A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks

Ahmad, F., Adnane, A., Kurugollu, F. & Hussain, R.

Original citation & hyperlink:
Ahmad, F, Adnane, A, Kurugollu, F & Hussain, R 2019, A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks. in 2019 Wireless Days (WD). IEEE, Manchester, United Kingdom, United Kingdom. https://dx.doi.org/10.1109/WD.2019.8734204

DOI 10.1109/WD.2019.8734204
ISBN 978-1-7281-0117-0

Publisher: IEEE

A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks

Farhan Ahmad*, Asma Adnane†, Fatih Kurugollu* and Rasheed Hussain‡
*Cyber Security Research Group, College of Engineering and Technology, University of Derby, Derby, United Kingdom
†Department of Computer Science, Loughborough University, Loughborough, United Kingdom
‡Institute of Information Systems, Innopolis University, Innopolis, Russia
Email: *{f.ahmad, f.kurugollu}@derby.ac.uk †a.adnane@lboro.ac.uk ‡r.hussain@innopolis.ru

***Abstract*—**
Vehicular Ad-hoc NETwork (VANET) is a vital transportation technology that facilitates the vehicles to share sensitive information (such as steep-curve warnings and black ice on the road) with each other and with the surrounding infrastructure in real-time to avoid accidents and enable comfortable driving experience.

To achieve these goals, VANET requires a secure environment for authentic, reliable and trusted information dissemination among the network entities. However, VANET is prone to different attacks resulting in the dissemination of compromised/false information among network nodes. One way to manage a secure and trusted network is to introduce trust among the vehicular nodes. To this end, various Trust Models (TMs) are developed for VANET and can be broadly categorized into three classes, Entity-oriented Trust Models (ETM), Data oriented Trust Models (DTM) and Hybrid Trust Models (HTM). These TMs evaluate trust based on the received information (data), the vehicle (entity) or both through different mechanisms. In this paper, we present a comparative study of the three TMs. Furthermore, we evaluate these TMs against the different trust, security and quality-of-service related benchmarks. Simulation results revealed that all these TMs have deficiencies in terms of end-to-end delays, event detection probabilities and false positive rates. This study can be used as a guideline for researchers to design new efficient and effective TMs for VANET.

***Keywords*—Trust Models, Internet-of-Things, Smart Cities, Intelligent Transportation Systems, Vehicular Ad-hoc Network**

I. Introduction

Recently, Internet-of-Things (IoT) has evolved as an innovative computing technology connecting billions of devices with the Internet, thus resulting in numerous applications including smart cities, smart transportation, smart e-healthcare and smart industries [1]. Vehicular Ad-hoc NETwork (VANET) is a fundamentally important transportation technology, complemented by IoT, and is poised to improve traffic efficiency and safety. In VANET, vehicles equipped with different sensors, computation, and communication technologies which intelligently share sensitive and life-saving information such as accident-avoidance, steep-curve or black-ice warnings with each other and with the infrastructure. There are fundamentally three modes of communication in VANET, i.e., Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and hybrid [2].

Ideally, information generated by the source vehicle must be shared with its neighbouring vehicles without any alteration to its content. However, vehicles highly rely on node-to-node communication in VANET, thus allowing the propagation of malicious traffic generated by dishonest vehicles. Due to the sensitive nature of the information involved in VANET, a secure and trustworthy environment is essential. However, ensuring security in VANET is very challenging due to its perceptivity to the wide range of attacks such as man-in-the-middle, Sybil, black-hole or denial-of-service [3]–[5].

To date, various solutions are proposed in the literature to guarantee VANET security. Recently, trust management is introduced as an efficient technique to secure VANET by creating a trusted environment for message propagation among vehicles. In the context of VANET, trust is defined as *the confidence which one vehicle places in another, for the accomplishment of the desired action*. Trust in the information can be calculated by vehicles based on various factors including neighbours' opinions, vehicles' reputation and their past interaction with the communicating vehicle [6]. However, due to the highly unpredictable mobility of vehicles, communication is short-lived and intermittent. Evaluating the trustworthiness of the critical message (such as steep-curve warnings) in such limited time-frame is very difficult and challenging.

Recently, various Trust Models (TMs) are proposed to evaluate the trustworthiness and authenticity of the disseminated messages in VANET. VANET integrates two revocation targets for trust management, i.e., (1) data and (2) entity. Based on these targets, TMs are broadly categorized into three classes, i.e., entity-oriented, data-oriented and hybrid trust models as depicted in Figure 1 [7], [8]. Entity-oriented Trust Models (ETMs) aim at excluding adversaries from the network by calculating trust values for the nodes (entities). Data-oriented Trust Models (DTMs), on the other hand, assess the trust of the shared messages (data), and, Hybrid Trust Models (HTMs) merge the properties of both DTM and ETM for trust management [9].

