisted resource optimization. In [150], a trust approach that uses edge nodes (substituting RSUs) is presented for securing VANET. The upper layer of the communication system consists of trusted authority and Cloud server, and the lower layer is represented by Edge and vehicle nodes. The trustworthiness of both sender entity and message are assessed by performing fuzzy rules. To this end, the proposal applies plausibility (location verification-based), experience, and vehicle type (i.e., for assessing authentication level) to calculate the trust score. Using the Cloud server, the trusted authority generates the main parameters to the Edge nodes and vehicles. The Edge nodes maintains the authentication level assigned to each registered vehicle. In order to extract the trust level, a query from the relevant Edge node is performed. On the basis of this trust score, the receiver vehicle makes the decision on the sent message. Finally, it is worth mentioning that the work used the k-nearest neighbors algorithm and the Cuckoo filter, to deal with the none line of sight condition and the volume of generated data,

respectively.

- Blockchain-based approaches

More recently, Blockchain technology is having an increasing interest for trust management in vehicular networks environment, by dint of its features. It is widely acknowledged that this technology can deal with centralization, security, and privacy issues, when storing, tracking, managing, and exchanging data. We refer here a few trust management research that adapted Blockchain [[152]-[156], including privacy preservation [157][158]. As example, authors in [152] designed a trust management solution for vehicular networks using Blockchain technology. The main procedure of the approach comprises rating generation and uploading phase, trust value offsets computation phase (node proprieties-based), miner election, new blocks generation phase, and consensus application phase. Receiver node assesses messages credibility based on Bayesian inference rule. According to the validation result, it generates score for each received message. Next, it uploads computed rates to RSU entity. The second phase consists in using weighted aggregation to obtain involved vehicles trust value offsets and pack them into a candidate block. Applying a proof-of-work and proof-of-stake algorithm, a miner is elected for new offset blocks generation (here, the consensus mechanism considers offsets absolute values as stakes, so, RSU with large stakes is more likely to be the miner). Once being validated, the new offset block is added to the trust Blockchain. Note that, the consensus algorithm deals with the Blockchain fork, in the case of receiving at similar time many blocks. The Blockchain-based trust management proposal [157] was combined with privacy-preserving scheme which is conducted by identity-based group signatures, for an effective conditional privacy. A consensus algorithm that exploits Proof-of-work and Practical Byzantine Fault Tolerates algorithm was further placed for efficiency reinforcement. The solution comprises a trusted authority entity which maintains the whole communication system (e.g., nodes registration, vehicles secret/public keys generation), as well, naturally, RSUs nodes with consistent ledgers. By this way, the trusted authority entity is able to trace dishonest

vehicle identity with the pseudonym in Blockchain. The anonymous packets aggregation process consists of generating an initiation packets for inviting other vehicles to join announcement, and then verifying signatures validity to produce responses and generate an aggregation packet. This latter will be then verified by the nearest RSU of the sender. When an event is produced, many initiators nodes send messages to nearest RSU. The RSU entity evaluates the initiators credibility through their reputation values (logistic regression-based). The reputation data is, then, stored in blocks. Next, a miner will be elected to add the new correct blocks into the Blockchain. The consensus algorithm will help to synchronize the trust data. Finally, malicious vehicle address will be removed from the Blockchain, which enables the trusted authority entity to add it to the revocation list. Similarly, the study [158] exploited Blockchain to design an anonymous reputation management method that deals with trust and privacy in VANET. Blockchain is placed to preserve privacy-authentication, during estimating trustworthiness. There are different components in the proposal such as (1) the certificate authority which manages certificates. The carried actions of this component are registered into the Blockchain, (2) the law enforcement authority which is responsible for vehicles' registration, supervising, and reputation assessment. It holds a dataset of public keys' and real identities linkability, (3) the certificates Blockchain (i.e., distributed certificates ledger), the removed keys Blockchain (i.e., revoked keys ledger), and (4) the messages Blockchain. Once being received, the certificate validity is verified, then, proofs of presence and revocation within concerned Blockchains are put. This procedure refers to the anonymous authentication algorithm. The reputation management (experience and recommendations metrics-based) adapts reward and punishment models to enhance trust establishment. Authors in [153] developed a two layered Blockchain architecture in which IoV nodes are able to evaluate the trustworthiness of each other. The trust is formed through reputation and location metrics. The proposal uses local Blockchains to deal with lower delay requirement in the IoV. Edge nodes are introduced to complete a local trust management, whereas the RSUs nodes host the general Blockchain to exhibit the global trust of the

communication system. The Blockchain was used along with deep learning algorithm in [154] to manage the trust in vehicular networks. Each vehicle assesses the messages received from the neighboring vehicles. The vehicle reports the identified untrustworthy vehicles to the nearby RSU node. The authenticity of the report and the identity of the vehicle are verified using the Blockchain. Next, the trust credentials of malicious vehicles are revoked by the RSU node. In [155], the regional federated learning was proposed to enhance the security in Blockchain-enabled IoV. The vehicles are divided into many regions to maintain local learning models, and a reputation mechanism is designed to ensure the trustworthiness of vehicles participating in the regional learning. Reference [156] provided trust in Named Data Networking (NDN) driven VANET using Blockchain.

- SDN-based approaches

Many studies have been concentrated on SDN incorporation in the vehicular networks over the past couple of years. SDN benefits like flexibility, programmability and infrastructure abstraction have been exploited in vehicular networks implementation to assist in improving QoS, resource utilization and network optimization. Reference [159] investigated the impact that SDN may have on VANET security. The related measures that SDN could provide against traditional security threats in vehicular networks are introduced, along with trust management establishment. The study supports the feasibility of the SDN paradigm within different uses cases like smart parking and smart grid of electric vehicle, and shows that the SDN can be instrumental in managing vehicular networks when using the trust factor. Likewise, authors in [160] deliberated the need of trust-based approaches for securing vehicular networks, as well the trust management concept vis-a-vis SDN-enabled vehicular networks. They assume that the SDN can probably better understand the nodes' behaviours (e.g., in case of sudden rise in the trust scores of a node with historically associated low trust scores). Consequently, it can perform appropriate actions and eliminate both malicious and selfish nodes. Authors in [161] aimed to identify the ma-

licious vehicles in SDN-based VANET using the trust factor and avoiding the untrustworthy vehicles. They proposed a double security check by means of trust based detection algorithm and malicious vehicle detection scheme. The SDN consists of "forwarding", "reverse", "trust of forwarding vehicle", "trust of reverse vehicle", "path trust", and "network performance", and the RSUs nodes undertake the work of trust scores calculation by verifying the licence plates of the vehicles. Moreover, the decision problem for routing selection in vehicular networks has been addressed in many works. The problem lies in discovering the best path, and the route selection can depend on various parameters e.g., the trust data. Thus, different approaches have been developed in such context, exploiting the SDN features. As an example, a SDN-based framework in VANET with trust management was suggested in [162]. Applying the on-demand distance vector routing, the proposal presents the control logic of VANET within the control entity to enhance the network performance. Hence, the framework structure consists of: (1) data forwarding layer, (2) controller layer to discover data route and manage network topology, and (3) application layer for controlling routing procedures. The node' trust value relies on the data packet forwarding ratio and the control packet forwarding ratio. However, considering the end-to-end delay, the proposal needs to be more enhanced. Reference [163] introduced a misbehavior detection system. The main tasks of the control plane in this system include: (1) vehicular clusters formation, (2) Watchdogs election, (3) trust assessment, (4) Sybil attacks detection, and (5) security parameters adjustment. A Watchdog supervises the surrounding vehicles and transmits its reports to the local SDN controller. This latter monitors the clusters members and determines their trust values. The reports of the local SDN controller are then sent to the regional SDN controller, which will in turn, monitors the local SDN controllers and computes their trust scores. Next, the regional SDN controllers gather all the vehicles' trust scores and the final report is transmitted to the global SDN controller. The calculation of the trust scores is based on the interactions of the vehicle with the local SDN controller and the Watchdogs, and the cluster head is selected according to the trust and the mobility

factors. An hybrid SDN-based geographic routing protocol was elaborated in [164]. The routing process applies a trust management model and an encrypted function. The nodes of the network are grouped into clusters. Each cluster head represents a semi-centralized controller and hosts the communication errors' log related to its clusters. The cluster members contain the distributed controllers. The cluster head selection is based on a map factor (i.e., a factor in which a vehicle maintains its public key and the weight of its neighbors). The weight of each vehicle is estimated from the load capacity determined from the received beacons and the trust level. The trustworthiness is deduced from the past interactions recorded in an error log. Authors in [165] employed the deep reinforcement learning in VANET routing, leveraging on the SDN. They separate the data forwarding plane from the control plane. The proposal consists mainly of path learning and trust establishment processes. The deep reinforcement learning algorithm is deployed into a centralized controller. Accordingly, honest nodes aim to discover the highest path trust score in order to establish data transfer. The path learning procedure applies deep Q-learning based convolution neural network algorithm, and the trust level is assessed using the packets forwarding ratios. Similarly, the authors evaluated the effectiveness of a trust-based dueling deep reinforcement scheme, wherein the SDN controller acts as a learning agent to find the high trusted routing path by means of deep neural network in [166]. Afterwards, the two works [[165], [166]] were extended to adopt the Markov decision process within the trust model, and consider further the reverse delivery ratio to assess the communication quality link [167]. In [168], authors investigated trust evaluation in VANET architecture leveraging SDN with Fog computing. The overall trust score is derived through reputation, experience, and understandings about the trustee node. The assessment of the reputation value can be deployed at the SDN controller, whereas, the experience-based trust value can be kept in the SDN controller, or in a distributed system (i.e., entity like vehicle, RSU, or base station can perform local storage and calculation). Two methods were applied in this study; the first method makes use of mathematical models (e.g., weighted sum, or Bayesian neural networks) to com-

