



Article

MESMERIC: Machine Learning-Based Trust Management Mechanism for the Internet of Vehicles

Yingxun Wang ^{1,2,*}, Adnan Mahmood ³ , Mohamad Faizrizwan Mohd Sabri ¹ , Hushairi Zen ⁴ and Lee Chin Kho ¹

¹ Faculty of Engineering, Universiti Malaysia Sarawak, Kota Samarahan 94300, Sarawak, Malaysia; msmfaizrizwan@unimas.my (M.F.M.S.); lckho@unimas.my (L.C.K.)

² Faculty of Computer and Information Engineering, Qilu Institute of Technology, Jinan 250200, China

³ School of Computing, Macquarie University, Sydney, NSW 2109, Australia; adnan.mahmood@mq.edu.au

⁴ Faculty of Engineering and Technology, i-CATS University College, Kuching 93350, Sarawak, Malaysia; hushairi@icats.edu.my

* Correspondence: wyx8586@qlit.edu.cn

Abstract: The emerging yet promising paradigm of the Internet of Vehicles (IoV) has recently gained considerable attention from researchers from academia and industry. As an indispensable constituent of the futuristic smart cities, the underlying essence of the IoV is to facilitate vehicles to exchange safety-critical information with the other vehicles in their neighborhood, vulnerable pedestrians, supporting infrastructure, and the backbone network via vehicle-to-everything communication in a bid to enhance the road safety by mitigating the unwarranted road accidents via ensuring safer navigation together with guaranteeing the intelligent traffic flows. This requires that the safety-critical messages exchanged within an IoV network and the vehicles that disseminate the same are highly reliable (i.e., trustworthy); otherwise, the entire IoV network could be jeopardized. A state-of-the-art trust-based mechanism is, therefore, highly imperative for identifying and removing malicious vehicles from an IoV network. Accordingly, in this paper, a machine learning-based trust management mechanism, MESMERIC, has been proposed that takes into account the notions of direct trust (encompassing the trust attributes of interaction success rate, similarity, familiarity, and reward and punishment), indirect trust (involving confidence of a particular trustor on the neighboring nodes of a trustee, and the direct trust between the said neighboring nodes and the trustee), and context (comprising vehicle types and operating scenarios) in order to not only ascertain the trust of vehicles in an IoV network but to segregate the trustworthy vehicles from the untrustworthy ones by means of an optimal decision boundary. A comprehensive evaluation of the envisaged trust management mechanism has been carried out which demonstrates that it outperforms other state-of-the-art trust management mechanisms.

Keywords: Internet of Vehicles; machine learning; trust management mechanism; direct trust; indirect trust; context; optimal decision boundary



Citation: Wang, Y.; Mahmood, A.; Sabri, M.F.M.; Zen, H.; Kho, L.C. MESMERIC: Machine Learning-Based Trust Management Mechanism for the Internet of Vehicles. *Sensors* **2024**, *24*, 863. <https://doi.org/10.3390/s24030863>

Academic Editor: Peter Han Joo Chong

Received: 20 December 2023

Revised: 18 January 2024

Accepted: 25 January 2024

Published: 29 January 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The rapid acceleration in urbanization and growth of the population has substantially increased the ownership of vehicles. A conservative estimate by the World Health Organisation suggests that traffic accidents kill approximately 1.35 million people every year and approximately 50 million people suffer from non-fatal injuries [1]. Furthermore, the congestion of traffic is a global issue which also results in increased noise pollution and vehicular emissions [2,3]. Accordingly, numerous researchers from academia and industry over the years have focused on resolving such issues. Ensuring both passenger road safety and traffic congestion mitigation, therefore, requires an intelligent system of vehicular communication.

Vehicles today are an indispensable constituent of the Internet of Things (IoT) network and are accordingly equipped with hundreds of sensors onboard [4]. As per an estimate,

modern vehicles are equipped with approximately 100 sensors onboard with each vehicle capable of producing nearly 380 TB to 4.9 PB data annually [5]. Therefore, vehicle-mounted sensors (position, velocity, acceleration, pressure, and temperature sensors) and IoT devices would be able to construct a safe and efficient intelligent network of transportation [6].

The IoV is an application of IoT in the context of intelligent transportation systems (ITS). The IoV has a similar architecture to the IoT and features a hierarchical structure that includes data source, edge, fog, and the cloud layers [7]. Vehicles share information with other vehicles, pedestrians, intelligent infrastructure, and backbone networks to establish vehicle-to-vehicle, vehicle-to-pedestrian, vehicle-to-infrastructure, and vehicle-to-network communication, thereby formulating vehicle-to-everything (V2X) communication. Figure 1 thus depicts the architecture of an IoV network. The main IoV communication node is a vehicle with an on-board unit (OBU) which can communicate with the Roadside Units (RSUs) and other vehicles in its proximity. Due to the unique characteristics of IoV, i.e., openness, dynamic topology, and high mobility, it is susceptible to attacks; dishonest entities can modify legitimate security messages, spread forged information, or delay forwarding messages, thereby endangering human lives [8].

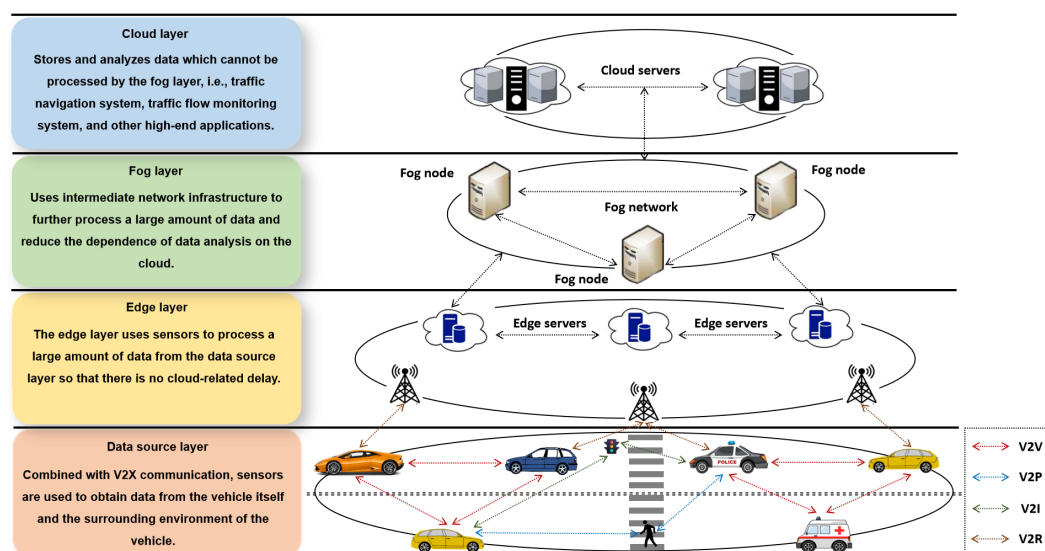


Figure 1. A system architecture of the IoV.

Accordingly, researchers have proposed several solutions for handling the issues pertinent to IoV security. Nevertheless, a number of these solutions rely on conventional cryptographic-related schemes and, therefore, rely on the notions of digital signatures, certificates, and public key infrastructure [9,10]. Moreover, conventional cryptographic-related schemes are only capable of mitigating external attacks and are ineffective against internal network attacks [11]. It is due to this reason that the paradigm of trust has been recently introduced in the research literature.

The notion of trust originated in sociology as a means to understand how people are interdependent within a social organization [12]. Trust, over the years, has also been employed in various other disciplines, including, but not limited to, philosophy, economics, engineering, and computer science. Trust is generally referred to as the confidence of a trustor in a trustee. Here, trustor refers to a node that is in a position to ascertain the trust of the other node (trustee) in the network, whereas the trustee refers to a node whose trust is being ascertained [13]. In the context of this paper, trust refers to the likelihood that a trustee can perform a particular operation (contribute to realizing a particular application or service) within a specific situation at a specific time. It is also important to mention that trust computation primarily involves a weighted aggregation of both the direct trust and the indirect trust [14]. Direct trust is ascertained as a result of direct interactions between a trustor and a trustee and is generally referred to as a trustor's direct observation of a

trustee [15,16]. On the contrary, indirect trust is computed by taking into account the direct trust ascertained by the one-hop neighbors of a trustor pertinent to a trustee. The literature argues that direct trust is more significant in contrast to indirect trust [1].

To date, a number of trust management models have been proposed in the research literature which have been broadly classified into three types: entity-oriented trust models, data-oriented trust models, and hybrid trust models [17]. Entity-oriented trust models aim to eradicate malicious entities (vehicles) from an IoV network by evaluating the reliability of the vehicles disseminating messages. Data-oriented trust models, on the other hand, eradicate the malicious messages instead of the entities from an IoV network [18]. Finally, hybrid trust models take into account the salient characteristics of both the entity-oriented and data-oriented trust models and, therefore, regard the reliability of the entities and the respective messages disseminated by them in a bid to make a decision.