The existing TMs proposed in VANET can be placed under one of the above mentioned TM categories. These trust categories evaluate the trustworthiness of data or vehicle through different techniques. For instance, ETM mostly evaluates the trustworthiness of the received information based on the reputation of the vehicles, while DTM relies on the opinion provided by the neighbours. On the other hand, HTM calculates trust using both vehicles' reputation and neighbours'

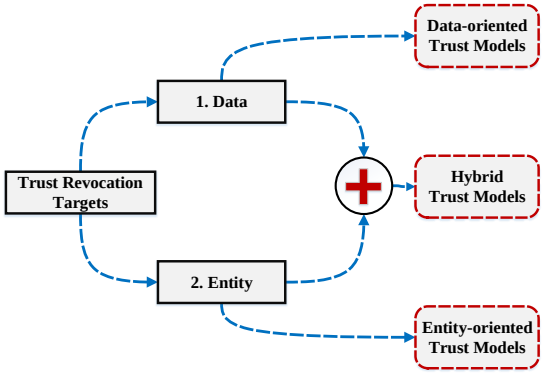

Fig. 1: Categories of Trust Models in VANET

opinion. This paper provides a detailed comparative analysis of the TMs by utilizing a simulation-based approach. The contribution of this paper is threefold. (1) We provided a detailed comparison of TMs which are designed solely for safety applications in VANET. (2) We presented a simulation-based study where we implemented and evaluated three TMs, one from each category of TM. (3) We evaluate these TMs in the presence of adversaries based on different realistic trust evaluation criteria.

The rest of the paper is organized as follows: Section II explains the related TMs in VANET. Section III provides the explanation of the compared TMs, while, simulation environment, trust metrics and simulation results are explained in Section IV. We conclude the paper in Section V.

II. Trust Management in VANET

In VANET, TMs are usually integrated within the vehicles to identify dishonest vehicles and their malicious content. As aforementioned, TMs are classified into DTM, ETM, and HTM. In this section, we outline some of the relevant TMs in VANET.

A. Data-oriented Trust Models (DTM)

As the name suggests, *"data"* is the important component in these TMs, where trust on the message (data) is computed based on the opinions generated by the neighbouring vehicles or previous interactions among the peers. Various DTM are proposed by researchers recently.

Raya et al. proposed a DTM, where Bayesian Inference (BI) and Dempster Shafer Theory (DST) are utilized to evaluate the evidence on the received events from neighbourhood [10]. This TM operates in three major phases. First, reports produced by the neighbouring vehicles are accumulated by the evaluator node (E_VN). Second, E_VN assigns weights to the received reports which depend on the spatiotemporal properties of the event. Third, E_VN forwards these reports to a decision logic module where BI and DST are utilized for trust calculation. The limitation of this technique is that trust is calculated based on the received data at the E_VN, making it inefficient for a network with high mobility.

A tier-based and analytic approach is adapted by Gazdar et al. where vehicles continuously evaluate the trustworthiness of the received data based on their direct experiences [11]. In this TM, trust is evaluated for every participating vehicle where the main purpose is to identify the pool of highly trusted vehicles and dishonest vehicles based on the data exchanged. Each vehicle maintains a trust table for its neighbours. Trust value is incremented for messages received from trusted vehicles, while it is decremented for malicious vehicles. This technique is efficient in identifying malicious vehicles as it only involves direct experiences of the participating vehicles. However, the scope of this TM is limited as it does not include any recommendations from honest vehicles regarding the event trustworthiness.

Wu et al. presented a centralized trust modelling framework for the evaluation of data by exploiting the advantages of adjacent infrastructure, Road-Side Unit (RSU) [12]. Trust is calculated at RSU based on two factors: 1) observation and 2) feedback. Vehicles detect an event and generate observations along with their confidence which depends on the distance from the event, its maximum message detection rate and the number of embedded sensors detecting the event. This observation is then shared with RSU which updates the recently observed event list. RSU evaluates the trustworthiness of the received observation by applying trust on it using the ant-colony optimization algorithm. This updated trust information is then distributed by RSU with vehicles in its vicinity. However, this approach fails in rural areas as it heavily relies on adjacent infrastructure for trust calculation.

B. Entity-oriented Trust Models (ETM)

Unlike DTMs, ETMs adopt a different technique to identify dishonest vehicles in the network. In ETM, trustworthiness is evaluated for the entity (vehicle). These TMs depend heavily on neighbouring vehicles that endorse recommendation about sender to the E_VN. To date, various ETMs have been proposed in the literature. For example, Khan et al. leveraged a cluster-based technique where Cluster Head (CH) is first elected and is liable for evaluating trust in the network [14]. In this TM, CH implements a watchdog mechanism where vehicles in its vicinity provide reports of the presence of the misbehaving vehicle. Upon detection of such vehicles, CH then informs the trusted authority (TA) who are responsible for the revocation of these vehicles in order to maintain a trusted network. However, the major constraint in this approach is the communication overhead incurred by message exchange with CH and thus reducing the efficiency of the overall network.