pute experience, reputation, and quantitative attributes. The second method uses an inference engine to derive trust data from an existing knowledge base. Authors in [169] addressed the trust management in an hybrid IoV architecture leveraging SDN with Blockchain. Behind the idea of building trust at the SDN control layer, the use of Blockchain was conceived. In sum, the system aims to control application identity and behaviour, and network resources allocation and management. The SDN controllers are considered as Blockchain nodes maintaining an encrypted database (evidently as known, database modification requires all entities agreement). On the basis of application's identities cards and trust index creation (behaviour-based), the trust management is carried and the communication between applications and SDN Blockchain-enabled controllers is achieved. Authors in [170] introduced a consortium Blockchain-based trust management scheme for vehicular SDN. The scheme elaborates a PoS-mPBFT algorithm to shorten the consensus time and improve the security. The trust is estimated based on the rating recorded in the distributed ledger. The rating refers to road-relevant messages. The measured trust value is used for the resource allocation problem. Accordingly, more resources are allocated for high trusted vehicles on the control plane of the SDN. Reference [171] presented a trust management approach for SDN-enabled 5G-VANET. The SDN data plane is separated from the control plane. The data plane is made up of the vehicles, the RSU nodes and the 5G base stations. The RUS nodes along with the 5G base stations are controlled by a centralized SDN controller. With the support of the Blockchain, the RSUs nodes verify the realness of the traffic data using the location proximity metric. In [172], the Blockchain was incorporated with the SDN and the Fog to efficiently manage and control the network in VANET. The Fog technology was introduced to avoid frequent handovers. The devices in the Fog zones are SDN-enabled. Moreover, the SDN control plane includes a Blockchain layer. The Blockchain was designed to support a reputation-based data propagation among the connected peers. The trust feature was also considered in [173] to enhance the throughput of Blockchain-SDN-enabled VANET. The network architecture contains device layer, area control layer, and domain

control layer. In the area control layer, the SDN controllers are able to collect the vehicles' trust. The trust data is then sent to the domain control layer which operates in the distributed Blockchain manner. The trust values are generated from the history of direct interactions.

6. Discussion

Based on the above survey, one can conclude that an effective trust management approach is required in vehicular networks to satisfy users applications' expectations. Diverse criteria as requirements could be defined for the evaluation of the proposal efficiency. These criteria are mostly based on the challenges within the advanced vehicular environment. We summarize the above surveyed approaches (in both presented classifications) in the following Tables 6, 7, 8, 9, 10 and 11 wherein we recap the approaches classes, the chosen trust metrics, the used tools and the selected simulation performance parameters, to enable a qualitative comparison. It is worth reminding that the acknowledged existing classification in trust that consists of entity-based, data-based and combined classes can serve as a core abstract classification. We mentioned that our taxonomy could be an associated sub-classification, and thus we conducted in Tables 6, 8, and 10 the assignment of both classes to the reviewed approaches in subsection 5.2. We remind that we introduced two general categories: (1) trust management approaches with artificial intelligence-enabling techniques, and (2) trust management approaches in emerging technologies-based frameworks. Hence, Tables 6,7 present the simple approaches of trust management in vehicular networks, Tables 8,9 depict the approaches of trust management in vehicular networks with artificial intelligence-enabling techniques, and Tables 10,11 show the approaches of trust management in vehicular networks with emerging technologies. Moreover, we selected the following overall criteria to further illustrate the difference between surveyed approaches: (1) dynamicity, (2) scalability, (3) complexity, (4) communication overhead, (5) robustness, and (6) privacy.

(1) Dynamicity: From Tables 7, 9, and 11, we see that a lot of referred approaches have satisfied dynamicity criteria (i.e., mobility patterns dependence, low infrastructure dependence, dynamic trust metrics, fast trust values update with larger variations, etc.). Usually, major data-based models are more dynamic than entity-based models (e.g., infrastructure less-based to extract global trust, there is no need for long interactions between nodes; e.g., contrarily within reputation-based models which may lead to connection loss when trust assessment, due to high nodes speed).

(2) Scalability: Scalability has also been in the interest of the previously-discussed approaches (i.e., persevering network performances regardless network size and traffic density; e.g., better detection, communication ratios with high density, or stable network results with high malicious nodes number, etc.).

(3) Complexity: Complexity (mainly, time complexity criteria) attribute should be as well considered for reliable performance evaluation. In fact, the importance of slight trust computation and fast data dissemination is high, in vehicular network environment (e.g., it is crucial to quickly derive accurate trust value; almost instantly for time critical-based applications). Most related-simulations experiments showed, for instance, that the delay of malicious nodes detection remains proportional to network density, besides, the delay can increase mainly with indirect trust computation.

(4) Communication overhead: Communication overhead as crucial parameter refers to the amount of forwarded packets. Therefore, the lower communication overhead ratio is, the more efficient the network is (e.g,. lower bandwidth use; cost-effective network; accordingly, fast and better real response time, etc.). However, this parameter has been not satisfied (or not really considered) in major previously discussed approaches. Only a few simulation results such in [111] showed, for example, that as the malicious nodes number increases, the forwarding rate decreases.

(5) Robustness: Because the basis of trust in vehicular networks is to distinguish dishonest nodes, so as to ensure reliable (further accurate) data delivery, robustness must been taken into account to define the communication system

security level. We identified reviewed approaches as (1) partially robust, and (2) robust (i.e., the proposal is partially robust when attacks are very slightly addressed).

(6) Privacy: Moreover, privacy criteria is obviously important when conceiving and evaluating such approaches. Yet, we can notice from Tables 7, 9, and 11 that a privacy preservation is lacking (except [157][158][171]).

In sum, artificial intelligence-enabling techniques have comparatively assisted in intuitive trust scores generation, approximation reasoning (e.g., fuzzy logic-based), better decision selection (e.g., Q-learning-based), malicious actions reducing (e.g., clustering-based; election of honest cluster head, game theory-based; incentive mechanism), and nodes selfishness coping (e.g., cooperative game-based), but also have faced some QoS concerns; mainly related to communication overhead and time complexity. Emerging technologies have proved their usability, as supporting more dynamicity, scalability, and typically efficient resource utilization that enhances QoS. As an example, Edge; Fog computing and SDN help in optimizing resource allocation, providing lower delays; simple time complexity and hence reducing transmission costs. Regarding security level, Table 11 clearly tells about robustness performances of Blockchain-based trust approaches. However, the incorporation of such technologies requires trust management solutions in vehicular networks to be revisited. This opens future research directions for trust management in vehicular networks.

7. Future directions for trust management in IoV

1. Considering the global IoV ecosystem: most of the exsiting approches proposed to define trust mechanism within IoV environment are based on the vehicles as trustee and trustor entities. An efficient trust management model should include the human dimension, the vehicles as well as infrastructure entities to be suitable to the IoV context. Considering the trust only on the VANET scope when dealing with IoV is limitative and may lead to non realistic models. Thus, well built trust models will be based

Table 6: *Summary of surveyed approaches: simple approaches*

Ref	**Class**	**Trust metrics**	**Used tools**	**Simulation**	
				Setup	Specific evaluation criteria
[94] 2012	Entity	Reputation	-Probability functions	Self-developed simulator: -Numb: vehicles, malicious nodes, RSUs, hops -Trust level	Accuracy of correct received messages -Scalability (+-collusion)
[95] 2015	Entity	Node proprieties (similarity)	-Association rule mining -Echo protocol	SUMO: -Numb: vehicles, malicious nodes -Traffic segment -Listening period -Trust level	Success rates (% of vehicles that believed true reports/false reports
[96] 2010	Entity	Node proprieties +knowledge (multifaceted)	-Defined formulas -Signature-based	SWANS: -Numb: vehicles, malicious nodes -Trust level	-Average speed of nodes (according to the % of malicious nodes) -Detection rate of malicious nodes -Communication ratio
[97] 2010	Entity	Reputation+ knowledge+ node proprieties	-Defined formulas	-Numb: vehicles, malicious nodes -Simulation time -Vehicle speed -Trust level	-Effect of malicious nodes on traffic congestion -Effect of role factor on traffic congestion -Effect of knowledge and role factors' combination on traffic congestion
[98] 2013	Entity	Reputation	-Statistical regularity method	not available	not available

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[99] 2016	Entity	Reputation	-Iterative filtering method	Matalab-based: -Numb: vehicles, malicious nodes -Simulation time -Trust level	-Vehicle' services quality level -Feedback accuracy level -Trust values measurement -Resilience to badmouth attack and ballot stuffing attack
[100] 2019	Entity	Reputation+ knowledge	-Markov method	Netlogo SUMO, NS-2: -Numb: vehicles, malicious nodes traffic lights -Simulation time -Transmission range -Vehicle speed, length -Trust level	-Detection rate of malicious nodes -Accuracy of malicious nodes detection -Packet delivery rate -Average end to end latency -Numb: transmitted control packet, transmitted total packets
[101] 2015	Entity	Reputation+ knowledge	-Correlation coefficient -Signature-based	Matlab-based: -Numb: vehicles, malicious nodes recommenders -Trust level	-Trust degree distribution - Indirect trust evaluation
[102] 2019	Entity	Reputation	-Elliptic curve method	Simulator not specified -Trust level	-Computation cost -Communication cost
[103] 2008	Data	Proximity (utility)	-DST-based -Signature-based	NS-2: -Numb: vehicles, malicious nodes, affirmative reports, hops	-Average trust level of malicious nodes -Speed of decision

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[103] 2008				-Trust level -Vehicles distance -Vehicle speed	
[104] 2014	Data	Proximity+ node proprieties +environment factors (similarity)	-Defined formulas -Signature-based	OMNET++, SUMO, VACaMobil: -Numb: vehicles, malicious nodes -Traffic segment length -Average speed -Average flow -Transmission range -Vehicle speed -Trust level	-Average density (+accident scenario) -Success rate (% of vehicles that received true reports)
[105] 2014	Data	Proximity	-Defined formulas -Signature-based	SWANS++: -Numb: vehicles, malicious nodes, reporters -Traffic segment -Transmission range -Trust level	-Fake location detection accuracy -False time stamp detection accuracy -False positives -Overall accuracy of malicious nodes detection -Time scarcity
[106] 2011	Data	Location+ node proprieties	-Ant colony optimization	NS-3: -Numb: vehicles, events -Road length -Vehicle speed -Transmission range	Data delivery delay -Performance under different observing condition

