electronics

MDPI

Review

A Survey of Trust Management in the Internet of Vehicles

Sarah Ali Siddiqui [1,2,*], Adnan Mahmood [1], Quan Z. Sheng [1], Hajime Suzuki [2] and Wei Ni [2]

[1] Department of Computing, Macquarie University, Sydney, NSW 2109, Australia; adnan.mahmood@mq.edu.au (A.M.); michael.sheng@mq.edu.au (Q.Z.S.)
[2] Commonwealth Scientific and Industrial Research Organisation (CSIRO) Data 61, Sydney, NSW 2109, Australia; hajime.suzuki@data61.csiro.au (H.S.); Wei.Ni@data61.csiro.au (W.N.)
* Correspondence: sarah-ali.siddiqui@hdr.mq.edu.au

Abstract: Over the past decade, the groundbreaking technological advancements in the Internet of Vehicles (IoV) coupled with the notion of trust have attracted increasing attention from researchers and experts in intelligent transportation systems (ITS), wherein vehicles establish a belief towards their peers in the pursuit of ensuring safe and efficacious traffic flows. Diverse domains have been taking advantage of trust management models in the quest of alleviating diverse insider attacks, wherein messages generated by legitimate users are altered or counterfeited by malicious entities, subsequently, endangering the lives of drivers, passengers, and vulnerable pedestrians. In the course of vehicles forming perceptions towards other participating vehicles, a range of contributing parameters regarding the interactions among these vehicles are accumulated to establish a final opinion towards a target vehicle. The significance of these contributing parameters is typically represented by associating a weighting factor to each contributing attribute. The values assigned to these weighting factors are often set manually, i.e., these values are predefined and do not take into consideration any affecting parameters. Furthermore, a threshold is specified manually that classifies the vehicles into honest and dishonest vehicles relying on the computed trust. Moreover, adversary models as an extension to trust management models in order to tackle the variants of insider attacks are being extensively emphasized in the literature. This paper, therefore, reviews the state of the art in the vehicular trust management focusing on the aforementioned factors such as quantification of weights, quantification of threshold, misbehavior detection, etc. Moreover, an overarching IoV architecture, constituents within the notion of trust, and attacks relating to the IoV have also been presented in addition to open research challenges in the subject domain.

Keywords: internet of vehicles; network security; trust management; misbehavior identification; adversary models

Citation: Siddiqui, S.A.; Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. A Survey of Trust Management in the Internet of Vehicles. *Electronics* **2021**, *10*, 2223. https://doi.org/10.3390/electronics10182223

Academic Editor: Gabriella Mazzulla

Received: 19 July 2021
Accepted: 7 September 2021
Published: 10 September 2021

1. Introduction

Recently, the number of vehicles on the road are increasing at an exponential rate and it is anticipated to reach up to 2.8 billion by 2036 [1]. Owing to such a momentous increase in the number, several issues, including but not limited to, traffic congestion and road accidents have transpired. According to the World Health Organization, the major cause of mortality among the population aged 5–29 years is via road accidents and the total number of road fatalities is nearly 1.3 million every year globally [2]. This creates a high demand for innovative and sophisticated traffic management systems. The continued expansions and advancements in connected vehicles are revolutionizing the notion of transportation by further enhancing intelligent transportation systems (ITS) to improve traffic throughput and road safety by reducing traffic congestion and the risk of road accidents [3,4]. These systems rely on acquisition, analysis, and processing of the immense volume of sensor data associated with the embedded sensors in modern vehicles. These sensors exchange information with other internal sensors and sensors in their immediate ambience utilizing the notion of the Internet of Things (IoT), wherein the interconnecting devices exchange

data about themselves and their surroundings to form intelligent networks [5]. It is estimated that about 152,200 IoT devices will be connecting to the Internet per minute, subsequently, increasing the data volume up to 73.1 ZB in 2025 [6,7]. Furthermore, a single car has nearly a 100 sensors embedded and according to an estimate, it can generate approximately 380 TB–4.9 PB of data annually [8]. The information shared among the onboard sensors (e.g., position, speed/velocity, pressure, temperature sensors, etc.) and IoT devices (e.g., traffic speed and density sensors, road cameras, etc.) assists in real-time traffic management by creating a true perception of the road and the traffic network [9].

Over the past few decades, researchers from both academia and industry have invested great efforts into technological advancements of mobile ad hoc networks (MANETs), wherein mobile devices create on the fly, self-organizing, and dynamic networks by communicating with one another without any communication infrastructure [10–13]. MANETs evolved over time and one of the advanced flavors of it, vehicular ad hoc networks (VANETs), was introduced whereby peer vehicles share information with one another [14,15]. Vehicles, in cooperation with the transportation infrastructure, engage in vehicle-to-everything (V2X) communication composed of a variety of communication forms primarily including vehicle-to-vehicle (V2V), vehicle-to-sensor (V2S), vehicle-to-pedestrian (V2P), and vehicle-to-infrastructure (V2I) communications [16]. The V2X communication is integral in materializing the Internet of Vehicles (IoV), an amalgamation of VANETs and the IoT, also known as IoT on wheels [17,18]. IoV is indeed a breakthrough in the context of both non-safety and safety-critical vehicular applications. It can serve as a bridge between the conventional media (i.e., radio, broadcast television) and the social media (i.e., infotainment applications) as smart connected vehicles offer a platform for the passengers to generate and request mobile media content [19,20]. Figure 1 depicts the notion of V2X communications in an IoV network. The V2X communication coupled with the aforementioned sensor embedded vehicles' capabilities helps improve traffic management and road safety by generating collision warnings, emergency brake notifications, hazard warnings, obstacle warning, and traffic congestion warnings [21]. Due to the sensitive nature of these applications, it is crucial that the exchanged information is secure and reliable. However, such messages are vulnerable to attacks where dishonest vehicles can counterfeit safety messages and introduce delays in the transmission resulting in accidents and loss of human lives [22]. The presence of even a single malicious vehicle can cause great damages, and therefore, it is of great importance to identify and eradicate such vehicles from within the network. Cryptography-based solutions have been widely proposed to eliminate misbehavior from the network; however, these techniques are only applicable for outsider attackers. With the aim to eradicate insider misbehaving entities from the vehicular network, the notion of trust has been introduced, wherein vehicles evaluate their peers (i.e., the evaluator, commonly known as the trustor, and the one being evaluated, referred to as a trustee or a target node) based on their behavior and the information disseminated by them in the network.

The development of trust management models helps prevent exchange of counterfeited data as well as eliminate the sources dispersing such data, consequently, ensuring safe, reliable, and efficacious traffic flows. Trust management models are classified into three categories [23]: (i) data-centric, wherein the authenticity of the exchanged messages is the primary focus; (ii) entity-centric, wherein the credibility of the vehicles exchanging the information is emphasized; and (iii) hybrid, wherein the legitimacy of both data and vehicles is considered. The said data and/or entity evaluations rely on a variety of attributes associated with the interactions among a pair of vehicles. In addition to interaction-based attributes, social parameters based on the driver (e.g., age, driving license score, and driving age), and his/her behavior (e.g., number of speeding tickets, number of traffic accidents, and number of traffic violations) are often taken into consideration as well to reflect a driver's honesty as drivers are usually the deciding authorities when it comes to driving-related critical decisions. While aggregating these attributes to compute a final trust score, an arithmetic mean of the said attributes is calculated which insinuates an equal

importance of each of these contributing attributes on the final trust value. Conversely, weights reflecting the importance of individual attributes are associated with respective attributes during the aggregation process. Once the final trust is computed, a steady predefined threshold is applied to identify malicious vehicles, i.e., vehicles possessing a trust score greater than the said threshold are categorized as trustworthy vehicles, whereas vehicles having a trust value below the defined threshold are tagged as malicious. Furthermore, trust management models are often designed with targeted attack resistant models such as man-in-the-middle attack, Sybil attack, bad-mouthing attack, on-off attack, black-hole attack, etc. [24–27].

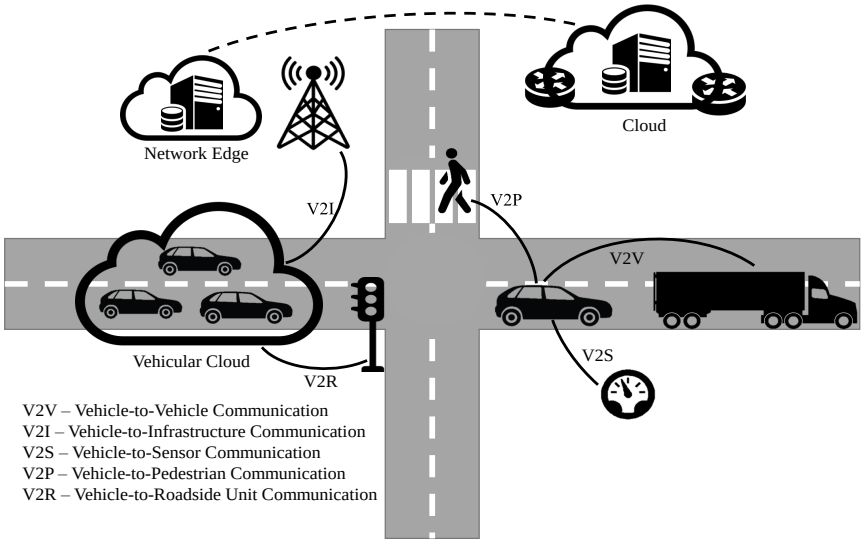


Figure 1. Vehicle-to-Everything (V2X) communication.

1.1. Motivations and Contributions

The employment of trust management schemes prevents vehicles from exchanging fake safety messages and help eradicate nodes dispersing counterfeited information by computing data and entity-based trust scores relying on trust attributes to guarantee safe and reliable traffic flows. Weights are assigned to these trust attributes to reflect their respective influence on the trust computation and a threshold is specified to identify dishonest vehicles based on the calculated trust scores. Defining precise values for the weights associated with the contributing attributes and the steady threshold is extremely challenging. Moreover, it is of considerable importance to evaluate the performance of the envisaged trust management models against diverse attacks by introducing attack specific adversaries. This survey provides a comprehensive review of the state-of-the-art in vehicular trust management employing diverse computational domains, including but not limited to, Bayesian inference, blockchain, machine learning, and fuzzy logic. Furthermore, the survey presents a comparison among the said trust management models in respect of the evaluation tools, quantification of weights, misbehavior detection, attack resistance, and quantification of threshold. Table 1 presents a comparison of the recently published surveys on the vehicular trust management vis-à-vis the current work. The table depicts that the recently published surveys do not account for the trust aggregation process (i.e., the trust attributes and the quantification of weights associated with them) and lack the discussion on the computational methodologies employed for trust evaluation. Considering these challenges, we summarize the salient contributions of this survey as follows:

1. We provide an overarching background of the IoV architecture along with a comprehensive discussion on the notion of trust (and its indispensable constituents) and some major attacks that can transpire on an IoV network;

2. We review the state of the art in the vehicular trust management with a focus on some key factors, including but not limited to, quantification of weights, quantification of threshold, and misbehavior detection;
3. We identify and subsequently discuss the open research challenges in the subject domain.

Table 1. Comparison of Recent Surveys.

Ref.	Title	Methodology Based	Misbehavior Detection	Trust Aggregation	Salient Contributions
[28]	Trust Management for Vehicular Networks: An Adversary- oriented Overview	✗	✓	✗	Adversary-oriented survey; discussion on cryptography, trust based solutions, and attacks that can overpower both.
[29]	A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy	✗	✓	✗	Background on VANETs; discussion on security services, location privacy protection schemes, and simulators; review of authentication schemes; analysis of trust management models.
[30]	Trust in VANET: A Survey of Current Solutions and Future Research Opportunities	✓	∼	✗	Comprehensive review on vehicular trust management; description of attack mitigation employing the said trust management mechanisms.
This survey	A Survey of Trust Management in the Internet of Vehicles	✓	✓	✓	Background on IoV; discussion on IoV architecture, trust and its constituents, and IoV attacks; comprehensive review of the state-of-the-art trust management employing diverse computational domains; comparison in respect of the evaluation tools, quantification of weights, misbehavior detection, attack resistance, and quantification of threshold; open research challenges.