Similarly, Yang proposed a TM by adapting a similarity mining approach for trust calculation [15]. E_VN upon receiving the message from vehicles, calculate similarity among the received messages based on Euclidean distance, and reputation of the transmitting vehicle. Since trust is calculated using Euclidean distances locally at E_VN, this TM fails to provide any global information on the similarity of the messages.

Marmol et al. presented a centralized ETM, where trust management technique relies on the adjacent infrastructure

TABLE I: Comparison of Trust Models

Trust Model Category	Trust Models	Approach		Trust Computation Technique
		Centralized	Distributed	
Data-oriented Trust Models	Raya et al. [10]	✓		BI and DST based trust evaluations
	Gazdar et al. [11]		✓	Direct trust calculations and evaluations
	Wu et al. [12]	✓		Observation and feedback
	Kerrache et al. [13]		✓	Evaluation based on message classification
Entity-oriented Trust Models	Khan et al. [14]		✓	Clustering alongside watchdog mechanism
	Yang [15]		✓	Similarity mining approach
	Minhas et al. [16]		✓	Multi-faceted trust management
	Marmol et al. [17]	✓		Fuzzy-logic trust computation
Hybrid Trust Models	Ahmed et al. [18]		✓	Weighted voting and logistic regression
	Shretha et al. [19]		✓	Clustering and random walk
	Chen et al. [20]	✓		Attack-resistant trust model based on DST
	Dhurandher et al. [21]		✓	Reputation-based trust management

[17]. Upon receiving a message from neighbours, E_VN computes a fuzzy-based trust score which depends on three sources: (1) recommendation provided by adjacent RSU, (2) recommendation given by neighbouring vehicles, and (3) previous reputation of the sender vehicle. Once the trust score at E_VN is calculated, decision about the message is taken based on following three conditions: (1) Drop the message if not trustworthy (no trust), (2) accept the message but do not forward (+/- trust), and (3) accept the message and forward it (trust). Further, messages are also classified into three levels depending on their severity, i.e., high, medium and low. High-level messages are accepted only from the vehicles placed in 'trust' group. The other groups 'no trust' and '+/- trust' accept only medium and low-level messages. Due to its reliance on infrastructure for trust computation, this TM may not perform well in rural areas due to limited infrastructure.

C. Hybrid Trust Models (HTM)

HTMs assess the credibility of both vehicles and the exchanged information. In other words, the trust of the data is calculated by taking advantage of the vehicle's trust. However, these TMs incur high computation overhead as a result of many control messages must be evaluated in a limited time. In the following, we outline existing HTMs.

Ahmed et al. proposed an HTM where a logistic-based trust computation is utilized to identify nodes injecting false information within the network [18]. In this TM, E_VN directly observes the events. As a result, when messages are shared by the neighbouring vehicles, E_VN can identify the trustworthiness of the events. Once the true event is identified, this information is then used to classify the behaviour of the sender node as legitimate or malicious. E_VN computes trust through weighted voting and logistic trust function. This TM is efficient in identifying dishonest vehicles that propagate wrong information. However, the major limitation of this TM is its dependence on weighted voting which can be biased in case of majority of dishonest vehicles.

Another HTM is proposed by Shrestha et al. which calculates trust on the vehicles in a fully distributed manner [19]. The trust is calculated in two steps, i.e., trust is evaluated for the vehicle while and the second step involves trust calculations for the information. Trust is achieved by employing a clustering algorithm where honest and dishonest vehicles are classified into two separate groups to identify the trustworthiness of the neighbouring nodes. Next, E_VN's trust in the received message is evaluated using the modified threshold random walk algorithm. The main drawback of this scheme is the assumption of uniform distribution of dishonest nodes in the network [22]. This assumption might not be true in VANET as malicious vehicles are randomly distributed across the network.

To enhance user privacy in the network, Chen et al. presented a beacon-based HTM combining the characteristics of both ETM and DTM [20]. Trust is calculated in two steps. First, entity trust is established based on the received beacons. Next, data trust is calculated based on various plausibility checks to identify and revoke dishonest vehicles along with their malicious content. This TM highly depends on Public Key Infrastructure (PKI) and the central authority for their trust evaluation, which makes it inefficient due to the high overheads added to each forwarded message.

In a nutshell, we can see that a wide range of TMs are designed in VANET as depicted in Table I. According to our literature review, there is a lack of comparative study of different TMs in VANET. Therefore, to fill this gap, we present a comparative study of these TMs.

III. Details of the Compared Trust Models

In this section, we outline in detail, the TMs considered for comparison in VANET. For this paper, we chose three particular TMs, i.e., one from each category.

A. DTM

In this paper, we implemented a DTM, presented by Kerrache et al. [13]. In this TM, E_VN calculates trust through two traditional methods: direct trust (T_{dir}) and indirect trust (T_{ind}). T_{dir} relies on the quality of the received information while T_{ind} is established using a broadcast/drop ratio from the sending vehicle.