The trust parameters, also referred to as the trust attributes, are integral constituents of any trust model. The existing literature suggests that a number of research studies determined the global trust value of a particular vehicle in an IoV network by taking into account the weighted sum of a number of such trust parameters and which, in fact, is also subject to limitations [19]. For instance, weights' settings are based on human subjectivity and, therefore, different researchers often set different weights for the same trust parameter which results in an inconsistent trust score. Keeping this in mind, the envisaged research employs the notion of machine learning to ascertain trustworthy and untrustworthy vehicles via an optimal trust boundary. In order to better express the running situation of vehicles and achieve the optimal trust evaluation results, the trust model needs more trust parameters, but it will lead to an increase in the amount of calculation, so we can use the learning method to train the trust model. In this way, the global trust value of each vehicle was established by combining all of its respective trust parameters such that the optimal influence of each trust parameter on the global trust value is prevalent.

Also, a number of trust models do not take into account the effect of context while ascertaining the trust of a particular vehicle. For instance, an urban scenario involves more vehicles and, therefore, the inter-vehicular interactions are much more as opposed to a highway scenario, wherein it is extremely challenging to establish trust among the vehicles. Similarly, public vehicles, including, but not limited to, police cars, ambulances, and fire brigades have higher trust values in contrast to private vehicles. Moreover, drivers with many years of driving experience generally have higher trust values than novice drivers. This research, therefore, regards two contextual factors, i.e., vehicle types and operating scenarios, in order to obtain a more optimal trust value. Therefore, not only were the direct trust and the indirect trust included in the global trust of our envisaged trust model but the context was also incorporated (see Figure 2).

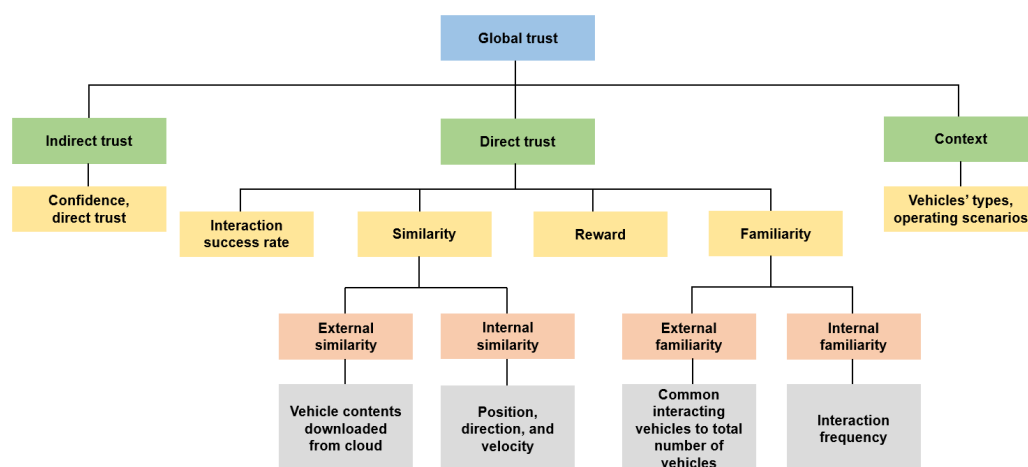


Figure 2. The composition of the global trust.

The salient contributions of the research-at-hand are as follows:

- We propose a novel trust management mechanism that takes into account direct trust (encompassing the trust attributes of interaction success rate, similarity, familiarity, and reward and punishment), indirect trust (involving recommendations via the one-hop neighboring nodes of a trustor pertinent to a trustee and the confidence of a trustor on the recommendations ascertained by the one-hop neighboring vehicles), and context (comprising vehicle types and operating scenarios) in order to ascertain the trust of vehicles in an IoV network.
- In contrast to the conventional trust management heuristics, we envisage a machine learning-based trust aggregation scheme in a bid to ascertain the optimal trust score of each vehicle in an IoV network so that they can be classified as either being trustworthy or untrustworthy.
- We carried out a comprehensive evaluation of our envisaged trust management mechanism and demonstrated that it outperforms other state-of-the-art trust management mechanisms.

The rest of the paper is systematically organized as follows. Section 2 delineates the state-of-the-art of trust management in IoV networks. Section 3 presents our envisaged trust management mechanism. Section 4 presents the experimental results and discussions pertinent to the same, and Section 5 concludes the paper.

2. Related Works

In recent years, there has been an increase in research on trust management in the IoV [2,5,11,19–24]. We can divide the existing trust management models into: learning-based and traditional methods-based trust management models.

2.1. Trust Parameters and Evaluation Parameters

A holistic overview of the existing trust management mechanisms reveals that a number of trust-based parameters have been applied in different settings in order to measure and evaluate trust. The trust-based parameters include, but are not limited to, resource availability [6], similarity [19,25,26], familiarity [6,7,22,27], timeliness [7], context [19,20,28,29], cooperativeness [19,30], community-of-interest (CoI) [19,30], confidence [31,32], reward [28,33], attitude, subjective norms, and perceptual behavioral control [5], freshness of data [34], and packet delivery ratio [7,25,31,35,36]. Also, the selection of a trust-based threshold for determining trustworthy and untrustworthy behavior is crucial. If the threshold is set too high by the system designers, the trustworthy nodes may be even removed from a network. Alternatively, if the threshold is set too low, the untrustworthy nodes would slowly jeopardize the entire network. A comparative summary of the trust parameters employed in the representative literature is depicted in Table 1.

It is interesting to note that context is the most frequently used trust parameter followed by cooperativeness, similarity and reward. Context is an extremely important trust parameter and a number of other trust parameters depend on the same, and are, therefore, dissimilar in different contexts. For instance, the number of interactions between vehicles is different in urban and highway scenarios. Also, different types of vehicles, i.e., high-priority vehicles, public transport vehicles, professional vehicles, and novice vehicles, have different trust values. Accordingly, this paper proposes a context-based trust management model. Table 1 further depicts that there are not many trust parameters employed in the state-of-the-art trust management models. If there are few trust parameters, the accuracy of the global trust value calculated will also decrease. To mitigate this problem, we propose a trust management model that includes six trust parameters, i.e., interaction success rate, similarity, familiarity, reward and punishment, confidence, and context.

There are two important steps in trust management, i.e., building a trust model and evaluating a trust model [31]. The purpose of trust evaluation is to evaluate the accuracy, reliability, and practicality of an envisaged trust model. The literature suggests that typical evaluation parameters employed for the trust-based models include precision, recall, and

F1-score [19,20,29,37], false positive rate, true positive rate, true negative rate [27], and computation overhead [38].

Table 1. Trust parameters in trust management model.

References	Similarity	Familiarity	Timeliness	Context	Cooperativeness	CoI	Confidence	Reward
[2]	-	-	-	✓	-	-	-	-
[7]	-	✓	-	✓	✓	-	✓	-
[19]	✓	-	-	-	✓	✓	-	-
[20]	-	-	-	-	✓	✓	-	✓
[23]	-	-	-	✓	-	-	-	-
[24]	-	-	✓	✓	-	-	-	-
[25]	✓	✓	-	✓	-	-	-	-
[26]	✓	-	-	-	-	-	-	-
[27]	✓	✓	-	✓	-	-	-	-
[33]	-	-	-	-	-	-	-	✓
[28]	-	-	-	-	-	-	-	✓
[29]	-	-	-	✓	✓	-	-	-
[31]	-	-	✓	✓	-	-	-	-
[32]	-	-	-	✓	✓	-	✓	-
[34]	-	✓	-	-	✓	-	-	-
[39]	-	-	-	✓	-	-	-	✓
[40]	✓	-	-	-	-	-	-	-
[41]	-	-	-	-	-	-	✓	-
[42]	-	-	-	-	-	-	-	✓
Our scheme	✓	✓	-	✓	✓	✓	✓	✓

2.2. Conventional Trust Management Models

A trust evaluation algorithm has been proposed in [5] that exploited the attributes (attitude towards behavior, subjective norms, and perceived behavioral control) from the theory of planned behavior, i.e., a human psychological theory, to ascertain the trustworthiness of vehicles in a vehicular network within a given context and to decide whether to accept or not the traffic-related warning messages from a particular vehicle. Moreover, the notion of fuzzy logic has been employed in a bid to segregate the vehicles' trust levels as CompleteTrust, MediumTrust, and DisTrust. The effectiveness of the trust evaluation algorithm was verified via false positive rates, true positive rates, and F1-score vis-à-vis different proportions of malicious vehicles.

A context-aware and attack-resistant trust model for the IoV networks has been suggested in [16]. This model takes into account (a) local trust encompassing the weighted sum of both direct trust (packet delivery ratio and time decay) and indirect trust (confidence factor) and (b) context-dependent trust (propagation delay, cooperativeness, and familiarity). Also, the notion of an adaptive misbehavior detection threshold has been proposed to segregate malicious vehicles from dishonest vehicles. Moreover, the resilience against on-off attacks and the selective node attacks has been demonstrated by employing optimal and rational influencing parameters as weights during the process of the weights' assignment.