✗ Not Addressed, ∼ Partially Addressed, ✓ Addressed.

1.2. Organization of the Paper

Figure 2 depicts the taxonomy of the survey at hand. The rest of this paper is organized as follows. Section 2 provides necessary background of the IoV architecture. Section 3 discusses the notion of trust and its constituents. Section 4 presents a comprehensive review of the existing state-of-the-art trust management models. Section 5 discusses the open challenges in the subject domain. Finally, Section 6 offers concluding remarks.

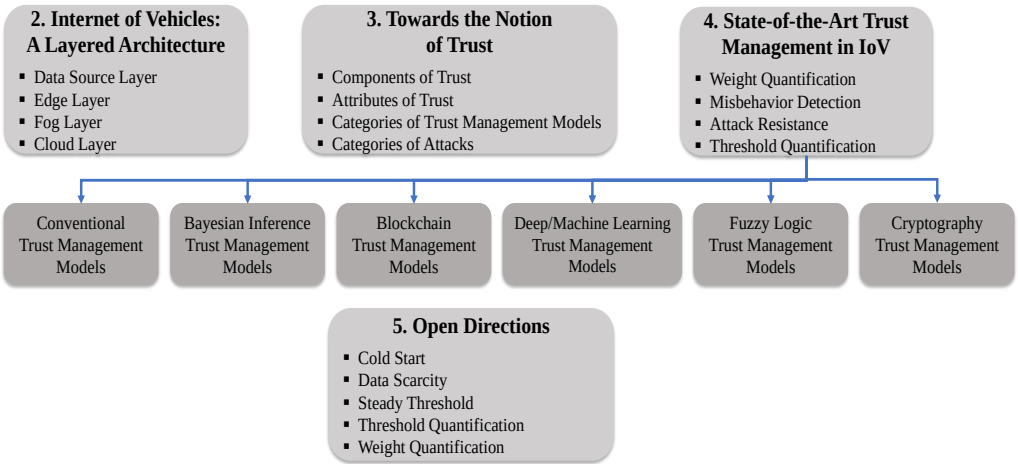


Figure 2. Taxonomy of this survey.

2. Internet of Vehicles: A Layered Architecture

The layered hierarchy of the Internet of Vehicles is similar to that of the Internet of Things as smart vehicles are connected to other vehicles and smart infrastructure to share data over the Internet. Figure 3 depicts the layered IoV architecture.

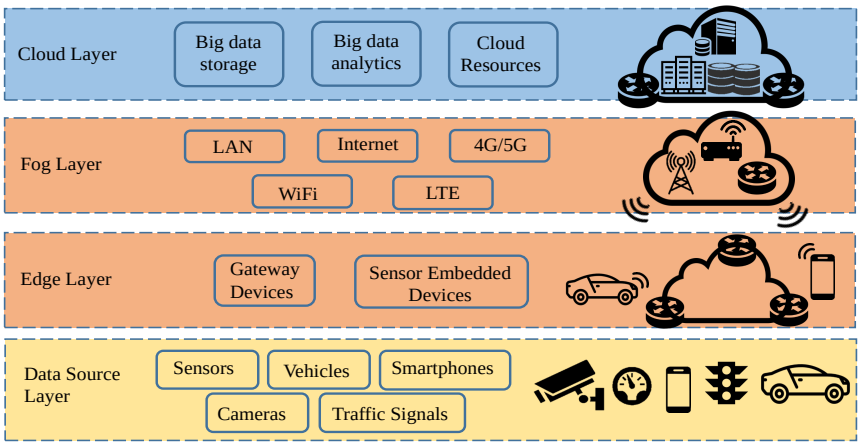


Figure 3. A layered architecture of an IoV network.

2.1. Data Source Layer

Nearly 100 sensors are embedded in modern vehicles, and it is anticipated that these sensors will increase to approximately double in number expeditiously [31]. These diverse sensors acquire data from the immediate ambience of the vehicle, which combined with the information gathered by V2V, V2R, and V2P communications belong to the data source layer. Due to the limited processing capability of a vehicle, only a limited volume of these data are processed at this layer.

2.2. Edge Layer

Owing to the critical nature of the vehicles' and traffic related information, the processing and analysis of the immense volume of the data gathered by the sensors and V2X communications need to be achieved in real-time. Accordingly, an edge layer is introduced to further process such data without incurring the cloud-related delays by utilizing the same sensor embedded smart vehicles, infrastructure or gateway devices.

2.3. Fog Layer

This layer, just like the edge layer, is introduced to reduce the dependence on cloud for data analysis. The fog layer accomplishes further processing of data at a local level utilizing intermediate networking infrastructure, V2I communications, Wi Fi, LAN, etc., consequently, ensuring prompt decision-making and preventing latency issues which might have transpired by relying only on cloud for all the processing [32].

2.4. Cloud Layer

This layer encompasses big data storage and cloud servers for storage and extensive computation of the massive volume of data which cannot be processed at the preceding layers. Due to the latency issues introduced by the cloud, the data that is not critical for expeditious decision-making, e.g., data required for high-end applications such as traffic navigation systems and traffic flow monitoring systems, is analyzed on this layer.

Vehicular networks are susceptible to attacks due to the dynamic topology and high mobility. To prevent the vehicular networks against the insider attacks, the notion of trust is introduced.

3. Towards the Notion of Trust

Most experts, irrespective of domain, conceptualize trust as a certain degree of risk, vulnerability, or uncertainty, and it establishes an expectation regarding the way an entity might behave in future [33]. Trust is a multifarious abstraction which relies entirely on the subject's perceptive. In psychology, trust is often defined as the degree of likelihood of an individual's anticipation/expectation towards another (i.e., a peer) with regards to the peer's conduct on which one's welfare relies [34,35]. Trusting reflects the belief of a trustor that the trustee will not exploit the trustor for its (i.e., the trustee's) benefit, the trustee will not exhibit malicious behavior towards the trustor and is inclined to sacrifice for the trustor, and that the trustee is capable of acting for the benefit of the trustor [35,36]. In sociology, it is believed that reciprocity and cooperation in social interactions or voluntary associations derive trust [37]. In economics, having confidence on the business associates' reliability and integrity, and on the transactions among them is defined as trust. Furthermore, given the nature of online businesses with no physical interaction among the trading parties and with the products, trust plays a significant role in reducing risks associated with business transactions and information asymmetry, and allows acclaimed sellers to achieve price premiums [34,38].

Trust, as a tactic to enhance the security, has been used with a variety of interpretations by researchers in computer science. It is said to be the belief of a trustor on the reliability of a target node with an aim to achieve a trust objective under certain conditions [39]. In other words, trust is the perception of an evaluator regarding the character, relying on past interactions with a target entity and/or the opinions of the trustworthy nodes [40]. We define trust as the confidence of a trustor towards a trustee based on the past experiences among the two and the recommendations received from the trustor's neighbors regarding the trustee. Most, if not all, of the trust management models discussed in this article are (more or less) using similar definitions of trust.

3.1. Components of Trust

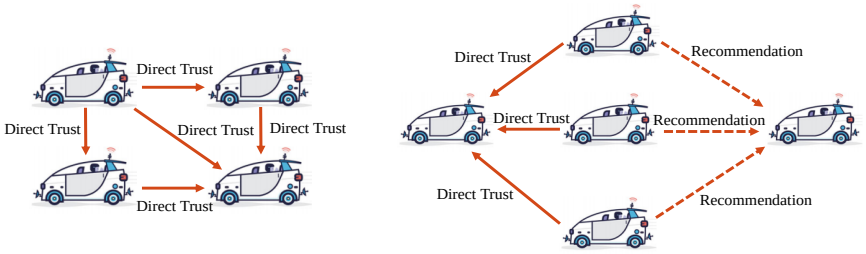
The notion of trust relies on the quality of interactions between two entities usually encompassing these components [41]:

3.1.1. Direct Trust

Direct trust exhibits the direct observations of a trustor on a target vehicle, relying on the interactions among the two [42]. Some researchers use the term *knowledge* to define the direct information gathered by the trustor to evaluate the trustee utilizing certain parameters relying on the participating nodes and the services [43]. It is believed that the significance of direct trust exceeds the indirect trust, however, the amalgamation of both is taken into consideration while assessing a vehicle [31]. Figure 4 delineates direct and indirect trust among vehicles.

3.1.2. Indirect Trust

Indirect trust manifests the opinions of the neighboring/trusted entities of a trustor regarding the target node (trustee), taking into account the past experiences with the node in question. Some researchers use the amalgamation of *reputation* and *experience* to explain indirect observation. Reputation accumulates all the past experiences with a target node to depict a global opinion regarding that node, whereas experience is a correlation among the trustor and the trustee relying on the belief of the trustor regarding the degree of confidence on the trustee to carry out a task [39].



(a) Direct Trust (b) Indirect Trust

Figure 4. Direct and indirect trust.

3.2. Attributes of Trust

A variety of influencing trust attributes are considered while computing the above-mentioned trust components:

3.2.1. Similarity

Similarity relates to the degree of similar content and services among any two vehicles. In the literature, similarity among the messages or vehicles is often taken as the Euclidean distance, the direction of movement of two nodes, i.e., cosine similarity, or the positioning based trajectory similarity [44–46].

3.2.2. Familiarity

Familiarity manifests how familiar/acquainted two vehicles are with one another. A high familiarity score reflects considerable prior knowledge of the evaluator regarding the trustee. This feature is adapted from social networks where more familiarity leads to a greater level of trust in interpersonal relations [47].

3.2.3. Timeliness

Timeliness delineates how recent the interaction among two vehicles is and is computed by taking into account the current time instance and the instance when the interaction took place [48]. It is of paramount significance to maintain the timeliness of data and the trust scores, as the outdated information reflects an obsolete trust value that can lead to dire repercussions [49].

3.2.4. Packet Delivery Ratio

The packet delivery ratio is the degree of how well a trustor is connected to the trustee. In the literature, it is often defined as the packet forwarding rate among nodes and is considered as the sole parameter to compute the direct trust towards a trustee. Furthermore, it is also regarded as a primary objective and core criterion while designing trust models and identifying malicious behavior, respectively [49–51].

3.2.5. Co-Work Relationship

Co-work relationship describes the interactions relying on the services instead of the physical proximity. Analogous to social networks, two nodes exhibit a working association when a node offers a service needed by the other and it can be computed through a comparison of multicast interactions [52].

3.2.6. Cooperativeness

Cooperativeness defines the willingness of a node to collaborate with its peers for improved network operations. This feature is of great significance to maintain stability in a vehicular network, consequently, incentives are introduced in order to promote cooperative behavior among different vehicles in a network [52–54].

3.2.7. Duration of Interactions

Duration depicts the length of the interaction among two nodes. It is presumed that considerably long interactions lead to better collaboration among entities which result in development of a much higher trust level. This is because the longer the interaction is, the more an entity can learn regarding the other's conduct and capability [52].

3.2.8. Frequency of Interactions

Frequency is the measure of how often the trustor and the trustee interact with each other. Every time a pair of nodes interact, they get an opportunity to acquire information concerning each other's communication and behavioral patterns which result in more accurate trust computations [52].