Let message is received at vehicle V_x from vehicle V_y, then the overall trust ($Trust_{(x,y)}$) at the V_x (which acts as E_VN in this case) at time (t) is calculated as:

$$Trust_{(x,y)}(t) = \sqrt{Trust_{(x,y)}(t-1) \times \sqrt{T_{dir} \times T_{ind}}} \quad (1)$$

T_{dir} relies on the quality of the received message. T_{dir} is updated with a factor of α (honesty reward) for every message satisfying the minimum trust threshold level. However, T_{dir} is decremented with factor β (punishment factor) if it falls below this trust threshold point. Let, $Broadcast(x, y)$ and $Drop(x, y)$ are the broadcasted and dropped packets by the transmitter, respectively. Then, T_{ind} is given by:

$$T_{ind}(x, y) = \frac{Broadcast(x, y)}{Broadcast(x, y) + Drop(x, y)} \quad (2)$$

Once T_{dir} and T_{ind} are identified, $E_V N$ calculates the overall trust. The message is accepted only if the overall trust is above the threshold, it is discarded, otherwise.

B. ETM

We consider Minhas et al.'s ETM where a multi-faceted approach is utilized for trust modelling [16]. Trust calculation on the entity is accumulated using the message producer's experience, priority, role and the majority opinions of the neighbours. In this TM, $E_V N$ first employs two trust management mechanisms in the network, i.e., role-based, and experienced-based, and the vehicles are prioritized in the neighbourhood based on these criteria. $E_V N$ then shares the messages with these vehicles and awaits their acknowledgement. Based on the location and time closeness, these prioritized vehicles send their opinions back to $E_V N$. Upon receiving opinions, $E_V N$ employs a majority decree for trust evaluation. $E_V N$ accepts the message if the majority agrees about the event trustworthiness, otherwise, $E_V N$ follows the advice provided by vehicles with higher experience and the highest role.

Role-based trust (T_{role}) has central importance in this TM. Every network mostly includes vehicles authorized from the higher and central authorities. T_{role} represents the generation of messages from such highly trusted vehicles. These include police vehicles, buses and taxis etc. It also includes vehicles with professional drivers having higher driving experience in the network.

On the other hand, experience-based trust (T_{exp}) is calculated for vehicles with no roles. As the behaviour of the vehicles usually changes over time, therefore, T_{exp} incorporates a forgetting factor (λ) for trust calculation to minimize the effect of old interactions. When a legitimate message is received from a sender, $E_V N$ increments the resultant trust by:

$$T_{exp} = \begin{cases} (\lambda)^t (1-\alpha) T_{exp} + \alpha & \text{if } T_{exp} \geq T_{Thr} \\ (\lambda)^{-t} (1-\alpha) T_{exp} + \alpha & \text{if } T_{exp} < T_{Thr} \end{cases} \quad (3)$$

In case of the compromised messages at $E_V N$, trust is decreased by:

$$T_{exp} = \begin{cases} (\lambda)^t (1-\beta) T_{exp} - \beta & \text{if } T_{exp} \geq T_{Thr} \\ (\lambda)^{-t} (1-\beta) T_{exp} - \beta & \text{if } T_{exp} < T_{Thr} \end{cases} \quad (4)$$

In equations 3 & 4, α is the honesty reward awarded to the message generator for providing true information, while, β is the punishment factor in case of malicious content. Further, t is the time closeness factor.

Once trust and distrust are accumulated by $E_V N$, then a majority rule is employed by $E_V N$. The message is accepted if maximum vehicles agree with the event trustworthiness, otherwise, the advice from the vehicle having the highest experience and role in the network is followed.

C. HTM

In this paper, we consider an event-oriented HTM called Vehicular Security through Reputation and Plausibility checks (VSRP) and implement it for comparison with the rest of the TMs [21]. The main component of this TM is the reputation-based trust management which can be used for the identification and isolation of the dishonest vehicles from the network. Following four steps are performed at the $E_V N$:

1) **Discovering Neighbors:** First, $E_V N$ identifies neighbors in its vicinity by broadcasting *neighbourreq* packets. Vehicles upon receiving *neighbourreq*, reply back to $E_V N$ with *neighbourrep*. Then $E_V N$ performs initial checks on the neighbour by consulting its trust table. $E_V N$ accepts the message if trust table contains an entry with non-zero trust value, otherwise, $E_V N$ revokes the message directly.

2) **Dispatching Content:** In this step, $E_V N$ transmits data to the recognized neighbors.

3) **Deciding Trust:** In this phase, trust is calculated through two important geographical factors. (1) threshold range, and (2) detection range of the vehicle. $E_V N$ discards the message if the sender is located outside the threshold range. In case the sender is within the threshold range, another check is performed by $E_V N$ using the detection range. $E_V N$ usually has a clear line-of-sight to the event in the detection range and $E_V N$ only accepts the received messages if the content agrees with the point-of-view of the $E_V N$. In this case, $E_V N$ increments the trust value of the sender with an honesty reward (α). In case of contradiction, $E_V N$ decreases the trust level of the sender with punishment (β) and discards its malicious content. However, if the sender is between detection and threshold range, then $E_V N$ consults its neighbours for message trustworthiness. $E_V N$ accepts messages only from neighbours if it satisfies the minimum trust threshold level, otherwise, the message is discarded and classified as malicious.

