NOTRINO: a NOvel hybrid TRust management scheme for INternet-Of-vehicles

Ahmad, F., Kurugollu, F., Kerrache, C. A., Sezer, S. & Liu, L.

Original citation & hyperlink:
Ahmad, F, Kurugollu, F, Kerrache, CA, Sezer, S & Liu, L 2021, 'NOTRINO: a NOvel hybrid TRust management scheme for INternet-Of-vehicles', IEEE Transactions on Vehicular Technology, vol. (In-Press), pp. (In-Press).
https://dx.doi.org/10.1109/TVT.2021.3049189

DOI 10.1109/TVT.2021.3049189
ISSN 0018-9545
ESSN 1939-9359

Publisher: Institute of Electrical and Electronics Engineers

NOTRINO: a NOvel hybrid TRust management scheme for INternet-Of-vehicles

Farhan Ahmad*, Fatih Kurugollu*, Chaker Abdelaziz Kerrache†, Sakir Sezer‡, Lu Liu§
*Cyber Security Research Group, College of Engineering and Technology, University of Derby, United Kingdom
†Department of Computer Science, University of Laghouat, Algeria,
‡Centre for Secure Information Technologies (CSIT), Queens University Belfast, United Kingdom
§Department of Informatics, University of Leicester, United Kingdom
Email: *{f.ahmad, f.kurugollu}@derby.ac.uk
†kr.abdelaziz@gmail.com; ch.kerrache@lagh-univ.dz
‡s.sezer@qub.ac.uk; §l.liu@leicester.ac.uk

***Abstract*—Internet-of-Vehicles (IoV) is a novel technology to ensure safe and secure transportation by enabling smart vehicles to communicate and share sensitive information with each other. However, the realization of IoV in real-life depends on several factors, including the assurance of security from attackers and propagation of authentic, accurate and trusted information within the network. Further, the dissemination of compromised information must be detected and vehicle disseminating such malicious messages must be revoked from the network. To this end, trust can be integrated within the network to detect the trustworthiness of the received information. However, most of the trust models in the literature relies on evaluating node or data at the application layer. In this study, we propose a novel hybrid trust management scheme, namely, NOTRINO, which evaluates trustworthiness on the received information in two steps. First step evaluates trust on the node itself at transport layer, while second step computes trustworthiness of the data at application layer. This mechanism enables the vehicles to efficiently model and evaluate the trustworthiness on the received information. The performance and accuracy of NOTRINO is rigorously evaluated under various realistic trust evaluation criteria (including precision, recall, F-measure and trust). Furthermore, the efficiency of NOTRINO is evaluated in presence of malicious nodes and its performance is benchmarked against three hybrid trust models. Extensive simulations indicate that NOTRINO achieve over 75% trust level as compared to benchmarked trust models where trust level falls below 60% for a network with 35% malicious nodes. Similarly, 92% precision and 87% recall are achieved simultaneously with NOTRINO for the same network, comparing to benchmark trust models where precision and recall falls below 87% and 85% respectively.**

***Keywords*—Connected Vehicles, Trust Management, Trust Model, Smart Cities, Internet-of-Vehicles**

I. Introduction

Recently, "Internet-of-Vehicles (IoV)" has emerged as a novel ground-breaking technology to ensure secure, smoother and safer transportation on the road by enabling the smart vehicles to share sensitive information with each other [1]. This visionary paradigm of IoV enables smart vehicle equipped with storage, computational power, communication technologies and IP-based module to connect to the traditional Internet, thus comprehending and realizing a significant application of "Internet-of-Things (IoT)" [2]. In IoV, the integrated multi-communication modules enable the vehicles to interact with each other, adjacent roadside units (RSUs) and neighbouring pedestrians via various distinct modes of communication, i.e., vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-pedestrian (V2P) communications, to offer a wide range of applications which can be categorized into safety (e.g., steep-curve or accident warnings) and non-safety (e.g., weather updates) applications. Security applications impose strict requirements on the network in terms of delay, safety, privacy and trust, while these requirements are bit relaxed in non-safety applications [3]. Fig. 1 illustrates the integration and realization of IoV within smart city environment, which shows that messages are transmitted and exchanged among vehicles via V2V, V2I and V2P, thus ensuring the overall traffic safety.

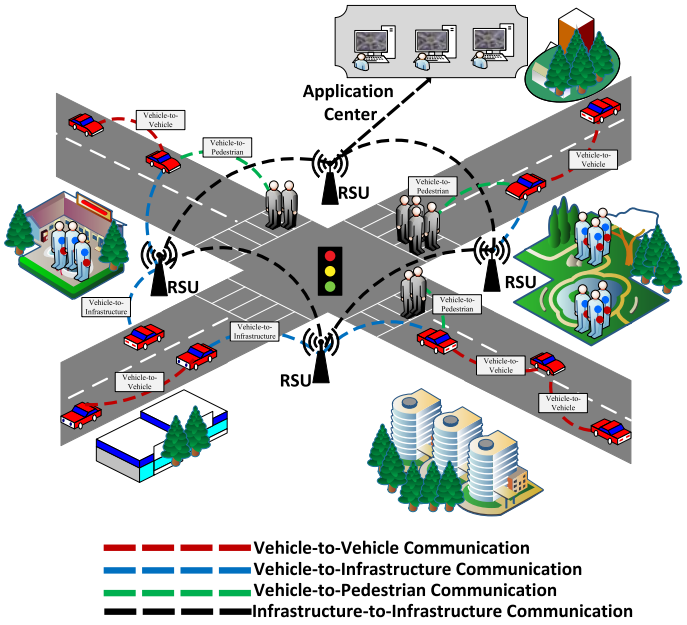


Fig. 1: Realization of IoV in Smart City

Same as all open medium-based networks, IoV is prone to several security issues [4]. Hence, securing IoV has attracted the attention of both academic and industrial researchers. Overall, existing solutions are classified into cryptography-

based solutions [5] and trust-based solutions [6]. While the first category is known to ensure most of the desired security services, it suffers from the high computational and time overhead which can lead to unwanted situations, especially for IoV safety applications. On the other hand, trust can be seen as an alternative solution that can ensure the same security services without exhausting the network's resources which makes of it more suitable to delay-sensitive and highly dynamic environment like IoV [7]. In the context of IoV, *trust* is defined as the faith which one vehicle places in other vehicle(s) for sharing reliable, trusted, accurate, and authentic messages [7], [8].

Trust models are generally classified into node-centric, data-centric, and combined models depending on the revocations target. To achieve this purpose various metrics are used such as interactions evaluation, exchange of recommendation, and messages analysis, to name a few. However, existing solutions are either application-specific (safety or infotainment) or involving various similarity measurements to compare the generated messages, and these measurements add a considerable undesired overhead. In addition, most of the solutions focus on eliminating dishonest vehicles or filtering out malicious messages based on identity related metrics or messages analysis metrics. Even combined trust models consider only one category of metrics. Whereas, a legitimate node can generate fake message due to a sensor problem, and a dishonest node can generate true messages about an occurring event. Thus, considering both nodes honesty and messages quality analysis is a must for an efficient trust establishment solution.

To overcome above issues, we propose 'NOTRINO', a novel hybrid trust management scheme for IoVs which enables the vehicles to efficiently evaluate the information authenticity by evaluating trust in two steps, i.e., first step classifies the message sender as trustworthy or malicious at the transport layer of IoV, and second step evaluates the authenticity of the received messages at the application layer. Data trustworthiness is performed only, if a node is classified as trustworthy at transport layer, thus enabling the vehicles to efficiently rely on the received message or not.

In summary, the significant contributions of this study are as follows:

- A novel hybrid trust model ('NOTRINO') based on the protocol stack of IoV is proposed.
- An efficient and light-weight trust model which can not only evaluate node trustworthiness, but also data trustworthiness is proposed.
- A fully distributed trust model to match the disperse and distributed nature of IoV environment is introduced.
- An attack-resistant trust model is proposed, as it has the ability to efficiently detect the attackers
- Extensive simulations are performed to validate our proposal, and evaluated the efficiency of NOTRINO from accuracy and trust aspects.

The remainder of this paper is organized as follows: In Section II, we present related work on trust management in IoV. Next, Section III introduces the system model of NOTRINO, while Section IV provides details on the design of our proposed NOTRINO scheme. Afterwards, the simulation environment is explained in Section V, while Section VI is dedicated to different simulation results of NOTRINO. Finally, conclusions based on NOTRINO are drawn in Section VII.

II. Related Work

In IoV, the main objective of the trust models is to provide an environment, where information can be propagated among network entities in a secure and trusted environment. Further, the trust model ensures that every participating node gets trusted information. However, due to the volatile, highly mobile nature of vehicles in IoV, evaluating trust in a short period of time is extremely challenging [9], [10].

IoV involves two significant revocation targets, i.e., (1) participating nodes, and (2) information shared between these nodes [6], [11]. Based on these targets, trust in IoV can be broadly classified into three distinct categories, i.e., (1) node-centric trust models, (2) data-centric trust models, and (3) combined trust models [12]–[14] as shown in Fig. 2.