3.3. Categories of Trust Management Models

Vehicular trust management models are generally categorized in three groups, namely data-centric, entity-centric, and hybrid trust management models:

3.3.1. Data-Centric Trust Management Models

This category of trust management models focuses mainly on the accuracy and legitimacy of the information shared among vehicles. This information primarily includes reports and warnings regarding an event. The data-oriented trust models evaluate the honesty of every incident, therefore, delays and data loss may be experienced in case of dense traffic scenario. Conversely, these trust models do not perform satisfactorily in information sparsity due to the lack of enough evidence. It is believed that in this category, the participating entities do not hold long-term trust associations [31,40,55]. Numerous data focused trust management schemes have been proposed in the existing research works, wherein (i) the trust level of the data is assessed by associating weights to the reports (i.e., regarding an event) shared by neighboring vehicles. The associated weights rely on the time and location proximity of a vehicle with regards to the reported event, i.e., a vehicle in the close proximity of an event will have more up-to-date and credible information regarding that event [56], or (ii) the trust level of the message is assessed by considering content conflict and similarity, and the similarity in routing path. Subsequently, a trust value reflecting the probability of the message being authentic is assigned to every exchanged message [57].

3.3.2. Entity-Centric Trust Management Models

This category of trust management models emphasizes on the reliability of the participating vehicle by utilizing the sender's reputation and neighbor recommendations towards it. Therefore, sufficient data is required regarding the originator of the message and its neighboring vehicles for accurate assessment which is rather complicated considering the highly mobile nature of vehicular networks. It is believed that the authenticity of the messages could be an issue as there is no guarantee that the messages originated/sent by the honest vehicles could not be corrupted [40]. Several entity focused trust management schemes have been proposed in the existing research works, wherein (i) the trust score of every vehicle is evaluated amalgamating direct and indirect trust scores prior to electing a cluster head. The vehicle having a trust score greater than a predefined threshold is classified as a trustworthy vehicle, or else, it is categorized as a malicious one [58,59], or (ii) to prevent the network from selecting a malicious vehicle as the data forwarding agent, an aggregated score for vehicles is computed based on the amalgamation of a vehicle's current level of trustworthiness, its cooperativeness, and the recommendation of the last hop. The highest scoring vehicle is selected as the relay vehicle for data dissemination [60].

3.3.3. Hybrid Trust Management Models

This category of trust management models encompasses both the data and the entity-based trust evaluation, i.e., authenticity of the exchanged data, neighbor's recommendation

towards the trustee and its (i.e., trustee's) reputation are taken into account. In other words, the honesty of an event is reflected by the trustworthiness of the sender vehicle. An extensive literature review suggests that numerous hybrid trust management models have been presented, wherein (i) both node and data trust are evaluated and performance is evaluated in the presence of dishonest nodes that counterfeit safety-critical information in addition to advertising false trust rating to deceive the trustworthy vehicles into trusting corrupt information [61], or (ii) both node and data trust are assessed to guarantee reliable data exchange among entities and authenticity of the data disseminated by these entities. The final trust computation aggregates the weighted trust score based on a vehicle's cooperation with its peers, and the weighted trust value reflecting the quality of data sent by the vehicle to its neighbor [62].

3.4. Categories of Attacks

The highly mobile and dynamic nature of the vehicular networks, and the lack of pervasive infrastructure lead to the vulnerability against numerous attacks classified according to their demeanor, nature, and the extent of the damage caused by them as:

3.4.1. Active Attack

The attackers in an active attack originate counterfeited messages or alter the contents of legitimate messages. It is rather easy and inexpensive to detect such attacks; however, they are not easy to avoid. The main objective of these attacks is to modify network operations and would need to implement physical security measures to be prevented [63].

3.4.2. Passive Attack

Passive attacks are launched to gain insight into the target node without altering the message content. The primary purpose of such attacks is to acquire disseminated data from the network and are harder to detect as they do not disrupt network operations. In passive attacks, the attackers do not take part in the network communications and encrypting data can help avoid these attacks [63,64].

3.4.3. Malicious Attack

Malicious attacks are initiated with a purpose to harm the participating nodes of the network instead of benefiting from the attacks. Such attacks can be awfully destructive and are regarded as extremely dangerous. In some cases, malicious attacker may drop or spread bogus safety-critical information endangering the safety of the drivers, passengers, and pedestrians [65].

3.4.4. Selfish Attack

Unlike malicious attackers, selfish attackers aim for personal gain from the attack, e.g., to preserve their resources by not relaying the received messages. This indicates a considerably low collaboration rate among vehicles. Incentive-based techniques are often employed to prevent selfish behaviors and encourage cooperation among vehicles [66].

3.4.5. Insider Attack

Insider attacks are launched by legitimate users of the network, i.e., the users who have already cleared the authentication phase and are a part of the network in question. Due to their knowledge of the network, the attackers are able to launch attacks rather easily. To mitigate such attacks, trust management is introduced in the networks.

3.4.6. Outsider Attack

In contrast to insider attacks, outsider attacks are executed by nodes that do not have a direct access to the authorized nodes of the network. The attackers do not possess prior knowledge of the network and so these attacks are relatively less damaging. Cryptography-based techniques are often employed to prevent such attacks.

The attacks falling under the aforementioned categories include but are not limited to:

3.4.7. Man-in-the-Middle Attack

Man-in-the-middle attack occurs when a dishonest vehicle intercepts and/or alters the data exchanged among honest vehicles. The said data may contain safety-critical information, e.g., a blind intersection warning, and altering or counterfeiting such messages threatens the lives of the drivers, passengers and the pedestrians [24].

3.4.8. Sybil Attack

When a malicious vehicle disrupts the network applications by claiming or stealing multiple identities, the attack is known as a Sybil attack. It can be used to deceive other vehicles into believing that there is a road congestion by showing a higher number of vehicles than actually exists on the road [25].

3.4.9. Bad-Mouthing and Ballot Stuffing Attack

Trust management models employing neighbor recommendations towards the target vehicle as a part of trust computations can fall victim to bad-mouthing attacks. In these attacks, dishonest vehicles collude to harm the reputation of a vehicle by providing unfair negative ratings for it. In ballot stuffing attacks, vehicles assign unfair positive ratings to a target vehicle to boost its reputation [26,67].

3.4.10. On-Off Attack

Dishonest vehicles do not necessarily depict malicious behavior persistently, instead, there are attackers who behave intelligently, i.e., they switch between honest mode (i.e., where they gain a higher trust score) and dishonest mode (i.e., where they launch an attack). Such attacks are known as on-off attacks and allow the intelligent attackers to cause damage without being tagged and evicted from the vehicular network [31].

3.4.11. Selective Behavior Attack

Analogous to on-off attacks, there might be a case where malicious vehicles behave maliciously (i.e., share counterfeited messages) with some nodes, whereas with other nodes, they behave honestly (i.e., share reliable information). This could result in contradictory trust scores (i.e., based on the direct or/and the indirect observation) assigned to a vehicle by its peers [68].

3.4.12. Black-Hole Attack

Black-hole attackers manipulate other vehicles to transmit data through them (i.e., the attackers) by advertising the route through them (i.e., the attackers) as the best route despite having no route to the desired destination. Once other vehicles send the data to these attackers, they create a blackhole by dropping the data sent towards them [27].

An illustration of Sybil attack, bad-mouthing attack, on-off attack, and selective behavior attack is depicted in Figure 5.

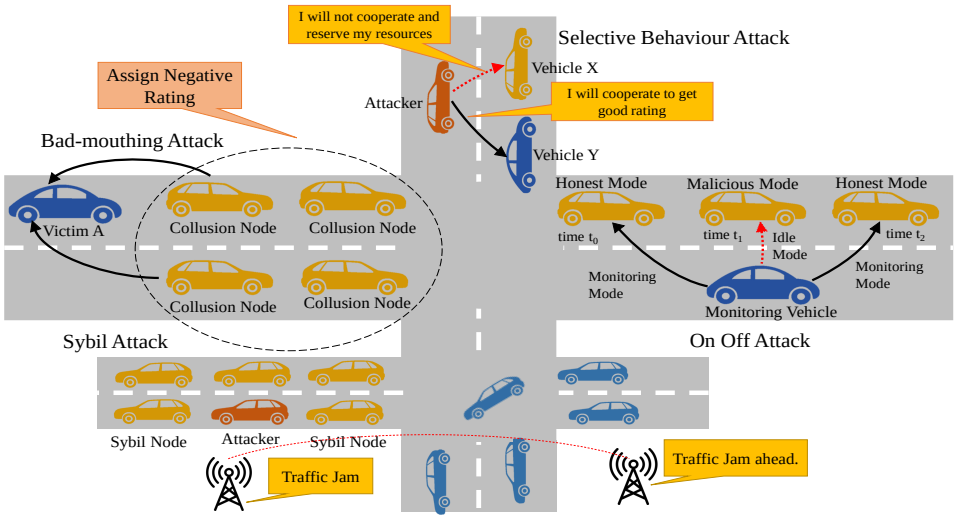


Figure 5. Attacks in the Internet of Vehicles.

4. State-of-the-Art Trust Management in IoV

As a consequence of high dynamicity, vulnerable communications, and scarcity of pervasive intercommunication infrastructure, IoV is susceptible to attacks from both inside and outside the network. The dishonest vehicles counterfeit safety-critical data and often introduce transmission delays to disrupt vehicular services, consequently endangering the lives of drivers, passengers, and vulnerable pedestrians. During the past decade or so, trust management has been employed to ensure safe and reliable vehicular networks. This section depicts a comprehensive review of the literature on the trust management in vehicular networks categorized into six classes including: (1) traditional, (2) Bayesian inference-based, (3) blockchain-based, (4) deep/machine learning-based, (5) fuzzy logic-based, and (6) cryptography-based trust management models. Table 2 presents existing state-of-the-art trust management models in IoV.

4.1. Conventional Trust Models

Conventional or traditional trust management models are defined as widely accepted frameworks that function without requiring complex data analysis or statistical inference tools. In this subsection, recent research employing traditional trust management models has been discussed in detail [69–73].

Ahmad et al. [69] presented MARINE that detects malicious vehicles, i.e., vehicles launching man-in-the-middle attacks, and cancel their credentials. MARINE is a hybrid trust model that also considers the possibility of an honest vehicle to initiate a false message due to malfunctioning hardware and a malicious vehicle to generate a genuine message. The proposed model takes into account the node trust, data trust, vehicle-to-vehicle trust, and the infrastructure-to-vehicle trust. Node trust is computed by aggregating the past interactions with the target vehicle and the opinions of its neighbors, whereas the data trust is calculated by taking into account the quality of the data received, neighbors' recommendations and the ability of the vehicle to forward messages. While computing the vehicle-to-vehicle trust, every vehicle forms a positive report that includes the honest vehicles and a negative report including details about the dishonest vehicles. These reports are then conveyed to the Roadside Unit (RSU) which, on its part, computes the infrastructure-to-vehicle trust and updates the above-mentioned reports. The up-to-date reports are then shared with the neighboring nodes. The proposed model has been tested against three attack scenarios utilizing simulation of urban mobility (SUMO) and vehicles in network simulation (VEINS).

Suo et al. [70] proposed a distributed, and a centralized trust-based system where trust authorities and vehicles join forces to alleviate dishonest behavior in vehicles. Every vehicle informs the trusted authority regarding suspicious behavior. The trusted authority,

on the basis of suspicious activity information received from different nodes, decides if the certificate issued to a particular vehicle should be revoked. The suggested system model addresses insider attacks and it is assumed that the adversary is capable of counterfeiting messages and disseminating them to the vehicles and roadside units in its vicinity via jeopardized vehicles. The trusted authority takes into account both the direct and the indirect interaction with the target vehicle. Different contributing parameters are assigned different context-based weightage while aggregating the trust score. The vehicles with higher trust scores have a higher impact on the trust establishment process. Both architectures, centralized and distributed, are evaluated using a python-based simulation for four different kinds of dishonest behaviors. The absence of a global perspective and the risk of over-trust are two of the main concerns regarding the distributed architecture mentioned by the authors.

