IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 12, 2018, accepted May 7, 2018, date of publication May 25, 2018, date of current version June 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2837887

TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks

FARHAN AHMAD, VIRGINIA N. L. FRANQUEIRA, AND ASMA ADNANE
Cyber Security Research Group, College of Engineering and Technology, University of Derby, Derby DE22 1GB, U.K.
Corresponding author: Farhan Ahmad (f.ahmad@derby.ac.uk)

ABSTRACT Vehicular ad-hoc network (VANET) provides a unique platform for vehicles to intelligently exchange critical information, such as collision avoidance messages. It is, therefore, paramount that this information remains reliable and authentic, i.e., originated from a legitimate and trusted vehicle. Trust establishment among vehicles can ensure security of a VANET by identifying dishonest vehicles and revoking messages with malicious content. For this purpose, several trust models (TMs) have been proposed but, currently, there is no effective way to compare how they would behave in practice under adversary conditions. To this end, we propose a novel trust evaluation and management (TEAM) framework, which serves as a unique paradigm for the design, management, and evaluation of TMs in various contexts and in presence of malicious vehicles. Our framework incorporates an asset-based threat model and ISO-based risk assessment for the identification of attacks against critical risks. The TEAM has been built using VEINS, an open source simulation environment which incorporates SUMO traffic simulator and OMNET++ discrete event simulator. The framework created has been tested with the implementation of three types of TMs (data oriented, entity oriented, and hybrid) under four different contexts of VANET based on the mobility of both honest and malicious vehicles. Results indicate that the TEAM is effective to simulate a wide range of TMs, where the efficiency is evaluated against different quality of service and security-related criteria. Such framework may be instrumental for planning smart cities and for car manufacturers.

INDEX TERMS Vehicular networks, trust management, smart cities, security, intelligent transportation systems, VEINS, SUMO, OMNET++, simulation.

I. INTRODUCTION

Recently, a preeminent interest has been observed in the technologies to improve transportation around the world. Vehicular Ad-hoc Networks (VANET) is the state-of-the-art technology in the domain of transportation where vehicles communicate with each other and static Roadside Units (RSUs) via vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication to offer various applications. It includes both safety (e.g., traffic safety and efficiency) and non-safety (e.g., infotainment) applications [1]–[5]. VANET performs a key role in the emerging smart cities and Internet-of-Things (IoT) with the aim to improve overall transportation [6], [7]. Figure 1 illustrates the integration of VANET in smart cities where traffic safety is achieved by connecting vehicles to each other by virtue of V2V or V2I communication.

Since, applications offered to connected vehicles involve very critical information (such as steep-curve, or accident warning), a secure, attack-free and trusted network is imperative for the propagation of reliable, accurate and authentic information. In case of VANET, ensuring such network is extremely difficult due to its large-scale and open nature, making it susceptible to diverse range of attacks including man-in-the-middle (MITM), replay, jamming and eavesdropping attacks [8]–[11].

Recently, various solutions have been proposed to achieve security in VANET. Most of these solutions rely on traditional cryptography where vehicles utilize certificates and Public Key Infrastructure (PKI) to ensure security in the network. However, cryptography-based solutions reduce network efficiency due to following reasons. (1) Firstly, VANET includes both low and highly mobile vehicles which are dispersed randomly throughout the network, (2) Secondly, presence of an infrastructure cannot be ensured permanently, e.g., in rural areas, and (3) lastly, cryptographic solutions can be compromised by insider attacks in VANET, which

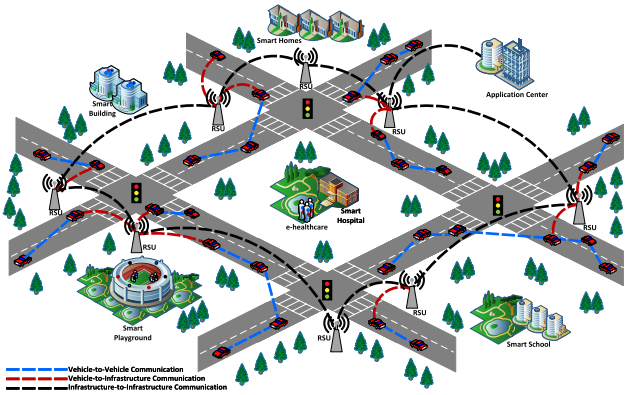

FIGURE 1. Illustration of VANET in smart cities.

results in the propagation of untrusted messages across the network [12].

In order to address these shortcomings, trust has been proposed as a relevant technique to achieve network security. Trust is defined as the confidence of one node on the other for performing a specific action or set of actions [13]. In VANET, it is established between two vehicles based on the messages exchanged regarding an event. Once, message is received, the evaluator node calculates trust based on numerous factors, including vehicles past interactions, vehicles reputation in the network and neighbors' recommendations about particular vehicle. However, trust between neighboring vehicles is created for a very limited duration of time due to highly mobile and randomly distributed vehicles [14], [15]. Therefore, establishing, calculating, and evaluating trust on received messages based on diverse factors in such short period of time is extremely challenging.

Trust, as a technique to achieve security in VANET, is in its early stage of development. Trust models (TMs) are embedded within vehicles to evaluate trustworthiness, accuracy and authenticity of received messages. TMs ensure the propagation of trusted information in the network by revoking both dishonest nodes (vehicle) and messages having malicious content. In VANET, TMs are classified into three distinct classes, i.e., entity-oriented, data-oriented and hybrid TMs [16]–[19]. Entity-oriented trust models (EOTM) aims to eliminate dishonest vehicles by evaluating trustworthiness on the node. Data-oriented trust models (DOTM) evaluates trust on the received messages (data) while hybrid trust models (HTM) relies on both vehicle and data for trust establishment.