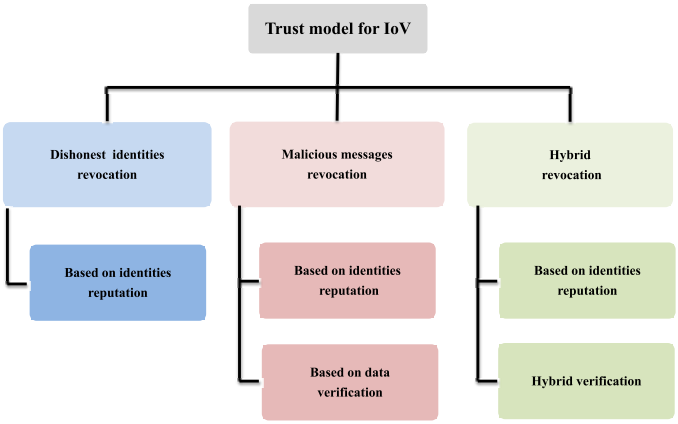


Fig. 2: Classification of Trust Models in IoV

A. Node-centric Trust Models (NCT)

These trust models aim at eliminating dishonest nodes from the network by evaluating trustworthiness of the message transmitting vehicles. These trust models highly rely on its neighbours, whose main responsibility is to provide opinions to message evaluator node (M_{Eval}) by endorsing the reputation of the message sender. Currently, various NCT are proposed in literature recently. For instance, Yang presented a novel NCT, namely 'Trust and Reputation Management Framework' where a similarity mining approach is utilized to evaluate the trustworthiness of the message transmitter [15]. When messages are disseminated within the network, M_{Eval} identifies the similarity among messages based on the Euclidean distances and the reputation weights of the participating nodes. The scope of this approach is limited as trust is computed locally at the M_{Eval}. Further, the details on recommendation reliability is missing from this study.

A centralized node-centric trust model was proposed by Marmol et al., where M_{Eval} relies on the adjacent infrastructure to evaluate neighbour's reputation [16]. M_{Eval} upon

reception of the messages generate a fuzzy-based trust score to classify the message sender as legitimate or dishonest. First, the M_{Eval} calculates trust score by aggregating information via three distinct sources, i.e., (a) recommendation provided by infrastructure, (b) recommendation from neighbouring nodes, and (c) previous reputation of the message transmitter. Second, M_{Eval} takes one of the following decisions based on the computed trust. (1) Drop the message if not trustworthy, (2) Accept the information but do not forward message, and (3) Accept the information and forward it. The main shortcoming of this trust model is its nature of evaluating trust via infrastructure, which cannot be guaranteed in rural areas.

Haddadou et al., on the other hand, adapted an economic incentive model to exclude dishonest nodes from the network [17]. In this model, every node within the network is assigned with a specific credit value. The increments and decrements of the credit depends solely on the behaviour of the node within the network, i.e., credits increment for good behaviour of the node. In case of an attack, credit of the participating node is decremented. M_{Eval} categorizes the node as malicious if the credit is 0 and, therefore, it excludes the node from the network. The major constraint of this trust model is its inability to differentiate between direct or indirect trust.

Another NCT was introduced by Khan et al., where a cluster-based approach is utilized to evaluate trust on the nodes [18]. In this method, cluster head (CH) is elected first in the network, which employs a watchdog mechanism within its vicinity, thus, providing an opportunity to honest nodes to submit their recommendation to CH about the presence of misbehaving entity in the network. Upon the detection of such misbehaving and dishonest nodes, CH informs the trusted authority (TA) which eliminates such nodes from the pool of trusted nodes. The major drawback of this approach is the generation of high amount of overheads which is caused to the continuous exchange of reports between nodes, thus reducing the overall efficiency of the network.

A similar cluster-oriented trust model was proposed by Jesudoss et al., where CH is responsible to eliminate dishonest nodes from the network [19]. In order to gain the reputation within the network, every node follows a truth-telling approach to share true information with the CH. Further, these nodes must participate in the election of CH in the network. Based on the participation of the nodes, CH provides incentives in the form of weights to these nodes. CH only trusts the information, if the participating node gains higher weights in CH election. This solution fails in a highly mobile and rural scenario due to limited number of neighbouring vehicles. As a result, the presence of dishonest nodes in such location may result in the biased selection of CH.

Recently, Alnasser et al. [20] proposed a recommendation-based trust model to deal with internal attackers of the network. In this proposed trust model, trust is computed based on the weighted-sum method in a fully decentralized manner. Further, this trust model provides the evaluator node to compute trust via both direct and indirect trust methods. However, the main drawback of this trust model is its nature of trust computation via weighted sum which can result in a biased trust computation if the evaluator node is surrounded by majority of the malicious nodes, thus compromising the network security.

B. Data-centric Trust Models (DCT)

Works falling under this category have the common aim of filtering out malicious messages rather than blacklisting vehicles (IDs), as the later action can lead to the undesired situation of network fragmentation. This task can be achieved either by eliminating messages coming from dishonest IDs or by verifying the exchanged messages themselves if not encrypted.

The data-centric trust model proposed by Gurung et al. [21] involves the message content similarity, message content conflict, and message routing path to decide whether the message is malicious or legal. The main problem with this solution is that it runs all the three-time consuming procedures for every single message. In addition, it does not consider the extreme cases of mobility (very dense and very sparse cases).

Authors of [22] proposed a data-centric trust model for anonymous VANET. Based on four parameters namely location closeness, time closeness, location verification, and time stamp verification they compute a confidence value regarding every message describing an event. While preserving vehicles' IDs, this scheme suffers from various environment-related problems including the huge number of messages describing the same event. In addition, safety messages are known to be very sensitive to the delay, waiting for the confidence processing time can lead to unwanted situations like late accident notification.

Unlike [22], Rawat et al. [23] introduced combined opportunistic/deterministic approaches. In the first one, they compute the similarity between messages describing a same event. Hence, with the assumption that legitimate messages are in majority, they filter out the different minority of messages. On the other hand, the deterministic approach is based on coordinates of vehicles position and received signal strength estimation. By comparing the two values malicious vehicles can be detected and hence also their messages. Same as [22], [23] is also time consuming and cannot perform as expected in critical cases. In addition, this solution also requires a large number of communicating vehicles to perform.

Kerrache et al. [24] proposed a safety-related data-centric trust model where the main purpose is how to disseminate only trustworthy messages while avoiding the known broadcast storm problem. Taking advantage of the standardized messaging services of ETSI [25], they piggybacked a belief degree about the occurring event and an ID of the selected next broadcaster of the message. Even though this solution has the advantage of respecting the ETSI ITS standard, only selected nodes will broadcast the events' messages. Hence, vehicles outside the communication range of the selected next broadcaster will not be informed about occurring events.

Finally, based on the evaluation of direct interactions among vehicles and without any exchanged recommendations, Gazdar et al. proposed a data-centric trust model called Enhanced Distributed Trust Computing Protocol (EDCTP) [26]. In this solution, every vehicle verifies the reliability of the event

triggered messages sent by its neighbors. In addition, the verification in this proposal is assumed to be made only by nodes within the same event zone, then a trust value will be given to the message source based on its credibility. Authors of this work also proposed a tier-based messages dissemination technique in order to detect altered messages and fake events. However, this work requires the existence of many vehicles within the event zone to perform.

C. Combined Trust Models (CT)

In this specific category of the trust models, both 'entity' and 'data' are taken into account in order to evaluate trustworthiness on the node and its shared data. Therefore, CT integrates both merits and demerits of NCT and DCT.

Recently, various studies are proposed in literature which evaluate trustworthiness on both data and node. For instance, Dhurandher et al. proposed an event-oriented trust model to distribute trusted content among the nodes by employing a wide range of reputation and plausibility checks throughout the network [27]. This trust model operates in following four steps to identify and revoke dishonest vehicles from the network: (1) discovering neighbour to the M_{Eval}, (2) dispatching *data* to the identified neighbours, (3) deciding trust on the received message based by defining detection and threshold ranges, and (4) continuously monitoring neighbourhood for possible neighbours around M_{Eval}. Though this technique can identify dishonest nodes in the network, however, there are some limitations in the proposed study: First, the study limits the detection range of M_{Eval} to 50 m, which is very short. Second, the detection solely depends on the vehicle's sensors. In case of sensor malfunction, the overall network will be polluted with compromised information as the M_{Eval} may classify legitimate messages as malicious.

In order to identify nodes transmitting compromised information within the network, Ahmed et al. proposed a logistic based trust computation technique, where M_{Eval} directly observes the events occurring within the network [28]. The neighbouring vehicles share the information about the event with M_{Eval}. Based on this provided information, M_{Eval} classifies the behaviour of the sender node as legitimate or malicious via weighted voting and logistic trust function. Though this technique can efficiently identify dishonest vehicles, it can propagate malicious content in the network. Due to its nature of evaluating trust based on weighted voting, the trust computation can be biased if M_{Eval} is surrounded by dishonest nodes.

Similarly, Li et al. introduced an efficient attack-resistant combined trust model, where M_{Eval} estimates trust on the received information, by evaluating both node and data-centric trust [29]. The data trustworthiness is calculated based on Bayesian Inference (BI), where M_{Eval} relies on the information received from multiple neighbours. On the other hand, M_{Eval} integrates functional trust (FT) and recommendation trust (RT) to evaluate node-centric trustworthiness. FT ensures that the participating node behaves properly while communicating with M_{Eval}, while, RT maintains that a certain level of trust is maintained before the node can be trusted. This scheme does not take data sparsity into account, which is pervasive in IoV.

Shrestha et al., proposed a combined trust model, where M_{Eval} calculates trust in two steps: (1) First it evaluates trust on the node, where a clustering algorithm distinguishes the honest and dishonest nodes, and categorized them into two separate groups [30]. Second, it calculates trust on the received messages based on the modified threshold random walk algorithm. The main drawback of this scheme is its assumption of uniform distribution of dishonest nodes in the network [34], which is invalid in IoV as the vehicles are placed randomly throughout the network.