Mahmood et al. [71] proposed a hybrid trust management model that amalgamates trust score and available resources of vehicles to compute a composite metric which is utilized to elect a cluster head and a proxy cluster head for a vehicular cluster. Available resources encompass the weighted sum of the measure of remaining power and bandwidth of a vehicle, whereas the trust score is an average of the direct and the indirect trust scores of a vehicle. Subsequently, vehicles with the highest and the second highest composite metric are elected as the cluster head and proxy cluster head, respectively, while the vehicles with a composite metric falling below a predefined threshold are classified as malicious vehicles. The performance evaluation of the proposed model has been carried out employing MATLAB.

Noorullah et al. [72] proposed a forwarding approach for critical information in vehicular social networks, wherein following the legitimacy verification of the emergency notification utilizing the information regarding the location and the social media of the source vehicle, significance of vehicles is computed to identify the vehicles most famous among their peers with the aim of rapid dissemination of the notification. The most well-connected vehicle is the one that shares interests, has common contacts, and is more similar in behavior to its peers. For computing a vehicle's reputation, its contribution in the network and the recommendations by its neighbors are taken into account, which is then utilized in calculating the trust value of that vehicle. The vehicles whose assigned trust values are close to the highest possible trust score are more likely to further improve their reputation and vice versa. Consequently, the dishonest vehicles will be isolated from the forwarding process. Accordingly, the emergency message is disseminated through the network utilizing the vehicle to vehicle and infrastructure communication. Simulations of the proposed scheme are carried out using VANETMobiSim and the performance evaluation metrics included the transmission rate, the propagation latency, the number of messages disseminated, the duration for which the emergency message will circulate in the network, and the number of vehicles selected for critical message dissemination.

Chuprov et al. [73] proposed a scheme to mitigate traffic management issues on the crossroads by identifying the vehicles sending illegitimate messages, wherein three parameters, truth, reputation, and trust, each having a value within [0,1], are computed to assess the legitimacy of the data sent by vehicles. Truth being the opinion regarding the legitimacy of the message exchanged by vehicles, reputation is defined as the temporal function of the truth value, and trust is the weighted aggregation of both of the above stated parameters. The computed trust score is compared with the predefined threshold and the vehicles having a trust score greater than the said threshold are considered trustworthy. The vehicle identified as the source of the misleading information, i.e., the untrustworthy vehicle, is isolated from interacting with its peer vehicles. The performance evaluation of the said system is conducted first by using a customized simulator and then the results are also validated utilizing hardware simulations based on an autonomous vehicle model developed by the authors.

4.2. Bayesian Inference-Based Trust Model

Bayesian inference employs Bayesian theory that delineates uncertainty of data-centric modeling and inference relying on probability and statistics [74]. Bayesian statistics utilize prior distribution for probabilistic distribution of parameters which is amalgamated with the likelihood function to generate posterior distribution [75]. This subsection comprises detailed discussions on recent research in vehicular trust management models utilizing Bayesian inference [76–80]. Zhang et al. [76] proposed a TrustRank algorithm-based trust management model that takes into consideration both local and the global trust of the vehicles. The local trust is computed by applying the Bayesian inference model to the past interactions of the vehicles. Once the local trust values are computed, a trust link graph is constructed. In order to calculate the global trust, social parameters based on the driver (e.g., age, driving license score, driving age, etc.), the vehicle (e.g., vehicle type, handling stability, breaking performance, etc.), and the behavior (e.g., number of speeding tickets, number of traffic violations, etc.) are combined with the local trust values and the previous global trust values before applying the TrustRank based algorithm. The most trustworthy vehicles named as the seed vehicles are identified using the PageRank algorithm which, subsequently, helps in determining the trust values of other vehicles. Simulations are performed using VEINS and the evaluation of the proposed model is measured using two performance metrics, i.e., true negative and true positive rates. Three different attacks have been considered while evaluating the system model, i.e., newcomer attack, on-off attack and collusion attack.

He et al. [77] envisaged a trust management scheme for enhancing the security of cognitive radio based VANETS and detected the JSSDT (i.e., joint spectrum sensing and data transmission) attackers that counterfeit reports and drop data in the spectrum sensing and transmission phases, respectively. While performing trust computations, an aggregation of weighted direct and indirect trust is calculated. The information regarding the neighboring vehicles' behavioral patterns is acquired, the neighbor trust is computed by employing techniques such as Bayesian inference, and is forwarded to other components of the model for other applications such as the data transmission unit which may utilize the computed trust score for route discovery, and the spectrum sensing unit which may utilize the calculated trust as a weightage for aggregation of spectrum detection. The performance of the proposed model is evaluated in terms of false alarm and miss detection probability, latency, and throughput.

Fang et al. [78] proposed a trust management model that employs Bayesian network to prevent on–off attack. The trust computations aggregate weighted direct and indirect trust, direct trust being the trust score relying on the direct interactions, both current and past, between two vehicles (i.e., a trustor and a trustee), whereas the indirect trust is the highest direct trust value assigned to the trustee by all of its neighboring vehicles, i.e., trustors. In the said attack, the vehicle alternates between honest and dishonest conduct quite frequently, consequently, the malicious vehicles end up achieving elevated trust scores. A window to identify the attack is defined based on the interactions between the trustor and the trustee. Every window has a highest, and a lowest trust score assigned to the trustee by the trustor and the number of times the trustee alters between the highest and the lowest score is counted. The dishonest vehicles switch from high to low and vice versa more often. Furthermore, their extreme trust scores are higher in comparison to honest vehicles which results in a smaller difference between the extremes and a higher switch count. If the switch count exceeds a predefined threshold, and the difference between the extremes is smaller or the highest trust score is greater than another predefined threshold, the vehicle is tagged as a malicious one. Simulations of the proposed model are carried out using MATLAB.

Li et al. [79] proposed a secure content delivery framework amalgamating the notions of trust and game theory. The vehicles are evaluated relying on their positivity and ability to communicate with their peers. Whenever a pair of vehicles communicate, the evaluator assigns an evaluation value to the evaluatee which is then cached in the evaluatee's local

storage. An average of this evaluation value and a punishment value is combined to compute the trust value of the evaluatee. To minimize the effects of malicious activities, the vehicles are given the opportunity to challenge the punishment value assigned to them by their peers. Moreover, an evaluatee is evaluated by the same evaluator only once. On the other hand, RSUs are evaluated based on quality of service and reliability, and the average of this evaluation along with the punishment scores are combined to calculate the trust score for the target RSU.

Talal et al. [80] proposed a Bayesian inference-based decentralized trust model that takes into consideration the quality of direct interactions among the vehicles and the event related data transmitted by a vehicle. A belief function is defined to update the trust scores of a vehicle relying on the correlation among the event information that the target vehicle transmitted and the actual status of that particular event. The proposed method assigns a low initial trust score based on the punishing strategy to any vehicle new to the network to prevent dishonest vehicles from gaining advantage by leaving and joining the network frequently to gain high trust scores. To overcome the negative impacts of the said punishing strategy, i.e., the lack of collaboration opportunities available for the newcomer due to a low trust score, a trust based vehicular coalition formation scheme to encourage collaboration among vehicles is utilized. The performance analysis of the proposed scheme is performed on MATLAB.

4.3. Blockchain-Based Trust Model

Blockchain technology deals with the distributed digital ledger of transactions. It consists of unalterable decentralized database comprising blocks of data forming chains [81,82]. In this subsection, a detailed overview of the recent research in trust management models employing blockchain technology has been presented [83–87]. Javaid et al. [83] proposed a privacy preserving model that utilizes blockchain for exchange of information as well as trust management in a distributed architecture. The vehicles are registered in the network which helps in developing information provenience and certificates are issued to them by a certificate authority (i.e., an RSU) to achieve data exchange security. To ensure the data trustworthiness, physical unclonable functions (PUF) are utilized after the registration of each vehicle. When data is generated, the list of trusted registered vehicles is examined for the originating vehicle. If the system is successful in locating the vehicle in the trusted list and the PUF response is also correct, a certificate is issued. The proposed model was simulated employing an Ethereum virtual machine and a threat model with an adversary, that can imitate/impersonate a vehicle and transmit counterfeited information to the RSU, and alter the information sent by a genuine vehicle, is utilized for system evaluation.

Khan et al. [84] proposed a model that amalgamates blockchain and trust for misbehavior prevention, wherein, a set of public and private keys is generated for every new vehicle, and a certificate is issued to the vehicle, which, in addition to the Certificate Blockchain (CertBC) having this certificate in its record and Revocation Blockchain (RevBC) not having the public key of the vehicle in its record, is used to authenticate the vehicle preceding the trust score acquisition from Trust Blockchain (TrustBC) and the information sharing among the vehicles. When an incident is reported by the vehicle, the receiving vehicle computes the legitimacy and the trust of the report, records it in a trust set, and employs it to calculate the likelihood of the reported incident happening. The report is considered legitimate if the resulting likelihood is greater than the predefined threshold and a positive ranking is assigned to it before it is recorded in the Message Blockchain (MesBC), which is forwarded to the RSU. The greater the number of positive rankings assigned to a vehicle, the more trustworthy the vehicle is, whereas a higher number of negative rankings (i.e., greater than a predefined threshold) results in the vehicle's public key and the certificate cancellation. The RSU, on the receipt of MesBC, computes the updated trust score of the vehicle and informs the network about it before recording it to the TrustBC. In order to become a miner, the hash value computed by the RSU should not exceed the predefined threshold and the sum of the absolute hash values of the RSU should not exceed the highest sum of these

values. The block of the miner is then published into the blockchain and it is ensured that the blockchain of every RSU is identical. The performance evaluation of the proposed scheme is conducted by utilizing VEINS, SUMO, and OMNET++ (i.e., Objective Modular Network Testbed in C++), with and without introducing the denial of service attack.

Lu et al. [85] presented a trust management scheme that relies on the blockchain technology to ensure privacy preservation while the certification authority (CA) issues and revokes certificates. It is achieved by splitting the linkage among a vehicle's true identity and its public key. Any action taken by the CA is recorded evidently in the blockchain without exposing any sensitive details regarding vehicles to make sure a vehicle's public key could be utilized as its authenticated pseudonym. Furthermore, every vehicle is assessed relying on the legitimacy of the information disseminated by it in addition to the neighbors' opinion towards the said vehicle. The record of all the messages is maintained in the blockchain and is used as an evidence to compute the reputation score for each vehicle which helps alleviate dishonest behavior and dissemination of counterfeited messages. The vehicles are rewarded for their cooperation, honesty and reporting misconduct, whereas the vehicles are liable to a penalty for misconduct and collusion. The experiments of the proposed scheme are carried out on an Intel Core i5, 2.5 GHz system and the performance is assessed in terms of overhead concerning the storage, transmission, and computation.

Yang et al. [86] proposed a blockchain based decentralized trust management model, wherein the vehicles evaluate the messages received from other vehicles and notify the RSUs about their evaluation results. The RSUs then compute the entity-based trust scores for the vehicles and create trust blocks. The RSU with the highest number of trust values in its block is selected as a miner to update the trust score of the particular vehicle by adding their block first. The adversarial model includes the spoofing attack where dishonest vehicles can counterfeit safety messages, and bad-mouthing attack where vehicles provide dishonest assessment on the legitimacy of messages. The employment of the notion of blockchain in the trust management process provides a decentralized architecture, prevention from data manipulation, persistent trust records throughout the network, fast convergence, and the information regarding the trust scores of a particular vehicle are easily available to all the RSUs. Simulations of the proposed scheme are carried out using vehicular and blockchain simulation platform on MATLAB.