A forest fire model has been proposed in [23] to select the minimum number of competent nodes suitable for broadcasting emergency messages in an IoV network. At first, a social community is established by calculating the similarity of the social characteristics between the nodes. Subsequently, some key factors, including, but not limited to, the number of connections, velocity of nodes, general activity of the nodes, and data forwarding capability of neighboring nodes, are used to select the core node and the complementary node for the dissemination of emergency messages within the established social community. This establishes a trust estimation and management mechanism for nodes based on their behavior in an IoV network. Experimental results suggest that this particular model demonstrated high accuracy under a high density of malicious nodes.

A novel hybrid trust management scheme for an IoV network has been proposed in [43] to evaluate both node-centric and data-centric trust. Node-centric trust has been determined by employing the distance between the message sender and the message evaluator in tandem with the antenna height of the message sender and the message evaluator, whereas data-centric trust has been ascertained by means of information quality and effective distance (via a tier-based approach) between the message sender and the message evaluator. A trust threshold has been further employed which facilitates rewarding (incrementing) and penalizing (decrementing) the trust score of the message sender. The performance of the trust management scheme has been evaluated under man-in-the-middle attacks and zigzag attacks.

2.3. Machine Learning-Based Trust Management Models

A trust computational heuristic model has been envisaged in [19] to establish trustworthy relationships among the physical objects, i.e., devices, and for mitigating potential risks throughout the decision-making process in an SIoT environment. The direct trust of a particular object (trustee) is ascertained by taking into consideration the trust attributes of friendship similarity, community of interest, cooperativeness, and reward/punishment. The indirect trust, on the other hand, is computed by requesting the direct trust from the nodes that have interacted with the trustee. The authors exploited the notion of machine learning to (a) aggregate the trust attributes in order to determine an optimal trust score and (b) determine the best possible boundary to segregate between the trustworthy, untrustworthy, and neutral interactions. The neutral interactions are later classified as trustworthy or untrustworthy via a percentage threshold mechanism so these interactions can be employed for real-world applications.

A quantifiable trust assessment model based on machine learning has been proposed in [20] to make decisions autonomously, i.e., without human intervention, in an IoT network. This model encompasses trust features, i.e., co-location relationship, co-work relationship, cooperativeness-frequency-duration, reward system, mutuality and centrality, and community of interest, in order to assess the knowledge of a trustor towards a trustee. These trust parameters are aggregated via machine learning to obtain a single trust value for each pair of nodes (trustor and trustee) and which are then further segregated into trustworthy and untrustworthy interactions via a decision boundary.

A trustworthy object classification framework, Trust-SIoT, has been further proposed in [29] to establish and maintain a trustworthy relationship between the IoT objects over time. The authors employed social characteristics of objects in the form of direct trust metrics, reliability and benevolence, credible recommendations, and the degree of relationships. A SIoT knowledge graph was further constructed in order to record five dynamic social relationships, including, but not limited to, co-location object relationships, parental object relationships, ownership object relationships, social object relationships (SOR), and a variant of SOR (to connect public and private mobile devices) to ascertain the degree of relationships. An artificial neural network-based model was further employed for decision-making purposes, i.e., to identify the trustworthiness level of a trustee. The performance of this framework is evaluated in terms of F1-score, MAE, and MSE.

Similarly, a machine learning-based trust model (encompassing trust parameters of similarity, familiarity, and packet delivery ratio) has been put forward in [25] to identify and eliminate malicious vehicles within an IoV network. A context-aware trust management framework for a VANET network has been suggested in [39] to ascertain the trustworthiness of messages received by vehicles to guarantee that no false information influences any driving decision-making process. This framework was composed of three modules, namely, information formalization, trust evaluation and strategy adjustment. The authors proposed a trust evaluation method based on evaluation strategy in different scenarios. In addition, information entropy theory was introduced into the trust calculation function to ensure more accurate evaluation results. Finally, a reinforcement learning model was proposed,

and the evaluation strategy was dynamically adjusted according to the feedback of previous evaluation results.

To sum up, over the years, a number of both conventional and machine learning-based trust management algorithms have been proposed in the research literature, and which have laid the foundations for the research envisaged in this paper. Whilst these research papers have made some outstanding contributions, they still lack the potential of being a generic algorithm that can be suitably adapted to a particular research domain. In addition, they only take into consideration the traditional and limited trust parameters and a number of them even do not consider the influence of context on the trust values. Therefore, this research paper envisages a machine learning-based trust management mechanism that considers key influential trust parameters and the context for ascertaining the trust of vehicles in an IoV network.

3. Proposed Trust Evaluation Model

We hereby design a novel trust management framework, as depicted in Figure 3, in a bid to ascertain the trustworthiness of vehicles in an IoV network. The envisaged trust model primarily encompasses the following three salient steps:

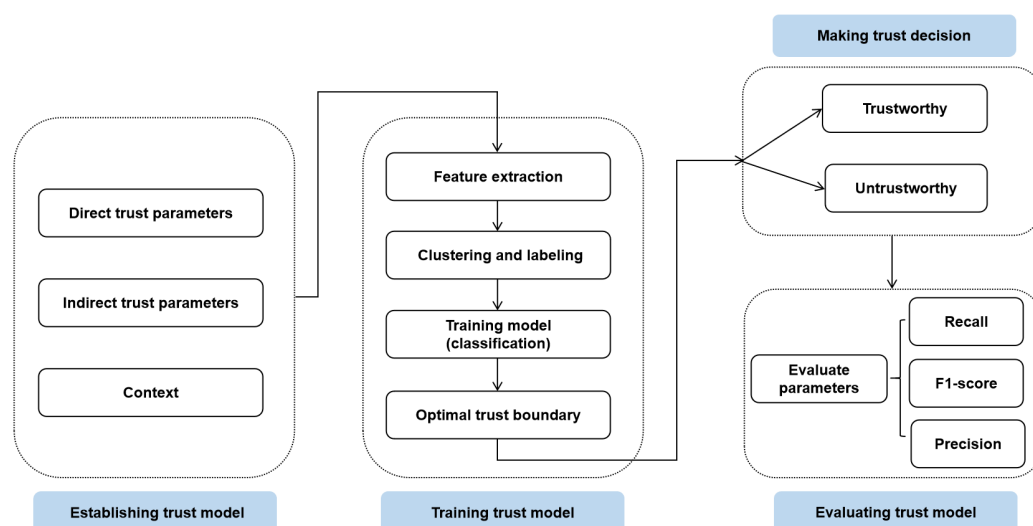


Figure 3. The framework of the proposed trust management model.

- *Step 1—Establishing the Trust Model*

The trust of any particular vehicle (trustee) is ascertained via a trust model which takes into account direct trust, indirect trust, and context. The direct trust is a trustor's direct observation pertinent to a trustee and is composed up of four parameters, i.e., interaction success rate, similarity, familiarity, and reward and punishment. On the contrary, the indirect trust is computed via the respective trustor's one-hop neighbors' recommendations pertinent to a trustee and the degree of confidence of the respective trustor on the recommendations of its corresponding one-hop neighbors. It is also pertinent to mention that the model further takes into consideration the impact of context (vehicle types and operating scenarios) of both trustor and trustee.

- *Step 2—Training the Trust Model*

Once the trust values have been computed via the trust model, we first employ unsupervised learning algorithms such as k-means, fuzzy c-means, and agglomerative (hierarchical) clustering, in order to ascertain two clusters, i.e., trustworthy and untrustworthy. Simply put, an unsupervised learning algorithm has been employed here to label the feature matrices ascertained in Step 1. Subsequently, we use supervised learning algorithms such as the k-nearest neighbors algorithm and random forest

algorithm for training with 5-fold cross-validation so as to identify the optimal trust boundary for distinguishing between trusted and untrusted vehicles.

- *Step 3—Evaluating the Trust Model*

The evaluation parameters, i.e., precision, recall, and F1-score are used for evaluating the performance of the envisaged IoV-based trust model.

We, therefore, define a set of vehicles V_m , $m = \{1, 2, \dots, M\}$, comprising both trustworthy (honest) as well as untrustworthy (malicious) vehicles. At every time instance t' , $t' = \{1, 2, \dots, t\}$, each vehicle interacts with vehicles in its immediate area to evaluate their trust based on the underlying interaction. This interaction takes place between a pair of a trustor i and a trustee j . The definitions of trust parameters employed in this section are delineated in Table 2.

Table 2. Mathematical symbols employed in the envisaged trust model.