4) **Monitoring Neighbors:** In VSRP, $E_V N$ crucially depends on its neighbours for information collection. Therefore, each vehicle in the network closely monitors its neighbouring vehicles continuously. Depending on the exchanged messages, $E_V N$ can determine the trustworthiness of the node and the shared messages.

IV. Evaluation of Trust Models

A. Simulation Setup

In this study, we have used OMNET++ (v5.0) and Veins (v4.4), which are used broadly for the simulation of vehicular networks [23]. Furthermore, a default map of Veins is used with an area of about 2.5×2.5 km, where both legitimate

and dishonest vehicles are introduced in the network. We considered the following two scenarios in Veins:

1) **Scenario 1:** Keeping the number of honest vehicles constant and increasing the number of dishonest vehicles.
2) **Scenario 2:** Keeping the number of dishonest vehicles constant and increasing the number of honest vehicles.

B. Attacker Model

To evaluate the efficiency of TMs, we designed a Man-In-The-Middle (MITM) attacker model which is one of the critical attacks in VANET [24]. We equipped the attacker with two capabilities. First, the attacker can change the content of the safety message. Second, the attacker can delay the safety message. Since VANET involves very critical information (e.g., accident avoidance messages), therefore, both of these abilities of MITM attacker can cause catastrophic effects in the network. Table II summarizes all the necessary simulation details.

TABLE II: Simulation Details

Parameter		Value
Simulation Details	Simulation Area (km × km)	2.5 × 2.5
	No. of RSU	5
	Communication Range	250 m
	Total Simulation Time	1000 sec
Scenario 1	Total Honest Vehicles	100
	Total Dishonest Vehicles (%)	10, 20, 30, 40
		50, 60, 70, 80
Scenario 2	Total Honest Vehicles	50, 100, 150,
		200, 250, 300
	Total Dishonest Vehicles (%)	10, 20
Protocols	MAC Protocol	IEEE 802.11p
	Network Protocol	IEEE 1609.4
	Radio Propagation Model	Simple Path Loss
	Data Size	1024 bits
	Header Size	256 bits
Trust Model	Initial Trust (T_{Init})	0.5
	Threshold (T_{Thr})	0.5
	Honesty Factor (α)	0.01
	Punishment Factor (β)	0.1
Attacker Model	Actions on Message	1) Tamper
		2) Delay
	Delay (d)	2 secs

Further, each simulation scenario is carried out twenty-five times with random seed value to ensure unique initial vehicle assignment within the network every time. Moreover, the simulation results presented below are the average of twenty-five runs for each simulation scenario.

C. Evaluation Metrics

We considered the following metrics for the evaluation of TMs in VANET.

1) End-to-end Delay: The Quality of Service (QoS) related criterion is defined to identify the delay introduced to packet which is generated by the benign vehicles to be shared with the neighboring vehicles. End-to-End (E2E) delay is the difference of packet generation time (T_{Gen}) and packet reception time (T_{Rec}) which is calculated as follows:

$$E2E\ delay = T_{Rec} - T_{Gen} \tag{5}$$

2) Event Detection Probability (EDP): Identifying correct events (messages) are of primary importance in VANET as these messages contain sensitive information. To determine such events within the network, we defined EDP. TMs should have the capability to detect true events efficiently [25]. Let E_{Tot} are the overall events generated in the network. E_{True} and E_{Mal} are true and malicious events respectively, then EDP can be represented by:

$$EDP = \frac{\sum(E_{Tot} - E_{Mal})}{E_{Tot}} \tag{6}$$

3) Trust: Trust is another important metric measuring the trust values of the vehicles in the network. Based on this trust, E_VN either accepts or discards messages. For our experimentation, we kept the trust threshold (T_{Thr}) to 0.5 to accept messages. If the trust falls below this threshold, the message is categorized as malicious and the trust of the sender is decremented with the punishment factor (β). The message is accepted only if the trust of the received message is higher than the threshold and reward (α) is awarded to the honest vehicles for their honesty. As trust of the vehicle is not easy to gain, therefore, we assigned higher weights to the punishment, i.e., $(\beta = 10 \times \alpha)$. Moreover, we assigned the initial trust (T_{Init}) value of 0.5 to all the vehicles in order to deal with cold-start problem [26]. Mathematically, Trust (T) can be given as:

$$T = \begin{array}{ll} T + \alpha & \text{if } T \geq T_{Thr} \\ T - \beta & \text{if } T < T_{Thr} \end{array} \tag{7}$$