In VANET, various TMs are developed to ensure security either by eliminating dishonest vehicles or tempered messages [20]–[23]. However, it is currently complicated to compare and evaluate the efficiency of these TMs due to absence of a unified trust evaluation framework. Moreover, high mobility and random distribution of vehicles across the network result in various contexts in VANET. Therefore, it becomes significantly important to take those contexts into account for trust management. For instance, in an urban location, extensive amount of messages (trusted & untrusted) are present due to low mobility of vehicles and abundant number of RSUs. On the other hand, rural areas cannot ensure the permanent presence of RSU. Moreover, high mobility and low number of vehicles in such locations produce minimum amount of messages. TMs which depends on high number of RSUs and vehicles for trust management will show poor results for a scenario with minimum number of vehicles. As a result, both scenarios demand separate techniques to evaluate trustworthiness on transmitting node and their messages. VANET can succeed only if secure and trusted messages are ensured in every context.

In this paper, we addressed this problem by proposing a novel trust evaluation and management framework called *TEAM*, which have the ability to evaluate TMs in numerous contexts of VANET. In TEAM framework, we model and evaluate the efficiency of different TMs based on main objects of VANET. i.e., data and node. Moreover, major attacks are also identified based on asset-based threat model and ISO-based risk assessment as a preliminary study. Once, the list of attacks related to TM is available, the TMs are evaluated under these attack models in different contexts of VANET. This can determine the impact of malicious attacks on TMs and their performance in various contexts. In order to do so, we conducted an extensive set of experiments to evaluate the performance of TMs from each category (EOTM, DOTM & HTM) using TEAM. Simulation results depict that our framework can accurately evaluate the efficiencies of TMs in various context of VANET.

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

- First, we proposed a novel trust evaluation framework in this paper, which has the ability to evaluate a wide range of TMs (EOTM, DOTM and HTM).
- Second, we introduced the concept of context for the evaluation of TM in VANET. Particularly, we identified four contexts based on the mobility of vehicles and attackers in the network.
- Third, we performed an asset-based threat modeling for the identification of attacks by directly mapping vulnerabilities with threats in VANET. Then, risk assessment is performed to identify attacks with higher severity. The attacks with higher severity levels are implemented in our framework.
- Fourth, we considered several realistic evaluation criteria for the TMs, focusing entirely on the Quality of Service (QoS) and security of the network, and
- Finally, we performed an extensive set of experiments for the evaluation of TMs in four contexts and in presence of malicious nodes.

The rest of the paper is organized as follows: Section II provides relevant information about TMs in VANET. Then, proposed trust evaluation framework is explained in detail in section III. Section IV provides the details of simulation environment, while section V is dedicated to the simulation

results and discussion of the performance of TEAM framework. Finally, conclusions are drawn in section VI.

II. RELATED WORK

In this section, we presented various categories of trust models (TMs) in VANET. Moreover, we also explored relevant research related to trust frameworks.

A. TRUST MODELS IN VANET

In VANET, main objective of the TM is to ensure secure and trusted data dissemination by identifying dishonest vehicles and revoking compromised messages from the network. Recently, various TMs have been proposed in VANET, which can be classified broadly into three categories: (1) data-oriented TM (DOTM), (2) entity-oriented TM (EOTM), and (3) hybrid TM (HTM).

1) DATA-ORIENTED TRUST MODELS

In these TMs, data plays a central role where trustworthiness in the accuracy and authenticity of received message is computed by the node. These TMs highly depend on their previous interactions with the peers, and the opinions shared from the vehicles in its vicinity.

One of the earlier work in this direction is the TM proposed by Raya *et al.*, where evidence on the received events is accumulated based on Bayesian inference (BI) and Dempster-Shafer Theory (DST) [24]. In this TM, evaluator node (E_V) first receive reports from vehicles in the neighborhood, and then assign weights to every received report based on location and time closeness to the event. At the E_V, these reports along with the assigned weights are then passed to a decision logic module where trust is calculated using BI and DST. The main shortcoming of this TM is the fact that trust is calculated every time a data is received, thus making it inefficient for highly dynamic and sparse environment.

Gurung *et al.* proposed a complex distributed DOTM where trustworthiness on event data is evaluated in real time by vehicles themselves, without any dependence on RSU [25]. This TM calculates trust in two phases, i.e., messages received from a large number of neighbors is firstly classified into two sub-groups using a clustering technique. First sub-group contains data having similar content, while the second sub-group include messages with conflicting content. Once messages are classified into respective sub-groups, the next phase evaluates the trustworthiness of the messages based on three factors, i.e., information similarity, information conflict and received routing path similarity. This TM is very complex as it involves real time validation of the received messages, which may not be feasible in high mobility and sparse scenario. Moreover, discussion on how this TM would behave in the presence of attack is not addressed.

Shaikh and Alzahrani filled this gap by proposing an intrusion-aware TM with the potential to efficiently identify and detect bogus messages in the network such as messages with fake location [26]. Trust by E_V is calculated in three phases. First, a confidence value on every data is calculated based on four factors: (1) location closeness, (2) time closeness, (3) location verification, and (4) time verification. Then, trust is calculated for every message based on the confidence value, and lastly, a fuzzy logic is employed on the message where a decision module either accepts or rejects the data. A message is accepted only if its trustworthiness value achieves a certain threshold level. Although this TM is very light and efficient for infotainment applications, it is not applicable for safety applications due to the delay introduced in the calculation of trust values.