Kang et al. [87] proposed a blockchain based trust model that selects evaluators called *miners* based on their trustworthiness in previous interactions. These minors are responsible for the creation, distribution and validation of different blocks. Every node, while computing the reputation on a target RSU, incorporates the recommendations from all the other nodes utilizing subjective logic. Moreover, different influencing parameters, i.e., weights are introduced according to how often the two nodes interacted, how recent the latest interaction between the two was, and the outcome of the interaction, are taken into consideration. Subsequently, the weighted recommendations are aggregated to obtain a single recommendation prior to the accumulation of the direct and the recommended opinions. To encourage the participation of the verifiers in the block validation process, a reward is offered, and these verifiers, as per their reputation, are offered contracts by the block managers. Convex (CVX) tool based on MATLAB is utilized to optimize the reward process.

4.4. Deep/Machine Learning-Based Trust Model

Machine learning is a subset of artificial intelligence and relies on learning from experience (i.e., data) to forecast and make decisions with precision over time [88]. Deep learning, a subgroup of machine learning, focuses on simulating the way a human brain works to learn from experience (i.e., large volume of data) by employing neural networks with multiple layers [89]. This subsection provides a detailed review of the recent research in trust management models applying the notion of machine learning and deep learning [90–94]. Tangade et al. [90] proposed a trust management model that utilizes the

notion of deep learning to enhance the reliability and offers reduced latency. Each vehicle communicates with the neighboring vehicles and based on this communication, reward points are granted to the vehicles that are used to categorize the drivers/messages as honest or dishonest and, subsequently, utilized for trust score computation by employing deep neural network. A message generated by a vehicle is broadcasted and upon receipt at the RSU, the source is authenticated, and deep neural network is employed to compute the reward points taking the factors concerning the driver's behavior into consideration. The received message is classified as honest or dishonest utilizing a deep neural network by the RSU and, subsequently, the mediator trusted authority calculates the updated trust score of the particular vehicle. The proposed model is evaluated via simulations carried out on TensorFlow and Network Simulator (NS-3).

Zhang et al. [91] suggested a trust management model for software-defined networking based VANETs, wherein the route discovery is ascertained by evaluating the trustworthiness of the next hop neighbors. The said heuristic encompasses state, action, and reward, and contains information pertaining to the forwarding ratio matrix, next hop neighbor selection made by the SDN (software-defined network) controller, and the route trust evaluation, respectively. Furthermore, the authors' defined a minimum acceptable trust score and the vehicles possessing a trust score below the same are categorized as dishonest vehicles. When a vehicle originates a message and the data routing information is unknown, route discovery method and trust calculations are utilized to learn the best data forwarding information. As a vehicle's position and forwarding ratio are likely to change, the trust of that particular vehicle is inclined to change which, subsequently, affects the trustworthiness of the discovered path. Simulations are carried out on TensorFlow and OPNET.

Siddiqui et al. [92] presented a trust management model relying on machine learning to compute an optimal threshold and to identify malicious vehicles in a vehicular network utilizing three contributing parameters, i.e., similarity, familiarity, and packet delivery ratio. The proposed model employs multiple unsupervised learning algorithms to cluster the data for label assignment prior to applying diverse supervised learning algorithms to classify honest and dishonest vehicles, and to acquire an optimal threshold. Simulations for the proposed scheme are carried out on MATLAB.

Gyawali et al. [93] proposed a misbehavior detection scheme relying on hybrid collaborative machine learning and reputation where machine learning is employed to identify malicious messages, whereas reputation is utilized to evaluate the trustworthiness of a vehicle. Every message from a trustworthy vehicle is assessed prior to the report being sent to the local authority which amalgamates the reports employing Dempster–Shafer theory in addition to using the vehicle's reputation or trust value to compute the updated reputation. Subsequently, the reputation score is shared with the certificate authority and a revocation alert is broadcasted if the reputation value of the vehicle falls below the predefined threshold. The performance evaluation of the proposed scheme is carried out employing VEINS, SUMO and OMNET++.

Zhang et al. [94] presented a trust management model that relies on deep reinforcement learning approach to enhance communication among connected vehicles. The said trust management scheme integrates a dueling networking architecture inside the SDN's logically centralized controller to ensure a reliable route is established for data forwarding employing a deep neural network. The route selection process is initiated by the vehicle that wishes to forward data to another vehicle and the trustworthiness of each vehicle, along the path, is evaluated to select the directly connected neighbor that is best suited, i.e., the most trustworthy, next hop in the route from the source to the destination vehicle. Simulations of the proposed scheme are carried out on TensorFlow and OPNET.

4.5. Fuzzy Logic-Based Trust Models

Fuzzy logic focuses on representing the imprecision of human reasoning for decision making in an imprecise and uncertain environment [95]. In this subsection, trust

management models employing fuzzy logic have been presented in detail [96–100]. Guleng et al. [96] presented a decentralized trust management framework that employs fuzzy logic to amalgamate a vehicle's direct experience and the recommendations of its peers towards a target vehicle in order to tag the unintended dishonest behavior of the said target vehicle. Furthermore, besides the direct trust, an indirect trust score is also computed towards the vehicles that do not have a direct connection to the trustor employing the notion of reinforcement learning. While evaluating the direct trust, the proportion of the messages relayed by the target vehicle, the ratio of legitimate messages forwarded by the target vehicle, and the fraction of the identified incidents that were reported by the target vehicle, were considered prior to employing fuzzy logic. The indirect trust score is computed by inquiring the opinions of neighboring vehicles on the target vehicle by employing Q-learning where the trust value is decremented on every hop along the path from the node expressing the opinion to the inquirer. Simulations of the presented model are carried out using NS-2.34.

Souissi et al. [97] proposed a model that amalgamates trust, in terms of the degree of similarity, and fuzzy logic to guarantee legitimate location information. The central authority validates the location information by cross checking the attributes of the reported lane and the reporting vehicle prior to storing it locally for future reference, e.g., optimum route selection and the status of road traffic, etc. To compute the similarity, three input parameters, i.e., time, speed, and energy, are used as inputs to the fuzzy system. The higher the resulting similarity index, the higher the trust of the reported location information. The shared location information is characterized as malicious if the resulting similarity index is less than the predefined threshold. Simulations of the suggested system are carried out using MATLAB and SUMO.

Kumar et al. [98] amalgamated the notions of fuzzy logic and trust to select the best path between two nodes and to identify blackhole attacks. The relationship of vehicles is estimated using trust computations, wherein the proportion of the successfully forwarded messages by the neighbor from the number of messages this neighbor is expected to forward, the ratio of the number of messages received through the neighbor but generated by other nodes to the total count of received messages, and the acknowledgment of the message receipt are aggregated. The neighbors are ranked as bad, unknown, and good according to the relationship and the trust scores. To select the best path, the neighbor ranked as good is the preferred option for the next hop node selection to forward the data. The vehicles having a bad association are the ones with lower trust scores and are suspected as blackhole attackers. Simulations of the proposed model are carried out using NS-2 and SUMO.

Tan et al. [99] proposed the reputation-based trust management model wherein, a credit account reflecting a node's behavior is associated with every node. The higher the credit score, the more the node is preferred, whereas if the credits of a node are depleted, the said node is eradicated from the network. The trust score of a node takes into consideration the node's reputation, opinion of the neighboring nodes, and historical interactions with other nodes in the network. Graph theory and fuzzy logic are amalgamated to compute the entity-based trust, to avoid the trust scores from increasing quickly while still allowing a swift decrease in trust scores decaying mechanism is employed. The proportion of the messages successfully delivered and the mean delay value are chosen to be the trust computation parameters, and fuzzy functions are defined for them to evaluate the trustworthiness of the routes. The trust score of a route drops down if a dishonest vehicle exists in that route, therefore, this trust score can be utilized to compute a vehicle's trust score. Simulations of the proposed scheme are carried out on MoSim based on MATLAB.

Marmol et al. [100] amalgamated the notions of trust and reputation, wherein to accept or reject a message generated by vehicles, each vehicle computes the trust scores of its peers by employing fuzzy sets. While calculating the said trust values, the node's past reputation, and the opinions of the roadside infrastructure and the other vehicles in the cluster are taken into consideration. Moreover, the vehicles are rewarded or punished as

per the comparison of the final decision of their opinions regarding a particular message. If the source vehicle is proved to be dishonest, a notification is sent to the infrastructure and the information on the vehicle is added to the dishonest vehicle database if the number of negative opinions exceed a predefined threshold. Every message generated in the network has a severity level associated to it, accordingly, the message with a high severity level is considered trustworthy only if it is generated by a trustworthy vehicle. Simulations of the proposed model are carried out using trust and reputation model simulator (TRMSim-V2V) developed by the authors.

4.6. Cryptography-Based Trust Model

Cryptography focuses on ciphering data to ensure confidentiality and to prevent unauthorized entities from interpreting the information [101]. This subsection discusses, in detail, the recent research employing the notion of trust along with cryptography [102–106]. Muhlbauer et al. [102] proposed a trust management model, wherein the notion of digital certificates and reputation are amalgamated in a centralized vehicular architecture without the necessity of constant connectivity with the road infrastructure. The proposed scheme relies on public key infrastructure (PKI) for vehicles where an ID, a set of public and private keys, and a certificate is assigned to each vehicle and RSU to be able to communicate and authenticate the exchanged messages. The incidents are validated by the traffic control authority (CCO) in a centralized manner. Every vehicle is required to have a frequent contact with a certificate authority that issues the certificates and pseudonyms to preserve privacy. A score is maintained by each vehicle regarding its own certified reputation which is utilized to compute trust among vehicles. Whenever a vehicle notifies its peers regarding an incident, the recipients verify the digital signatures of the source vehicle using the certificate issued to it prior to the evaluation of the message legitimacy. The proposed scheme employs reputation for weighted voting, and message selection by applying simple summation, and Bayesian inference-based reputation prior to the comparison of the resulting score with the predefined threshold. Simulations of the said model are carried out utilizing VEINS, SUMO, OMNET++, and MiXiM (i.e., a mixed simulator for wireless mobile communication network).

Gai et al. [103] proposed a trust management model, wherein cookies are used by an inquirer to rate, in the range [0, 1], the services provided by another vehicle which are then signed by a certificate authority to keep the vehicle from counterfeiting them. Whenever a vehicle entertains a request by another vehicle, it forwards its cookies along with the service requested which is used by the requester to evaluate the trustworthiness of the service provider. In the event of first interaction between the two, the trust score assigned by the requester is the same as the cookie reported by the service provider. However, if the two have interacted in the past, the requester computes an aggregate of weighted direct and indirect trust based on the cookies. The direct trust being the one computed by the cookies in the record of the requester based on their historic interactions, whereas the indirect trust is the one computed using the cookies shared by the service provider. Simulations of the proposed model are carried out on VANETsim.

Table 2. Existing State-of-the-Art viz. Trust Management in Vehicular Networks.