4) False Positive Rate (FPR): FPR illustrates the capability of the TM to determine those dishonest vehicles which are incorrectly detected as honest. The TMs with low FPR are considered good. Let $P_{Dis|Hon}$ describes the probability of detecting vehicle as dishonest, given the vehicle is honest, and $P_{Hon|Hon}$ is the probability of detecting vehicle as honest, given the vehicle is honest, then FPR is expressed as:

$$FPR = \frac{P_{Dis|Hon}}{P_{Hon|Hon} + P_{Dis|Hon}} \tag{8}$$

D. Simulation Results

*1) **Scenario 1**:* Figure 2 depicts E2E delay of three TMs in the presence of dishonest vehicles. It can be observed that among the three considered TMs, high E2E delay is achieved for HTM, while ETM experiences lowest E2E delays. There are two main reasons for this behaviour. First, ETM incorporates role-based and experienced-based mechanisms to revoke dishonest vehicles, thus enabling honest vehicles to receive trusted information in time. Second, DTM and HTM are based on data trust evaluation mechanism where data is deliberately delayed by dishonest vehicles. Since, one of the characteristics of the attacker model is to delay the messages by factor d, as a result, network experiences high E2E delays. This delay further increases when the number of adversaries is increased within the network. Further, a network utilizing ETM experiences low E2E delays than the network using DTM and HTM. For instance, when a network contains 50%

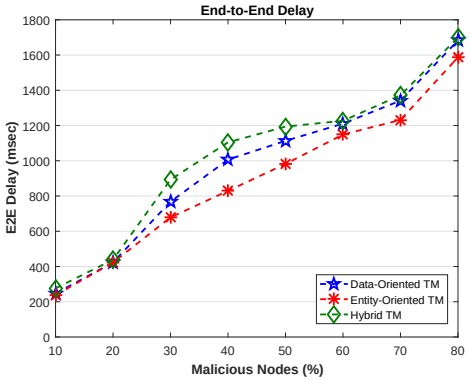

Fig. 2: End-to-End Delay vs. Malicious Nodes

malicious nodes then ETM achieves 21.58% less E2E delay than DTM.

The ability of the TMs to determine true events can be expressed by determining Event Detection probability (EDP). Since two forms of messages propagate in the network, i,e, (1) *legitimate messages* which are generated by the honest vehicles, and (2) *compromised messages* which are generated by attackers. Therefore, this metric is helpful in determining the performance of TMs to detect true events. The capability of three TMs to detect true event is illustrated by Figure 3, showing that ETM can detect a high number of true events than DTM and HTM. Since ETM integrates a role-based trust model, therefore, there is a high probability that these vehicles provide correct information, resulting in higher detection rates. For instance, ETM and DTM detect 24.36% and 9.82% more events correctly than HTM, if the network contains 50% malicious vehicles.

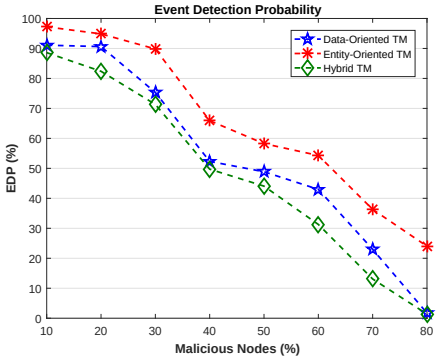

Fig. 3: Event Detection Probability vs. Malicious Nodes

Figure 3 also depicts that EDP of the network decreases when malicious vehicles are introduced in the network. Since one aspect of the attacker model is to change the content of the legitimate messages. Therefore, as the attack vector of malicious vehicles increases in the network, the ability of TMs to identify true messages decreases. In this regard, when the adversaries are increased in the network from 10% to 80%, EDP for ETM decreases from 97.21% to 24.02%, for DTM, it jumps down from 91.09% to 1.722 %, while for HTM, EDP declines from 88.60% to 1.38%.

Furthermore, Figure 4 shows the behaviour of the trust metric in the network for different TMs in the presence of dishonest vehicles. It can be seen that increasing the number of malicious vehicles in the network decreases trust within the network. In other words, the presence of malicious vehicles decreases the propagation of trusted packets in the network. Since the attacker model in our simulator is changing the content of the packet before broadcasting, thus resulting in the generation of compromised information in the network. Moreover, the trust metric is behaving much better in ETM than other TMs. As mentioned earlier, vehicles with the highest roles ensure the propagation of authentic and trusted messages in the network, thus achieving better trust values than DTM.

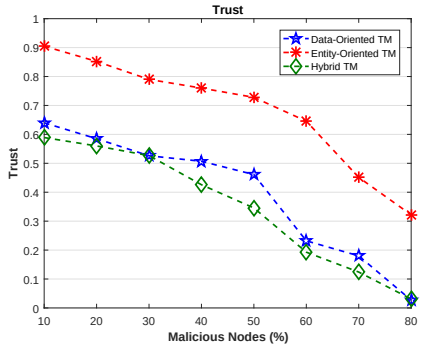

Fig. 4: Trust vs. Malicious Nodes

False positive rate (FPR) for the TMs is depicted in Figure 5. For VANET applications, FPR should be minimum. Lower FPR values mean better TM. It can be seen that the TMs achieve low FPR values (less than 4.5%), however, ETM outperforms DTM and HTM in terms of FPR by ensuring lower values. For 30% adversaries, ETM achieves about 54% better FPR values than DTM. This is due to the fact that ETM includes both experienced based and role-based vehicles, thus increasing the probability of detecting false positives in the network.