Mahmood et al. presented a novel combined trust model which relies on traditional clustering mechanism to evaluate trust on the network nodes [31]. In this trust model, CH is elected in the network based on the trust of the participating nodes and their available resources. CH is responsible for transmitting trusted messages within the network. However, the main drawback of this approach is the biased election of CH, if majority of the nodes are dishonest in the network.

To share resources in a secure way among different network entities, Hatzivasilis et al. proposed a new combined trust model, namely, MobileTrust [32]. This proposal takes into account the advantages of the back-end centralised cloud and 5G technologies to provide an environment where trusted information can be disseminated in VANET. Further, MobileTrust encourages cryptographic communication between network entities, thus providing partially privacy in the network. However, the main drawback of this approach is its reliance on the centralized cloud for trust computation. In case the access to the cloud is denied by intruders, MobileTrust fails to compute trust of the participating vehicles, which ultimately compromise the overall network security.

Further Khan et al. recently proposed a combined trust model where blockchain is utilized to prevent attacks within VANET [33]. In this proposal, the node trustworthiness is evaluated based on the data added within the public blockchain in the infrastructure domain. Though this solution provides immutability and data integrity to some extent, this solution results in high delay due to the fact that all the trustworthiness is calculated at the back-end infrastructure. Further, the authors didn't provide any details about scalability of their solution, which is a standard issue in the blockchain systems.

In a nutshell, various trust models have been proposed in IoV, which ensures the propagation of trusted content in the network. According to our literature review, most of these trust models operate only at the application layer, which arises technical challenges including higher network delays. Table I summarizes the main exiting trust models for IoV. In this paper, we propose a novel combined trust model which operates at the two layers, i.e., network and application layer. Trustworthiness of the node is computed at the transport layer, while, data trustworthiness is evaluated only at the application layer, if a node is classified as trustworthy at the lower layer. This makes our proposed method very efficient to evaluate the overall trust in IoV environments.

In the next section, we provide explanations of our proposed trust model.

TABLE I: Main Trust Models for IoV.

	Trust class			Type of applications		Trust metrics				
	Node-centric	Data-centric	Combined	Safety	Infotainment	Messages analysis	Interactions' evaluation	Exchanged recommendations	Role of vehicles	RSUs and TA opinions
[15]	✓				✓	✓		✓		
[16]	✓				✓		✓	✓		✓
[17]	✓				✓		✓			
[18]	✓				✓		✓	✓		✓
[19]	✓				✓		✓	✓		
[20]	✓			✓			✓	✓		✓
[21]		✓		✓	✓	✓				
[22]		✓		✓		✓				
[23]		✓		✓		✓				
[24]		✓		✓		✓	✓			
[26]		✓		✓		✓	✓			
[27]			✓		✓		✓	✓		
[28]			✓	✓		✓	✓			
[29]			✓	✓	✓	✓	✓		✓	
[30]			✓		✓	✓	✓			✓
[31]			✓		✓		✓	✓		
[32]			✓	✓		✓	✓		✓	✓
[33]			✓	✓		✓	✓		✓	✓

III. System Model

A. Preliminaries and Assumptions

To design a hybrid trust management scheme, it is assumed that every vehicle in the network is equipped with NOTRINO, which can evaluate both node-centric and data-centric trustworthiness. Further, every vehicle maintains two databases. (1) First database to keep track of all the encountered vehicles, and (2) Second database to maintain respective trust ratings. Moreover, it is also assumed that RSUs are only used to disseminate messages over a greater geographical location. Furthermore, all the vehicles are equipped with GPS modules which provide the exact location of the participating nodes. Last, all the nodes are equipped with IEEE 802.11p module to interact with other nodes via V2V communication.

B. Network Model

IoV refers to a network where vehicles rely on each other and trusted sources to share trusted, accurate and authentic information in order to increase traffic efficiency. Therefore, a network model is designed to test the proposed trust model in presence of dishonest nodes, whose solely aim is to distribute malicious content to network nodes. At any given time, a safety event (an accident) is generated within the network where this information is propagated among network nodes via V2V communication. As majority of the nodes are stranger to each other, all the nodes evaluate the authenticity of the received information in two dimensions, i.e., (1) trust against sending node, and (2) trust against received information. These legitimate nodes broadcast and share only that information which is classified as authentic and trustworthy. Messages, which fail to satisfy trust criteria, are dropped in order to reduce the probability of propagating compromised information within network nodes.

C. Adversary Model

An adversary represents such class of nodes which can gain unauthorized access with the intention to perform different attacks within IoV [35]. The decentralized, large-scale and open nature of IoV can provide opportunity to adversary to be part of the network. In IoV, the main motivation of the adversary can be to detect legitimate communication between legitimate vehicles and tamper, forge, jam or delay the safety messages within the network. Moreover, attackers can also pollute the network with bogus information and recommendations [36], [37]. In this paper, we considered two different attacker models, which not only tamper the safety messages, but also, dodge the legitimate nodes to trust the compromised messages by sharing bogus trust ratings.

1) Man-in-the-Middle (MiTM) Attacks: These attacks are considered as one of the significant attacks in IoV, as the nodes can modify, tamper, forge, delay or drop the messages which may contain sensitive information [4], [38]. In this paper, we considered the MiTM attackers with modification capability. Upon receiving the safety messages, MiTM attacker will modify the content before sharing it with neighbouring vehicles. Further, the attackers will share compromised trust ratings with their neighbours. Moreover, MiTM attacker remains active throughout the network at all the time.

2) Zig-Zag Attacks: These attacks are also known as "On-and-Off" attacks, where the malicious nodes adapt a random pattern for their attacks in the network. First, these nodes behaves normally in order to get trust within the network. Once, these nodes become part of the network, these attacks behave maliciously and launch attacks within the network. These attacks are hard to be detected by the trust management schemes as they use both legitimate and malicious behaviours within the network. In this paper, these attackers share legitimate messages for some time. Once, they gain trust within the network, the attackers launch an attack, where they impose

false trust ratings with the neighbouring nodes.

IV. NOTRINO: A Novel Trust Model

In this section, we provide details of our novel trust model, i.e., NOTRINO. Further, Table II lists important abbreviations used in this manuscript.

TABLE II: Abbreviations List

	Terms	Explanation
Transport Layer	TM_{ENTITY}	Trust model at the transport layer
	M_{TR}	Message threshold range
	h_t	Antenna height of message sender
	h_r	Antenna height of message evaluator
	T_{Value}	Trust Value
	TV_{min}	Minimum trust value
	$T_{Threshold}$	Minimum trust threshold
	$\alpha_{Partial}$	Represents partial reward
	T_{Level}	Trust level at transport layer
	$Veh_{Database}$	Vehicular Database
Application Layer	TM_{DATA}	Trust model at the application layer
	RoT	Role-oriented trust
	$InfoQ$	Quality of the received information
	δ	Effective distance
	η	Tier-boundary
	$Trust_{Level}$	Trust level at application layer
	α	Overall reward for honesty
	β	Punishment factor for dishonesty

A. Overview of the Proposed Trust Model

In this work, a novel combined trust model is designed, where a layered approach is taken to evaluate trust on both entity and received data. *Entity* verification is performed at the transport layer, while, *Data* verification is operated at the application layer of IoV. M_{Eval} accepts information only if both node and data are verified. Otherwise it rejects the received messages and classify the transmitter as dishonest.

The protocol stack of IoV according to OSI reference model is depicted in Fig. 3. For the sake of simplicity, we presented a generalized protocol stack for IoV. In addition to the presented layers, a vertical layer of security and management can also be considered [39]. Further, it also depicts that our trust model is composed of two parts which are distributed over two layers, i.e., TM_{ENTITY} lies at the transport layer, while TM_{DATA} is present at the application layer. Both of these trust parts work

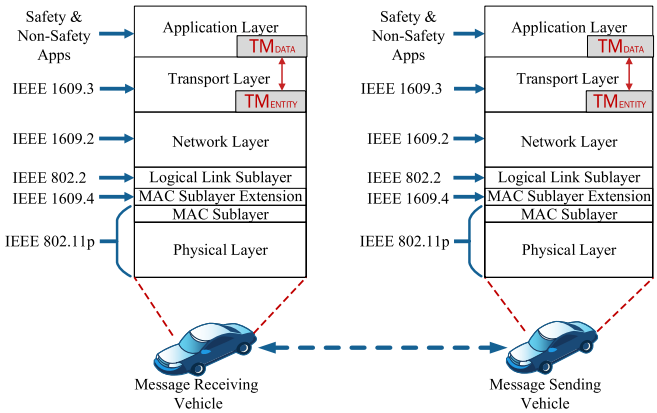


Fig. 3: Integration of Proposed Trust Model in IoV

in conjunction together for the calculation of overall trust. The high-level working mechanism of the proposed trust model is highlighted in Fig. 4, depicting, it involves two major steps.

Step 1: M_{Eval} upon receiving the packet from a message transmitter forwards it to the transport layer, where trustworthiness against the node is performed. If the entity is not reliable, then the distrust for the sender node is computed and message is discarded.

Step 2: If the node is reliable, message is passed to the application layer to verify the received data. If data is not verified, then the message is discarded, and the distrust is computed for the sender node. However, in case of successful verification of the data, M_{Eval} accepts the message and reward the sender node with maximum trust value.