2) ENTITY-ORIENTED TRUST MODELS

Unlike DOTMs, these TMs adopt an approach to eliminate malicious entities from the network by evaluating trustworthiness on the vehicle. These TMs rely heavily on neighbors and message originators for trust management, where the neighbors endorse a reputation and recommendation about message sender to E_V.

Several studies have been proposed in the literature which focus entirely on EOTM. For instance, Khan *et al.* proposed a cluster-oriented approach where the elected cluster head (*CH*) in the network is responsible for the calculation and evaluation of trust in the network [27]. *CH* employs a watchdog mechanism in its neighborhood where legitimate vehicles provide their recommendation to *CH* about the presence of misbehaving vehicle in its vicinity. Once, such malicious vehicles are identified, *CH* informs the trusted authority (*TA*) about these vehicles which are then removed from the network of trusted vehicles. However, major drawback of this approach is high overhead caused due to the report, thus reducing network efficiency. Moreover, the communication details among vehicles, *CH*, and *TA* is missing in this study.

A similar TM is presented by Jesudoss *et al.* where trust is calculated by electing a *CH* in the network [28]. The *CH* is responsible to disseminate trusted information in the network. All the participating nodes follow a truth-telling approach to gain reputation in the network. The information is trusted only by *CH* if participating node gains higher weights in *CH* election and by continuously monitoring its neighboring nodes and identifying malicious information. However, this solution will fail in a highly mobile and rural location where *CH* might not have enough neighbors and the presence of the malicious vehicles may result in a biased selection of *CH*.

Unlike cluster-based approaches in EOTM, Haddadou *et al.* adapted a different technique based on economic incentive model to exclude malicious nodes from the network [29]. In this model, all nodes in the neighborhood are assigned with a specific credit value in a distributed manner. The increase or decrease in the credit depends on node behavior in the network. In case of an attack, the credit is decreased. When the node has no credit left, it is assumed to be malicious and is excluded from the network. The main limitation of this TM is its inability to differentiate between direct or indirect trust.

Minhas *et al.*, on the other hand presented a TM where trust is calculated and aggregated based on 4 sources, i.e., (1) sender node's experience, (2) priority, (3) role and (4) majority opinion [30]. When a message is received, E_V identifies and prioritizes vehicles (V_P) in its vicinity based on their reputation and experience, thus incorporating role and experience-based trust. The E_V then broadcast requests to V_P about the event authenticity, and waits for their response. Based on time and location closeness, V_P reply back to the E_V with their opinions. Once messages from all V_P are received, E_V applies a majority rule to identify the trustworthiness of the vehicle. If the majority of the vehicles agree about the event, E_V accepts the messages, otherwise it follows the advice of vehicle with the highest role and experience in the network. Main limitation of this TM is its reliance on PKI cryptography for the calculation of role-based trust where the presence of a central authority is required for the verification of those certificates.

Another EOTM based on trust and reputation is presented in [31], where a similarity mining approach is adapted to calculate trust in the network. Whenever a message propagates in the network, E_V identify similarity between received messages which is calculated based on euclidean distance and reputation weights of the participating vehicles. However, the main shortcoming of this TM is its dependence on euclidean distance between the two vehicles as this does not provide a global information on similarity of the messages.

3) HYBRID TRUST MODELS

Hybrid trust models (HTM) evaluate trust based on the trustworthiness of vehicles and the data they exchange. In other words, these TMs evaluate trust of data by utilizing trust of vehicles, assuming a trade-off between data authenticity and sender's reputation. Therefore, vehicles' reputation and neighborhood opinions about a particular vehicle play a vital role in evaluating trust. These TMs involve a high level of complexity, as a significant number of control messages have to be processed in a very short span of time.

The following hybrid trust models can be found in the literature. Sedjelmaci and Senouci proposed a TM to evaluate the trustworthiness of a message in presence of various attacks including sybil and packet duplication attacks [32]. This TM adopts a two level approach for trust management. First level identifies *CH* which evaluates the message trustworthiness in a fully distributed manner. The second level relies on an adjacent Road Side Unit (RSU) to calculate trust in a global manner. Therefore, it assumes that stable clusters are always present in the surroundings of RSU which is the main limitation of this TM. Moreover, the formation of a cluster around a RSU, and the selection of *CH* are time-intensive processes which increase the overall complexity of the network.

In order to identify malicious nodes in the network, Dhurandher *et al.* adapted an event-oriented approach to achieve security in VANET by employing reputation and various plausibility checks to disseminate safety related messages in the network [33]. This approach integrates a reputation-based trust management to identify and isolate malicious nodes from the network. The E_V performs following four steps for trust management and eviction of the malicious nodes from the network: (1) neighbor discovery, (2) data dispatching once neighbors are discovered, (3) trust decision on the event message received, and (4) continuous monitoring of the neighborhood. However, this approach has some limitations: First, the detection range as proposed by the authors in trust decision is very short, i.e., 50m. Secondly, detection relies heavily on the vehicle's sensors. If the sensors malfunction for some reason, then this approach may classify compromised messages as legitimate which result in the propagation of false information in the network.