Symbol	Definition
i	Trustor
j	Trustee
k	The neighbor of i
t'	A time instance
t	The current time instance
Th_C	Confidence threshold (0.8)
Th_T	Trust value threshold (0.6)
ISR	Interaction success rate
Sim	Similarity
ES	External similarity
IS	Internal similarity
Fam	Familiarity
EF	External familiarity
IF	Internal familiarity
RP	Reward and punishment
VT	Vehicle types
OS	Operating scenarios
n	3266 pairs of interactions

3.1. Direct Trust ($T_{d(i,j,t)}$)

Direct trust refers to a trustor's direct observation of a trustee. However, it is pertinent to mention that the historical interactions between a trustor and a trustee should also be taken into consideration, i.e., in addition to the current interaction, for ascertaining the trust of a trustee since a malicious vehicle may behave intelligently by altering between a malicious and a non-malicious behavior. In our envisaged model, we employ four key trust parameters, i.e., *interaction success rate*, *similarity*, *familiarity*, *reward and punishment*, in order to ascertain the direct trust between a trustor i and a trustor j . The details of these parameters are as follows:

- *Interaction Success Rate (ISR)*—The $ISR_{i,j,t}$ ($0 \leq ISR_{i,j,t} \leq 1$) manifests the degree of interaction between a trustor i and a trustee j in an IoV network, and is depicted as:

$$ISR_{i,j,t} = \frac{\sum_{t'=1}^t R_{i,j,t'}}{\sum_{t'=1}^t S_{i,t'}} \quad (1)$$

where $\sum_{t'=1}^t R_{i,j,t'}$ signifies total number of messages successfully received by a trustee j from a trustor i and $\sum_{t'=1}^t S_{i,t'}$ represents the total number of messages sent by the trustor i over the said time period.

- *Similarity (Sim)*—The similarity ($0 \leq Sim_{i,j,t} \leq 1$) itself is a weighted amalgamation of external similarity (ES) and internal similarity (IS). The external similarity herein implies the degree of similar content accessed by a trustor i and a trustee j over

the time t (Equation (3)), whereas the internal similarity represents the exchange of information, i.e., position, direction, and velocity between a trustor i and a trustee j (Equation (4)).

$$Sim_{i,j,t} = w_{ES}ES_{i,j,t} + w_{IS}IS_{i,j,t} \quad (2)$$

where w_{ES} and w_{IS} refers to the weight of the $ES_{i,j,t}$ and $IS_{i,j,t}$, respectively, ($w_{ES} + w_{IS} = 1$). The $ES_{i,j,t}$ and $IS_{i,j,t}$ are ascertained as:

$$ES_{i,j,t} = \sum_{t'=1}^t w_{ES_{t'}} ES_{i,j,t'} \quad (3)$$

$$IS_{i,j,t} = \sum_{t'=1}^t w_{IS_{t'}} IS_{i,j,t'} \quad (4)$$

where $w_{ES_{t'}}$ and $w_{IS_{t'}}$ manifests the weights of $ES_{i,j,t'}$ and $IS_{i,j,t'}$, respectively, at a time t' ($w_{ES_{t'}} + w_{IS_{t'}} = 1$). The $ES_{i,j,t'}$ and $IS_{i,j,t'}$ are ascertained as:

$$ES_{i,j,t'} = \begin{cases} 1, & \text{if } C_{v_{i,t'}} = C_{v_{j,t'}} \\ 0, & \text{if } C_{v_{i,t'}} \neq C_{v_{j,t'}} \end{cases} \quad (5)$$

where $C_{v_{i,t'}}$ and $C_{v_{j,t'}}$ implies the content accessed by a trustor i and a trustee j , respectively. Similarly, the $IS_{i,j,t'}$ is computed as:

$$IS_{i,j,t'} = \frac{Pos_{i,j,t'} + Dir_{i,j,t'} + Vel_{i,j,t'}}{3} \quad (6)$$

$$Pos_{i,j,t'} = \begin{cases} 1, & \text{if } Pos_{i,t'} = Pos_{j,t'} \\ 0, & \text{if } Pos_{i,t'} \neq Pos_{j,t'} \end{cases} \quad (7)$$

$$Dir_{i,j,t'} = \begin{cases} 1, & \text{if } Dir_{i,t'} = Dir_{j,t'} \\ 0, & \text{if } Dir_{i,t'} \neq Dir_{j,t'} \end{cases} \quad (8)$$

$$Vel_{i,j,t'} = \begin{cases} 1, & \text{if } Vel_{i,t'} = Vel_{j,t'} \\ 0, & \text{if } Vel_{i,t'} \neq Vel_{j,t'} \end{cases} \quad (9)$$

where $Pos_{i,t'}$, $Pos_{j,t'}$, $Dir_{i,t'}$, $Dir_{j,t'}$, $Vel_{i,t'}$, and $Vel_{j,t'}$ represent the position, direction, and velocity, respectively, of a trustor i and a trustee j at a time t' .

- **Familiarity (Fam)**—The familiarity ($0 \leq Fam_{i,j,t} \leq 1$) is also segregated into external familiarity (EF) and internal familiarity (IF). The external familiarity refers to the ratio of the number of common vehicles interacting with a trustor i and a trustee j to the total number of vehicles interacting with a trustor i over the time t , i.e., the more the number of common interacting vehicles, the higher the familiarity between a trustor i and a trustee j . On the contrary, the internal familiarity signifies the interaction frequency between a trustor i and a trustee j over the time t , i.e., the higher the interaction frequency, the higher is the familiarity between the two. The same is illustrated in Equations (10)–(12).

$$Fam_{i,j,t} = w_{EF}EF_{i,j,t} + w_{IF}IF_{i,j,t} \quad (10)$$

where w_{EF} and w_{IF} refers to the weight of $EF_{i,j,t}$ and $IF_{i,j,t}$, respectively, ($w_{EF} + w_{IF} = 1$). The $EF_{i,j,t}$ is ascertained as:

$$EF_{i,j,t} = \frac{\sum_{t'=1}^t F_{i,j,t'}}{\sum_{t'=1}^t F_{i,t'}} \quad (11)$$

where $\sum_{t'=1}^t F_{i,j,t'}$ represents the number of common interacting vehicles of a trustor i and a trustee j , whereas $\sum_{t'=1}^t F_{i,t'}$ is the total number of vehicles interacting with i . Similarly, the $IF_{i,j,t}$ is computed as:

$$IF_{i,j,t} = \frac{\sum_{t'=1}^t I_{i,j,t'}}{t} \quad (12)$$

where $\sum_{t'=1}^t I_{i,j,t'}$ signifies the number of interactions between a trustor i and a trustee j .

- **Reward and Punishment (RP)**—The RP is employed to evaluate the rewards and punishments accorded to a trustee j by a trustor i depending on its behavior, i.e., a trustee j is rewarded by a trustor i for its cooperation, honesty, and reporting a critical event, and is punished for any misconduct. The RP is, therefore, calculated as:

$$RP_{i,j,t} = ISR_{i,j,t} e^{-\frac{N_p}{N_p + N_r}} \quad (13)$$

where $ISR_{i,j,t}$ is the interaction success rate between a trustor i and a trustor j . Also, N_p suggests the number of negative interactions, whereas N_r exhibits the number of positive interactions.

3.2. Indirect Trust ($T_{ind(i,j,t)}$)

The indirect trust, also generally referred to as the recommendation trust, is ascertained by (a) soliciting the recommendations via the one-hop neighboring nodes of a trustor pertinent to a trustee and (b) by taking into account the confidence of a trustor on the recommendations ascertained by the one-hop neighboring vehicles [32,44]. The indirect trust is computed as:

$$T_{ind(i,j,t)} = \frac{\sum_{k=1}^n C_{i,k,t} T_{d(k,j,t)}}{n} \quad (14)$$

where $C_{i,k,t}$ implies the confidence score assigned by a trustor to the recommendations of its one-hop neighboring vehicles pertinent to a trustee, $T_{d(k,j,t)}$ refers to the recommendations ascertained by the said one-hop neighboring nodes, and n implies the total number of one-hop neighboring nodes. The confidence score, $C_{i,k,t}$, is calculated as:

$$C_{i,k,t} = \begin{cases} 1, & \text{if } T_{d(i,k,t)} \geq Th_C \\ 0.5, & \text{if } Th_T \leq T_{d(i,k,t)} < Th_C \\ 0, & \text{if } T_{d(i,k,t)} < Th_T \end{cases} \quad (15)$$

where Th_C and Th_T refer to the confidence threshold and the trust threshold, respectively, and act as a weight for distinguishing between a good, an average, or a bad recommendation [39].