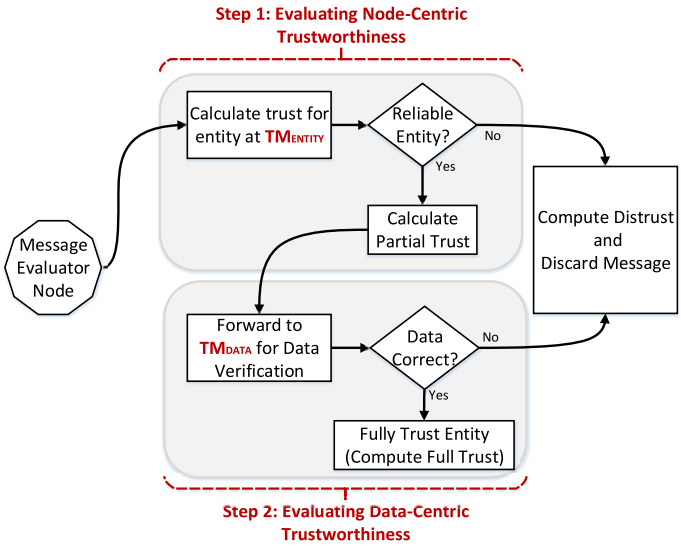


Fig. 4: Flow Chart of Proposed Trust Model

B. Operation of Proposed Trust Model

As depicted in Fig. 4, our trust model operates in two steps, i.e., TM_{ENTITY}, and TM_{DATA}.

1) TM_{ENTITY}*:* First stage of the trust model is dedicated to evaluate the entity trustworthiness at the M_{Eval}. Every M_{Eval} in the network has a specific range, i.e., M_{TR}. According to [40], M_{TR} depends directly upon (1) the distance $(Dist_{M_{Eval}}^{M_{Sender}})$ between M_{Eval} and message sender (M_{Sender}), (2) antenna height (h_t) of M_{Sender}, and (3) antenna height (h_r) of M_{Eval}. In a delay-sensitive network like VANET, a slight change in the antenna position and height can distort the signal strength, which ultimately results in a signal loss [41], [42]. This directly impacts the M_{TR} and the neighbouring vehicles may be unable to receive the transmitted messages in time. Based on this information, we define M_{TR} as follows:

$$M_{TR} = \sqrt{\left(Dist_{M_{Eval}}^{M_{Sender}}\right)^2 + (h_t + h_r)^2} \quad (1)$$

Next, M_{Eval} performs an initial check on the received message based on this M_{TR}. If received message is from outside of the M_{TR}, the message is dropped and classified

as malicious. However, for every message received within the M_{TR}, M_{Eval} will check the presence of the (M_{Sender}) within its database, i.e., Veh_{DB}, across its ID, i.e., ID_{Node}. For every past encounter with vehicles, M_{Eval} keeps record of the behaviour based on the trustworthiness of the transmitted message. For every previous good behaviour and message transmission, M_{Eval} always provides a positive rating and for malicious transmission a negative rating is assigned. If the vehicle resides in the Veh_{DB}, then M_{Eval} checks its trust value (T_{Value}). If the T_{Value} surpasses the minimum trust threshold ($T_{Threshold}$) level, then M_{Eval} forwards the data towards the application layer, where, the trust is evaluated against the received data, i.e., TM_{DATA}. Further, M_{Eval} increments the T_{Value} of the message transmitter by a value of $\alpha_{Partial}$. If the T_{Value} of the received message is below $T_{Threshold}$, then the M_{Eval} directly classify the message as malicious, and provides a minimum trust value (TV_{min}) to the message sender, in order to discourage the sender to transmit compromised and malicious messages in future.

However, for vehicles encountering with the M_{Eval} for the first time, an entry (ID_{Node}) is created within Veh_{DB} for the new vehicle. Further, M_{Eval} assigns an initial trust value ($Trust_{Initial}$) to new vehicles, and forwards the message towards TM_{DATA} for data verification.

It is worth mentioning here that message transmitter receives full reward only, if it satisfies trust conditions in both step 1 (TM_{ENTITY}) and step 2 (TM_{DATA}). Algorithm 1 shows the algorithm for trust calculation at stage 1, i.e., TM_{ENTITY}.

Algorithm 1: Trust Calculation at TM_{ENTITY}

Result: Trust Calculation at TM_{ENTITY}
Required: Message = M; Node ID = ID_{Node}; Database = $Veh_{Database}$; Trust Value = T_{Value}; Minimum Trust Value = TV_{min}; Initial Trust Value = $Trust_{Initial}$; Trust Threshold = $T_{Threshold}$; Message Threshold Range = M_{TR}; Partial Reward = $\alpha_{Partial}$

```
if (M ∈ M_TR) then
    Check Node ID (ID_Node);
    if (ID_Node ∈ Veh_Database) then
        Check T_Value;
        if (T_Value ≥ T_Threshold) then
            Forward M to TM_DATA;
            T_Level = T_Level + α_Partial;
        else
            Classify as malicious node;
            T_Level = TV_min;
        end
    else
        Insert ID_Node to Veh_Database;
        Assign T_Value = Trust_Initial;
        Forward to TM_DATA;
    end
else
    Discard M;
    Insert ID_Node to Veh_Database;
    Assign T_Value = T_Min;
end
```

2) TM_{DATA}: Once, the entity is evaluated at the lower layers, the next step involves the evaluation of data at the application layer, i.e., TM_{DATA}. We define trust at this level as follows:

$$Trust = f(RoT, InfoQ, \delta) \tag{2}$$

Equation 2 depicts that $Trust$ is a function of three parameters, i.e., role-oriented trust ("RoT"), information quality ("InfoQ") and effective distance ("δ"). As the data is being evaluated at this layer, therefore, the trust function must take into account the information quality and the geographical information provided by the vehicles. Further, RoT is integrated within the network to maintain minimum trust level. Based on this information, equation 2 can be further expended as:

$$Trust = \sqrt{InfoQ + (RoT \times \sqrt{\frac{\delta}{3}})} \tag{3}$$

Role-oriented Trust (RoT): RoT corresponds to such vehicles, whose information is regarded as highly trusted. Every vehicular network incorporates such vehicles within its network at most of the times. These include police, taxis and ambulances, to name a few. In order to incorporate the information from such vehicles, our trust management scheme integrates RoT in order to provide higher weight to the information disseminated by such vehicles. Therefore, the presence of following four classes of vehicles (Veh) are considered in the network. (1) *High Authority Vehicles* (Veh_{HA}): This class includes police vehicles and ambulances. Since, these vehicles are authorized from the central authority, therefore, the information generated by these vehicles is highly trusted. (2) *Public Transport Vehicles* (Veh_{PT}): includes public buses and local council supported taxis. The information is considered as highly authentic as these are authorized by a specific governmental department such as department of transportation. (3) *Professional Vehicles* Veh_{Pro}: represents private car-hire vehicles and drivers having high experience of travel within the network. (4) *Traditional Vehicles* Veh_{Trad}: are vehicles with minimum or no travel history. For first three classes, higher RoT trust values are assigned, while for the last class, we assign low weights. These vehicles have to gain trust of the participating vehicles in order to be able to have impact within the network. We calculate RoT using equation 4:

$$RoT = \eta \times Trust(t-1) \tag{4}$$

where η is the weight assigned to the information generated by the vehicles. For the first three classes of the vehicles (Veh_{HA}, Veh_{PT}, Veh_{Pro}), higher weights are assigned, and for traditional vehicles (veh_{Trad}), lower weights are assigned, i.e.,

$$\eta = \begin{cases} 0.8 \leq \eta \leq 1.0 & \text{if } veh = Veh_{HA}, Veh_{PT}, Veh_{Pro} \\ 0.5 \leq \eta < 0.8 & \text{if } veh = Veh_{Trad} \end{cases} \tag{5}$$

Once, η is calculated using equation 5, the overall RoT is calculated via equation 4. We summarize the process of assigning weight to RoT-factor in Algorithm 2.

Algorithm 2: Weight Calculation for RoT

Result: Weight Calculation for RoT
Required: Message = M; vehicle type = veh; High Authority vehicles (veh_{HA}); Public transport vehicles veh_{PT}; Professional vehicles veh_{Pro}; Traditional vehicles veh_{Trad}; weight η;
Get vehicle type (veh);
if *((veh) =* veh_{HA} *or* veh_{PT} *or* veh_{Pro} *)* **then**
  $0.8 \leq \eta \leq 1.0$;
else
  $0.5 \leq \eta < 0.8$;
end

Effective Distance: Once, the message (M) is received at the application layer, M_{Eval} calculates the effective distance (δ) based on the tier-based approach. Specifically, three distant levels (i.e., tier-1, tier-2, and tier-3) are identified between M_{Eval} and M_{Sender} to incorporate geographical parameters. In order to calculate δ, M_{Eval} first calculates the actual distance for the received message based on the Euclidean distance, i.e.,

$$Dist = \sqrt{(M_{Eval_x} - M_{Sender_x})^2 + (M_{Eval_y} - M_{Sender_y})^2} \tag{6}$$

In above equation, M_{Eval_x} and M_{Eval_y} represents the x and y coordinates of M_{Eval}, while M_{Sender_x} and M_{Sender_y} corresponds to resulting x and y coordinates of event generator, i.e., M_{Sender}.