Abdelaziz *et al.* [34] proposed a light-weight TM to efficiently relay messages towards their destination by utilizing advantages of the DSRC communication protocol. In this TM, messages received via communication module are classified into four classes, where safety messages are given higher priority. Moreover, its intrusion detection module utilizes anomaly-based detection algorithms to keep statistical information of neighboring nodes, thus, resulting in the ability to detect DoS attacks. The main issue with this approach is its assumption that malicious nodes will behave consistently throughout their journey, which is invalid in VANET.

To sum up this section, we see that various TMs are designed to ensure trust management between vehicles in VANET. However, current solutions have various issues resulting from inability to cope with attacks, performance and complexity overheads. Moreover, according to our literature, there is no TMs for context-enabled VANET based on mobility of vehicles and adversaries.

B. EVALUATION FRAMEWORKS FOR TRUST MANAGEMENT

In the previous section, we identified various available TMs in VANET. These TMs establish trust via different mechanisms which range from trusting the vehicle to trusting its data. However, very little work has been done for the evaluation of these TMs. In this section, we focus on such frameworks which provide some sort of evaluation of TMs.

Chen *et al.* proposed a trust management framework where *CH* is responsible to establish trust on vehicles based on neighbors' opinion aggregation mechanism in a dynamic environment [35]. In this framework, messages are disseminated only by *CH* after verification of its authenticity. Every member of the cluster shares its opinion with *CH*, where trust on the aggregated message is calculated based on its validity and correctness. *CH* then applies majority rule, where messages are accepted only if majority of the members agree with the authenticity of the event. This trusted message is then broadcast by *CH* which propagates throughout the network. The main drawbacks of this frameworks are: (1) This solution fails in a highly mobile and rural scenario due to low availability of the cluster members. (2) This framework can only

evaluate the EOTMs, and (3) lastly, the behavior of attackers on the TM is missing from the paper.

In order to address this issue, Oluoch proposed a theoretical framework incorporating RSU for trust evaluation in VANET [36]. In this framework, a threat model is designed at first place which consists of means of access of attackers in the network (either V2V communication, or updates from RSU), type of attacks launched by attackers (e.g., Sybil and Betrayal attacks) and the action (such as active or passive) of the attacker in the network. In the next step, threat model is integrated with trust establishment module, where trust is calculated by two methods, i.e., global trust establishment and local trust establishment. Global trust establishment is accomplished via RSU, where vehicles in its vicinity share their opinions about the event with available RSU. RSU performs majority rule to authorize trusted information in the network. Local trust establishment between vehicles is also computed in the absence of RSU, where information received at E_V is analyzed for its authenticity. In such case, a dynamic threshold is set for trust at the E_V. Message is dropped if it falls below certain threshold, and it is accepted only if it surpasses the threshold value. This framework has several drawbacks. First, the authors only proposed a theoretical framework for trust establishment with no mathematical foundations. Secondly, very basic threat model is considered in the framework, and the information about threats and vulnerabilities are missing in the proposed framework. Third, this is very generic framework and it doesn't provide any information about the evaluation of different trust models.

From our literature review, we realized that currently available frameworks have various limitations for trust evaluation. Therefore, we fill this gap by proposing a novel trust evaluation framework, which has the capability to evaluate different TMs (EOTM, DOTM and HTM). Moreover, our framework integrates an asset-based threat model where attacks are mapped directly from threats and vulnerabilities in assets. Further, attacks with serious impact on the network are identified and prioritized via ISO-based risk-assessment. Moreover, our framework provides a context establishment module where we identified four scenarios based on node's mobility. Once, attacks with high risks and contexts are identified, TMs are then evaluated against these attacks in different contexts using realistic trust evaluation criteria in the trust evaluation platform.

III. PROPOSED TRUST EVALUATION FRAMEWORK

In this section, we provide details of our proposed trust evaluation and management (TEAM) framework. Figure 2 depicts high level idea of our proposed framework. It can be seen that framework is composed of five distinct modules.

1) **Module 1:** Threat model
2) **Module 2:** Risk assessment
3) **Module 3:** Identification and categorization of TMs
4) **Module 4:** Context establishment
5) **Module 5:** Trust evaluation platform

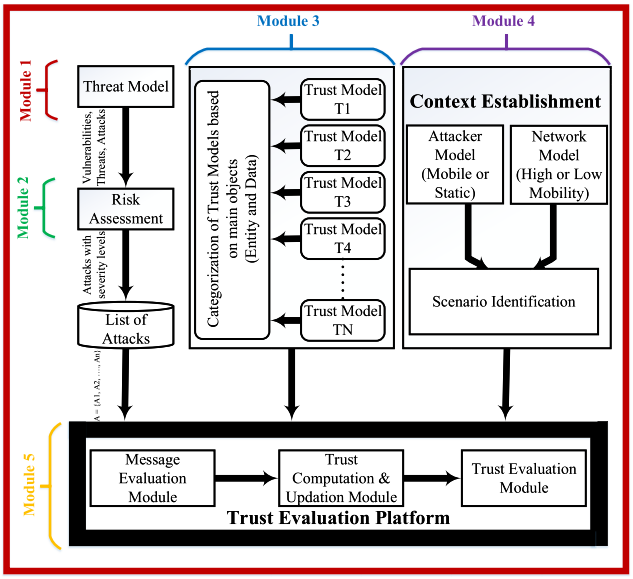

FIGURE 2. Proposed Trust Evaluation Framework.

The first two modules (threat model and risk assessment) are designed to identify various attacks in VANET. Once, attacks with critical risks are identified, then the efficiency of TMs are evaluated in various contexts and in the presence of attacks.