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[106] 2011				-Expectation of event values -Variance of perceived values	
[107] 2012	Data	Beacon	-Tanimoto coefficient	NS-2, SUMO: -Numb: vehicles -Transmission range -Beacon time to live -Event time to live -Vehicle speed -Trust level	-Precision, recall -Detection delay
[108] 2013	Data	Location	-Defined formulas	Simulator not specified -Numb: vehicles, malicious nodes -Trust level	-Effect of malicious nodes on trust -Time complexity
[109] 2013	Data	Messages similarity	-Defined formulas	Java-based: -Numb: received messages during defined period -Trust level	-Effect of conflicting value and path similarity on trust score -Effect of false messages on true messages acceptance -Processing time
[93] 2013	Hybrid	-Beacon+event +reputation	-Cosine similarity rule -Signature-based	NS-2: -Numb: vehicles, malicious nodes -Vehicle speed -Traffic segment -Beacon+Event time to live -Trust level	-Attacks detection rate -Misbehaving vehicle rate -Detection delay

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[110] 2015	Hybrid	Reputation+ knowledge+ environment (similarity)	-DST-based -Cosine similarity rule	GloMoSim: -Numb: vehicles, malicious nodes -Traffic segment -Transmission range -Vehicle speed -Vehicle placement -Trust level	-Precision, Recall of malicious nodes detection -Communication overhead
[111] 2016	Hybrid	knowledge+ node proprieties	-Defined formulas -Stochastic cellular	-Automata model: -Numb: vehicles, malicious nodes and data -Vehicle speed -Vehicles distance -Vehicle delay -Trust level	-Accuracy of malicious data detection -Average delay of vehicles with malicious data
[112] 2012	Hybrid	Knowledge+ location	-Particle filter	-Filter area size -Vehicle speed -Trust level	-Trust and confidence values with radar area violation -Runtime of particle filer -Accuracy of trust values measurement
[113] 2013	Hybrid	Reputation+ Knowledge+ message type	-Perron Frobenius theorem	not available	not available
[114] 2014	Hybrid	Knowledge+ location	-Defined formulas	NCTUns: -Numb: vehicles, malicious nodes -Path loss mode -Antenna options	Percentage of incorrect decisions

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[115] 2009	Hybrid	Reputation+ event	-Fibonacci number function	NS-2: Numb: vehicles -Transmission range -Event+ time simulation - Vehicle speed -Trust level	- Average accumulation speed of event reputation/confidence values
[116] 2011	Hybrid	Context	-Defined formulas -Signature-based	VNSim: -Numb: vehicles, malicious nodes -Trust level	-Effect of malicious nodes on trust values measurement
[117] 2014	Hybrid	Reputation+ event	-Decision making process	NS-2: Numb: vehicles, malicious nodes -Transmission range -Time to live -Vehicle velocity -Trust level	- Detection accuracy -Decision delay

Table 7: *Qualitative comparison of surveyed approaches: simple approaches*

Ref	Dynamicity	Scalability	T. complexity	C.overhead	Robustness	Privacy
[94] 2012	partially	partially	partially	not available	partially	no
[95] 2015	partially	partially	not available	not available	no	no
[96] 2010	yes	partially	partially	medium	partially	no
[97] 2010	yes	yes	not available	not available	yes	no
[98] 2013	yes	not available	not available	not available	not available	not available
[99] 2016	yes	not available	not available	not available	yes	no
[100] 2019	yes	not available	simple	partially	yes	no
[101] 2015	yes	not available	not available	not available	yes	partially
[102] 2019	yes	not available	simple	partially	yes	yes
[103] 2008	yes	partially	simple	medium	partially	no
[104]	yes	yes	complex	not available	partially	no
[105] 2014	yes	yes	partially	medium	partially	partially
[106] 2011	yes	not available	partially	not available	yes	no
[107] 2012	yes	not available	simple	not available	yes	yes
[108] 2013	yes	not available	simple	not available	yes	partially
[109] 2013	yes	not available	simple	not available	yes	no
[110] 2015	yes	partially	simple	low	yes	no
[93] 2013	yes	yes	partially	not available	yes	partially

Ref	Dynamicity	Scalability	T. complexity	C.overhead	Robustness	Privacy
[111] 2016	yes	partially	complex	not available	partially	no
[112] 2012	yes	yes	partially	not available	yes	no
[113] 2013	yes	not available	partially	not available	no	no
[114] 2014	yes	not available	not available	not available	partially	partially
[115] 2009	yes	not available	not available	not available	yes	no
[116] 2011	yes	not available	not available	not available	yes	no
[117] 2014	yes	not available	simple	not available	yes	no

on entities, on exchanged data and on environments constraints. In this case, hybrid solutions should be applied. Moreover, different properties and metrics should be considered.

2. Resiliency: some of the proposed approaches in literature consider an attack pattern to evaluate their model. However, the set of considered attack patterns do not cover the large scope of attacks that may occur on an IoV network. For that, the new approaches within such context have to define attack-free frameworks to ensure their resiliency. The resiliency is more critical when the connected vehicles are used in sensitive contexts such as the medical context (we can consider for example the connected vehicles when used as ambulances in emergency contexts).

3. Federated learning: the use of the artificial intelligence in the existing trust models aims mainly to define the trust formula. When considering the whole IoV ecosystem, a distributed approach of the intelligence on the different components of the IoV environment could be very useful to optimize the proposed model. Thus, integrated the federated learning approaches when building trust management approaches could has an

Table 8: *Summary of surveyed approaches: approaches with artificial intelligence techniques*

Ref	**Class**	**Trust metrics**	**Used tools**	**Simulation**	
				Setup	Specific evaluation criteria
[121] 2019	Hybrid	Knowledge+ node proprieties	Clustering-based: -defined formulas	Matlab-based: -Cluster size -Numb: malicious nodes, hops -Trust level	-Trust composite metric value with malicious nodes
[122] 2018	Hybrid	Reputation+ node proprieties (similarity)	Clustering-based: -defined formulas	Omnet++: -Cluster size -Numb: malicious nodes -Vehicle speed -Vehicles distance -Traffic segment -Trust level	-Cluster head duration -Cluster head election time -Rate of dishonest vehicles elected as cluster head -Packet delivery rate
[123] 2013	Hybrid	Knowledge+ node proprieties	Clustering-based: -defined formulas	C-based: -Percentage of authority roles -Average number of vehicles per cluster -Probability of turning left/right at cross -Traffic segment -Maximum distance for trust opinion	-Percentage of messages as Spam -System evolution time -Numb of deliveries in each hour

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[123] 2013				-Vehicle speed -Trust level	
[124] 2018	Entity	Knowledge	Clustering: -bio-inspired algorithm -bat optimization method	Matlab-based: -Numb: vehicles -Energy factor -Electronics of transmitter -Transmitter amplifier -Data aggregation energy -Packet length -Percentage of nominated cluster heads	-Network lifetime -Average residual energy -Average trust value of cluster heads
[125] 2021	Entity	Reputation+ Knowledge	Clustering: -ant colony optimization	NS-2, MobiSim: -Numb: vehicles -Trust level	-Packet delivery ratio -End to end delay -Average of hops number -Detection rate of malicious nodes -Communication overhead
[132] 2020	Entity	Knowledge	Clustering: -ensemble learning	SUMO: Numb: vehicles for training and testing -Transmission range -Vehicle mobility -Vehicle speed -Trust level	-Detection rate of malicious nodes -Accuracy of malicious nodes detection -False positives -False negatives

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[133] 2017	Entity	Knowledge+ Reputation	Fuzzy logic-based: -defined formulas	NS-2, SUMO, MOVE: -Numb: vehicles, malicious nodes, -Vehicle speed -Transmission range -Traffic segment -Trust level	-Correlation behaviour -Detection accuracy without collusion -Detection accuracy with collusion
[134] 2019	Entity	Reputation	Evolutionary game theory-based: -fuzzy C-means clustering -certain factor -Attribute-weighted K-means algorithm	MobiSim, NS-2: -Numb: vehicles, malicious nodes -Vehicle speed -Transmission range -Traffic segment -Trust level	-False alarm rate -Missed detection rate (message identification) -Accuracy rate of decision making -Throughput -Forwarding rate -Packet delivery delay -Cooperative nodes ratio
[135] 2019	Entity	Reputation	Evolutionary game theory-based	-Numb: vehicles, malicious nodes -Group distribution -Utility of groups -Overall utility -Vehicle speed -Traffic segment -Trust level -Payoff	-Nodes strategy changes -Average growth rate of overall utility

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[136] 2019	Entity	Knowledge	Cooperative game theory-based: (hedonic) -bayesian inference	Matlab-based: -Numb: vehicles, malicious nodes -Coalitions partition -Trust level	-Rate of compromised decisions -Rate of false reports in coalitions -Computational time
[137] 2017	Hybrid	Reputation+ knowledge+ node proprieties	Game theory-based: (Nash equilibrium) -probability functions	Matlab-based: -Numb: vehicles, malicious nodes -Transmission range -Traffic segment -Traffic type -Trust level -Payoff	-Retransmission attempts rate -Throughput -Data drop rate
[138] 2014	Entity	Reputation+ knowledge	Signaling game-based: (Job market signaling) -markov chain -signature-based -probability functions	NS2-34,SUMO, VanetMobisim: -Numb: vehicles, malicious nodes -Vehicle speed -Transmission range -Traffic segment -Data rate -Trust level	-Detection rate of malicious nodes -Percentage of false positive -Detection delay -Average ratio of corrupted data -Reception ratio with selfish nodes
[139] 2013	Entity	Reputation+ Knowledge	Signaling game-based: -defined formulas	NS-2, VanetMobiSim: -Numb: vehicles malicious nodes, -Vehicle speed -Traffic segment -Transmission range	-Detection rate of malicious nodes -False positives -Average ratio of corrupted data -Average ratio of received data

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[139] 2013			-Trust level		
[140] 2018	Entity	Reputation	Game theory+ clustering: -neural network -Vickrey-Clarke-Groves method	NS-3, SUMO: -Numb: vehicles per cluster -Simulation time -Vehicle mobility -Propagation model -Transmission range -Trust level	-Detection rate of malicious nodes -False alarm rate -Average cluster membership duration of vehicles -Intrusion detection traffic volume -True positives -False positives -False negatives

impact on its robustness since the role of different IoV entities could be different (humans, devices, infrastructure entities), and thus, their trust formula could be based on different metrics and different parameters.