Further, we define a parameter 'ξ' as tier-boundary. As depicted in Fig. 5, we defined three tiers between M_{Eval} and event generator, thus resulting in three tier-boundaries between M_{Eval} and the event generator, namely, ξ_1, ξ_2 and ξ_3. Further, $\xi_1 = \frac{M_{TR}}{3}$, $\xi_2 = (\xi_1 + \frac{M_{TR}}{3})$ and $\xi_3 = (\xi_2 + \frac{M_{TR}}{3})$. Based on these tier-boundaries, we assign following value to distance parameter (δ), i.e.,

$$\delta = \begin{cases} 1 & \text{if } 0 < Dist \leq \xi_1 \\ \frac{\delta}{2} & \text{if } \xi_1 < Dist \leq \xi_2 \\ 0 & \text{if } \xi_2 < Dist \leq \xi_3 \end{cases} \tag{7}$$

Information Quality (InfoQ): $InfoQ$ corresponds to the quality of the information generated by the event generator as proposed by ETSI [25]. $InfoQ$ directly relies on the distance of the M_{Eval} and event generator. Greater the distance between M_{Eval} and event generator, low value of the $InfoQ$ is assigned by the M_{Eval}. This value increases as the distance between the M_{Eval} and event generator decreases. As our model has three tiers (depicted in Fig. 5), we can co-relate and translate $InfoQ$ according to the distance parameter δ. i.e., if the event generator lies within first tier, high weights for $InfoQ$ are assigned, while, it decreases for tier-2 and tier-3 event generators as the distance between them and the M_{Eval} increases. For every message arriving from outside of the M_{TR}, '0' is assigned as the M_{Eval} is unknown about the event generator. We assign following values to $InfoQ$ based on our tier-based topology according to eq. 8.

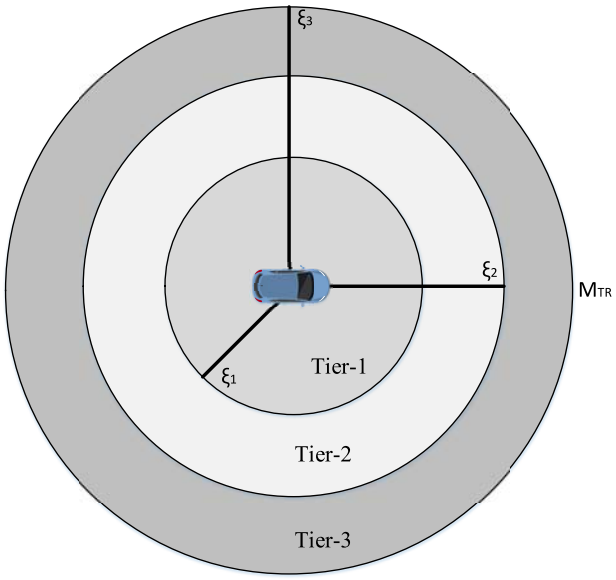


Fig. 5: Tier-based Threshold Approach

$$InfoQ = \begin{cases} 1 & \text{if } 0 < d \leq \xi_{1/2} \\ 0.833 & \text{if } \xi_{1/2} < d \leq \xi_1 \\ 0.666 & \text{if } \xi_1 < d \leq \xi_{2/2} \\ 0.500 & \text{if } \xi_{2/2} < d \leq \xi_2 \\ 0.333 & \text{if } \xi_2 < d \leq \xi_{3/2} \\ 0.167 & \text{if } \xi_{3/2} < d \leq \xi_3 \\ 0 & \text{if } d \geq \xi_3 \end{cases} \tag{8}$$

C. Trust Decision

Once, the desired parameters $(RoT, \delta, InfoQ)$ are calculated using equations 4, 7 and 8, the M_{Eval} calculates trust using equation 3. In case, the M_{Eval} accepts the data of the sender, M_{Eval} increments the trust level of the sender with a factor of α, and decrements it in the same fashion with a factor of β for distrust, i.e.,

$$Trust_{Level} = \begin{cases} T_{Value} + \alpha & \text{if } T_{Level} \geq T_{Threshold} \\ T_{Value} - \beta & \text{if } T_{Level} < T_{Threshold} \end{cases} \tag{9}$$

In above equation, α is the full reward given by M_{Eval} to M_{Sender} for his honesty and providing true content. Similarly, β is the punishment provided by M_{Eval} for malicious content. α and β have relative values and their values can be dependent on the considered application. In our case, we design trust model to ensure propagating trusted messages, therefore, we assign higher weights to α than β to encourage legitimate nodes to keep providing true content and discouraging dishonest nodes to share malicious content in future. Further, we

adapted a phenomenon that trust is very hard to gain, therefore, we modelled α and β according to equation 10.

$$\frac{\beta}{\alpha} = 10 \tag{10}$$

The selection of α and β are user-defined and it depends on the user requirement within the network [43]. Strictness of this criterion will result in the propagation of higher number of trusted messages in the network. However, relaxing this criterion will enable the vehicles to receive messages, which may be generated from dishonest vehicles.

V. Performance Evaluation

A. Simulation Scenario

We evaluated the performance of our proposed trust model using VEINS, a popular open-source simulator to model different components of vehicular networks [44], [45]. We validated our proposal on a real map from the city of Derby, United Kingdom, which we extracted from OpenStreetMap [46], [47] as shown in Fig. 6. We placed five RSUs at fixed locations in the network, which only disseminate the messages over large distances. Further, we generated the mobility of 100 vehicles in this network via SUMO, which is enough for many urban scenarios [48].

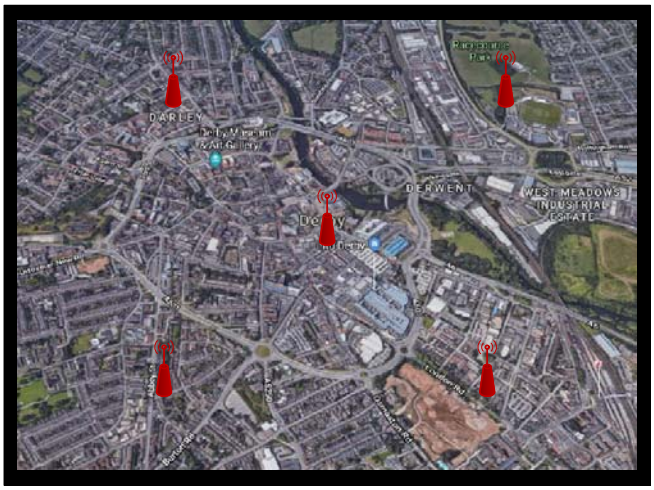


Fig. 6: Simulated Map of Derby, United Kingdom

In order to evaluate the efficiency of our trust model, a safety-related event (accident) is generated at a random location within the network. Every node is able to receive this information which is generated by the first available node in the network. Next, we introduced malicious nodes in the network to evaluate the efficiency of the trust model to tackle the attacker behaviour. Initially, we considered 5% malicious nodes in the network which are sharing compromised messages with its neighbours. We then increased the proportion of malicious nodes step-wise to 40% to study the efficiency of trust model in detecting true content in the network.

In our simulations, legitimate vehicles are equipped with our proposed trust model, thus enabling them to validate the authenticity and trustworthiness of the generated event. Further, the antenna height (h_t and h_r) of the message transmitting and message receiving vehicles is kept constant, i.e., 1.895 m. In our model, this information regarding h_t and h_r is always piggybacked along with the message, so that the receiver can detect the messages transmitted by the vehicle. Moreover, a Two-Ray Interference radio propagation model is used in our simulations [40].

Every simulation scenario has twenty-five runs with random seed value to ensure unique initial vehicle assignment in the network. Furthermore, the experimental results for every scenario is also generated by averaging over twenty-five runs. The details of simulation are listed in Table III.

TABLE III: Simulation Details

Parameters	Details
Simulation Time (secs)	600 secs
Simulation Area (km × km)	4km × 2.5km
Vehicles Distribution	Random
Total Vehicles	100
RoT Vehicles (%)	5
Total RSUs	5
Total Dishonest Vehicles (%)	5, 10, 15, 20, 25, 30, 35, 40
MAC Protocol	IEEE 802.11p
Network Protocol	WAVE
Radio Propagation Model	Two-Ray Interference
h_t (m)	1.895
h_r (m)	1.895
Packet Size (Data + Header)	1280 (1024 + 256) bits
$Trust_{Initial}$	0.5
$Trust_{Threshold}$	0.5, 0.55, 0.6, 0.65, 0.7
α	0.01
β	0.1

B. Evaluation Metrics

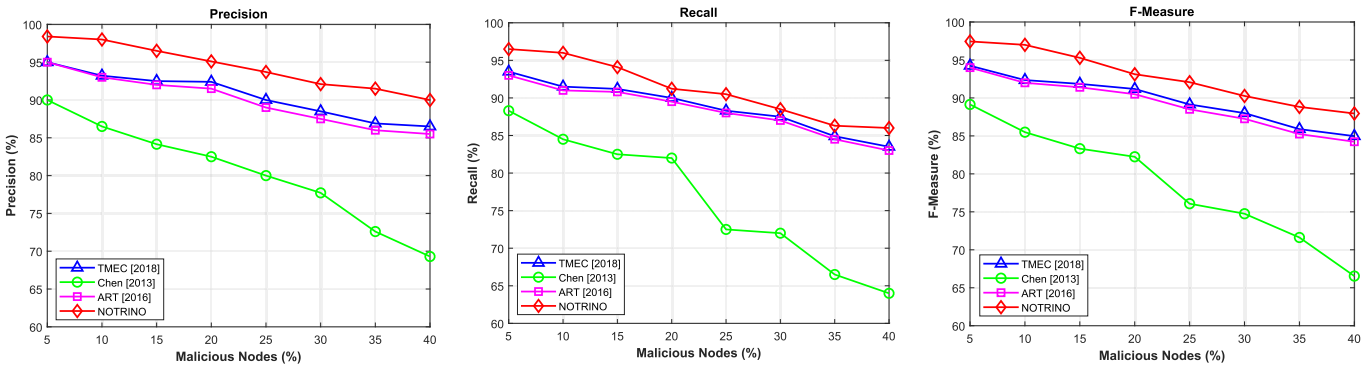
We chose following three significant trust evaluation criteria to evaluate the efficiency of our proposed trust model, i.e., (1) How accurate is the trust model, (2) How many true events the trust model can detect? and (3) How trusted information is disseminated in the network [49]. To satisfy these trust evaluation criteria, we use following metrics:

- *Precision* – when trustworthy event is predicted, how often it is predicted correctly. Let $P_{A|H}$ illustrates the probability of the node to detect as an attacker, given the legitimate node and $P_{A|A}$ represents the probability to detect node as an attacker, given an attacker, then Precision (P) can be given as:

$$P = \frac{P_{A|A}}{P_{A|H} + P_{A|A}} \tag{11}$$

- *Recall* – when the event is actually trustworthy, how often trust model predicts it. Let $P_{A|A}$ presents the probability of trust model to detect node as an attacker, given node is an attacker and $P_{H|A}$ resents probability of detecting malicious node as legitimate node, given the node is an attacker, then Recall (R) can be mathematically expressed as:

$$R = \frac{P_{A|A}}{P_{H|A} + P_{A|A}} \tag{12}$$



(a) (b) (c)

Fig. 7: Accuracy of Proposed Trust Model under MiTM attacks (a) Precision (b) Recall (c) F-Measure

- *F-Measure* – overall, how often event (i.e., accident) classification is correct. F-Measure is given as:

$$F - Measure = 2 \times \left[\frac{P \times R}{P + R}\right] \tag{13}$$

- *Trust Metric* – A significant metric elaborating the ability of trust model to classify received messages as trustworthy or malicious. Let 'α' is the reward assigned to the legitimate sender for their honesty, and 'β' is the corresponding punishment factor awarded to the attacker, then trust factor (T) can be given as:

$$T = \begin{cases} T + \alpha & \text{if } T \geq Trust_{Threshold} \\ T - \beta & \text{if } T < Trust_{Threshold} \end{cases} \tag{14}$$

- *Variation of Trust in Legitimate Nodes* – Depicts, how trust changes for legitimate nodes, in presence of dishonest nodes disseminating malicious data, and
- *Variation of Trust in Dishonest Nodes* – how strictly trust model ensures minimum trust level of dishonest nodes.
- *End-to-End (E2E) Delay* – The Quality-of-Service (QoS) related metric indicating the time taken by the packets to reach the destination. Since, very sensitive data is present in VANET, therefore packets should be shared with legitimate nodes with minimum possible E2E delays. Let $T_{Generated}$ is the packet generated time and $T_{Arrival}$ depicts the time of packet arrival at the destination, then E2E delay can be given as:

$$E2E\ Delay = T_{Arrival} - T_{Generated} \tag{15}$$

- *Packet Detection Rate vs Trust Threshold* – ability of trust model to detect true packets against different threshold levels of trust.

VI. Simulation Results

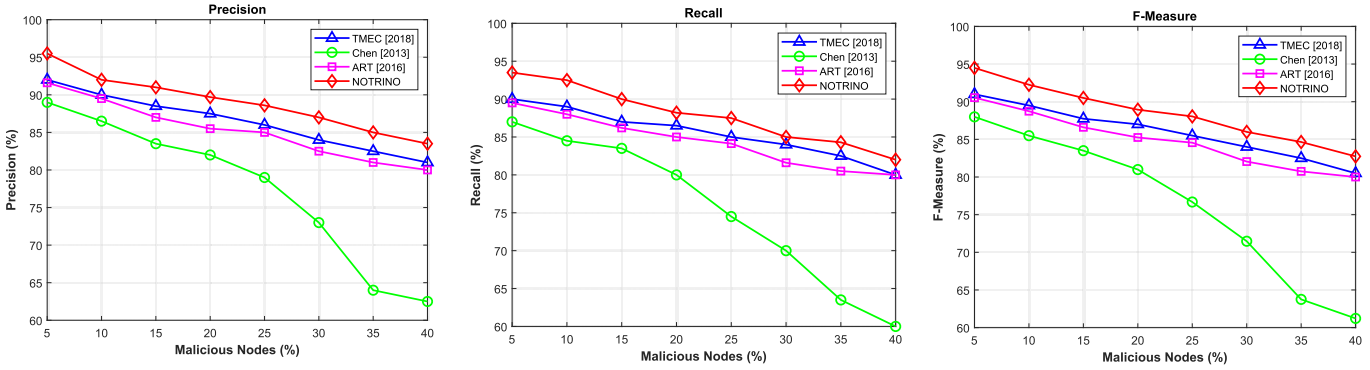
We compared the efficiency of our trust model with three baseline trust management schemes, i.e., ART [29], Chen [50] and TMEC [51]. We chose these trust models as they are hybrid in nature, i.e., they not only evaluate trust on node, but also relies on data trustworthiness for trust calculations.

A. Accuracy of Trust Model under MiTM Attacks

Fig. 7 depicts the accuracy of NOTRINO against MiTM attacks, where the attacker is changing the content of the safety messages and polluting the network with malicious and compromised messages. Fig. 7a and Fig. 7b shows precision and recall of NOTRINO and baseline trust models for a network where the quantity of MiTM attackers are increased from 5% to 40%. It depicts that high precision and recall values are achieved for low number of MiTM attackers. However, as the quantity of MiTM attackers are increased in the network, both precision and recall decreases, as expected due to the fact that MiTM pollutes the network with malicious content, hence limiting the ability of the legitimate vehicles to classify between true and malicious content. However, compared to the baseline trust models, NOTRINO ensures high precision and recall even in presence of high number of MiTM attackers, illustrating that our proposal is efficient in coping and dealing with MiTM attackers. There are two main reasons behind this efficiency. (1) First, NOTRINO quickly detects dishonest nodes at the lower layer, thus, messages are revoked and stopped being further disseminated in the network. (2) Second, integrated RoT trust scheme ensures that legitimate vehicles in the network receive trusted content, even in presence of adversaries. Further, comparing to baseline trust models, NOTRINO achieves high accuracy of detecting MiTM attacks as illustrated by F-Measure in Fig. 7c. For instance, NOTRINO ensures accuracy over 90%, while baseline trust model achieves F-score, less than 87.5% for a network with 15% MiTM adversaries.

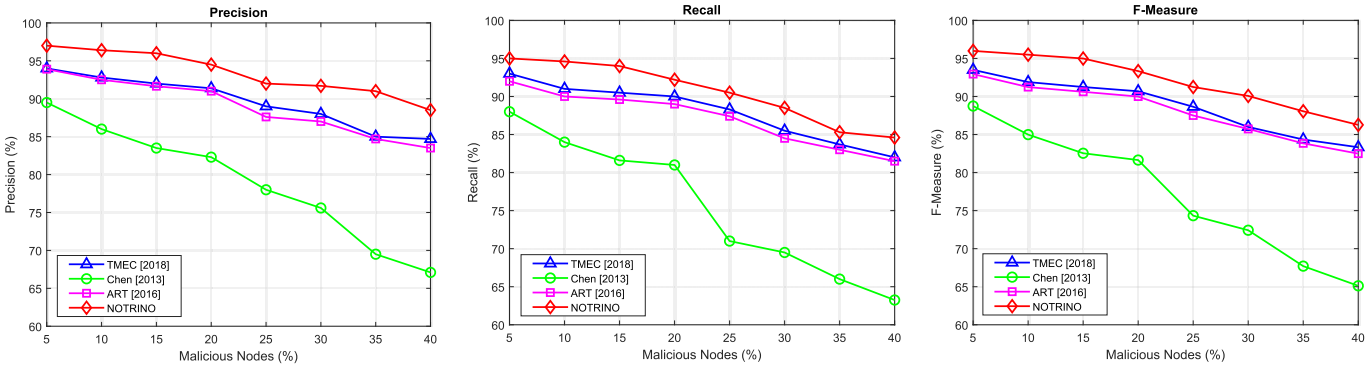
B. Accuracy of Trust Model under Zig-zag Attacks

Fig. 8 shows the accuracy of the proposed trust model in terms of precision, recall and F-Measure respectively for an advanced attack, i.e., zig-zag attacks where attackers randomly change their behaviour in order to deceive legitimate vehicles. When such dishonest nodes are introduced within the network, the accuracy decreases significantly in terms of precision and recall as shown in Fig. 8a and Fig. 8b. This is due to the fact that these malicious vehicles can dominate the network, thus limiting the ability of the legitimate vehicles by introducing more and more malicious data in the network. However,



(a) (b) (c)

Fig. 8: Accuracy of Proposed Trust Model under zig-zag attacks (a) Precision (b) Recall (c) F-Measure



(a) (b) (c)

Fig. 9: Accuracy of Proposed Trust Model under combined attacks (a) Precision (b) Recall (c) F-Measure

NOTRINO achieves high accuracy compared to the baseline trust models, i.e., high precision and recall can be achieved via our method. For instance, for a network with 35% malicious nodes, the precision and recall achieved via our trust model is nearly 85%. The main reason behind achieving this accuracy is the integration of role-oriented trust management scheme which can ensure the propagation of trusted information in the network by identifying malicious vehicles and their content. Finally, Fig. 8c shows F-Measure of the trust models which is one of the significant metrics to measure the accuracy of the trust model. As shown in Fig. 8a and Fig. 8b, varying the number of malicious nodes can affect the overall performance of VANET. Therefore, F-Measure can show that how accurate is the trust model. The results suggest that compared to baseline trust models, the proposed trust model can achieve high accuracy in terms of F-Measure, i.e., in presence of 40% malicious nodes, our trust model ensures accuracy of 82.7%, while the baseline trust model achieves accuracy of less than 80%.