A. MODULE 1: THREAT MODEL

The first and foremost module of our framework is threat model, where we adopted a systematic approach for attack identification. In this work, we identified vulnerabilities and threats in assets of VANET which are exploited by adversaries to launch several attacks. The major steps of the threat model are:

1) Identification and classification of assets based on their role, mobility and impact in VANET.
   a) *Information:* carrying sensitive messages across different assets.
   b) *Vehicular System:* contains vehicular user, vehicles and communication network.
   c) *Infrastructure:* includes static entities of the network, such as RSU and CA.
2) Identification of vulnerabilities in assets of VANET.
   a) **V1:** Insecure algorithms for exchanging user credentials.
   b) **V2:** Software flaws such as buffer over flow, key management failure, insecure cryptographic algorithms.
   c) **V3:** Non-availability of wireless communication channel during message transfer.
   d) **V4:** Hardware malfunction and error.
3) Identification of threats in VANET, such as
   a) **T1:** Message transmission with weak encryption tools.

b) **T2:** Exposing sensitive information such as confidential communication between law enforcement vehicles.
c) **T3:** Message interception by adversaries.
d) **T4:** Hardware damage due to natural disasters.

4) Identification of attacks in VANET. For instance,
a) **A1:** Social engineering attack dealing with moral ethics of VANET users.
b) **A2:** Man-in-the-Middle (MITM) attacks to intercept and modify messages.
c) **A3:** Replay attacks by injecting obsolete messages in the network.
d) **A4:** Jamming attacks by launching denial of service attacks.
e) **A5:** Bogus information addition attacks by introducing false information in the networks

The attack mapping from threats and vulnerabilities is depicted in Table 1. For instance, Social Engineering Attack (A1) occurs due to weak passwords and lack of users education and awareness (T1) which results in the exploitation of user credentials (V1). Similarly, the attacker can expose the sensitive information (T2) such as road accident warning by exploiting wireless communication interface of vehicle and insecure algorithms (V1) used for message transfer by adding bogus information to the message (A5). The rest of the vulnerability-threat-attack (VTA) mapping can be done in the same way. The details of threat model is given in our previous work [37].

TABLE 1. Vulnerability-threat-attack mapping.

Threats (T)	Vulnerabilities (V)	Attacks (A)
T1	V1	A1
T2	V1	A5
T3	V2	A3, A4, A5
T4	V3, V4	A2, A4

B. MODULE 2: RISK ASSESSMENT

Once, attacks in various components of VANET are identified, the next phase involves risk assessment to identify risks caused by attacks in VANET. Risk is directly related to the vulnerability identified in assets which are exploited by threats in form of attacks, causing damage to the whole network. As VANET is an emerging technology with lacking statistical attack history, a quantitative based approach can not be utilized for risk assessment. Therefore, we performed a qualitative based risk assessment according to ISO 27005 [38]. Risk is a measurable quantity which depends on "likelihood of attack occurrence", and "impact of an attack on network assets". Likelihood and impact can be mapped into three categories. The resulting risk can be given as:

$$Risk = function\ (Likelihood\ ,\ Impact) \tag{1}$$

Corresponding risk is also categorized into three classes, i.e., *Minor, Major* and *Critical*. Risks identified as major and critical need urgent attention from the user. Table 2 shows the corresponding risk levels based on the likelihood and the impact values.

TABLE 2. Risk analysis: scale.

Likelihood (L)	Impact (I)	Risk (R) = L * I
L1 = 1 (Unlikely)	I1 = 1 (Low)	R1 = 1, 2, 3 (Minor)
L2 = 2 (Possible)	I2 = 2 (Medium)	R2 = 4 (Major)
L3 = 3 (Likely)	I3 = 3 (High)	R3 = 6, 9 (Critical)

Table 3 performs the risk assessment for attacks identified in module 1. It can be seen that MITM and DoS attacks have high risk values in VANET. This is due to the fact that both jamming and modifying the sensitive message can result in disaster in the network. The detail risk assessment can be found in our previous work [39].

TABLE 3. Risk assessment for attacks in VANET.

Attacks (A)	Likelihood (L)	Impact (I)	Risk (R)
A1	Possible:2	High:3	Critical:6
A2	Likely:3	High:3	Critical:9
A3	Possible:2	Low:1	Minor:2
A4	Likely:3	High:3	Critical:9
A5	Possible:2	High:3	Critical:6

Module 1 (threat model) and module 2 (risk assessment) represents the preliminary study of the framework and is responsible for the identification of the attacker models in VANET. Let $A = \{A_1, A_2, A_3, ..., A_N\}$ are such attacks with critical and major risks in VANET. This list of attacks is provided to the framework as an input where the efficiency of the TMs has to be evaluated in presence of malicious nodes.