3.3. Context (T_C)

A number of existing trust models ignore the significance of context, thereby making them quite unrealistic for real-world settings. In our model, the notion of context has been primarily determined by two factors, i.e., the vehicle types and the operating scenarios, the details of which are as follows:

- **Vehicle types (VT)**—Five types of vehicles have been taken into consideration in the proposed model. Police cars, ambulances, and fire engines are regarded as high-priority (HP) vehicles since the information disseminated by these particular vehicles possesses considerable confidence of a centralized trusted authority. The second

type is public transport (PT) vehicles, i.e., buses, taxis, and subways, which are also considered reasonably trustworthy since they have been approved by specific authorized departments. Similarly, private vehicles are classified into professional (P) vehicles and novice (N) vehicles primarily depending on their respective driver's driving experience, i.e., professional drivers are regarded to have extensive driving expertise in contrast to beginners and are, therefore, considered to be more trustworthy. Finally, we consider malicious vehicles to be untrustworthy in nature. Equation (16) illustrates the trust values vis-à-vis the suggested vehicle types:

$$T_{VT} = \begin{cases} 1, & \text{if Vehicles} = \text{HP} \\ 0.8, & \text{if Vehicles} = \text{PT} \\ 0.6, & \text{if Vehicles} = \text{P} \\ 0.4, & \text{if Vehicles} = \text{N} \\ 0, & \text{if Vehicles} = \text{Malicious} \end{cases} \quad (16)$$

- *Operating Scenarios (OS)*—In the envisaged model, we have considered two operating scenarios, i.e., an urban and a highway one. In Section 4, the simulation results for these two scenarios have been delineated in detail. It is pertinent to highlight here that the high mobility and the random geographical distribution of vehicles in an IoV network results in several different contextual scenarios. Therefore, it is indispensable to consider such settings while ascertaining the trust of a trustee. For instance, owing to the limited mobility of vehicles and the high density of RSUs in an urban scenario, there is a considerable number of interactions, both trustworthy and untrustworthy, between the vehicles. However, in scenarios involving highways, the mobility of the vehicles is generally much higher than that in an urban scenario. Furthermore, vehicles in highway settings have a more sparse geographical distribution, thereby resulting in fewer interactions between them. Trust management often relies on a large number of RSUs, but there are fewer RSUs on highways, so trust management cannot be well implemented in this scenario.

4. Results and Discussion

4.1. Simulation Setup and Feature Extraction

We used the Epinions dataset (<https://cse.msu.edu/tangjili/datasetcode/truststudy.htm>, Accessed: 1 June 2023) in order to map the data traces for the trust parameters of our envisaged IoV-based trust model. Epinions, in essence, is a publicly available trust dataset that encompasses six parameters: userid, productid, categoryid, rating, helpfulness, and timestamps. For instance, a data trace of [1, 2, 3, 4, 5, 6] in the Epinions dataset implies that user 1 accords a rating of 4 to product 2 belonging to category 3 at timestamp 6. The helpfulness of the accorded rating is 5. For the sake of the research at hand, we have appropriately transformed the Epinions dataset into an IoV dataset in light of the similar transformations envisaged in [45].

A total of 3266 pairs of interactions between trustors and trustees, i.e., pertinent to 64 nodes (vehicles), have been taken into consideration. The same are arranged in the form of a feature matrix M as illustrated in Equation (17).

$$[M_{n \times 7}] = \begin{bmatrix} ISR_1 & Sim_1 & Fam_1 & RP_1 & confidence_1 & VT_1 & OS_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ ISR_n & Sim_n & Fam_n & RP_n & confidence_n & VT_n & OS_n \end{bmatrix}_{n \times 7} \quad (17)$$

The dimension of this feature matrix is $n \times 7$, wherein $n = 3266$ and 7 implies the trust-based feature vectors vis-à-vis each of the 3266 trustor trustee pairs. It is pertinent to mention here that there is no need for the features' normalization since each trust feature value falls in the range of [0, 1]. The seven features are concatenated into three features, i.e., direct trust, indirect trust, and context, in a bid to form a new feature matrix N with

a dimension of $n \times 3$, wherein the direct trust implies interaction success rate, similarity, familiarity, and reward and punishment, the indirect trust is ascertained via direct trust and confidence, and the context comprises vehicle types and operating scenarios. Since it is not feasible to display a three-dimensional vector, two out of three features are selected and displayed at a time for demonstration purposes.

$$[N_{n \times 3}] = \begin{bmatrix} \text{direct} & \text{trust}_1 & \text{indirect} & \text{trust}_1 & \text{context}_1 \\ \vdots & & \vdots & & \vdots \\ \text{direct} & \text{trust}_n & \text{indirect} & \text{trust}_n & \text{context}_n \end{bmatrix}_{n \times 3} \quad (18)$$

Table 3 depicts the trust-based parametric values of 20 randomly selected vehicles in the IoV network. Figure 4 further portrays two of such parameters, i.e., ISR and RP, for all of the 64 vehicles in the IoV network. It is evident that the change in the parametric values of RP is proportional to the parametric values of ISR with the exception of a few. For instance, vehicles 3, 32, 48, 52, and 58 possess high ISR values but low RP values. This is owing to the fact that although the interactions carried out by these vehicles are considerable, most of them were accounted for as being negative.

Table 3. Trust parameters' values pertinent to 20 random vehicles in an IoV network (ISR here implies interaction success rate, and RP refers to reward and punishment).

Vehicles	ISR	Similarity	Familiarity	RP	Confidence	Context
1	0.500	0.614	0.167	0.500	0.000	0.333
2	0.894	0.593	0.120	0.542	0.000	0.711
3	0.982	0.665	0.119	0.361	1.000	0.800
4	0.982	0.770	0.111	0.704	1.000	0.567
5	0.950	0.453	0.104	0.950	0.500	0.850
6	0.964	0.484	0.107	0.964	0.000	0.857
7	1.000	0.515	0.125	1.000	1.000	0.650
8	0.911	0.541	0.226	0.552	1.000	0.771
9	0.833	0.476	0.262	0.735	1.000	0.686
10	1.000	0.524	0.217	1.000	1.000	0.720
11	1.000	0.600	0.292	1.000	1.000	0.933
12	1.000	0.763	0.200	1.000	0.500	0.840
13	0.833	0.750	0.222	0.833	1.000	0.600
14	0.855	0.750	0.375	0.855	1.000	0.550
15	1.000	0.540	0.229	1.000	1.000	0.500
16	1.000	0.529	0.319	1.000	1.000	0.600
17	0.893	0.638	0.351	0.893	0.500	0.729
18	0.815	0.700	0.100	0.815	1.000	0.618
19	0.834	0.585	0.323	0.683	1.000	0.775
20	0.915	0.700	0.333	0.915	1.000	0.600

4.2. Clustering and Labeling

Subsequent to the extraction of the desired trust features, three unsupervised learning algorithms, i.e., k-means, fuzzy c-means, and agglomerative clustering, have been employed to label the feature matrices. It is noteworthy that unsupervised learning algorithms have been employed in a bid to ascertain a credible and reliable ground truth. Accordingly, two clusters, trustworthy and untrustworthy, have been obtained as a result of the same and are depicted in Figures 5–7.

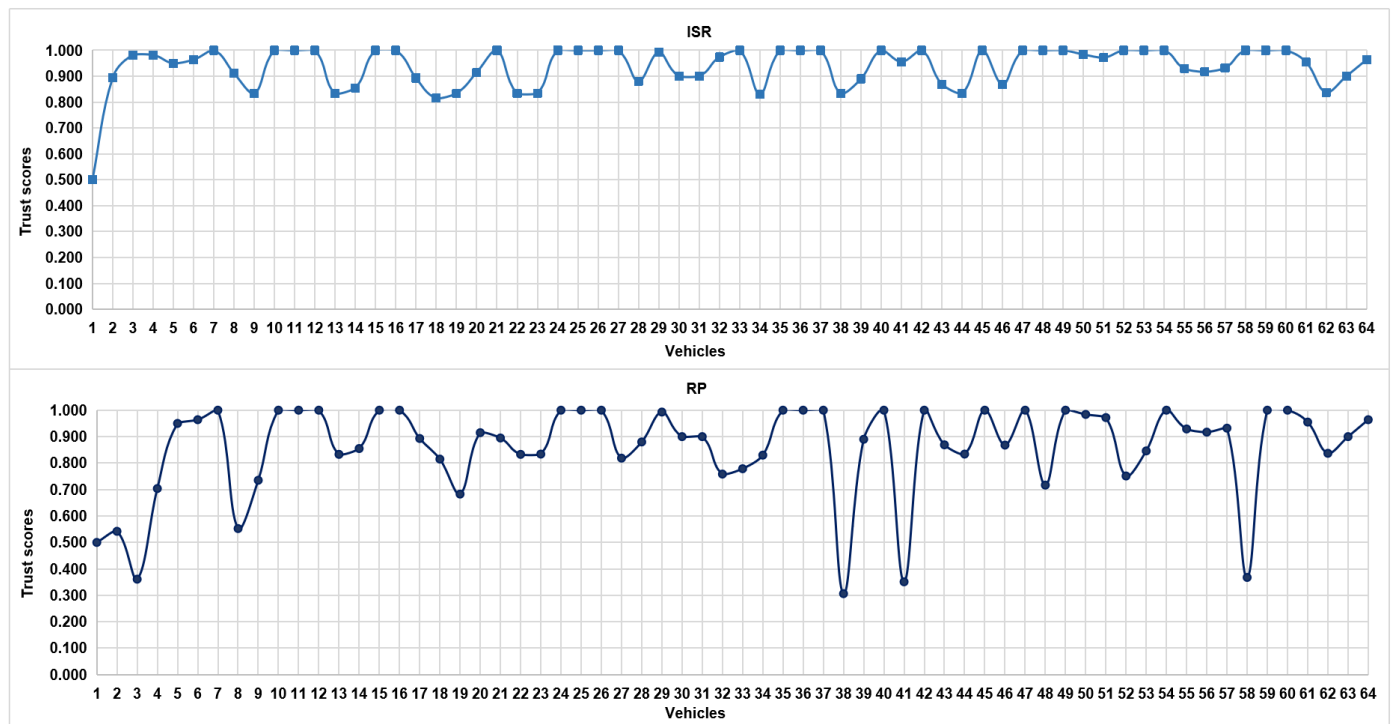


Figure 4. Trust scores of vehicles in an IoV network vis-à-vis ISR and RP (ISR here implies interaction success rate, and RP refers to reward and punishment).