C. Accuracy of Trust Model under Combined Attacks

We also validated the performance of NOTRINO by considering a scenario where both MiTM and zig-zag attackers are present in the network. In this scenario, both MiTM and zig-zag attackers are kept in equal proportion within the network. Fig. 9 shows the efficiency of NOTRINO in operating efficiently in presence of combined attackers, where it achieves higher precision, recall and respective F-Measure. NOTRINO achieves higher accuracy as compared to baseline trust models for a small number of malicious nodes in the network. However, as the network is polluted with high number of combined attackers, accuracy in terms of precision, recall and F-Measure decreases for all trust models. For a network with 30% attackers, NOTRINO ensures an accuracy of nearly 90% as compared to baseline trust models, where it falls below 86%.

D. Impact of Node Density on Trust Models

We also conducted experiments to evaluate the performance of NOTRINO based on various legitimate vehicles within the network. Fig. 10 depicts the precision, recall and F-Measure of NOTRINO, for a network containing different legitimate vehicles. As shown, the smaller number of legitimate vehicles generates a smaller number of trusted contents within the network. However, as the network experience more legitimate vehicles, respective precision, recall and F-measure increases. This is due to the fact that more and more legitimate vehicles will be present in order to disseminate trusted content in the network. However, comparing to baseline trust models, NOTRINO performs better even for a network containing low number of legitimate vehicles. This is true because our proposal integrates RoT trust scheme, which ensures the

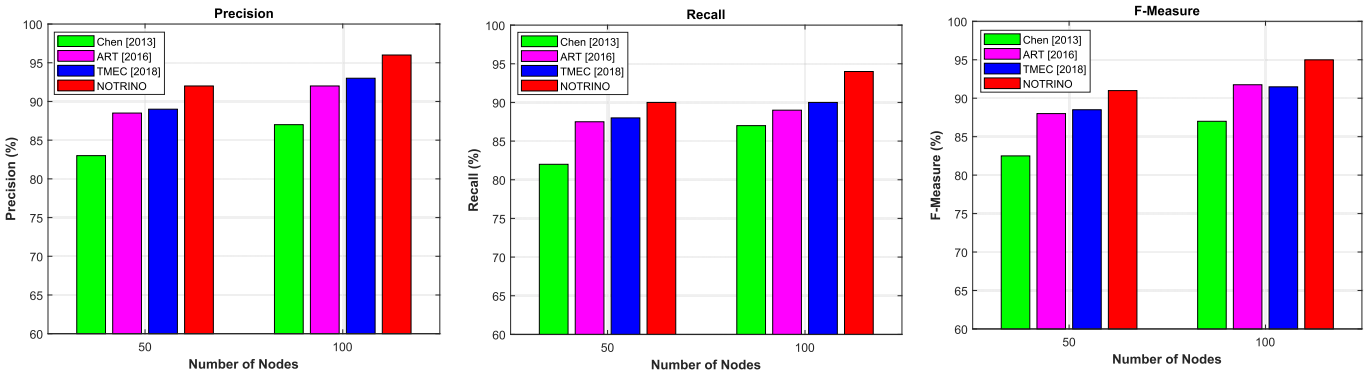


Fig. 10: Impact of Node Density on Trust Models (a) Precision (b) Recall (c) F-Measure

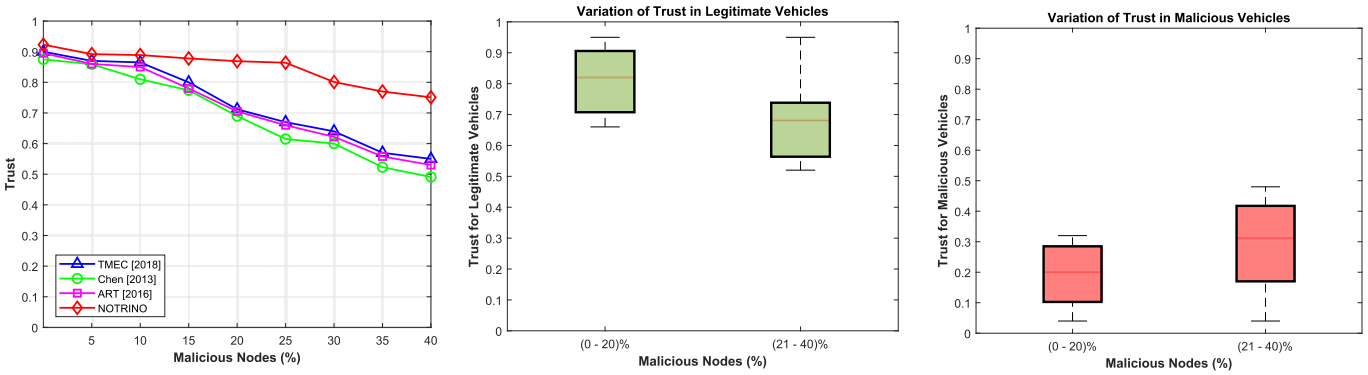


Fig. 11: (a) Trust Metric (b) Trust Variation for Legitimate Nodes (c) Trust Variation for Malicious Nodes

propagation of trusted content within the network. For a network with 50 legitimate nodes, NOTRINO achieves over 90% accuracy in terms of F-measure. This increases to 95% if the number of legitimate nodes are doubled within the network, illustrating the high efficiency of our proposal.

E. Impact of Trust on Legitimate and Dishonest Nodes

Fig. 11a depicts the behaviour of trust metric in the network for our trust model, bench-marked against three baseline methods. It can be seen that our proposed TM ensures high trust values, as compared to other trust models. This is due to the presence of role-oriented vehicles in the network which ensures the propagation of trusted information in the network. Further, we can see that trust decreases with the increase of malicious nodes. As these nodes generate malicious content by compromising the original content of the messages, therefore, the overall trust decreases. Compared to bench-marked trust models, our proposed trust model maintains high trust metric for high number of malicious nodes. For instance, for the network with 40% malicious nodes, our trust model achieves trust metric of about 75% level, while, the metric for bench-marked trust models is below 60%.

Further, we also plotted the behaviour and variation of trust metric for both legitimate and malicious nodes in Fig. 11b and Fig. 11c. We can see from Fig. 11c, that for a network with low malicious (0% - 20%) and high malicious (21% - 40%) nodes, the trust is always below the trust threshold, i.e., 0.5. This ensures that a very low number of false negatives are generated through our proposal. On the other hand, the trust for legitimate vehicles is always higher than the trust threshold, thus assuming that few false positives are generated in the network.

F. Packet Detection Rate vs Trust Threshold

Fig. 12 depicts the comparison of trust threshold on the overall packet detection rate of the network. Clearly, our pro-

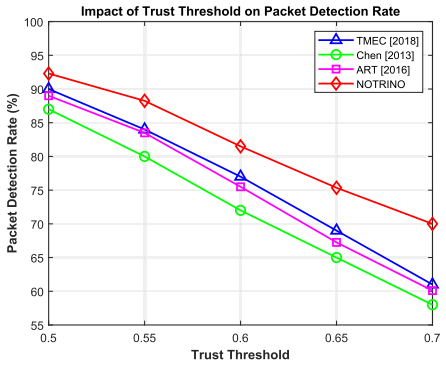


Fig. 12: Impact of Trust Threshold on Packet Detection Rate

posal ensures higher detection rates for different trust threshold as compared to baseline methods where the increasing trust threshold reduces the packet detection rates. It should be noted that increasing trust threshold will reduce the overall packet detection rates as the criteria to classify the message as trustworthy will be stricken. However, our trust model performs better even for higher trust threshold, i.e., about 70% packets can be detected through our trust model for threshold level of 0.7. On the other hand, baseline methods achieve less than 60% packet detection rate, if trust threshold is set to 0.7.

G. Impact of Time on Trust Model

In this paper, we evaluated the time parameter within the VANET from the perspective of end-to-end (E2E) delay. Fig. 13 shows the overall E2E delay of NOTRINO, compared to other baseline trust models. It shows that all the baseline trust models achieve high E2E delay when malicious nodes are introduced in the network. Especially, this E2E delay is high when the network is polluted with high number of malicious nodes. On the other hand, NOTRINO ensures lower E2E delays even if the network is polluted with high number of malicious nodes. This is due to the reason that our proposed trust model operates in two stages, therefore, if the entity is classified as malicious, the content is revoked from the network, therefore, enabling the other vehicles to access the correct information with minimum delays. Fig. 13 depicts that NOTRINO achieves E2E delays of less than 1.5 seconds, while the baseline trust models achieve E2E delay of more than 2 seconds. As stated earlier, VANET propagates sensitive information among its peers, therefore, the network must guarantee minimum E2E delays in the network [52].

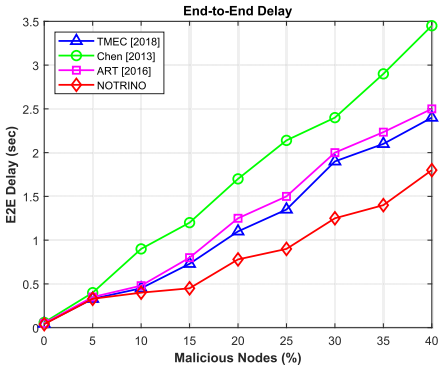


Fig. 13: End-to-End Delay

VII. Conclusion

Disseminating accurate, authentic and trusted information is of paramount importance within IoV environment. Due to open nature of IoV, adversaries can also be part of the network which mostly aim to distribute compromised information among network nodes. To solve this issue, we proposed NOTRINO, a novel hybrid trust model for IoV. NOTRINO operates in two steps to efficiently revoke not only the dishonest nodes, but also its compromised messages. Extensive simulations are carried out to validate our proposal. Simulation results depicted that NOTRINO performs better than other hybrid benchmarked trust models in terms of achieving better precision, recall, F-Measure, event detection probability, and efficiently detecting and classifying messages as trustworthy or malicious. This is due to the fact that NOTRINO enables the participating nodes to efficiently identify dishonest nodes at the lower layer. This enables the nodes within the network to quickly detect and classify nodes as legitimate or dishonest in short duration of time.