Ref.	Category	Proposed Scheme	Evaluation Tools	Weight Quantification	Misbehavior Detection	Attack Resistance	Threshold Quantification
[69]	Traditional	MARINE	VEINS, SUMO	✗	✓	✓	✗
[70]	Traditional	Real-time Trust-Building Schemes for Mitigating Malicious Behaviors in Connected and Automated Vehicles	Python-based simulator	✗	✓	–	✗
[71]	Traditional	A Hybrid Trust Management Heuristic for VANETs	MATLAB	✗	✓	✗	✗
[72]	Traditional	Emergency warning messages dissemination in vehicular social networks: A trust based scheme	VANETMobiSim, ONE simulator	✓	✓	✓	✗
[73]	Traditional	Reputation and Trust Approach for Security and Safety Assurance in Intersection Management System	Custom software simulator	✗	✓	✗	✗
[76]	Bayesian Inference	AATMS in VANET	VEINS, OMNeT++, SUMO	✗	✓	✓	✓
[77]	Bayesian Inference	Trust management for secure cognitive radio vehicular ad hoc networks	Computer simulations	✗	✓	✓	✗
[78]	Bayesian Inference	BTDS for Intelligent Connected Vehicles in VANETs	MATLAB	✗	✓	✓	✗
[79]	Bayesian Inference	Trust Based Secure Content Delivery in Vehicular Networks: A Bargaining Game Theoretical Approach	–	✗	✗	✗	–
[80]	Bayesian Inference	Trust-Based Cooperative Game Model for Secure Collaboration in the Internet of Vehicles	MATLAB	✗	✓	✓	✗
[83]	Blockchain	DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts	Ethereum virtual machine based simulations	–	✓	✓	–
[84]	Blockchain	Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET	VEINS, SUMO, OMNET++	–	✓	✓	✗
[85]	Blockchain	BARS for Trust Management in VANETs	Intel Core i5, 2.5 GHz system based	–	–	–	–
[86]	Blockchain	Blockchain-based Decentralized Trust Management in Vehicular Networks	MATLAB	∼	✓	✓	✗
[87]	Blockchain	Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory	MATLAB based CVX	✗	✗	✓	✗
[90]	Deep/Machine Learning	A Deep Learning Based Driver Classification and Trust Computation in VANETs	TensorFlow, NS3	–	✓	✗	–

Table 2. *Cont.*

Ref.	Category	Proposed Scheme	Evaluation Tools	Weight Quantification	Misbehavior Detection	Attack Resistance	Threshold Quantification
[91]	Deep/Machine Learning	A Machine Learning Approach for Software-Defined Vehicular Ad Hoc Networks with Trust Management	TensorFlow, OPNET	✗	✓	✗	✗
[92]	Deep/Machine Learning	Machine Learning Based Trust Model for Misbehavior Detection in Internet-of-Vehicles	MATLAB	–	✓	✗	✓
[93]	Deep/Machine Learning	Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks	VEINS, SUMO, OMNET++	✗	✓	✓	✗
[94]	Deep/Machine Learning	A Deep Reinforcement Learning-based Trust Management Scheme for Software-defined Vehicular Networks	TensorFlow, OPNET	✗	✓	✗	✗
[96]	Fuzzy Logic	Decentralized Trust Evaluation in Vehicular IoT	NS-2.34	✗	✓	✓	–
[97]	Fuzzy Logic	A New Fuzzy Logic Based Model for Location Trust Estimation in Electric Vehicular Networks	MATLAB, SUMO	–	✓	✓	✗
[98]	Fuzzy Logic	A Fuzzy Logic-Based Control System for Detection and Mitigation of Blackhole Attack in VANET	NS2, SUMO	–	✓	✓	–
[99]	Fuzzy Logic	A Trust Management System for Securing Data Plane of Ad Hoc Networks	MATLAB based MoSim	∼	✓	✓	–
[100]	Fuzzy Logic	TRIP for Vehicular Ad hoc Networks	TRMSim-V2V	✗	✓	✓	✗
[102]	Cryptography	Bring your own reputation: a feasible trust system for VANETs	VEINS, SUMO, OMNET++, MiXiM	–	✓	✓	✗
[103]	Cryptography	Ratee-Based Trust Management System for Internet of Vehicles	VANETsim	✗	✓	✓	–
[104]	Cryptography	A Trustworthiness-Based Time-Efficient V2I Authentication Scheme for VANETs	GMP, PBC libraries, C language, Ubuntu based system	–	–	–	–
[105]	Cryptography	Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs	NS-3, SUMO, MOVE	–	✓	✓	✗
[106]	Cryptography	TPPR Scheme in VANET	Java based, NS-2, SUMO	✓	✓	✓	✗

✗ Not Addressed, ∼ Partially Addressed, ✓ Addressed, – Not Mentioned.

Wang et al. [104] proposed an authentication framework that utilizes trust to expedite the re-authentication process in the event of handover between the former and the current RSU where vehicles dissociate from the previous RSU and connect to another RSU in their vicinity. The cloud server is responsible for the evaluation of the trust score of every vehicle based on its characteristics. The RSU utilizes the trust score of a vehicle to complete the authentication process and the creation of the session key. As a vehicle traverses from the service range of one RSU (i.e., former) to the other (i.e., current), a certificate affirming the handover is received by the vehicle, and the current RSU forwarded by the former RSU. A token is generated to the vehicle by the current RSU prior to the generation of the session key between the two. Simulations of the proposed scheme are carried out utilizing GNU MultiPrecision (GMP) and Pairing-based Cryptography (PBC) libraries, C language, and a Ubuntu based system.

Tangade et al. [105] proposed a trust management model relying on hybrid cryptography for authentication to ensure robust and efficient trust management. The trusted authority registers the vehicles, road side units, and intermediary trusted authorities prior to their participation in the network. The trustworthiness of these vehicles is then verified by its neighbors via exchange of a test message and the resulting trust score is forwarded to the trusted authority which is responsible for computing and updating the trust value of the target vehicle. When communicating with one another in the network, vehicles also send their trust score in addition to other information such as safety messages, and is verified by the receiving vehicle through comparison with the one stored at the trusted authority. The safety alerts are trusted if the compared trust scores are identical and greater than the predefined threshold else, they are discarded. The performance evaluation of the proposed scheme is carried out utilizing NS-3, SUMO, and MOVE (i.e., a mobility model generator).

Zhang et al. [106] presented a trust management scheme to prevent the election of malicious platoon heads and to preserve the privacy of participating vehicles utilizing paillier cryptosystem. A proof of handshake among a platoon head and the vehicle is generated by every vehicle joining a platoon. At the end of the journey, both the platoon head and the vehicle create and send driving reports to the RSU which, after verifying the vehicle's authenticity, computes the reputation of the platoon head based on the vehicle's trust score and opinion before delivering it to the service provider. Subsequently, the service provider assesses the performance of the vehicle prior to forwarding it to the trusted authority that forecasts the future behavior of the vehicle relying on the past experiences. The performance evaluation of the platoon selection is carried out utilizing a Java-based simulation, whereas the network performance is assessed by employing NS-2 and SUMO.

5. Open Directions

A thorough glimpse of the existing literature demonstrates a considerable amount of research in vehicular trust management models. Nevertheless, they do not account for the challenges pertinent to:

5.1. Cold Start

Owing to the high mobility, cold start or bootstrapping is a crucial problem in vehicular trust management models. No information is available regarding the previous interactions for newly joining vehicles which makes it impossible to compute the trust score relying on the historical interactions for a newcomer. Consequently, a static initial trust value is assigned to all incoming vehicles. If the said initial value is kept too low, there is a high chance that an honest vehicle will get eliminated from the network owing to a low trust score. On the contrary, if it is set too high, it will take too long to eradicate dishonest nodes (based on trust scores), consequently, jeopardizing the network security. The bootstrapping issue has been addressed in social networks and recommender systems, nevertheless, it is still a major challenge in vehicular trust management models [107,108].

5.2. Data Scarcity

Due to the highly dynamic topology of vehicular networks, scarcity of information availability can lead to ineffective trust management and failure to identify misbehaving entities. Analogous to the cold start problem, data scarcity is caused by minimal or no prior interactions by a vehicle in the network. In the case of a newcomer vehicle, there are no historical interactions, whereas in a low traffic density scenario, there is a limited number of interactions available. Accurate trust computations and vehicle eviction relying on these computations require sufficient information regarding a vehicle's past experiences with its peers. Amalgamating both direct and indirect observations regarding a target vehicle occasionally helps with data scarcity; however, trust management models relying primarily on entity-based trust do not perform well in sparse environments [109].

5.3. Steady Threshold

While designing trust management models, a steady predefined threshold is often employed to detect malicious vehicles, i.e., the vehicles having a greater trust score than the said threshold are classified as trustworthy, whereas the vehicles with trust values falling below the same threshold are categorized as malicious. As mentioned earlier in Section 3.4.10, intelligent attackers (i.e., on-off attackers) do not depict malicious behavior persistently, i.e., they switch their behaviors from honest to dishonest and back frequently in order to avoid detection. Therefore, a steady threshold does not help in the elimination of these intelligent attackers. To mitigate on-off attacks, adaptive threshold is employed which also helps in early detection of dishonest vehicles; however, trust management models with such a threshold are quite computer intensive [31].

5.4. Threshold Quantification

With the intention to identify misbehaving entities in a vehicular network, an acceptable trust threshold is often employed, i.e., vehicles with a lower trust value as compared to the said threshold are tagged as untrustworthy, whereas the ones with a higher trust score are grouped as trustworthy. It is, therefore, of paramount importance that the value of such threshold is precisely defined so as to detect and evict malicious vehicles accurately from the network. If the said threshold is kept too high, the probability of honest vehicles getting eliminated increases. If the threshold is set too low, the malicious vehicles will stay in the network for too long, consequently, causing harm to the network. The existing literature assigns a steady value as a threshold without taking the dynamic nature of the vehicular network into consideration [52].

5.5. Weights Quantification

The trust computation process requires the contributing trust parameters (e.g., direct and indirect trust) to be aggregated to acquire a final trust score for a trustee. In some cases, the contributing parameters are averaged out to obtain the final trust score which implies that each contributing factor has the exact same impact on the final trust score. Alternatively, the notion of weights is commonly applied, wherein different contributing parameters are assigned different weightage relying on their respective contribution/importance in the final trust value computation. Determining precise values for these weights in proportion to the relevance and significance of the said parameters is of great importance. The existing research literature addresses the quantification of the aforementioned weights to some extent, nevertheless, this problem demands considerable attention [92].

6. Conclusions

To satisfy the ever-growing transportation demands in megacities, efficient and effective utilization of the existing transportation infrastructure is of paramount importance, especially in ITS in the context of smart cities. Smart connected vehicles form IoV network that facilitates both non-safety, e.g., infotainment, and safety-critical, e.g., warning and alert generating applications, by exploiting V2X communications. To ascertain the

reliability and trustworthiness of such communications, the notion of trust is introduced and, subsequently, trust management schemes are employed in vehicular networks. This paper presents a comprehensive review of the state-of-the-art trust management models in the IoV employing diverse computational domains. The paper emphasizes on comparing the said trust management schemes in respect of the evaluation tools utilized, quantification of weights applied while trust aggregation, misbehavior detection, attack resistance, and quantification of the threshold defined for misbehavior detection. Furthermore, a brief glimpse of the IoV layered architecture, the notion of trust and its constituents, and the attacks associated with vehicular networks is also provided. Finally, open research directions in the area are discussed as well. In a nutshell, this survey can provide useful guidance for future research in trust management in the IoV.

Author Contributions: Conceptualization, S.A.S., A.M., Q.Z.S., H.S. and W.N.; investigation, S.A.S. and A.M.; methodology, S.A.S. and A.M.; validation, S.A.S. and A.M.; writing—original draft preparation, S.A.S. and A.M.; writing—review and editing, A.M., Q.Z.S., W.N. and H.S.; supervision, Q.Z.S., W.N. and H.S. All authors have read and agreed to the published version of the manuscript.