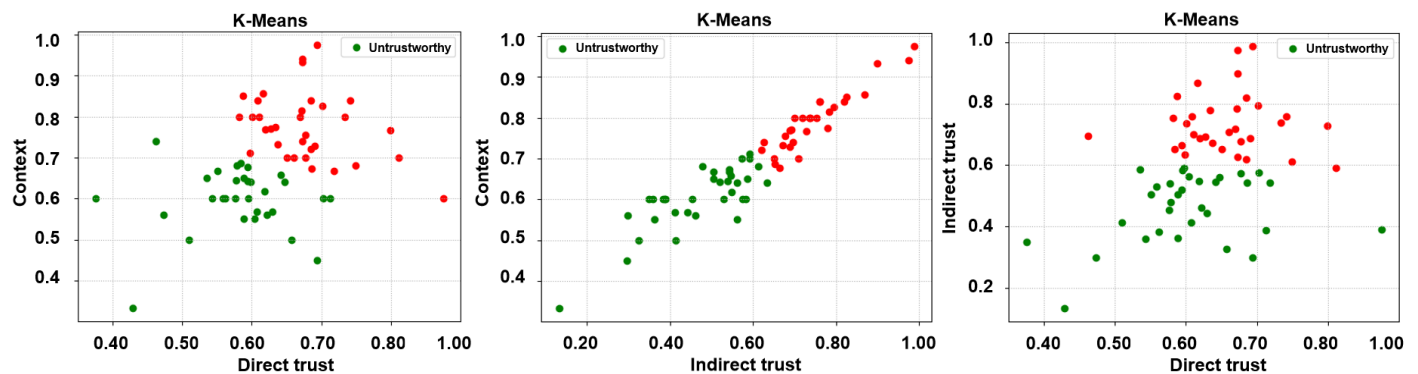


Figure 5. Labels via unsupervised learning (k-means clustering)—direct trust vs. context, indirect trust vs. context, and direct trust vs. indirect trust.

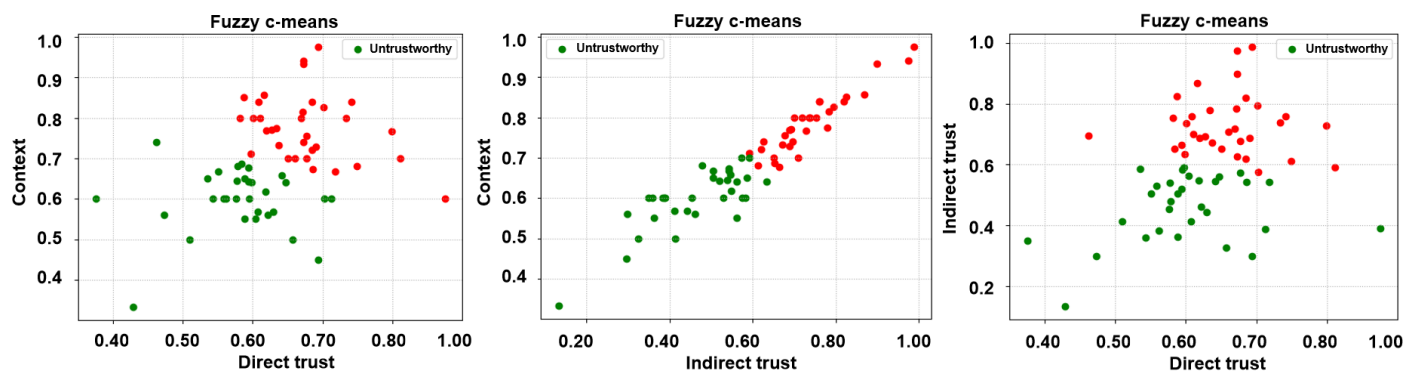


Figure 6. Labels via unsupervised learning (fuzzy c-means clustering)—direct trust vs. context, indirect trust vs. context, and direct trust vs. indirect trust.

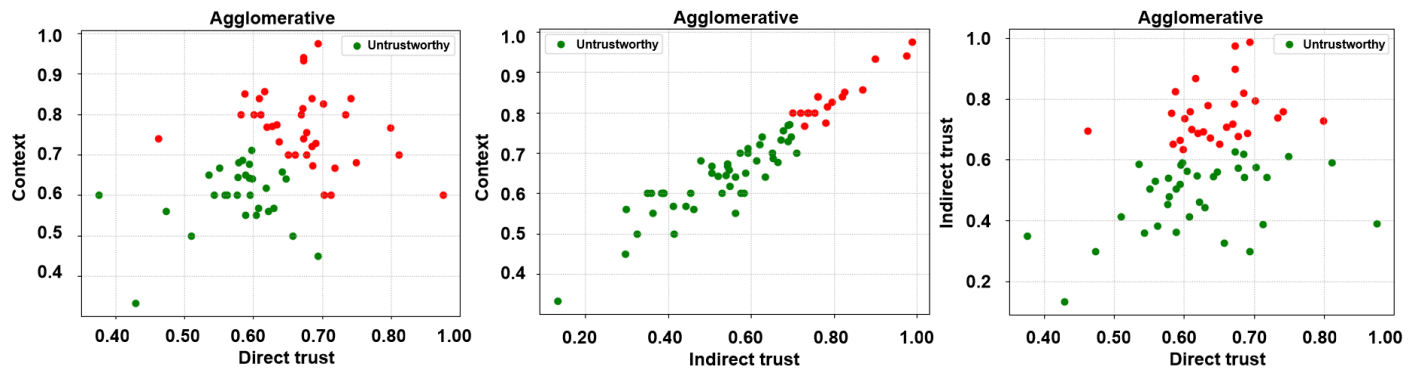


Figure 7. Labels via unsupervised learning (agglomerative clustering)—direct trust vs. context, indirect trust vs. context, and direct trust vs. indirect trust.

4.3. Classification and Model Evaluation

A number of supervised learning algorithms, including, but not limited to, k-nearest neighbor (KNN), support vector machine (SVM), random forest (RF), and ensemble ones have been employed in the research literature for classification purposes [7,19,46,47]. For the manuscript at hand, we have employed KNN and RF classifiers on the resulting feature matrix for training purposes via a 5-fold cross-validation approach in a bid to ascertain the malicious nodes via a decision boundary. The same is depicted in Figures 8 and 9 for KNN and RF classifiers, respectively, wherein the trusted and untrusted regions can be clearly observed. We have subsequently evaluated the accuracy of our envisaged trust model via the following three evaluation parameters:

- Precision: Precision depicts the ability of the envisaged trust model to correctly predict malicious vehicles as being malicious.
- Recall: Recall refers to the proportion of malicious vehicles that have been correctly ascertained by the envisaged trust model.
- F1-score: F1-score implies the weighted harmonic mean of the precision, and recall and ascertains the model's accuracy.

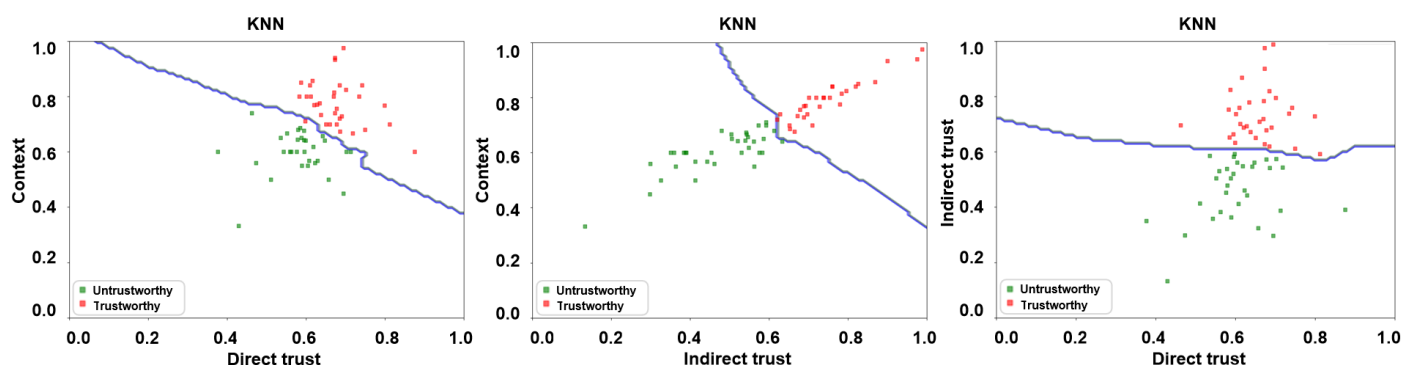


Figure 8. Trust boundary results for KNN algorithm—direct trust vs. context, indirect trust vs. context, and direct trust vs. indirect trust.