4. Clustering approaches: the clustering techniques help alot in designing reliable trust management framework since the trust management is decentralized. However, these techniques can be improved when used with the association of the emerging technologies such as the blockchain or the SDN. These techniques can facilitate the coordination between the different cluster heads and bring better traçeability of the trust management process.

5. Trust Negotiation: the existing approaches are mainly based on a calculation process of the trust. This process can be alliveated through the use of trust negotiation mechanism. Further works can consider the trust negotiation through defining a procedure describing the requirements to reach the required trust level. When a vehicle or a human entity needs to join the IoV network, a negotiation process is trigerred in order to achieve

Table 9: *Qualitative comparison of surveyed approaches: approaches with artificial intelligence techniques*

Ref	Dynamicity	Scalability	T. complexity	C.overhead	Robustness	Privacy
[121] 2019	partially	partially	not available	not available	partially	no
[122] 2018	partially	partially	partially	medium	partially	no
[123] 2013	yes	yes	partially	medium	yes	no
[124] 2018	yes	not available	not available	not available	partially	no
[125] 2021	yes	not available	partially	medium	yes	no
[132] 2020	yes	not available	partially	medium	yes	no
[133] 2017	yes	yes	not available	not available	partially	no
[134] 2019	yes	not available	simple	medium	yes	no
[135] 2019	yes	not available	not available	not available	yes	no
[136] 2019	yes	yes	partially	medium	yes	partially
[137] 2017	yes	not available	not available	partially	yes	no
[138] 2014	yes	not available	partially	medium	yes	no
[139] 2013	yes	yes	not available	medium	yes	no
[140] 2018	yes	yes	not available	partially	yes	partially

Table 10: *Summary of surveyed approaches: approaches with emerging technologies*

Ref	**Class**	**Trust metrics**	**Used tools**	**Simulation**	
				Setup	Specific evaluation criteria
[142] 2017	Entity	Reputation+ knowledge	Cloud-based: -defined formulas	Performance Evaluation Process Algebra: -Numb: vehicles, virtual vehicular machines -Rate of requesting service -Trust level	-Resource utilization -Capacity planning for trust calculation -Queue length of trust computation -Throughput -Response time
[143] 2018	Entity	Reputation+ Knowledge	Cloud-based: -flipit game -signaling game	Matlab-based: -Vehicle position +angle -Trust level	Probability of controlling cloud services -Vehicle dynamics -State trajectories
[145] 2019	Hybrid	Reputation+ knowledge+ event	Cloud-based: -DST-based -fuzzy rules	Java-based: -Numb of vehicles -Trust level	-Response time -Basic probability task of vehicles -Outcome of fuzzy analyzer -Trust value change (reward+penalty)
[146] 2017	Entity	Node proprieties	Cloud-based: -DST	not available	not available
[148] 2019	Entity	Node proprieties	Fog-based: -signature-based -bidding price	-Numb: vehicles malicious nodes -Traffic segment -Trust level -Payoff -Bidding price	-Transactions number (according to bidding price, and payoff) -Attacks number

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[149] 2017	Entity	Reputation	Edge-based: multi-weighted subjective logic	-Actual urban area: -Numb: served nodes, malicious nodes -Traffic segment -Vehicle speed -Trust level	-Average reputation value of malicious nodes -Detection rate of malicious nodes -Comparison of detection rate of malicious vehicles -Resource budgets of served nodes -Utility of served nodes
[150] 2020	Hybrid	Knowledge+ node proprieties+ event	Edge-based: -fuzzy logic -k-nearest neighbor algorithm	NS-2, SUMO, MOVE: -Numb: vehicles, malicious nodes -Traffic segment -Vehicle speed -Vehicle type -Transmission range -Trust level	-Precision, Recall of malicious nodes detection -Overall accuracy of malicious nodes detection -Communication overhead
[152] 2018	Entity	Node proprieties	Blockchain-based: -Proof-of-Work+ Proof-of-stake -SHA-256 -Bayesian inference	Matlab-based: -Numb: vehicles, false reports -Vehicles distance -Packet size -Trust level	-% of unfair ratings vs false reports reports, rates -Trust value offset vs % of negative ratings -Generation time of offset blocks -Transmission latency (reports, rates)
[153] 2021	Hybrid	Reputation+ location	Blockchain-based: -Proof-of-Work	Own sumilator: -Numb: vehicles, malicious nodes -Vehicle speed -Trust level	-Detection rate of malicious nodes -Communication overhead -Spending time for trust establishment

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[154] 2020	Entity	Node proprieties	Blockchain-based: -deep learning (feedforward neural network)	NS-2, SUMO: -Numb of vehicles, malicious nodes -Vehicle speed -Vehicles placement -Transmission range -Trust level -Simulation time	Precision, recall of malicious nodes detection
[155] 2021	Entity	Reputation	Blockchain-based: -regional federated learning algorithm -signature-based	-Numb: vehicles, malicious nodes -Trust level	-Model accuracy rate under reputation/non reputation selection -Convergence of knowledge price -Impacts brought by competition on the utility of the optimal provider -Impacts brought by competition on social welfare
[157] 2019	Entity	Reputation+ knowledge	Blockchain-based: -Proof-of-work+ Practical Byzantine Fault Tolerates -logistic regression	Python+Golang-based: -Numb: vehicles, malicious nodes, updating requests -Vehicles speed -Transmission range -Trust level	-Evaluation of announcement protocol (average computation time) -Trust value change -Detection rate of malicious nodes -False detection rate -Average latency of consensus algorithm

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[158] 2018	Entity	Reputation+ knowledge	Blockchain-based: -Proof-of-work -signature-based -SHA-256	-Numb of vehicles -Trust level -Simulation time	-Storage and transmission overhead
[161] 2018	Entity	Node proprieties	SDN-based: NP-completeness	OMNET ++, Modeler: -Numb: vehicles, malicious nodes -Traffic segment -Trust level -Simulation time	-Throughput -Average end-to-end delay
[162] 2016	Entity	Node proprieties	SDN-based: -defined formulas	OPNET: -Numb of vehicles -Traffic segment -Trust level -Simulation time	-Average end-to-end delay -Throughput -Total messages sent
[163] 2020	Entity	Reputation+ Knowledge	SDN-based: -clustering scheme	Veins, SUMO: -Numb: vehicles, malicious nodes -Transmission range -Traffic segment -Trust level -Simulation time	-Detection rate of malicious nodes -False positives
[164] 2020	Entity	Knowledge	SDN-based: -clustering scheme	NS-2.34, VanetMobiSim: -Numb: vehicles,	-Average end-to-end delay -Packet delivery ratio

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[164] 2020			-signature-based	malicious nodes -Vehicle speed -Transmission range -Traffic segment -Medium capacity -Trust level -Simulation time	
[165] 2018	Hybrid	Knowledge+ node properties	SDN-based: -Q-learning	TensorFlow, OPNET: -Numb: vehicles, malicious nodes -Traffic segment -Packet size -Trust level -Simulation time	-Convergence performance -Packet delivery ratio -Throughput
[166] 2018	Hybrid	Knowledge+ node properties	SDN-based: -deep neural network	TensorFlow, OPNET: -Numb of vehicles -Trust level	-Convergence performance -Throughput -Average end-to-end delay
[167] 2020	Hybrid	Knowledge+ node properties	SDN-based: -deep Q-learning -Markov decision process	TensorFlow: -Numb of vehicles -Learning rate -Trust level	-Convergence performance -Expected transmission count -Expected transmission count delay
[168] 2017	Entity	Reputation+ Knowledge	SDN+Fog-based	not available	not available
[169] 2018	Entity	Knowledge	SDN+ Blockchain-based:	not available	not available

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[169] 2018			-Proof of Elapsed Time -signature-based		
[170] 2020	Entity	Knowledge	SDN+ Blockchain-based: -Proof-of-stake+ modified practical Byzantine fault tolerance -signature-based	Python-based: Numb: vehicles malicious nodes -Vehicles distance -Numb of reference set -Message group -Trust level -Number of paths -Virtual network average lifetime	-Path mapping -Prediction accuracy -Transactions number -Transaction confirmation time
[171] 2019	Data	Location+ time-based	SDN+ Blockchain-based: -Proof-of-stake -signature-based -SHA-256	OMNeT++, crypto++ library: Numb: vehicles, malicious nodes -Vehicles speed -Transmission range -Traffic segment -Trust level	-Accuracy of malicious nodes detection -Processing time of blocks -Transaction transmission delay -Video encryption time overhead
[172] 2019	Entity	Reputation	SDN+ Blockchain+ Fog-based: -practical byzantine fault	NS-3: -Numb of vehicles -Packet size -Traffic segment -Vehicles speed	-Packet delivery rate -Transmission delay -Processing time of blocks

Ref	Class	Trust metrics	Used tools	Simulation	
				Setup	Specific evaluation criteria
[172] 2019			tolerance -clustering scheme -signature-based	-Transmission range -Trust level	
[173] 2019	Entity	Reputation	SDN+ Blockchain-based: -redundant byzantine fault tolerance -dueling deep Q-Learning -signature-based	TensorFlow: -Numb of vehicles -Packet size -Block size -Traffic segment -Trust level	-Throughput -Convergence performance

Table 11: *Qualitative comparison of surveyed approaches: approaches with emerging technologies*

Ref	Dynamicity	Scalability	T. complexity	C.overhead	Robustness	Privacy
[142] 2017	partially	not available	partially	medium	no	no
[143] 2018	yes	not available	not available	not available	yes	no
[145] 2019	yes	yes	partially	not available	yes	no
[146] 2017	yes	not available	not available	not available	not available	no
[148] 2019	yes	not available	not available	medium	yes	no
[149] 2017	yes	partially	partially	medium	yes	no
[150] 2020	yes	yes	supposed to be simple (e.g., local computation)	medium	yes	partially
[152] 2018	yes	yes	simple	medium	yes	no
[153] 2021	yes	yes	simple	medium	yes	partially
[154] 2020	yes	yes	partially	medium	yes	no
[155] 2021	yes	not available	not available	not available	yes	no
[157] 2019	yes	not available	partially	not available	yes	yes
[158] 2018	yes	not available	partially	medium	yes	yes
[161] 2018	yes	not available	partially	not available	yes	no
[162] 2016	yes	not available	partially	partially	partially	no
[163] 2020	yes	not available	not available	not available	yes	partially
[164] 2020	yes	not available	partially	low	yes	no

Ref	Dynamicity	Scalability	T. complexity	C.overhead	Robustness	Privacy
[165] 2018	yes	not available	not available	medium	yes	no
[166] 2018	yes	not available	partially	not available	yes	no
[167] 2020	yes	not available	partially	medium	yes	no
[168] 2017	yes	not available	not available	not available	not available	not available
[169] 2018	yes	yes	not available	not available	not available	no
[170] 2020	yes	not available	partially	medium	yes	partially
[171] 2019	yes	yes	partially	not available	yes	yes
[172] 2019	yes	yes	partially	medium	yes	no
[173] 2019	yes	yes	partially	not available	yes	no

a common agreement with the central entity (for example, the ITS entity or the roadside unit). The trust negotiation is based on exchanging a set of credentials in order to be consider the entity as trustworthy. Getting a higher trust level requires exchanging more sensitive credentials.