Our future step includes the integration of social networks with NOTRINO, which is one significant source of providing information within IoV.

References

[1] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. Lin, and X. Liu, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016, doi:10.1109/ACCESS.2016.2603219.

[2] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, Sep. 2017, doi:10.1109/MCOM.2017.1600514.

[3] C. A. Kerrache, N. Lagraa, R. Hussain, S. H. Ahmed, A. Benslimane, C. T. Calafate, J. Cano, and A. M. Vegni, "TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles," *IEEE Internet of Things Journal*, pp. 1–1, 2019, doi:10.1109/JIOT.2018.2880332.

[4] F. Sakiz and S. Sen, "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017, doi:10.1016/j.adhoc.2017.03.006.

[5] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional Privacy-Preserving Authentication Using Registration List in Vehicular Ad Hoc Networks," *IEEE Access*, vol. 6, pp. 2241–2250, 2018, doi:10.1109/ACCESS.2017.2782672.

[6] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-oriented Overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[7] F. Ahmad, A. Adnane, C. A. Kerrache, V. N. L. Franqueira, and F. Kurugollu, "Trust Management in Vehicular Ad-Hoc Networks and Internet-of-Vehicles: Current Trends and Future Research Directions," in *Global Advancements in Connected and Intelligent Mobility: Emerging Research and Opportunities*, F. Outay, A.-U.-H. Yasar, and E. Shakshuki, Eds. IGI Global, 2019, pp. 135–165, doi:10.4018/978-1-5225-9019-4.ch004.

[8] J. Grover, M. S. Gaur, and V. Laxmi, "Trust Establishment Techniques in VANET," in *Wireless Networks and Security, Signal and Communication Technology*, S. Khan and A.-S. Khan Pathan, Eds. Springer, 2013, pp. 201–213, doi:10.1007/978-3-642-36169-2_8.

[9] H. El-Sayed, M. Chaqfeh, H. El-Kassabi, M. A. Serhani, and H. Alexander, "Trust Enforcement in Vehicular Networks: Challenges and Opportunities," *IET Wireless Sensor Systems*, 2019.

[10] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 6, pp. 28 643–28 660, May 2018, doi: 10.1109/ACCESS.2018.2837887.

[11] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. Rezazadeh Baee, and S. Mandala, "Trust Management in Vehicular Ad Hoc Network: A Systematic Review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 146, May 2015.

[12] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, Feb 2019, doi:10.1109/TITS.2018.2818888.

[13] N. Fan and C. Q. Wu, "On Trust Models for Communication Security in Vehicular Ad-Hoc Networks," *Ad Hoc Networks*, August 2018, doi:10.1016/j.adhoc.2018.08.010.

[14] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310–3322, 2020.

[15] N. Yang, "A Similarity based Trust and Reputation Management Framework for VANETs," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 2, pp. 25–34, 2013.

[16] F. G. Mrmol and G. M. Prez, "TRIP, a Trust and Reputation Infrastructure-based Proposal for Vehicular Ad Hoc Networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934 – 941, 2012, doi:10.1016/j.jnca.2011.03.028.

[17] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3657–3674, Aug 2015.

[18] U. Khan, S. Agrawal, and S. Silakari, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks," in *International Conference on Information and Communication Technologies (ICICT)*. Elsevier, December 2014, pp. 965 – 972.

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

[20] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-based Trust Model for Vehicle-to-Everything (V2X)," *IEEE Internet of Things Journal*, pp. 1–1, 2019, doi:10.1109/JIOT.2019.2950083.

[21] S. Gurung, D. Lin, A. C. Squicciarini, and E. Bertino, "Information-Oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks." in *7th International Conference on Network and System Security (NSS)*. Springer, June 2013, pp. 94–108.

[22] R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware Trust Model for Vehicular Ad-hoc Networks," *Security and Communication Networks*, vol. 7, no. 11, pp. 1652–1669, 2014.

[23] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust On the Security of Wireless Vehicular Ad-hoc Networking," *Ad Hoc & Sensor Wireless Networks*, vol. 24, pp. 283–305, 2014.

[24] C. A. Kerrache, C. T. Calafate, N. Lagraa, J. C. Cano, and P. Manzoni, "Trust-Aware Opportunistic Dissemination Scheme for VANET Safety Applications," in *International IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, July 2016, pp. 153–160.

[25] ETSI EN 302 637-3 v1.2.1, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service (2014-09)," ETSI, Tech. Rep., 2014.

[26] T. Gazdar, A. Belghith, and H. Abutair, "An Enhanced Distributed Trust Computing Protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, October 2017, doi:10.1109/ACCESS.2017.2765303.

[27] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular Security Through Reputation and Plausibility Checks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 384–394, June 2014, doi:10.1109/JSYST.2013.2245971.

[28] S. Ahmed and K. Tepe, "Using Logistic Trust for Event Learning and Misbehaviour Detection," in *IEEE 84th Vehicular Technology Conference (VTC-Fall)*. IEEE, Sept 2016, pp. 1–5.

[29] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, April 2016.

[30] R. Shrestha and S. Y. Nam, "Trustworthy Event-Information Dissemination in Vehicular Ad Hoc Networks," *Mobile Information Systems*, p. 16 pages, November 2017, doi:10.1155/2017/9050787.

[31] A. Mehmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A Hybrid Trust Management Heuristic for VANETs," in *PerVehicle'19 - 1st International Workshop on Pervasive Computing for Vehicular Systems*. IEEE, 2019, pp. 748–752.

[32] G. Hatzivasilis, O. Soultatos, S. Ioannidis, G. Spanoudakis, G. Demetriou, and V. Katos, "MobileTrust: Secure Knowledge Integration in VANETs," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 2, 2019.

[33] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET," *Sensors*, vol. 19, no. 11, 2019, doi:10.3390/s19224954.

[34] W. B. Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, "The Impact of Malicious Nodes Positioning on Vehicular Alert Messaging System," *Ad Hoc Networks*, vol. 52, pp. 3 – 16, 2016, doi:10.1016/j.adhoc.2016.08.008.

[35] F. Ahmad, A. Adnane, and V. N. L. Franqueira, "A Systematic Approach for Cyber Security in Vehicular Networks," *Journal of Computer and Communications*, vol. 4, pp. 38–62, December 2016.

[36] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-preserving Authentication Scheme in Vehicular Ad-hoc Networks," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2019.

[37] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: Reputation System-based Lightweight Message Authentication Framework and Protocol for 5G-enabled Vehicular Networks," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[38] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies," *Sensors*, vol. 18, no. 11, 2018, doi:10.3390/s18114040.

[39] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[40] C. Sommer and F. Dressler, "Using the Right Two-Ray Model? A Measurement based Evaluation of PHY Models in VANETs," in *17th ACM International Conference on Mobile Computing and Networking (MobiCom 2011), Poster Session*. Las Vegas, NV: ACM, September 2011.

[41] D. Eckhoff, A. Brummer, and C. Sommer, "On the Impact of Antenna Patterns on VANET Simulation," in *2016 IEEE Vehicular Networking Conference (VNC)*, Dec 2016, pp. 1–4.

[42] S. Kaul, K. Ramachandran, P. Shankar, S. Oh, M. Gruteser, I. Seskar, and T. Nadeem, "Effect of Antenna Placement and Diversity on Vehicular Network Communications," in *4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2007, pp. 112–121.

[43] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Intelligent Agents in Mobile Vehicular Ad-Hoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty," in *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, vol. 2, Aug 2010, pp. 243–247.

[44] Veins, "Vehicles in Network Simulation, The Open Source Vehicular Simulation Framework," available online: http://veins.car2x.org (Accessed: 29th January, 2019).

[45] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, January 2011.

[46] OpenStreetMap, "OpenStreetMap," Available online: https://www.openstreetmap.org (Accessed: 29th January, 2019).

[47] M. Haklay and P. Weber, "OpenStreetMap: User-Generated Street Maps," *IEEE Pervasive Computing*, vol. 7, no. 4, pp. 12–18, Oct 2008, doi: 10.1109/MPRV.2008.80.

[48] D. Alishev, R. Hussain, W. Nawaz, and J. Lee, "Social-Aware Bootstrapping and Trust Establishing Mechanism for Vehicular Social Networks," in *IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[49] F. Ahmad, J. Hall, A. Adnane, and V. N. L. Franqueira, "Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-hoc Network," in *Proceeding of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, June 2017, pp. 44–52.

[50] I. Chen, F. Bao, M. Chang, and J. Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, May 2014, doi:10.1109/TPDS.2013.116.

[51] J. Chen, T. Li, and J. Panneerselvam, "TMEC: A Trust Management Based on Evidence Combination on Attack-Resistant and Collaborative Internet of Vehicles," *IEEE Access*, pp. 1–1, 2018, doi:10.1109/ACCESS.2018.2876153.

[52] F. Ahmad, A. Adnane, F. Kurugollu, and R. Hussain, "A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks," in *11th IEEE Wireless Days (WD)*, 2019, pp. 1–8.