For our trust model, we further consider vehicles under two different operating scenarios, i.e., urban and highway. Also, owing to the space constraint, only the figures pertinent to the urban scenario have been portrayed. Nevertheless, the precision, recall, and F1-score for both urban and highway scenarios have been depicted in Table 4. It is pertinent to mention here that the precision, recall, and F1-score of our envisaged trust model as demonstrated by the KNN classifier under both urban and highway settings is much higher in contrast to the precision, recall, and F1-score demonstrated by the RF classifier under the same settings. KNN is regarded as one of the simplest classification algorithms, i.e., with mature theory, low training time complexity, and insensitivity to

outliers. This particular algorithm is quite suitable for an automatic classification of class domains with large sample size [7]. It is also noteworthy to mention that the trust can be ascertained in a relatively more accurate manner in an urban setting in contrast to the highway setting since vehicles interact much more frequently in the former owing to their low speeds as opposed to the latter which is designed to enable them to traverse with high speeds.

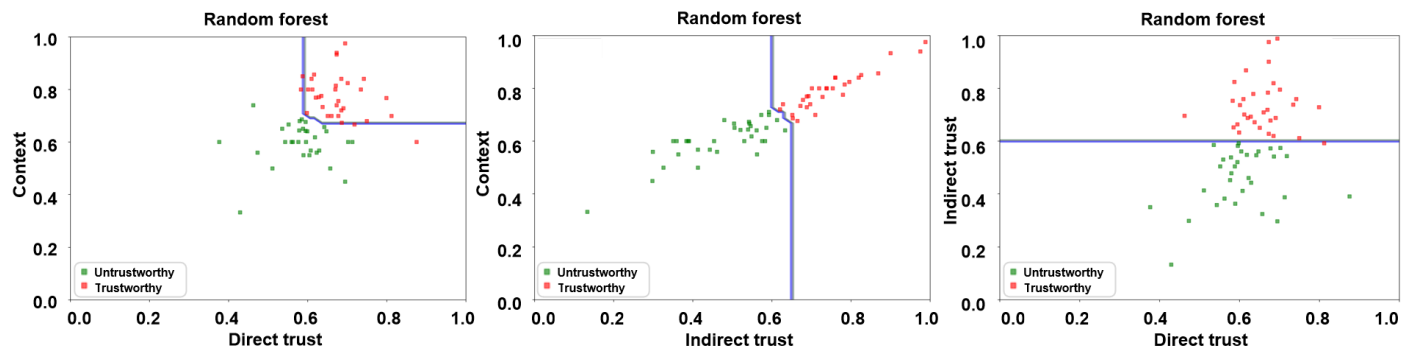


Figure 9. Trust boundary results for RF algorithm—direct trust vs. context, indirect trust vs. context, and direct trust vs. indirect trust.

Table 4. Evaluation results via supervised learning algorithms, i.e., KNN and RF (KNN here implies k-nearest neighbor and RF refers to random forest).

Scenarios	Classifier	Precision	Recall	F1-Score
Urban	KNN	1.0000	1.0000	1.000
	RF	1.0000	0.9400	0.9684
Highway	KNN	0.9804	0.9623	0.9713
	RF	0.9764	0.9338	0.9546

Table 5 depicts the comparison of our envisaged trust model vis-à-vis machine learning-based trust mechanisms, i.e., [47,48]—labeled as NC—1 and NC—2, respectively, that have not taken the notion of context into consideration. Whilst the said trust models demonstrate high precision, our envisaged trust model still outperforms them since it takes into account the context pertinent to the interactions on the premise that the interaction between a trustor and trustee is different in different contexts. Table 5 further outlines the comparison of our envisaged trust model vis-à-vis conventional (weighted sum) trust mechanisms, i.e., [23,27,49]—labeled as Conv1, Conv2, and Conv3, respectively. It can once again be seen clearly that the envisaged trust model performs considerably better in terms of precision in contrast to the conventional trust mechanisms. This reinforces the fact that the weighted sum mechanisms have strong subjectivity and are influenced by numerous underlying factors. Hence, when a number of trust parameters are in play, a machine learning-based mechanism is optimal for not only aggregating the same but ascertaining an intelligent trust boundary.

Table 5. Comparison of the precision of trust models (NC—1: [47], NC—2: [48], Conv1: [23], Conv2: [27], Conv3: [49]).

Model	Proposed	NC—1	NC—2	Conv1	Conv2	Conv3
Precision	1.0000	0.9234	0.9005	0.9700	0.9700	0.9750

5. Conclusions and Future Directions

An intelligent transportation system is an intrinsic component of smart cities since it allows vehicles to employ vehicle-to-everything communication in a bid to exchange safety-critical messages with the other road entities and the supporting infrastructure to

ensure highly secure and intelligent traffic flows. However, road entities within an IoV network are vulnerable to a number of attacks and malicious actors prevailing in the same are always on the lookout to manipulate the IoV network for their malicious gains. In this manuscript, a machine learning-based trust management mechanism, MESMERIC, has been proposed that takes into account direct trust, indirect trust, and context (each with a number of qualifying attributes) to not only ascertain the trust of vehicles in an IoV network but to segregate the trustworthy vehicles from the untrustworthy ones by means of an optimal decision boundary. In the near future, the authors would investigate designing and launching a number of dynamic trust-related attacks via a state-of-the-art trust-based IoV testbed in order to understand the underlying nitty gritty of such dynamic attacks so that more resilient IoV-based trust models could be formulated. Additionally, the authors aim to propose an intelligent weighting-based conventional mechanism in a bid to mitigate any possible subjectivity that could arise during the trust aggregation process.

Author Contributions: The following are the contributions made by the authors: conceptualization, Y.W. and A.M.; methodology, Y.W. and A.M.; software, Y.W.; validation, Y.W.; formal analysis, Y.W.; investigation, Y.W.; resources, Y.W. and A.M.; data curation, Y.W.; writing—original draft preparation, Y.W. and A.M.; writing—review and editing, A.M.; visualization, Y.W. and A.M.; supervision, A.M., M.F.M.S., H.Z. and L.C.K.; funding acquisition, Y.W. All authors have read and agreed to the published version of the manuscript.

Funding: The corresponding author's PhD research at Universiti Malaysia Sarawak, Malaysia has been funded by the Qilu Institute of Technology, Jinan, Shandong, P.R. China.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

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

References

1. Mirzadeh, I.; Sayad Haghigh, M.; Jolfaei, A. Filtering Malicious Messages by Trust-Aware Cognitive Routing in Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 1134–1143. [\[CrossRef\]](#)
2. Akwirry, B.; Bessis, N.; Malik, H.; McHale, S. A Multi Tier Trust Based Security Mechanism for Vehicular Ad-Hoc Network Communications. *Sensors* **2022**, *22*, 8285. [\[CrossRef\]](#) [\[PubMed\]](#)
3. Afrin, T.; Yodo, N. A Survey of Road Traffic Congestion Measures Towards a Sustainable and Resilient Transportation System. *Sustainability* **2020**, *12*, 4660. [\[CrossRef\]](#)
4. Mo, W.; Liu, W.; Huang, G.; Xiong, N.N.; Liu, A.; Zhang, S. A Cloud-Assisted Reliable Trust Computing Scheme for Data Collection in Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4969–4980. [\[CrossRef\]](#)
5. Fabi, A.K.; Thampi, S.M. A Psychology-inspired Trust Model for Emergency Message Transmission on the Internet of Vehicles (IoV). *Int. J. Comput. Appl.* **2020**, *8*, 480–490. [\[CrossRef\]](#)
6. 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**, *8*, 255–268. [\[CrossRef\]](#)
7. Siddiqui, S.A.; Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. Towards a Machine Learning Driven Trust Management Heuristic for the Internet of Vehicles. *Sensors* **2023**, *23*, 2325. [\[CrossRef\]](#) [\[PubMed\]](#)
8. Wang, Y.X.; Zen, H.; Sabri, M.F.M.; Wang, X.; Kho, L.C. Towards Strengthening the Resilience of IoV Networks—A Trust Management Perspective. *Future Internet* **2022**, *14*, 202. [\[CrossRef\]](#)
9. Singh, M.; Limbasiya, T.; Das, D. Pseudo-identity Based Secure Communication Scheme for Vehicular Ad-hoc Networks. In Proceedings of the 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), GOA, India, 16–19 December 2019; pp. 1–6.
10. Hussain, R.; Lee, J.; Zeadally, S. Trust in VANET: A Survey of Current Solutions and Future Research Opportunities. *IEEE Trans. Intell. Transp. Syst.* **2022**, *14*, 2553–2571. [\[CrossRef\]](#)
11. Li, X.; Yin, X.; Ning, J. Trustworthy Announcement Dissemination Scheme with Blockchain Assisted Vehicular Cloud. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 1786–1800. [\[CrossRef\]](#)
12. Drobot, A.; Zhang, T.; Buonarosa, M.L.; Kargl, F.; Schwinke, S.; Sikdar, B. The Internet of Vehicles (IoV)—Security, Privacy, Trust, and Reputation Management for Connected Vehicles. *IEEE Internet Things* **2023**, *6*, 6–16. [\[CrossRef\]](#)