6. Green trust and Energy consumption: applying the trust management within an IoV environment leads to a communication overhead and thus increases the time complexity. This is becomes more critical when considering real time applications that are delay sensitive. For that, these parameters have to be taken into account for reliable performance evaluation. All this let us recommend conceiving lightweight trust management frameworks characterized by a low energy consumption. In this regard, future researches have to give more attention to considering the evaluation of the energy efficiency of their trust models. This is more critical in the context of green-IoT deployment when defining a green communication across the IoV ecosystem. Emerging technologies can be used to improve this parameter since they propose innovative approaches to enhance the energy efficiency methodologies that have to be considered during the trust building process.

7. Applications requirements & QoS satisfaction: The reviewed approaches have not been adjusted to meet the necessities of each category of applications in vehicular networks (e.g., critical time-based safety applications). Most of cited approaches have been addressed to all kinds of applications regardless their importance level. Therefore, it is important to conceive adjusted schemes that deal differently with specific applications requirements (e.g., using particular trust metrics, on the basis of encountered situation), and more incorporate proper trustworthiness evaluation parameters (e.g., taking into consideration more contextual information; traffic segment conditions; weather, road type; highway, rural, etc.).

   Besides, the overall criteria that we have selected to interpret the efficiency of the reviewed schemes in Tables 7, 9 and 11 (section 6) have not been totally satisfied. For example, robustness and privacy have not

been mainly preserved, which makes hard maintaining the whole communication system security. Also, cited approaches have not drawn greater attention to QoS requirements. Consequently, the quality of trust-based services needs to be improved (e.g., reliable and accurate delivery of data in time). Scalability, complexity, communication overhead, robustness, and privacy must get more interest to maintain system performance when trust management approaches are deployed.

8. Trust bootstrapping & update: In other respects: (1) Trust bootstrapping (i.e., computing real initial trust value) may need further research; indeed, a random initial trust value can be assigned for the newly encountered nodes, yet, the assumed trust value may do not match with the real trust value, hence more research is required to determine the precise initial trust value. (2) Fast update and decay of trust value may be an important issue to deal with in future studies; in fact, each stored trust value is subject to be fast updated or decayed every time a node makes interactions with other entities, thus it is essential to define an appropriate update of the stored trust values (that emphases mainly the trustee node computational capacities) or a lifetime (as nodes are not capable to store all the contacted nodes trust values). Also, (3) Reputation computation can be more handled; actually the reputation is a broadly used metric, and primarily an efficient and a fast value computation processing is required as this metric is based on different other factors like recommendations integrity, requested nodes cooperativeness, and hops number. In other words the reputation computation scheme should take into account the different factors that are related to the reputation-based metric like the willingness of nodes to exchange data, or the distance from the asked entities, etc.

9. Trust in emerging technologies: On the other hand, trust management in emerging technologies such Cloud, Fog, Edge, SDN and Blockchain (further Blockchain sharding, Blockchain directed acyclic graph, sidechain, and lightning network) can be in the core of future works interest, mainly

within advanced IoV network that has expanded its scope from simple VANET to V2X communications. As aforementioned in the previous section, these technologies can assist in providing QoS and devising architectures that ensure dynamic, scalable, credible and secure trust management; for instance data are digitally signed, immutable, verified by all mining nodes and stored with resiliency and traceability with Blockchain. Likewise, Cloud and SDN can help mainly in supporting network dynamicity and scalability, and Fog technology provides fundamentally localized processing, storage and decision making, that offer timely context management within the trust approach. Despite of dealing with these aforesaid notable requirements, there is still a lack in the current use of such technologies to more enhance the trust management; the Cloud-based trust approaches need further research in terms of time complexity (e.g., as trust data may take time to travel from the node back to the Cloud center) and security, as well within a Fog, Edge or SDN-driven environment the trust management requires mainly the address of the security issue; that is to say that the related approaches should secure the link between the technology infrastructure and the peripheral applications and consider the whole procedure of trust data requests/responses. Finally, within the Blockchain-based trust management approaches there may be some issues around forks, consensus and blocks generation delay, and hence power consumption.

10. Data perception trust: Another last important point is that the data perception trust should be more investigated. It refers to the data trust during collection and pre-processing. Therefore, the inspection of the quality of sensed data is inevitably crucial for supporting IoV services trust (since associated services rely on data mining and analysis). In fact, trust assessment is required before nodes interaction to define any deficiency, particularly within autonomous driving context (for instance, to cope with sensors failures at the right time, to verify the sensor information that is collected from multiple sensors, etc.). Thus, ongoing research should pay

attention to this kind of trust properties in the IoV physical perception layer (i.e., sensor sensibility, preciseness, persistence, data aggregation efficiency, etc.), and additionally take into consideration the hardware platform issues (e.g., sensors security and sensors lifetime) when embed a trust management solution. We can refer that a cooperative perception-based trust scheme such in [18] may be helpful in this requirement context. From another side, the privacy of user data should be ensured. The two main relevant techniques that are considered as active research topics about privacy preserving are the anonymization techniques and the homomorphic encryption techniques. A great attention should be reserved to the data management especially by regards to the new regulations; e.g., general data protection regulation that requires specific compliance to ensure privacy and respect data security.

8. Conclusion

In this survey, we have discussed security trust pillar in vehicular networks. Differently from previous surveys that focused on this context, we highlight in our work the classes of the proposed solutions for managing trust in vehicular networks. Firstly, we have presented the main related challenges. Thereafter, we have explored the existing trust management approaches in vehicular networks from the three acknowledged perspectives which comprise entity-based, data-based, and combined solutions. Afterward, we have emphasized on the recent approaches that apply different tools for managing trust such as artificial intelligence-enabling techniques; e.g. clustering, fuzzy logic, and game theory, as well as emerging technologies; e.g., Cloud computing, Fog computing, SDN and Blockchain. This classification draws the subject of our contribution in this paper. Next, we have discussed in short the reviewed approaches with respect to different selected criteria, and along with summary of associated deployment tools, to interpret correlated strengths and shortcomings and enable a qualitative comparison. The paper has also provided a brief overview of future research

directions for trust management in IoV. Ultimately, we have stressed that the design of an efficient trust management approach aims at finding a good trade off in terms of security, QoS, and privacy.

Compliance with Ethical Standards. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. This paper does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.

[2] Patel, P., Narmawala, Z., Thakkar, A. (2019). A Survey on Intelligent Transportation System Using Internet of Things. In Emerging Research in Computing, Information, Communication and Applications (pp. 231-240). Springer, Singapore.

[3] Veres, M., Moussa, M. (2019). Deep learning for intelligent transportation systems: A survey of emerging trends. IEEE Transactions on Intelligent Transportation Systems.

[4] Priyan, M. K., Devi, G. U. (2019). A survey on internet of vehicles: applications, technologies, challenges and opportunities. International Journal of Advanced Intelligence Paradigms, 12(1-2), 98-119.

[5] Hbaieb, A., Rhaiem, O. B., Chaari, L. (2018, June). In-car Gateway Architecture for Intra and Inter-vehicular Networks. In 2018 14th International Wireless Communications Mobile Computing Conference (IWCMC) (pp. 1489-1494). IEEE.

[6] MacHardy, Z., Khan, A., Obana, K., Iwashina, S. (2018). V2X access technologies: Regulation, research, and remaining challenges. IEEE Communications Surveys Tutorials, 20(3), 1858-1877.

[7] Zhou, H., Xu, W., Chen, J., Wang, W. (2020). Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities. Proceedings of the IEEE, 108(2), 308-323.

[8] IEEE 1609.0-2019 - IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture

[9] IEEE 1609.2b-2019 - IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages - Amendment 2–PDU Functional Types and Encryption Key Management

[10] IEEE 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation

[11] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," in Proceedings of the IEEE, vol. 99, no. 7, pp. 1162-1182, July 2011, doi: 10.1109/JPROC.2011.2132790.

[12] Architecture enhancements for V2X services 3GPP Technical specification (TS) (2019)

[13] Matthaeia, R., Reschkaa, A., Riekena, J., Dierkesa, F., Ulbricha, S., Winkleb, T., Maurera, M. (2015). Autonomous Driving: Technical, Legal and Social Aspects.

[14] Shreyas, V., Bharadwaj, S. N., Srinidhi, S., Ankith, K. U., Rajendra, A. B. (2020). Self-driving Cars: An Overview of Various Autonomous Driving Systems. In Advances in Data and Information Sciences (pp. 361-371). Springer, Singapore.

[15] Hbaieb, A., Rezgui, J., Chaari, L. (2019, April). Pedestrian Detection for Autonomous Driving within Cooperative Communication System. In 2019 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[16] Rezgui, J., Hbaieb, A., Chaari, L., Maryland, J.,. (2019, December). Traffic Sign Recognition Using Neural Networks Useful for Autonomous Vehicles. In 2019 International Conference on Smart Applications, Communications and Networking (SmartNets 2019). IEEE.