Funding: Sarah Ali Siddiqui's work is supported via the International Macquarie University Research Excellence Scholarship (Allocation No. 2018360) and CSIRO's Data61 PhD Top-Up Scholarship (Position No. 50075957). Adnan Mahmood's work is supported by the Government of the Commonwealth of Australia via its International Research Training Program (Allocation No. 2017560) and Macquarie University, Australia's Postdoctoral Research Fellowship.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. How Many Cars Are There in the World? Available online: https://www.carsguide.com.au/car-advice/how-many-cars-are-there-in-the-world-70629 (accessed on 12 July 2021).
2. Road Traffic Injuries. Available online: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries (accessed on 12 July 2021).
3. Miucic, R. Introduction. In *Connected Vehicles: Intelligent Transportation Systems*; Miucic, R., Ed.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1–10.
4. Oncken, J.; Chen, B. Real-time model predictive powertrain control for a connected plug-in hybrid electric vehicle. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8420–8432. [CrossRef]
5. Zhang, W.E.; Sheng, Q.Z.; Mahmood, A.; Zaib, M.; Hamad, S.A.; Aljubairy, A.; Alhazmi, A.A.F.; Sagar, S.; Ma, C. The 10 research topics in the Internet of Things. In Proceeding of the 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1–3 December 2020; pp. 34–43.
6. Internet of Things Statistics for 2021—Taking Things Apart. Available online: https://dataprot.net/statistics/iot-statistics/ (accessed on 12 July 2021).
7. IDC Forecasts Connected IoT Devices to Generate 79.4ZB of Data in 2025. Available online: https://futureiot.tech/idc-forecasts-connected-iot-devices-to-generate-79-4zb-of-data-in-2025/ (accessed on 12 July 2021).
8. Autonomous Cars Generate More than 300 TB of Data per Year. Available online: https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/ (accessed on 12 July 2021).
9. Arthurs, P.; Gillam, L.; Krause, P.; Wang, N.; Halder, K.; Mouzakitis, A. A Taxonomy and Survey of Edge Cloud Computing for Intelligent Transportation Systems and Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**. [CrossRef]
10. Ruiz, P.; Bouvry, P. Survey on broadcast algorithms for mobile ad hoc networks. *ACM Comput. Surv. CSUR* **2015**, *48*, 1–35. [CrossRef]
11. Cho, J.H.; Swami, A.; Chen, R. A survey on trust management for mobile ad hoc networks. *IEEE Commun. Surv. Tutor.* **2010**, *13*, 562–583. [CrossRef]
12. Aftab, F.; Zhang, Z.; Ahmad, A. Self-Organization Based Clustering in MANETs Using Zone Based Group Mobility. *IEEE Access* **2017**, *5*, 27464–27476. [CrossRef]
13. Datta, R.; Marchang, N. Security for Mobile Ad Hoc Networks. In *Handbook on Securing Cyber-Physical Critical Infrastructure*; Das, S.K., Kant K., Zhang, N., Eds.; Elsevier: Amsterdam, The Netherlands, 2012; pp. 147–190.
14. Alfadhli, S.A.; Lu, S.; Fatani, A.; Al-Fedhly, H.; Ince, M. SD2PA: A fully safe driving and privacy-preserving authentication scheme for VANETs. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 38. [CrossRef]
15. Cooper, C.; Franklin, D.; Ros, M.; Safaei, F.; Abolhasan, M. A comparative survey of VANET clustering techniques. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 657–681. [CrossRef]
16. Mahmood, A.; Zhang, W.E.; Sheng, Q.Z. Software-defined heterogeneous vehicular networking: The architectural design and open challenges. *Future Internet* **2019**, *11*, 70–87. [CrossRef]

17. Nanda, A.; Puthal, D.; Rodrigues, J.J.P.C.; Kozlov, S.A. Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions. *IEEE Wirel. Commun.* **2019**, *26*, 60–65. [CrossRef]
18. Siddiqui, S.A.; Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. A Time-aware Trust Management Heuristic for the Internet of Vehicles. In Proceedings of the 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 18–20 August 2021.
19. Yu, Z.; Jin, D.; Song, X.; Zhai, C.; Wang, D. Internet of vehicle empowered mobile media scenarios: In-vehicle infotainment solutions for the mobility as a service (MaaS). *Sustainability* **2020**, *12*, 7448–7469. [CrossRef]
20. Yu, Z.; Jin, D.; Zhai, C.; Ni, W.; Wang, D. Internet of Vehicles Empowered Mobile Media: Research on Mobile-Generated Content (MoGC) for Intelligent Connected Vehicles. *Sustainability* **2021**, *13*, 3538–3549. [CrossRef]
21. Gyawali, S.; Xu, S.; Qian, Y.; Hu, R.Q. Challenges and solutions for cellular based v2x communications. *IEEE Commun. Surv. Tutor.* **2020**, *23*, 222–255. [CrossRef]
22. Biron, Z.A.; Dey, S.; Pisu, P. Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3893–3902. [CrossRef]
23. Eziama, E.; Tepe, K.; Balador, A.; Nwizege, K.S. Jaimes, L.M.S. Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning. In Proceedings of the Global Communications Conference Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
AATMS: An Anti-Attack Trust Management Scheme in VANET. *IEEE Access* **2020**, *8*, 21077–21090.
24. Ahmad, F.; Adnane, A.; Franqueira, V.N.L.; Kurugollu, F.; Liu, L. Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. *Sensors* **2020**, *18*, 4040. [CrossRef]
25. Hamdan, S.; Hudaib, A.; Awajan, A. Detecting Sybil attacks in vehicular ad hoc networks. *Int. J. Parallel Emergent Distrib. Syst.* **2019**, *36*, 69–79. [CrossRef]
26. Wang, J.; Zhang, Y.; Wang, Y.; Gu, X. RPRep: A Robust and Privacy-Preserving Reputation Management Scheme for Pseudonym-Enabled VANETs. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 6138251. [CrossRef]
27. Gautham, P.S.; Shanmughasundaram, R. Detection and isolation of Black Hole in VANET. In Proceedings of the International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kerala, India, 6–7 July 2017; pp. 1534–1539.
28. Kerrache, C.A.; Calafate, C.T.; Cano, J.C.; Lagraa, N.; Manzoni, P. Trust management for vehicular networks: An adversary-oriented overview. *IEEE Access* **2016**, *4*, 9293–9307. [CrossRef]
29. Lu, Z.; Qu, G.; Liu, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 760–776. [CrossRef]
30. Hussain, R.; Lee, J.; Zeadally, S. Trust in VANET: A survey of current solutions and future research opportunities. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 2553–2571. [CrossRef]
31. Mahmood, A.; Zhang, W.E.; Sheng, Q.Z.; Siddiqui, S.A.; Aljubairy, A. Trust Management for Software-Defined Heterogeneous Vehicular Ad Hoc Networks. In *Security, Privacy and Trust in the IoT Environment*; Mahmood, Z., Ed.; Springer: Cham, Switzerland, 2019; pp. 203–226.
32. Alshouiliy, K.; Agrawal, D.P. Confluence of 4G LTE, 5G, Fog, and Cloud Computing and Understanding Security Issues. In *Fog/Edge Computing For Security, Privacy, and Applications*; Chang, W., Wu, J., Eds.; Springer: Cham, Switzerland, 2021, Volume 83, pp. 3–32.
33. Burgoon, J.K.; Dunbar N.E.; Jensen M.L. An Integrated Spiral Model of Trust. In *Detecting Trust and Deception in Group Interaction*; Subrahmanian, V.S., Burgoon, J.K., Dunbar, N.E., Eds.; Springer: Cham, Switzerland, 2021; pp. 11–33.
34. Ghafari, S. M.; Beheshti, A.; Joshi, A.; Paris, C.; Mahmood, A.; Yakhchi, S.; Orgun, M.A. A Survey on Trust Prediction in Online Social Networks. *IEEE Access* **2020**, *8*, 144292–144309. [CrossRef]
35. Ben-Ner, A.; Halldorsson, F. Trusting and trustworthiness: What are they, how to measure them, and what affects them. *J. Econ. Psychol.* **2010**, *31*, 64–79. [CrossRef]
36. Jøsang, A.; Ismail, R.; Boyd, C. A survey of trust and reputation systems for online service provision. *Decis. Support Syst.* **2007**, *43*, 618–644. [CrossRef]
37. Witmer H, Hakansson P. Social media and trust: A systematic literature review. *J. Bus. Econ.* **2015**, *6*, 517–524.
38. Ba, S.; Pavlou, P.A. Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Q.* **2002**, *26*, 243–268. [CrossRef]
39. Truong, N.B.; Um, T.; Zhou, B. ; Lee, G.M. From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Singapore, 4–8 December 2017; pp. 1–7.
40. Soleymani, S.A.; Abdullah, A.H.; Hassan, W.H. Trust management in vehicular ad hoc network: A systematic review. *EURASIP J. Wirel. Commun. Netw.* **2015**, *21*, 146. [CrossRef]
41. Cui, Q.; Zhu, Z.; Ni, W.; Tao, X.; Zhang, P. Edge-Intelligence-Empowered, Unified Authentication and Trust Evaluation for Heterogeneous Beyond 5G Systems. *IEEE Wirel. Commun.* **2021**, *28*, 78–85. [CrossRef]
42. Yong-hao, W. A Trust Management Model for Internet of Vehicles. In Proceedings of the 4th International Conference on Cryptography, Security and Privacy (ICCSP), Nanjing, China, 10–12 January 2020; pp. 136–140.
43. Jayasinghe, U.; Otebolaku, A.; Um, T.; Lee, G.M. Data centric trust evaluation and prediction framework for IOT. In Proceedings of the ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), Nanjing, China, 27–29 November 2017; pp. 1–7.