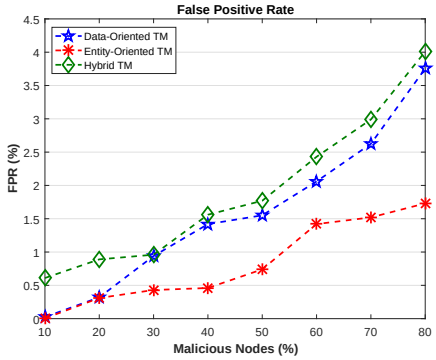

Fig. 5: False Positive Rate vs. Malicious Nodes

*2) **Scenario 2**:* Figure 6 shows E2E delay for three TMs when honest vehicles are increased in the network. It can be seen that HTM and DTM achieve high E2E delays as compare to ETM due to the fact that trust is evaluated for data which may be delayed by the adversaries in the network. On the other hand, role-based vehicles in the ETM ensure the revocation of such adversaries from the network, thus creating a trusted environment for message propagation. Further, increasing honest vehicles in such a network will increase the probability of disseminating trusted information among vehicular nodes. For a network with 300 legitimate nodes, DTM achieves 11% and 19% higher E2E delay than ETM and HTM when it is polluted with 10% and 20% malicious nodes, respectively.

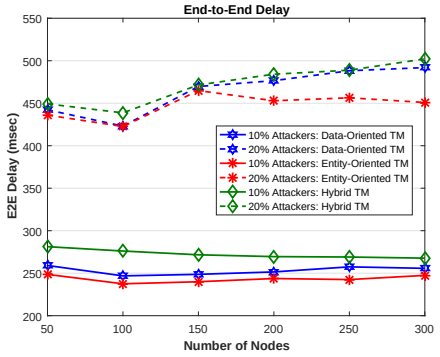

Fig. 6: End-to-End Delay vs. Legitimate Nodes

EDP of the TMs for increasing honest vehicles in the network is depicted in Figure 7. EDP increases for all TMs when honest vehicles are increased in the network. For instance, the detection probability for ETM is increased from almost 92% to 97%, DTM detection probability is increased from 87% to 94% and for HTM, EDP increases from 82% to 89% when honest vehicles are increased from 50 vehicles to 300 vehicles in existence of 20% malicious vehicles. Moreover, ETM provides higher EDP than DTM and HTM. Since in this experiment, the attacker is delaying and changing the content of the packet. therefore, identifying and detecting true events become difficult when malicious nodes are introduced in the network.

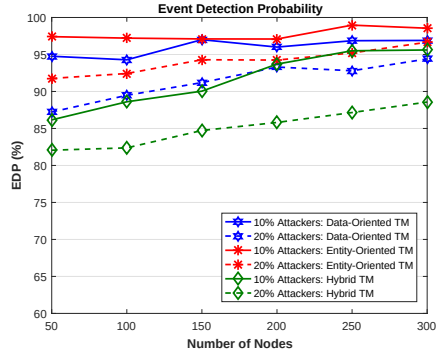

Fig. 7: Event Detection Probability vs. Legitimate Nodes

Figure 8 highlights the behaviour of trust metric when honest vehicles with the TMs are increased in the network. It can be seen that trust increases when the number of honest vehicles is increased in the network. This is due to the fact that more vehicles are available in the network to calculate the trustworthiness which results in the identification and revocation of dishonest vehicles and their malicious content. Moreover, ETM achieves the highest trust than other TMs. It is because of the presence of role-based authorities and experienced-based trust in ETM. On the other hand, DTM depends on the evaluation of the data for trustworthiness. Since the attacker can tamper with the data, therefore, trust decreases in DTM and HTM. It is worth mentioning that ETM outperforms DTM by about 31.1% when the network contains 300 honest vehicles and 20% malicious vehicles.

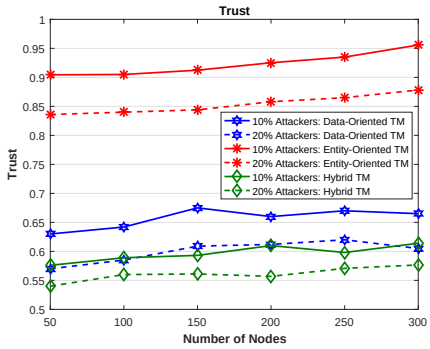

Fig. 8: Trust vs. Legitimate Nodes

Figure 9 depicts the FPR of all TMs. It can be seen that TMs achieve less than 2% FPR values for 10% and 20% malicious vehicles. This means that these TMs have the ability to detect the error margins by correctly detecting malicious vehicles. FPR decreases when honest vehicles are increased in the network. This is due to the fact that a high number of legitimate nodes can detect more and more legitimate messages correctly, resulting in fewer messages that are incorrectly identified as legitimate messages. Moreover, ETM performs better than DTM and HTM by achieving low FPR values due to the presence of vehicles with the highest roles in the network, thus resulting in less error in identifying malicious vehicles.