[17] http://autopilot-project.eu/

[18] Hurl, B., Cohen, R., Czarnecki, K., Waslander, S. (2019). TruPercept:Trust Modelling for Autonomous Vehicle Cooperative Perception from Synthetic Data. arXiv preprint arXiv:1909.07867.

[19] Kerrache, C. A., Lagraa, N., Hussain, R., Ahmed, S. H., Benslimane, A., Calafate, C. T., ... Vegni, A. M. (2018). TACASHI: Trust-aware communication architecture for social internet of vehicles. IEEE Internet of Things Journal, 6(4), 5870-5877.

[20] Xia, H., Zhang, S. S., Li, Y., Pan, Z. K., Peng, X., Cheng, X. Z. (2019). An attack-resistant trust inference model for securing routing in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 68(7), 7108-7120.

[21] Dahmane, S., Kerrache, C. A., Lagraa, N., Lorenz, P. (2017, May). WeiSTARS: A weighted trust-aware relay selection scheme for VANET. In 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[22] Rostamzadeh, K., Nicanfar, H., Torabi, N., Gopalakrishnan, S., Leung, V. C. (2015). A context-aware trust-based information dissemination framework for vehicular networks. IEEE Internet of Things journal, 2(2), 121-132.

[23] Govindan, K., Mohapatra, P. (2011). Trust computations and trust dynamics in mobile adhoc networks: A survey. IEEE Communications Surveys Tutorials, 14(2), 279-298.

[24] Suo, D., Sarma, S. E. (2019, October). Real-time Trust-Building Schemes for Mitigating Malicious Behaviors in Connected and Automated Vehicles. In 2019 IEEE Intelligent Transportation Systems Conference (ITSC) (pp. 1142-1149). IEEE.

[25] Arif, M., Wang, G., Bhuiyan, M. Z. A., Wang, T., Chen, J. (2019). A survey on security attacks in VANETs: Communication, applications and challenges. Vehicular Communications, 100179.

[26] Sheikh, M. S., Liang, J., Wang, W. (2019). A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). Sensors, 19(16), 3589.

[27] Wang, Z., Wang, Y., Zhang, Y., Liu, Y., Ma, C., Wang, H. (2019, October). A Brief Survey on Cyber Security Attack Entrances and Protection Strategies of Intelligent Connected Vehicle. In International Conference on Smart Computing and Communication (pp.1650 73-82)

[28] Ghosal, A., Conti, M. (2020). Security Issues and Challenges in V2X: A Survey. Computer Networks, 107093.

[29] Alnasser, A., Sun, H., Jiang, J. (2019). Cyber security challenges and solutions for V2X communications: A survey. Computer Networks, 151, 52-67

[30] Ivanov, I., Maple, C., Watson, T., Lee, S. (2018). Cyber security standards and issues in V2X communications for Internet of Vehicles.

[31] Yoshizawa, T., Preneel, B. (2019, October). Survey of Security Aspect of V2X Standards and Related Issues. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 1-5). IEEE.

[32] Marojevic, V. (2018). C-V2X Security Requirements and Procedures:Survey and Research Directions. arXiv preprint arXiv:1807.09338.

[33] Lautenbach, A., Nowdehi, N., Olovsson, T., Zaragatzky, R. (2019, April). A Preliminary Security Assessment of 5G V2X. In 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring) (pp. 1-7). IEEE.

[34] Muhammad, M., Safdar, G. A. (2018). Survey on existing authentication issues for cellular-assisted V2X communication. Vehicular Communications, 12, 50-65.

[35] Ometov, A., Bezzateev, S. (2017, November). Multi-factor authentication: A survey and challenges in V2X applications. In 2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) (pp. 129-136). IEEE.

[36] Vaibhav, A., Shukla, D., Das, S., Sahana, S., Johri, P. (2017). Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey. IJ Wireless and Microwave Technologies, 3, 36-48.

[37] Pesé, M. D., Shin, K. G. (2019). Survey of Automotive Privacy Regulations and Privacy-Related Attacks (No. 2019-01-0479). SAE Technical Paper.

[38] Zhao, P., Zhang, G., Wan, S., Liu, G., Umer, T. (2019). A survey of local differential privacy for securing internet of vehicles. The Journal of Supercomputing, 1-22.

[39] Poddar, M., Ganta, S., Swaraj, K. R., Das, D. (2019, January). Privacy in the Internet of Vehicles: Models, Algorithms, and Applications. In 2019 International Conference on Information Networking (ICOIN) (pp. 78-83). IEEE.

[40] Ali, I., Hassan, A., Li, F. (2019). Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. Vehicular Communications.

[41] Talat, H., Nomani, T., Mohsin, M., Sattar, S. (2019, January). A survey on location privacy techniques deployed in vehicular networks. In 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST) (pp. 604-613). IEEE

[42] Atmaca, U. I., Maple, C., Dianati, M. (2019). Emerging Privacy Challenges and Approaches in CAV Systems

[43] Ahmad, F., Adnane, A., Kerrache, C. A., Franqueira, V. N., Kurugollu, F. (2020). Trust Management in Vehicular Ad-Hoc Networks and Internet-of-Vehicles: Current Trends and Future Research Directions. In Global Advancements in Connected and Intelligent Mobility: Emerging Research and Opportunities (pp. 135-165). IGI Global.

[44] Hussain, R., Lee, J., Zeadally, S. (2020). Trust in VANET: A Survey of Current Solutions and Future Research Opportunities. IEEE Transactions on Intelligent Transportation Systems.

[45] Iqbal, R., Butt, T. A., Afzaal, M., Salah, K. (2019). Trust management in social Internet of vehicles: Factors, challenges,blockchain, and fog solutions. International Journal of Distributed Sensor Networks, 15(1), 1550147719825820.

[46] Souissi, I., Azzouna, N. B., Berradia, T. (2019). Trust management in vehicular ad hoc networks: a survey. International Journal of Ad Hoc and Ubiquitous Computing, 31(4), 230-243.

[47] Qurashi, J. M. (2019). Survey on Risk-Based Decision-Making Models for Trust Management in VANETs. In Secure Cyber-Physical Systems for Smart Cities (pp. 52-73). IGI Global.

[48] Sumithra, S., Vadivel, R. (2018, July). An overview of various trust models for vanet security establishment. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

[49] Gillani, M., Ullah, A., Niaz, H. A. (2018, November). Trust Management Schemes for Secure Routing in VANETs-A Survey. In 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) (pp. 1-6). IEEE.

[50] Srivastava, A., Prakash, A., Tripathi, R. (2020). Location based routing protocols in VANET: Issues and existing solutions. Vehicular Communications, 100231.

[51] Alouache, L., Nguyen, N., Aliouat, M., Chelouah, R. (2019). Survey on IoV routing protocols: Security and network architecture. International Journal of Communication Systems, 32(2), e3849.

[52] Ksouri, C., Jemili, I., Mosbah, M., Belghith, A. (2019, October). VANETs Routing Protocols Survey: Classifications, Optimization Methods and New Trends. In International Workshop on Distributed Computing for Emerging Smart Networks (pp. 3-22). Springer, Cham.

[53] Tripp-Barba, C., Zaldivar-Colado, A., Urquiza-Aguiar, L., Aguilar-Calderon, J. A. (2019). Survey on Routing Protocols for Vehicular Ad Hoc Networks Based on Multimetrics. Electronics, 8(10), 1177.

[54] Hotkar, D. S., Biradar, S. R. (2019). A review on existing QOS routing protocols in VANET based on link efficiency and link stability. In Advances in Communication, Cloud, and Big Data (pp. 89-96). Springer, Singapore.

[55] Sattar, S. A. (2018). A Survey on secure routing protocols for VANET based on node trust.

[56] Ahmad, S. A., Shcherbakov, M. (2018, July). A Survey on Routing Protocols in Vehicular Adhoc Networks. In 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-8). IEEE.

[57] Sivaraman, K., Azaraffali, K. M. (2018). An extensive survey on different routing protocols and issue in VANETs. International Journal of Pure and Applied Mathematics, 119(12), 9507-9514

[58] Boussoufa-Lahlah, S., Semchedine, F., Bouallouche-Medjkoune, L. (2018). Geographic routing protocols for Vehicular Ad hoc NETworks (VANETs): A survey. Vehicular Communications, 11, 20-31.

[59] Kumar, M., Nigam, A. K., Sivakumar, T. (2018). A Survey on Topology and Position Based Routing Protocols in Vehicular Ad hoc Network (VANET). International Journal on Future Revolution in Computer Science Communication Engineering, 4(2), 432-440.

[60] Hussain, S. A., Yusof, K. M., Hussain, S. M., Singh, A. V. (2019, February). A Review of Quality of Service Issues in Internet of Vehicles (IoV). In 2019 Amity International Conference on Artificial Intelligence (AICAI) (pp. 380-383). IEEE.

[61] Smida, K., Tounsi, H., Frikha, M., Song, Y. Q. (2019, June). Software Defined Internet of Vehicles: a survey from QoS and scalability perspectives. In 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC) (pp. 1349-1354). IEEE.

[62] Shafiq, Z., Zafar, M. H., Qazi, A. B. (2018). QoS in Vehicular Ad Hoc Networks-A Survey. Journal of Information Communication Technologies and Robotic Applications, 48-58.

[63] Benmir, A., Korichi, A., Bourouis, A., Alreshoodi, M. (2018). Survey on QoE/QoS Correlation Models for Video Streaming over Vehicular Adhoc Networks. Journal of computing and information technology, 26(4), 267-287.

[64] Mchergui, A., Moulahi, T., Alaya, B., Nasri, S. (2017). A survey and comparative study of QoS aware broadcasting techniques in VANET. Telecommunication Systems, 66(2), 253-281.

[65] Fatih Sakiz, Sevil Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV, Ad Hoc Networks, Volume 61,2017.