44. Yang, N. A similarity based trust and reputation management framework for vanets. *Int. J. Future Gener. Commun. Netw.* **2013**, *6*, 25–34.
45. Sousa, R.S.D.; Boukerche, A.; Loureiro, A.A. Vehicle Trajectory Similarity: Models, Methods, and Applications. *ACM Comput. Surv. CSUR* **2020**, *53*, 1–32. [CrossRef]
46. Mahmood, A.; Siddiqui, S.A.; Zhang, W.E.; Sheng, Q.Z. A Hybrid Trust Management Model for Secure and Resource Efficient Vehicular Ad hoc Networks. In Proceedings of the 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Gold Coast, Australia, 5–7 December 2019; pp. 154–159.
47. Xia, H.;Xiao, F.; Zhang, S.; Hu, C.; Cheng X. Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Paris, France, 29 April–2 May 2019; pp. 838–846.
48. Huang, X.; Yu, R.; Kang, J.; Zhang, Y. Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks. *IEEE Access* **2017**, *5*, 25408–25420. [CrossRef]
49. Wang, D.; Chen, X.; Wu, H.; Yu, R.; Zhao, Y. A Blockchain-Based Vehicle-Trust Management Framework Under a Crowd-sourcing Environment. In Proceedings of the 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021; pp. 1950–1955.
50. Yu, Y.; Jia, Z.; Tao, W.; Xue, B. ; Lee, C. An Efficient Trust Evaluation Scheme for Node Behavior Detection in the Internet of Things. *Wirel. Pers. Commun.* **2017**, *93*, 571–587. [CrossRef]
51. Lim, J.; Keum, D.; Ko, Y.B. A Stepwise and Hybrid Trust Evaluation Scheme for Tactical Wireless Sensor Networks. *Sensors* **2020**, *20*, 1108. [CrossRef]
52. Jayasinghe, U.; Lee, G.M.; Um, T.; Shi, Q. Machine Learning Based Trust Computational Model for IoT Services. *IEEE Trans. Sustain. Comput.* **2019**, *4*, 39–52. [CrossRef]
53. Rehman, G.U.; Ghani, A.; Zubair, M.; Naqvi, S.H.A.; Singh, D.; Muhammad, S. IPS: Incentive and Punishment Scheme for Omitting Selfishness in the Internet of Vehicles (IoV). *IEEE Access* **2019**, *7*, 109026–109037. [CrossRef]
54. Haddadou, N.; Rachedi, A.; Ghamri-Doudane, Y. A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2015**, *64*, 3657–3674. [CrossRef]
55. Zhang, J. A Survey on Trust Management for VANETs. In Proceedings of the International Conference on Advanced Information Networking and Applications, Biopolis, Singapore, 22–25 March 2011; pp. 105–112.
56. Raya, M.; Papadimitratos, P.; Gligor, V.D.; Hubaux, J.P. On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In Proceedings of the 27th Conference on Computer Communications (INFOCOM), Phoenix, AZ, USA, 13–18 April 2008; pp. 1238–1246.
57. Gurung, S.; Lin, D.; Squicciarini, A.; Bertino, E. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In Proceedings of the International Conference on Network and System Security, Madrid, Spain, 3–4 June 2013; pp. 94–108.
58. Sugumar, R.; Rengarajan, A.; Jayakumar, C. Trust based authentication technique for cluster based vehicular ad hoc networks (VANET). *Wirel. Netw.* **2018**, *24*, 373–382. [CrossRef]
59. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. A security solution for V2V communication within VANETs. In Proceedings of the Wireless Days (WD), Dubai, United Arab Emirates, 3–5 April 2018; pp. 181–183.
60. Dahmane, S.; Kerrache, C.A.; Lagraa, N.; Lorenz, P. WeiSTARS: A weighted trust-aware relay selection scheme for VANET. In Proceedings of the International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
61. Ahmad, F.; Kurugollu, F.; Kerrache, C.A.; Sezer, S.; Liu, L. NOTRINO: A NOvel hybrid TRust management scheme for INternet-Of-vehicles. *IEEE Trans. Veh. Technol.* **2021**, 1. doi: 10.1109/TVT.2021.3049189. [CrossRef]
62. Oubabas, S.; Aoudjit, R.; Rodrigues, J.J.; Talbi, S. Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme. *Veh. Commun.* **2018**, *13*, 128–138. [CrossRef]
63. Gür, G.; Bahtiyar, Ş.; Alagöz, F. Security analysis of computer networks: Key concepts and methodologies. In *Modeling and Simulation of Computer Networks and Systems*; Obaidat, M.S., Nicopolitidis, P., Zarai, F., Eds.; Elsevier: Amsterdam, The Netherlands, 2015; pp. 861–898.
64. Kim, S. Blockchain for a trust network among intelligent vehicles. In *Advances in Computers*; Raj, P., Deka, G.C., Eds.; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 43–68.
65. Tangade, S.S.; Manvi, S.A. A survey on attacks, security and trust management solutions in VANETs. In Proceedings of the 4th International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 4–6 July 2013; pp. 1–6.
66. Patel, P.; Jhaveri, R. A Honeypot Scheme to Detect Selfish Vehicles in Vehicular Ad-hoc Network. In *Computing and Network Sustainability, Proceedings of the International Research Symposium on Computing and Network Sustainability (IRSCNS), Goa, India, 1–2 July 2016*; Vishwakarma, H.R., Akashe, S., Eds.; Springer: Singapore, 2017; pp. 389–401.
67. Banković, Z.; Vallejo, J.C.; Fraga, D.; Moya, J.M. Detecting bad-mouthing attacks on reputation systems using self-organizing maps. In Proceedings of the 4th International Conference on Computational intelligence in security for information systems (CISIS), Torremolinos-Málaga, Spain, 8–10 June 2011; pp. 9–16.
68. Chen, J.M.; Li, T.T.; Panneerselvam, J. TMEC: A trust management based on evidence combination on attack-resistant and collaborative internet of vehicles. *IEEE Access* **2018**, *7*, 148913–148922. [CrossRef]

69. Ahmad, F.; Kurugollu, F.; Adnane, A.; Hussain, R.; Hussain, F. MARINE: Man-in-the-middle Attack Resistant trust model IN connEcted vehicles. *IEEE Internet Things J.* **2020**, *7*, 3310–3322. [CrossRef]
70. Suo, D.; Sarma, S.E. Real-time Trust-Building Schemes for Mitigating Malicious Behaviors in Connected and Automated Vehicles. In Proceedings of the Intelligent Transportation Systems Conference (ITSC), Auckland, New Zealand, 27–30 October 2019; pp. 1142–1149.
71. Mahmood, A.; Butler, B.; Zhang, W.E.; Sheng, Q.Z.; Siddiqui, S.A. A Hybrid Trust Management Heuristic for VANETs. In Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 748–752.
72. Ullah, N.; Kong, X.; Ning, Z.; Tolba, A.; Alrashoud, M.; Xia, F. Emergency warning messages dissemination in vehicular social networks: A trust based scheme. *Veh. Commun.* **2020**, *22*, 100199. [CrossRef]
73. Chuprov, S.; Viksnin, I.; Kim, I.; Marinenkov, E.; Usova, M.; Lazarev, E.; Melnikov, T.; Zakoldaev, D. Reputation and Trust Approach for Security and Safety Assurance in Intersection Management System. *Energies* **2019**, *12*, 4527. [CrossRef]
74. Fei, Z.; Liu, K.; Huang, B.; Zheng, Y.; Xiang, X. Dirichlet Process Mixture Model Based Nonparametric Bayesian Modeling and Variational Inference. In Proceedings of the Chinese Automation Congress (CAC), Hangzhou, China, 22–24 November 2019; pp. 3048–3051.
75. Jun, S. Bayesian Inference and Learning for Neural Networks and Deep Learning. In Proceedings of the International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 19–21 February 2020; pp. 569–571.
76. Zhang, J.; Zheng, K.; Zhang, D.; Yan, B. AATMS: An Anti-Attack Trust Management Scheme in VANET. *IEEE Access* **2020**, *8*, 21077–21090. [CrossRef]
77. He, Y.; Yu, F.; Wei, Z. Trust Management for Secure Cognitive Radio Vehicular Ad Hoc Networks. *Ad Hoc Netw.* **2019**, *86*, 154–165. [CrossRef]
78. Fang, W.; Zhang, W.; Liu, Y.; Yang, W.; Gao, Z. BTDS: Bayesian-based trust decision scheme for intelligent connected vehicles in VANETs. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3879. [CrossRef]
79. Li, J.; Xing, R.; Su, Z.; Zhang, N.; Hui, Y.; Luan, T.H.; Shan, H. Trust Based Secure Content Delivery in Vehicular Networks: A Bargaining Game Theoretical Approach. *IEEE Trans. Veh. Technol.* **2020**, *69*, 3267–3279. [CrossRef]
80. Halabi, T.; Zulkernine, M. Trust-Based Cooperative Game Model for Secure Collaboration in the Internet of Vehicles. In Proceedings of the International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
81. Jayaprasanna, M.C.; Soundharya, V.A.; Suhana, M.; Sujatha, S. A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain. In Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 253–257.
82. Mahmood, Z.; Vacius, J. Privacy-Preserving Blockchain Framework Based on Ring Signatures (RSs) and Zero-Knowledge Proofs (ZKPs). In Proceedings of the International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain, 20–21 December 2020; pp. 1–6.
83. Javaid, U.; Aman, M.N.; Sikdar, B. DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts. In Proceedings of the 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
84. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors* **2019**, *19*, 4954. [CrossRef]
85. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. BARS—A Blockchain-based Anonymous Reputation System for Trust Management in VANETs. In Proceedings of the 17th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications/12th International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 98–103.
86. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C.M. Blockchain-based Decentralized Trust Management in Vehicular Networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]
87. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, K.I.; Zhao, J. Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
88. Ray, S. A Quick Review of Machine Learning Algorithms. In Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 14–16 February 2019; pp. 35–39.
89. What Is Deep Learning? Available online: https://machinelearningmastery.com/what-is-deep-learning/ (accessed on 2 July 2021).
90. Tangade, S.; Manvi, S.S.; Hassan, S. A Deep Learning Based Driver Classification and Trust Computation in VANETs. In Proceedings of the 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22-25 September 2019; pp. 1–6.
91. Zhang, D.; Yu, F.R.; Yang, R. A Machine Learning Approach for Software-Defined Vehicular Ad Hoc Networks with Trust Management. In Proceedings of the Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
92. Siddiqui, S.A.; Mahmood, A.; Zhang, W.E.; Sheng, Q.Z. Machine Learning Based Trust Model for Misbehavior Detection in Internet-of-Vehicles. In *Communications in Computer and Information Science, Proceedings of the 26th International Conference on Neural Information Processing (ICONIP), Sydney, Australia, 12–15 December 2019*; Gedeon T., Wong K., Lee M., Eds.; Springer: Cham, Switzerland, 2019; pp. 512–520.

93. Gyawali, S.; Qian, Y.; Hu, R.Q. Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8871–8885. [CrossRef]
94. Zhang, D.; Yu, F.R.; Yang, R.; Tang, H. 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 (DIVANet'18), New York, NY, USA, 28 October–2 November, 2018; pp. 1–7.
95. Zadeh, L.A. Fuzzy logic. *Computer* **1988**, *21*, 83–93. [CrossRef]
96. Guleng, S.; Wu, C.; Chen, X.; Wang, X.; Yoshinaga, T.; Ji, Y. Decentralized Trust Evaluation in Vehicular IoT. *IEEE Access* **2019**, *7*, 15980–15988. [CrossRef]
97. Souissi, I.; Azzouna, N.B.; Berradia, T.; Said, L.B. A New Fuzzy Logic Based Model for Location Trust Estimation in Electric Vehicular Networks. In Proceedings of the 33rd International Conference on Advanced Information Networking and Applications (AINA), Matsue, Japan, 27–29 March 2019; pp. 341–352.
98. Kumar, A.; Dadheech, P.; Beniwal, M.K.; Agarwal, B.; Patidar, P.K. A Fuzzy Logic-Based Control System for Detection and Mitigation of Blackhole Attack in Vehicular Ad Hoc Network. In Proceedings of the 2nd International Conference on Emerging Technologies in Computer Engineering (ICETCE), Rajasthan, India, 1–2 February 2019; pp. 163–178.
99. Tan, S.; Li, X.; Dong, Q. A Trust Management System for Securing Data Plane of Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7579–7592. [CrossRef]
100. Mármol, F.G.; Pérez, G.M. TRIP, A Trust & Reputation Infrastructure-based Proposal for Vehicular Ad hoc Networks. *J. Netw. Comput. Appl.* **2012**, *35*, 934–941.
101. Qadir, A.M.; Varol, N. A Review Paper on Cryptography. In Proceedings of the 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 10–12 June 2019; pp. 1–6.
102. Mühlbauer, R.; Kleinschmidt, J. Bring your own reputation: A feasible trust system for vehicular ad hoc networks. *J. Sens. Actuator Netw.* **2018**, *7*, 37. [CrossRef]
103. Gai, F.; Zhang, J.; Zhu, P.; Jiang, X. Ratee-Based Trust Management System for Internet of Vehicles. In Proceedings of the 12th International Conference on Wireless Algorithms, Systems, and Applications (WASA), Guilin, China, 19–21 June 2017; pp. 344–355.
104. Wang, C.; Shen, J.; Lai, J.F.; Liu, J. A Trustworthiness-Based Time-Efficient V2I Authentication Scheme for VANETs. In Proceedings of the International Conference on Blockchain and Trustworthy Systems (BlockSys), Guangzhou, China, 7–8 December 2019; pp. 794–799.
105. Tangade, S.; Manvi, S.S.; Lorenz, P. Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5232–5243. [CrossRef]
106. Zhang, C.; Zhu, L.; Xu, C.; Sharif, K.; Ding, K.; Liu, X.; Du, X.; Guizani, M. TPPR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in VANET. *IEEE Trans. Serv. Comput.* **2019**, 1. doi: 10.1109/TSC.2019.2961992. [CrossRef]
107. Alishev, D.; Hussain, R.; Nawaz, W.; Lee, J. Social-Aware Bootstrapping and Trust Establishing Mechanism for Vehicular Social Networks. In Proceedings of the 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, Australia, 4–7 June 2017; pp. 1–5.
108. Son, L.H. Dealing with the new user cold-start problem in recommender systems: A comparative review. *Inf. Syst.* **2016**, *58*, 87–104. [CrossRef]
109. Ahmad, F.; Hall, J.; Adnane, A.; Franqueira, V.N. Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-Hoc Network. In Proceedings of the International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and Cyber, Physical and Social Computing (CPSCom) and Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 44–52.