13. Tripathi, K.N.; Yadav, A.M.; Nagar, S.; Sharma, S.C. ReTrust: Reliability and Recommendation Trust-based Scheme for Secure Data Sharing Among Internet of Vehicles (IoV). *Wirel. Netw.* **2023**, *29*, 2551–2575. [[CrossRef](#)]
14. Yuan, M.Y.; Xu, Y.; Zhang, C.; Tan, Y.L.; Wang, Y.C.; Ren, J.; Zhang, Y.X. TRUCON: Blockchain-Based Trusted Data Sharing with Congestion Control in Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3489–3500. [[CrossRef](#)]
15. Wang, Y.H. A Trust Management Model for Internet of Vehicles. In Proceedings of the 4th International Conference on Cryptography, Security and Privacy (ICCSP), Tianjin, China, 14–16 January 2022; pp. 136–140.
16. Siddiqui, S.A.; Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 9546–9560. [[CrossRef](#)]
17. Qi, J.X.; Zheng, N.; Xu, M.; Wang, X.D.; Chen, Y.Z. A Multi-dimensional Trust Model for Misbehavior Detection in Vehicular Ad Hoc Networks. *J. Inf. Secur. Appl.* **2023**, *76*, 103528. [[CrossRef](#)]
18. 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 IEEE Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1238–1246.
19. Sagar, S.; Mahmood, A.; Sheng, M.; Zaib, M.; Zhang, W.E. Towards a Machine Learning-driven Trust Evaluation Model for Social Internet of Things: A Time-aware Approach. In Proceedings of the 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Darmstadt, Germany, 7–9 December 2020; pp. 283–290.
20. Jayasinghe, U.; Lee, G.M.; Um, T.W.; Shi, Q. Machine Learning Based Trust Computational Model for IoT Services. *IEEE Trans. Sustain. Comput.* **2019**, *4*, 39–52. [[CrossRef](#)]
21. Atwa, R.J.; Flocchini, P.; Nayak, A. A Fog-based Reputation Evaluation Model for VANETs. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021; pp. 1–7.
22. Rehman, A.; Hassan, M.F.; Hooi, Y.K.; Qureshi, M.A.; Duc, T. Context and Machine Learning Based Trust Management Framework for Internet of Vehicles. *Comput. Mater. Contin.* **2021**, *68*, 1238–1246. [[CrossRef](#)]
23. Fabi, A.K.; Thampi, S.M. A Trust Management Framework Using Forest Fire Model to Propagate Emergency Messages in the Internet of Vehicles (IoV). *Veh. Commun.* **2022**, *33*, 28643–28660. [[CrossRef](#)]
24. Bhargava, A.; Verma, S. DUEL: Dempster Uncertainty-Based Enhanced Trust Level Scheme for VANET. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 15079–15090. [[CrossRef](#)]
25. Siddiqui, S.A.; Mahmood, A.; Zhang, W.E.; Sheng, Q.Z. Machine Learning Based Trust Model for Misbehaviour Detection in the Internet-of-Vehicles. *Commun. Comput. Inf. Sci.* **2019**, *1142*, 512–520.
26. Mao, M.; Yi, P.; Hu, T.; Zhang, Z.; Lu, X.Y.; Lei, J.W. Hierarchical Hybrid Trust Management Scheme in SDN-Enabled VANETs. *Mob. Inf. Syst.* **2021**, *14*, 14550–14565. [[CrossRef](#)]
27. Xia, H.; Xiao, F.; Zhang, S.S.; Hu, C.Q.; Cheng, X.Z. Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; Volume 2, pp. 838–846.
28. Atwa, R.J.; Flocchini, P.; Nayak, A. RTEAM: Risk-based Trust Evaluation Advanced Model for VANETs. *IEEE Access* **2021**, *9*, 117772–117783. [[CrossRef](#)]
29. Sagar, S.; Mahmood, A.; Sheng, Q.Z.; Zhang, W.E. Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach. In Proceedings of the ICC 2020–2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
30. Chen, I.R.; Bao, F.; Guo, J. Trust-Based Service Management for Social Internet of Things Systems. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 684–696. [[CrossRef](#)]
31. Ahmad, F.; Franqueira, V.N.L.; Adnane, A. TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks. *IEEE Access* **2018**, *6*, 28643–28660. [[CrossRef](#)]
32. Alnasser, A.; Sun, H.; Jiang, J. Recommendation-Based Trust Model for Vehicle-to-Everything (V2X). *IEEE Internet Things J.* **2020**, *7*, 440–450. [[CrossRef](#)]
33. Wu, Q.; Shi, S.; Wan, Z.Y.; Fan, Q.; Fan, P.Y.; Zhang, C. Towards V2I Age-aware Fairness Access: A DQN Based Intelligent Vehicular Node Training and Test Method. *Chin. J. Electron.* **2023**, *32*, 1230–1244.
34. Oubabas, S.; Aoudjit, R.; Rodrigues, J.J.P.C.; 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](#)]
35. Harika, E. A Trust Management Scheme for Securing Transport Networks. *Int. J. Comput. Appl.* **2017**, *8*, 440–450. [[CrossRef](#)]
36. Lu, Y.; Zhang, G.; Wang, X.; Li, X. Trust-Based Reliability Enhancements Provisioning with Resilience Under Information Asymmetry in IoV System. *IEEE Access* **2023**, *11*, 82362–82376. [[CrossRef](#)]
37. 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* **2019**, *7*, 148913–148922. [[CrossRef](#)]
38. Feng, X.; Shi, Q.; Xie, Q.; Wang, L. P2BA: A Privacy-Preserving Protocol With Batch Authentication Against Semi-Trusted RSUs in Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3888–3899. [[CrossRef](#)]
39. Guo, J.J.; Li, X.H.; Liu, Z.Q.; Ma, J.F.; Yang, C.; Zhang, J.W.; Wu, D.P. TROVE: A Context Awareness Trust Model for VANETs Using Reinforcement Learning. *IEEE Internet Things J.* **2020**, *7*, 6647–6662. [[CrossRef](#)]
40. Yin, D.; Gong, B. Auto-Adaptive Trust Measurement Model Based on Multidimensional Decision-Making Attributes for Internet of Vehicles. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3537771. [[CrossRef](#)]

41. Xu, Y.; Li, Y. A Hybrid Approach to Trust Node Assessment and Management for VANETs Cooperative Data Communication: Historical Interaction Perspective. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 16504–16513.
42. Jing, T.; Liu, Y.; Wang, X.X.; Gao, Q.H. Joint Trust Management and Sharing Provisioning in IoV-Based Urban Road Network. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6942120. [[CrossRef](#)]
43. 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**, *70*, 9244–9257. [[CrossRef](#)]
44. 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.
45. Kerrache, C.A.; Lagraa, N.; Hussain, R.; Ahmed, S.H.; Benslimane, A.; Calafate, C.T.; Cano, J.C.; Vegni, A.M. TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles. *IEEE Internet Things J.* **2019**, *6*, 5870–5877. [[CrossRef](#)]
46. Deng, S.G.; Huang, L.T.; Xu, G.D.; Wu, X.D.; Wu, Z.H. On Deep Learning for Trust-Aware Recommendations in Social Networks. *IEEE Trans. Neural Netw. Learn. Syst.* **2017**, *28*, 1164–1177. [[CrossRef](#)] [[PubMed](#)]
47. El-Sayed, H.; Ignatiou, H.A.; Kulkarni, P.; Bouktif, S. Machine Learning Based Trust Management Framework for Vehicular Networks. *Veh. Commun.* **2020**, *25*, 100256. [[CrossRef](#)]
48. 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](#)]
49. Rai, I.A.; Shaikh, R.A.; Hassan, S.R. A Hybrid Dual-mode Trust Management Scheme for Vehicular Networks. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720939372. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.