[66] P. Golle, D. Greene and J. Staddon. Detecting and correcting malicious data in VANETs. Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (2004), p. 29

[67] B. Xiao, B. Yu and C. Gao. Detection and localization of sybil nodes in VANETs. Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (2006), p. 1

[68] B. Yu, C.-Z. Xu and B. Xiao. Detecting sybil attacks in VANETs. J. Parallel Distrib. Comput., 73 (6) (2013), pp. 746-756

[69] G. Guette and B. Ducourthial. On the sybil attack detection in VANET. Mobile Adhoc and Sensor Systems (2007), pp. 1-6

[70] T. Zhou, R.R. Choudhury, P. Ning and K. Chakrabarty. Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services (2007), pp. 1-8

[71] I. Aad, J.-P. Hubaux and E.W. Knightly. Denial of service resilience in ad hoc networks. Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (2004), pp. 202-215

[72] J. Soryal and T. Saadawi. DoS attack detection in Internet-connected vehicles. 2013 International Conference on Connected Vehicles and Expo (ICCVE) (2013), pp. 7-13.

[73] K. Verma, H. Hasbullah and A. Kumar. Prevention of DoS attacks in VANET. Wireless Person. Commun., 73 (1) (2013), pp. 95-126

[74] K. Verma and H. Hasbullah. Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET. Secur. Commun. Netw., 8 (5) (2015), pp. 864-878

[75] 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. Vehic. Commun. (2016)

[76] A. Daeinabi and A.G. Rahbar. Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks. Multimed. Tools Appl., 66 (2) (2013), pp. 325-338

[77] U. Khan, S. Agrawal and S. Silakari. Detection of malicious nodes (dmn) in vehicular ad-hoc networks. Procedia Comput. Sci., 46 (2015), pp. 965-972

[78] R. Baiad, O. Alhussein, H. Otrok and S. Muhaidat. Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET. Vehic. Commun., 5 (2016), pp. 9-17

[79] X. Yao, X. Zhang, H. Ning and P. Li. Using trust model to ensure reliable data acquisition in VANETs. Ad Hoc Netw., 55 (2017), pp. 107-118

[80] S.M. Safi, A. Movaghar and M. Mohammadizadeh . A novel approach for avoiding wormhole attacks in VANET. 2009 First Asian Himalayas International Conference on Internet (2009), pp. 1-6

[81] S. Biswas and J. Misic. A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs. IEEE Trans. Veh. Technol., 62 (5) (2013), pp. 2182-2192

[82] T.H.-J. Kim et al.. Vanet alert endorsement using multi-source filters. Proceedings of the Seventh ACM International Workshop on VehiculAr InterNETworking (2010), pp. 51-60

[83] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J.-P. Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. IEEE J. Select. Areas Commun., 25 (8) (2007), pp. 1557-1568

[84] M. Ghosh, A. Varghese, A. Gupta, A.A. Kherani and S.N. Muthaiah. Detecting misbehaviors in VANET with integrated root-cause analysis. Ad Hoc Netw., 8 (7) (2010), pp. 778-790

[85] G. Yan, S. Olariu and M.C. Weigle. Providing VANET security through active position detection. Comput. Commun., 31 (12) (2008), pp. 2883-2897

[86] N. Kumar and N. Chilamkurti. Collaborative trust aware intelligent intrusion detection in VANETs. Comput. Electr. Eng., 40 (6) (2014), pp. 1981-1996

[87] H. Sedjelmaci and S.M. Senouci. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. Comput. Electr. Eng., 43 (2015), pp. 33-47

[88] O.A. Wahab, A. Mourad, H. Otrok and J. Bentahar. CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. Expert Syst. Appl., 50 (2016), pp. 40-54

[89] J. Grover, V. Laxmi and M.S. Gaur, P.S. Thilagam, A.R. Pais, K. Chandrasekaran, N. Balakrishnan. Misbehavior detection based on ensemble learning in VANET. (Eds.), Advanced Computing, Networking and Security, vol. 7135, Springer, Berlin, Heidelberg (2012), pp. 602-611

[90] T. Bouali, S.-M. Senouci and H. Sedjelmaci. A distributed detection and prevention scheme from malicious nodes in vehicular networks. Int. J. Commun. Syst., 29 (10) (2016), pp. 1683-1704

[91] 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., 93 (2016), pp. 68-83

[92] K. Zaidi, M.B. Milojevic, V. Rakocevic, A. Nallanathan and M. Rajarajan. Host-based intrusion detection for VANETs: a statistical approach

to rogue node detection. IEEE Trans. Veh. Technol., 65 (8) (2016), pp. 6703-6714

[93] Chen, Y. M., Wei, Y. C. (2013). A beacon-based trust management system for enhancing user centric location privacy in VANETs. Journal of Communications and Networks, 15(2), 153-163.

[94] Mármol, F. G., Perez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of network and computer applications, 35(3), 934-941.

[95] Al Falasi, H., Mohamed, N. (2015, December). Similarity-based trust management system for detecting fake safety messages in vanets. In International Conference on Internet of Vehicles (pp. 273-284). Springer, Cham.

[96] Minhas, U. F., Zhang, J., Tran, T., Cohen, R. (2010). A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 41(3), 407-420.

[97] Minhas, U. F., Zhang, J., Tran, T., Cohen, R. (2010). Towards expanded trust management for agents in vehicular ad-hoc networks. International Journal of Computational Intelligence Theory and Practice, 5.

[98] Li, X., Liu, J., Li, X., Sun, W. (2013, September). RGTE: A reputation-based global trust establishment in VANETs. In 2013 5th International Conference on Intelligent Networking and Collaborative Systems (pp. 210-214). IEEE.

[99] Hu, H., Lu, R., Zhang, Z., Shao, J. (2016). REPLACE: A reliable trust-based platoon service recommendation scheme in VANET. IEEE Transactions on Vehicular Technology, 66(2), 1786-1797

[100] Xia, H., Zhang, S. S., Li, Y., Pan, Z. K., Peng, X., Cheng, X. Z. (2019). An attack-resistant trust inference model for securing routing in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 68(7), 7108-7120.

[101] Zhou, A., Li, J., Sun, Q., Fan, C., Lei, T., Yang, F. (2015). A security authentication method based on trust evaluation in VANETs. EURASIP Journal on Wireless Communications and Networking, 2015(1), 1-8.

[102] Cui, J., Zhang, X., Zhong, H., Ying, Z., Liu, L. (2019). RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. IEEE Internet of Things Journal, 6(4), 6417-6428.

[103] Raya, M., Papadimitratos, P., Gligor, V. D., Hubaux, J. P. (2008, April). On data-centric trust establishment in ephemeral ad hoc networks. In IEEE INFOCOM 2008-The 27th Conference on Computer Communications (pp. 1238-1246). IEEE.

[104] Zaidi, K., Milojevic, M., Rakocevic, V., Rajarajan, M. (2014, September). Data-centric rogue node detection in VANETs. In 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 398-405). IEEE.

[105] Shaikh, R. A., Alzahrani, A. S. (2014). Intrusion-aware trust model for vehicular ad hoc networks. Security and communication networks, 7(11), 1652-1669.

[106] Wu, A., Ma, J., Zhang, S. (2011, September). RATE: a RSU-aided scheme for data-centric trust establishment in VANETs. In 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (pp. 1-6). IEEE.

[107] Wei, Y. C., Chen, Y. M. (2012, June). An efficient trust management system for balancing the safety and location privacy in VANETs. In 2012

IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 393-400). IEEE.

[108] Shaikh, R. A., Alzahrani, A. S. (2013, January). Trust management method for vehicular ad hoc networks. In International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (pp. 801-815). Springer, Berlin, Heidelberg.

[109] Gurung, S., Lin, D., Squicciarini, A., Bertino, E. (2013, June). Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In International conference on network and system security (pp. 94-108). Springer, Berlin, Heidelberg.

[110] Li, W., Song, H. (2015). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4), 960-969.

[111] Placzek, B., Bernas, M. (2016, June). Detection of malicious data in vehicular ad hoc networks for traffic signal control applications. In International Conference on Computer Networks (pp. 72-82). Springer, Cham.

[112] Bißmeyer, N., Mauthofer, S., Bayarou, K. M., Kargl, F. (2012, November). Assessment of node trustworthiness in vanets using data plausibility checks with particle filters. In 2012 IEEE Vehicular Networking Conference (VNC) (pp. 78-85). IEEE.

[113] Chaurasia, B. K., Verma, S., Tomar, G. S. (2013, April). Trust computation in VANETs. In 2013 International Conference on Communication Systems and Network Technologies (pp. 468-471). IEEE.

[114] Huang, Z., Ruj, S., Cavenaghi, M. A., Stojmenovic, M., Nayak, A. (2014). A social network approach to trust management in VANETs. Peer-to-peer networking and applications, 7(3), 229-242.

[115] Lo, N. W., Tsai, H. C. (2009). A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP Journal on Wireless Communications and Networking, 2009, 1-10

[116] Mazilu, S., Teler, M., Dobre, C. (2011, October). Securing vehicular networks based on data-trust computation. In 2011 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 51-58). IEEE.

[117] Wei, Y. C., Chen, Y. M. (2014, September). Adaptive decision making for improving trust establishment in VANET. In The 16th Asia-Pacific Network Operations and Management Symposium (pp. 1-4). IEEE.

[118] Ortega, V., Bouchmal, F., Monserrat, J. F. (2018). Trusted 5G vehicular networks: Blockchains and content-centric networking. IEEE Vehicular Technology Magazine, 13(2), 121-127.

[119] Han, B., Wong, S., Mannweiler, C., Dohler, M., Schotten, H. D. (2017, May). Security trust zone in 5G networks. In 2017 24th International Conference on Telecommunications (ICT) (pp. 1-5). IEEE.

[120] Xiao, Y., Liu, Y. (2019). Bayestrust and vehiclerank: Constructing an implicit web of trust in vanet. IEEE Transactions on Vehicular Technology, 68(3), 2850-2864.

[121] Mahmood, A., Butler, B., Zhang, W. E., Sheng, Q. Z., Siddiqui, S. A. (2019, March). A Hybrid Trust Management Heuristic for VANETs. In 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)(pp. 748-752). IEEE.

[122] Oubabas, S., Aoudjit, R., Rodrigues, J. J., Talbi, S. (2018). Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme. Vehicular Communications, 13, 128-138.

[123] Zhang, J., Chen, C., Cohen, R. (2013). Trust modeling for message relay control and local action decision making in VANETs. Security and Communication Networks, 6(1), 1-14.

[124] Gaber, T., Abdelwahab, S., Elhoseny, M., Hassanien, A. E. (2018). Trust-based secure clustering in WSN-based intelligent transportation systems. Computer Networks, 146, 151-158.