C. MODULE 3: IDENTIFICATION AND CATEGORIZATION OF TMS

This module has two major responsibilities: (1) Firstly, it identifies the desired TM and, (2) secondly, it categorize TMs into their respective class, i.e., DOTM, EOTM, and HTM. Let $T = \{T_1, T_2, T_3, ..., T_N\}$ are 'N' TMs in VANET. In order to identify respective TM, these TMs are categorized into three classes according to their trust evaluation mechanism. In order to illustrate the framework, we have implemented one TM from each category. The details of these TMs are as follows:

1) DOTM

As mentioned earlier, these TMs rely on data for trust establishment. In this paper, we implemented a data-oriented TM proposed by Kerrache *et al.*, where, trustworthiness on the data is calculated [40]. In this model, trust is established among vehicles based on two methods: direct trust and indirect trust. Direct trust is calculated directly among the vehicles where vehicles evaluate each other based on the quality of the messages they provide. On the other hand, indirect trust establishment is calculated based on the broadcast/drop ratio from the sender. Let V_a is the vehicle which received message

from V_b, the trust is computed as follows:

$$Trust(a,b) = \sqrt{Trust(a,b) \times \sqrt{Trust_{ind} \times Trust_{dir}}} \quad (2)$$

$Trust_{dir}$ depends on the received message quality where it is updated with a factor of α if the message quality is above certain trust threshold. $Trust_{dir}$ is decreased with factor β if message quality falls below threshold value. $Trust_{ind}$, on the other hand, and is calculated as:

$$Trust_{ind}(a,b) = \frac{B(a,b)}{B(a,b) + D(a,b)} \quad (3)$$

where, $B(a,b)$ and $D(a,b)$ are the number of broadcast and drop packets by the vehicle.

Whenever a message is received by V_a, it computes trust on the received information based on two values, i.e., (1) Quality of Information (*infoQ*), and (2) Belief Degree (BD). *InfoQ* depends on the quality of the message received, where, $infoQ \in (0,1)$. This factors takes into account the distance between the nodes and reporting time. If reporting nodes are away from the event location and the reporting time is old, then it assigns the lowest *infoQ* value, while messages with closest reporting location and time are assigned with highest values [41]. On the other hand, based on *BD*, the report is either classified as true or false. *BD* is computed as follows:

$$BD(a,b) = \sqrt{Trust(a,b) \times \sqrt{BD(a,b) \times infoQ}} \quad (4)$$

2) EOTM

For the demonstration of our framework, we implemented an entity-oriented TM proposed by Minhas *et al.* [30]. This model incorporates a multifaceted approach for trust modeling where trust on the entity is established based on experience, priority, role and majority opinion based trust. When E_V received a message from other vehicles, it identifies vehicles with highest role and highest experience in the network. Messages received from these vehicles are assigned with higher weights in the network. If E_V receive messages from other vehicles in its vicinity, then it generates a report based on time closeness and location closeness. Based on these reports, E_V performs a majority opinion for its trust calculation. If majority of the vehicles agree on the message validity, then the message is accepted, otherwise, E_V follows the advise of vehicles with highest roles.

Let T_{V2V} denote the vehicle-to-vehicle trust of vehicle i, then

$$T_{V2V} = \begin{cases} T_{role(i)} & \text{if } \textit{vehicle has a role} \\ T_{exp(i)} & \text{else} \end{cases} \quad (5)$$

Role based trust (RBT) is significantly important in this TM, as these represent highly trusted vehicles which are approved from higher authorities. Thus, messages transmitted from these vehicles are mostly trusted. These vehicles include (1) law-enforcement authorities such as police vehicles, (2) public transport such as buses and taxis, and (3) professional vehicles with higher experience of driving.

For vehicles with no roles, experience based trust (EBT) is calculated. EBT integrates a forgetting factor (λ), which ensures that old interactions with vehicles gets less weight as the behavior of vehicles may change over time. If trusted message is shared from the vehicle, then the overall trust of the vehicle is increased by:

$$T_{exp(i)} = \begin{cases} (\lambda)^t(1-\alpha)T_{exp(i)} + \alpha & \text{if } T_{exp(i)} \geq T_{Thr} \\ (\lambda)^{-t}(1-\alpha)T_{exp(i)} + \alpha & \text{if } T_{exp(i)} < T_{Thr} \end{cases} \quad (6)$$

In case of tempered and compromised messages by the attackers, E_V decreases trust of the sender by:

$$T_{exp(i)} = \begin{cases} (\lambda)^t(1-\beta)T_{exp(i)} + \beta & \text{if } T_{exp(i)} \geq T_{Thr} \\ (\lambda)^{-t}(1-\beta)T_{exp(i)} + \beta & \text{if } T_{exp(i)} < T_{Thr} \end{cases} \quad (7)$$

In equations 6 & 7, α is the honesty reward for providing correct information and the value is $(0 < \alpha < 1)$, while, β is the dishonesty reward for the malicious information. Value of β is in range $(0 < \beta < 1)$. Moreover, $\lambda \in (0,1)$. In above equations, t is the time closeness factor. Let t_{event} is the time of occurrence of event, $t_{current}$ represents the current time, t_{max} is the maximum forgetting time of EBT, time closeness factor (t) is modeled as follows:

$$t = \begin{cases} \dfrac{t_{current} - t_{event}}{t_{max}} & \text{if } (t_{current} - t_{event}) < t_{max} \\ 1 & \text{if } \textit{else} \end{cases} \quad (8)$$

Once, trust and distrust on the received message is calculated, then majority opinion is performed by E_V to decide the trustworthiness of the message. If majority of vehicles agree to the event occurrence, then E_V accepts the information, otherwise, it follows advise from the vehicles with the highest roles in the network.

3) HTM

As stated earlier, these TMs rely on both node and data for the evaluation of trust. In this paper, we implemented an event-oriented HTM known as VSRP (Vehicular Security through Reputation and Plausibility checks) [33]. VSRP integrates a reputation-based trust model to quickly identify and isolate adversaries from the network. In this TM, every node is equipped with two tables: (1) neighboring table and (2) trust table. Whenever, E_V encountered any neighbor, it stores its ID and reputation in the neighboring table and its trust value in the corresponding trust table.