V. Conclusion

A secure, privacy-aware and trusted environment is a prerequisite for the distribution and propagation of safety messages in VANET. In this regard, trust among the vehicles ensures the dissemination of trusted messages in the network. A wide range of TMs are proposed in different studies where trust is calculated via different techniques. In this paper, we provided a comparative study of three TMs from each category, i.e., ETM, DTM and HTM. Further, we adopted a simulation-based approach where the efficiency of these TMs is evaluated against MITM attacks. Simulation results indicated that ETM outperformed other TMs due to the presence of role-based and experience-based trust techniques

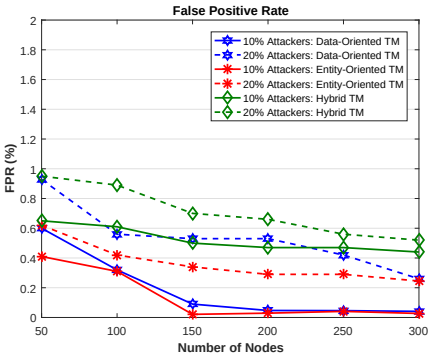

Fig. 9: False Positive Rate vs. Legitimate Nodes

which ensured the dissemination of trusted information among vehicular entities. Further, the results also depicted that DTM and HTM are more prone to MITM attacks.

This study can be used as a guideline by the researchers in order to design new TMs. We conclude that the future TMs should include role-based and experience-based trust management techniques to provide a trusted environment for message dissemination. As a future work, we will design an efficient TM which integrates these trust management techniques in order to achieve overall network security.

REFERENCES

[1] 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, 2017, doi: 10.1109/MCOM.2017.1600514.

[2] A. Boualouache, S. Senouci, and S. Moussaoui, "A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2018, doi:10.1109/COMST.2017.2771522.

[3] Q. E. Ali, N. Ahmad, A. H. Malik, G. Ali, and W. Rehman, "Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy," *Applied Sciences*, vol. 8, no. 10, 2018, doi:10.3390/app8101964.

[4] F. Ahmad and A. Adnane, "A Novel Context-based Risk Assessment Approach in Vehicular Networks," in *IEEE 30th International Conference on Advanced Information Networking and Applications Workshops*. IEEE, March 2016.

[5] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali, and S. Begum, "VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead," *Hindawi Journal of Sensors*, vol. 2018, doi:10.1155/2018/6576841.

[6] 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.

[7] J. Zhang, "Trust Management for VANETs: Challenges, Desired Properties and Future Directions," *International Journal of Distributed Systems and Technologies*, vol. 3, no. 1, pp. 48–62, Jan. 2012.

[8] 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 (Early Access)*, pp. 1–17, April 2018, doi:10.1109/TITS.2018.2818888.

[9] R. Hussain, W. Nawaz, J. Lee, J. Son, and J. T. Seo, "A Hybrid Trust Management Framework for Vehicular Social Networks," in *Computational Social Networks*, H. T. Nguyen and V. Snasel, Eds. Cham: Springer International Publishing, 2016, pp. 214–225.

[10] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," in *IEEE 27th Conference on Computer Communications (INFOCOM)*. IEEE, April 2008, pp. 39–68.

[11] 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.

[12] A. Wu, J. Ma, and S. Zhang, "RATE: A RSU-Aided Scheme for Data-Centric Trust Establishment in VANETs," in *7th International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE, Sept 2011, pp. 1–6.

[13] 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)*. IEEE, July 2016, pp. 153–160.

[14] 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.

[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] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A Multifaceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad Hoc Vehicular Networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 3, pp. 407–420, May 2011.

[17] 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.

[18] 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.

[19] 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.

[20] Y. Chen and Y. Wei, "A Beacon-based Trust Management System for Enhancing User Centric Location Privacy in VANETs," *Journal of Communications and Networks*, vol. 15, no. 2, pp. 153–163, April 2013, doi:10.1109/JCN.2013.000028.

[21] 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.

[22] 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.

[23] Veins, "Vehicles in Network Simulation, The Open Source Vehicular Simulation Framework," available online: http://veins.car2x.org (Accessed: 30th October, 2018).

[24] 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.

[25] 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)*. IEEE, June 2017, pp. 44–52.

[26] L. H. Son, "Dealing With the New User Cold-start Problem in Recommender Systems: A Comparative Review," *Elsevier Information Systems*, vol. 58, pp. 87 – 104, 2016.