[125] Fatemidokht, H., Rafsanjani, M. K., Gupta, B. B., Hsu, C. H. (2021). Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms With UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems.

[126] Siddiqui, S. A., Mahmood, A., Zhang, W. E., Sheng, Q. Z. (2019, December). Machine Learning Based Trust Model for Misbehaviour Detection in Internet-of-Vehicles. In International Conference on Neural Information Processing (pp. 512-520). Springer, Cham.

[127] Guo, J., Li, X., Liu, Z., Ma, J., Yang, C., Zhang, J., Wu, D. (2020). TROVE: A Context Awareness Trust Model for VANETs Using Reinforcement Learning. IEEE Internet of Things Journal.

[128] Xing, R., Su, Z., Zhang, N., Peng, Y., Pu, H., Luo, J. (2019). Trust-evaluation-based intrusion detection and reinforcement learning in autonomous driving. IEEE Network, 33(5), 54-60.

[129] Guleng, S., Wu, C., Chen, X., Wang, X., Yoshinaga, T., Ji, Y. (2019). Decentralized trust evaluation in vehicular Internet of Things. IEEE Access, 7, 15980-15988.

[130] Shams, E. A., Rizaner, A., Ulusoy, A. H. (2018). Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks. Computers Security, 78, 245-254.

[131] Zhang, D., Yu, F. R., Yang, R., Tang, H. (2018, October). A deep reinforcement learning-based trust management scheme for software- defined vehicular networks. In Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (pp. 1-7).

[132] A Ghaleb, F., Saeed, F., Al-Sarem, M., Ali Saleh Al-rimy, B., Boulila, W., Eljialy, A. E. M., ... Alazab, M. (2020). Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET. Electronics, 9(9), 1411.

[133] Soleymani, S. A., Abdullah, A. H., Zareei, M., Anisi, M. H., Vargas-Rosales, C., Khan, M. K., Goudarzi, S. (2017). A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. IEEE Access, 5, 15619-15629.

[134] Fan, N., Wu, C. Q. (2019). On trust models for communication security in vehicular ad-hoc networks. Ad Hoc Networks, 90, 101740.

[135] Tian, Z., Gao, X., Su, S., Qiu, J., Du, X., Guizani, M. (2019). Evaluating reputation management schemes of internet of vehicles based on evolutionary game theory. IEEE Transactions on Vehicular Technology, 68(6), 5971-5980.

[136] Halabi, T., Zulkernine, M. (2019, May). Trust-Based Cooperative Game Model for Secure Collaboration in the Internet of Vehicles. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[137] Mehdi, M. M., Raza, I., Hussain, S. A. (2017). A game theory based trust model for Vehicular Ad hoc Networks (VANETs). Computer Networks, 121, 152-172.

[138] Haddadou, N., Rachedi, A., Ghamri-Doudane, Y. (2014). A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. IEEE transactions on vehicular technology, 64(8), 3657-3674.

[139] Haddadou, N., Rachedi, A., Ghamri-Doudane, Y. (2013, April). Trust and exclusion in vehicular ad hoc networks: an economic incentive model based approach. In 2013 Computing, Communications and IT Applications Conference (ComComAp) (pp. 13-18). IEEE.

[140] Subba, B., Biswas, S., Karmakar, S. (2018). A game theory based multi layered intrusion detection framework for VANET. Future Generation Computer Systems, 82, 12-28.

[141] Li, J., Xing, R., Su, Z., Zhang, N., Hui, Y., Luan, T. H., Shan, H. (2020). Trust based secure content delivery in vehicular networks: a bargaining game approach. IEEE Transactions on Vehicular Technology.

[142] Chen, X., Wang, L. (2017). A cloud-based trust management framework for vehicular social networks. IEEE Access, 5, 2967-2980.

[143] Pawlick, J., Chen, J., Zhu, Q. (2018). iSTRICT: An interdependent strategic trust mechanism for the cloud-enabled internet of controlled things. IEEE Transactions on Information Forensics and Security, 14(6), 1654-1669.

[144] Bowers, K. D., Van Dijk, M., Griffin, R., Juels, A., Oprea, A., Rivest, R. L., Triandopoulos, N. (2012, November). Defending against the unknown enemy: Applying FlipIt to system security. In International Conference on Decision and Game Theory for Security (pp. 248-263). Springer, Berlin, Heidelberg.

[145] Chaurasia, B. K., Sharma, K. (2019). Trust Computation in VANET Cloud. In Transactions on Computational Science XXXIV (pp. 77-95). Springer, Berlin, Heidelberg.

[146] Mudengudi, S. S., Kakkasageri, M. S. (2017, August). Establishing trust between vehicles in vehicular clouds: An agent based approach. In 2017 international conference on smart technologies for smart nation (SmartTechCon) (pp. 529-533). IEEE.

[147] Lin, B., Chen, X., Wang, L. (2017, December). A cloud-based trust evaluation scheme using a vehicular social network environment. In 2017 24th Asia-Pacific Software Engineering Conference (APSEC) (pp. 120-129). IEEE.

[148] Dewanta, F., Mambo, M. (2019, March). Bidding Price-Based Transaction: Trust Establishment for Vehicular Fog Computing Service in Rural Area. In 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 882-887). IEEE.

[149] Huang, X., Yu, R., Kang, J., Zhang, Y. (2017). Distributed reputation management for secure and efficient vehicular edge computing and networks. IEEE Access, 5, 25408-25420.

[150] Soleymani, S. A., Goudarzi, S., Anisi, M. H., Kama, N., Adli Ismail, S., Azmi, A., ... Hanan Abdullah, A. (2020). A Trust Model Using Edge Nodes and a Cuckoo Filter for Securing VANET under the NLoS Condition. Symmetry, 12(4), 609.

[151] El-Sayed, H., Chaqfeh, M., El-Kassabi, H., Serhani, M. A., Alexander, H. (2019). Trust enforcement in vehicular networks: challenges and opportunities. IET Wireless Sensor Systems, 9(5), 237-246.

[152] Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2), 1495-1505. (01).

[153] Hbaieb, A., Ayed, S., Chaari, L. (2021). Blockchain-Based Trust Management Approach for IoV. In AINA (1) (pp. 483-493).

[154] Zhang, C., Li, W., Luo, Y., Hu, Y. (2020). AIT: An AI-enabled Trust Management System for Vehicular Networks Using Blockchain Technology. IEEE Internet of Things Journal.

[155] Zou, Y., Shen, F., Yan, F., Lin, J., Qiu, Y. (2021, March). Reputation-Based Regional Federated Learning for Knowledge Trading in Blockchain-

Enhanced IoV. In 2021 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[156] Khelifi, H., Luo, S., Nour, B., Moungla, H., Ahmed, S. H. (2018, October). Reputation-based blockchain for secure NDN caching in vehicular networks. In 2018 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 1-6). IEEE.

[157] Liu, X., Huang, H., Xiao, F., Ma, Z. (2019). A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. IEEE Internet of Things Journal.

[158] Lu, Z., Wang, Q., Qu, G., Liu, Z. (2018, August). Bars: a blockchain-based anonymous reputation system for trust management in vanets. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 98-103). IEEE.

[159] Di Maio, A., Palattella, M. R., Soua, R., Lamorte, L., Vilajosana, X., Alonso-Zarate, J., Engel, T. (2016). Enabling SDN in VANETs: What is the impact on security?. Sensors, 16(12), 2077.

[160] Mahmood, A., Zhang, W. E., Sheng, Q. Z., Siddiqui, S. A., Aljubairy, A. (2019). Trust management for software-defined heterogeneous vehicular ad hoc networks. In Security, Privacy and Trust in the IoT Environment (pp. 203-226). Springer, Cham.

[161] Vasudev, H., Das, D. (2018, January). A trust based secure communication for software defined VANETs. In 2018 International Conference on Information Networking (ICOIN) (pp. 316-321). IEEE.

[162] Zh ang, D., Yu, F. R., Wei, Z., Boukerche, A. (2016, November). Software-defined vehicular ad hoc networks with trust management. In Proceedings

of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications (pp. 41-49).

[163] Boualouache, A., Soua, R., Engel, T. (2020, May). SDN-based Misbehavior Detection System for Vehicular Networks. In 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring) (pp. 1-5). IEEE.

[164] Alouache, L., Maachaoui, M., Chelouah, R. (2020). Securing Hybrid SDN-based Geographic Routing Protocol using a Distributed Trust Model. Advances in Science, Technology and Engineering Systems Journal.

[165] Zhang, D., Yu, F. R., Yang, R. (2018, December). A machine learning approach for software-defined vehicular ad hoc networks with trust management. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[166] Zhang, D., Yu, F. R., Yang, R., Tang, H. (2018, October). A deep reinforcement learning-based trust management scheme for software-defined vehicular networks. In Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (pp. 1-7).

[167] Zhang, D., Yu, F. R., Yang, R., Zhu, L. (2020). Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach. IEEE Transactions on Intelligent Transportation Systems.

[168] Truong, N. B., Lee, G. M. (2017, April). Trust evaluation for data exchange in vehicular networks. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 325-326). IEEE.

[169] Mendiboure, L., Chalouf, M. A., Krief, F. (2018, November). Towards a blockchain-based SD-IoV for applications authentication and trust management. In International Conference on Internet of Vehicles (pp.265-277). Springer, Cham.

[170] Zhao, N., Wu, H., Zhao, X. (2020). Consortium blockchain-based secure software defined vehicular network. Mobile Networks and Applications, 25(1), 314-327.

[171] Xie, L., Ding, Y., Yang, H., Wang, X. (2019). Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access, 7, 56656-56666.

[172] Gao, J., Agyekum, K. O. B. O., Sifah, E. B., Acheampong, K. N., Xia, Q., Du, X., ... Xia, H. (2019). A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. IEEE Internet of Things Journal, 7(5), 4278-4291.

[173] Zhang, D., Yu, F. R., Yang, R. (2019). Blockchain-Based Distributed Software-Defined Vehicular Networks: A Dueling Deep QLearning Approach. IEEE Transactions on Cognitive Communications and Networking, 5(4), 1086-1100.