E_V performs following four steps for trust management and eviction of the malicious nodes from the network:

1) **Neighbor discovery:** This phase identifies neighbors by broadcasting a *neighbourreq* packets. Neighbors in the vicinity respond back to this message via *neighbourrep*. Once, neighbor is identified, then initial check is performed on the message from that node by checking the trust table. If entry for the specific node is present with trust value other than 0, then message is accepted, otherwise, message is discarded from such node.

2) **Data dispatching:** In this phase, data is dispatched to the identified neighbors.

3) **Trust decision:** This step calculate trust on the received information based on the threshold range and detection range of the node. If the message is received from a node which lies beyond the threshold range, message is discarded by the fact that node lies very far from the E_V. If message is received from the node inside threshold range, then second check on the detection range is performed on the message. If E_V receives a message from within the detection range, then it calculate trust on the message. Since, E_V has direct information about the event within the detection range, then if message received from the transmitting vehicle contradicts the point of view of E_V, then message is assumed to be compromised and is discarded. However, if received message is correct, then E_V increments the trust of the message sender with an honesty factor. In the next step, if E_V node lies outside the detection range of the message, then it collects responses from its neighbors. If total received responses exceeds the defined threshold, then information is accepted and trust is increases, otherwise, message is classified as malicious and trust is decreased.

4) **Neighbor monitoring:** E_V relies heavily on its neighborhood for information collection in VSRP, therefore, every vehicle monitors its neighbors continuously. Based on the shared information from neighbors, E_V can decide whether the node is transmitting correct message or compromised message.

D. MODULE 4: CONTEXT ESTABLISHMENT

1) CONTEXT IDENTIFICATION

In this section, we present the contexts where efficiency of the TMs are to be evaluated. In our work, we have identified two contexts based on the mobility of the vehicles in the network.

CON1: Vehicles with high mobility
CON2: Vehicles with low mobility

2) IDENTIFICATION OF ATTACKER MODEL

In order to evaluate the efficiency of different TMs in presence of adversaries, we considered attacker model (AM) which is altering and delaying legitimate messages with the factor of "d". The following two AMs were considered in this work:

AM1: Attackers are static in the network
AM2: Attackers are mobile in the network

3) VANET ATTACK SCENARIO

With the identification of the context and AMs in VANET, following four combinational scenarios are possible as shown in Table 4. Scenario 1 represents a network with highly mobile legitimate vehicles and attackers which are statically present in the network. In scenario 2, both legitimate vehicles and attackers are mobile. Scenario 3 is composed of network where vehicles have low mobility and attackers are static in the network, while in scenario 4, legitimate vehicles have low mobility, but attackers are also mobile in the network.

TABLE 4. VANET attack scenario.

Scenario	Context	Attacker Model
Scenario 1 (S1)	High Mobility (CON1)	Static Attacker (AM1)
Scenario 2 (S2)	High Mobility (CON1)	Mobile Attacker (AM2)
Scenario 3 (S3)	Low Mobility (CON2)	Static Attacker (AM1)
Scenario 4 (S4)	Low Mobility (CON2)	Mobile Attacker (AM2)

E. MODULE 5: TRUST EVALUATION PLATFORM

Trust Evaluation Platform (TEP) represents the most significant module of the trust evaluation framework where TMs are evaluated according to several proposed criteria. The message received at E_V is acceptable only when it is verified in terms of its authenticity and integrity. According to Figure 2, TEAM framework has three inputs, i.e., (1) list of attacks, (2) trust models, and (3) identified contexts. TEAM has following four modules for the evaluation of TMs:

1) Message Evaluation Module
2) Trust Computation Module
3) Trust Updation Module
4) Trust Evaluation Module

1) MESSAGE EVALUATION MODULE

This module is responsible for the early identification of false events in the network by performing initial checks on the messages. The messages generated about specific event is verified and evaluated for its authenticity and accuracy. In our framework, the received message (M) is composed of two sub-messages:

$$M = M_O + M_T \tag{9}$$

where M_O represents original message containing information regarding location and time of event generation, while M_T is the trust message incorporating confidence of sender about the event. Once M is received at E_V, it is verified in the following two dimensions:

- **Message Validity (M_V):** Every M have respective validity depending upon the event. For instance, the information related to route closure due to construction should be valid for about 60-120 minutes while temporary road blockage due to minor accident should be valid for 30-40 minutes in that specific region. This information regarding the message validity can be verified by time stamps of M.
- **Message Relevancy (M_R):** ensures accurate information dissemination to the vehicular users. For example, if E_V is located at Kedleston Road in Derby, UK, and the received messages contains information about road accident in Birmingham, UK, then this information is irrelevant for E_V. M_R can be achieved with GPS coordinates of the message sender.

Based on M_V and M_R, following four cases arises. Figure 3 shows that E_V computes trust on received M only if it provides both valid and relevant messages. Distrust is computed by E_V in all other cases if M violates these early checks on

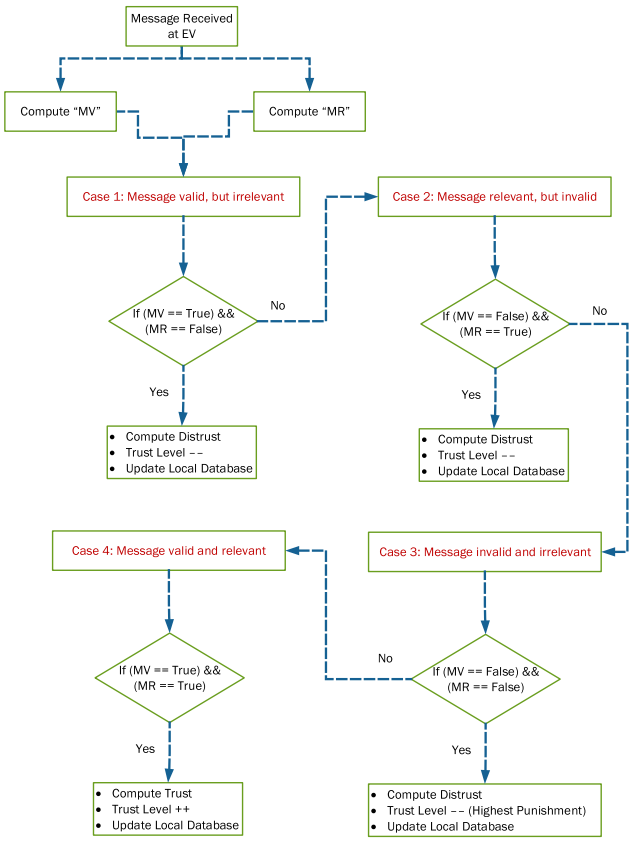

FIGURE 3. Use Cases for Message Verification and Evaluation.

the messages. Once, M is evaluated in terms of its validity and relevancy, then in the next step, trust on M is computed.

2) TRUST COMPUTATION MODULE

This module is responsible for trust computation on the received message. Particularly, following two steps are involved in this module: (1) Identification of initial trust computations, and (2) Trust up-gradation of vehicle in a given time span at the E_V.

The trust computation module is further categorized into two submodules: (1) trust computation on vehicle, and (2) trust computation on data.

a: TRUST COMPUTATION ON THE VEHICLE

Whenever a message is received at E_V, trust is either computed on vehicle or its data based on the above two submodules. This module integrates two basic trust computation methods: 1) Role-based trust (RBT), and 2) Experienced-based trust (EBT). RBT incorporates trust from those vehicles which are highly trusted in the network. For instance, law-enforcement vehicles or ambulances etc. In our framework, we have defined four types of vehicles (*veh*) in the network. (1) Higher authority (*HA*) vehicles (such as law-enforcement, and ambulances) – the messages from such vehicles are highly trusted as they are authorized by the central authority. (2) Public transport (*PT*) vehicles (such as buses, and taxis) – highly trusted as they are authenticated and authorized by specific department, (3) Professional (*P*) vehicles – individual drivers with higher travel experience, (4) Ordinary (*O*) Cars – cars with no travel history. Since, to ensure the realistic behavior of the network in terms of trusted vehicles, we assume that *HA* vehicles are most trusted as the information generated by such vehicles is authenticated by the central authority. Next, the information shared by *PT* is also trusted due to their authorization by a specific department. Similarly, for *P* vehicles, node authorization is done at the node level. Therefore, we can model RBT according to equation 10.

$$Trust_{RBT} = \begin{cases} 1 & \text{if } veh = HA \\ 0.9 & \text{if } veh = PT \\ 0.8 & \text{if } veh = P \end{cases} \tag{10}$$

As stated earlier, VANET is a large scale, therefore, we assume that the network will have majority of ordinary vehicles and a minority of role-based vehicles. In our model, messages received from first three types of vehicles are highly trusted as shown in equation 10. However, if message is received from ordinary vehicles, then EBT is computed to check the authenticity and accuracy of the message. As explained earlier, EBT incorporates location and time closeness factor into account to calculate trustworthiness on the received message. If vehicle transmitted correct message (M), then E_V increase trust level of the message sender vehicle by an honesty factor. However, trust of the transmitting vehicle is decreased by a punishment factor if shared M is malicious as described by equation 11.

$$Trust_{EBT} = \begin{cases} Honesty & \text{if } M = Trusted \\ Punishment & \text{if } M = Untrusted \end{cases} \tag{11}$$

b: TRUST COMPUTATION ON THE DATA

Whenever, sender vehicle transmits a message, it also integrates its confidence level (C_L) on the message. C_L plays a significant role in trust computation, where it ensures that the sender vehicle is confident enough on the authenticity and accuracy of the transmitted message. C_L depends on two aspects: (1) high C_L values are desirable if vehicle has direct link to the event, (2) C_L varies from high to low for indirect interaction of vehicle with the event. Thus, trust computation on the message depends on the link between the sender and the E_V. For direct message, trust is calculated based on the quality of message which depends on C_L and the information quality (*infoQ*). Vehicles residing close to event have high C_L and (*infoQ*), thus messages received from such vehicles are trusted. On the other hand, trust from vehicles decreases with its increasing distance from the event. In case of trust evaluation for indirect messages, a broadcast/drop ratio is employed according to equation 3. High trust is assigned to vehicles if this ratio is high and vice versa.

(a) (b)

FIGURE 4. Simulated Maps of Derby (a) Urban (b) Rural.

3) TRUST EVALUATION MODULE

Once, trust on the node and data is computed, next step is to evaluate the trust via trust evaluation module. In order to do so, we proposed and implemented sixteen distinct evaluation criteria in our framework based on network topology, data generation and time duration [42]. For demonstration of our framework, we evaluated TMs against eight criteria depending upon network topology (legitimate & malicious vehicles), QoS of network, security and amount of trusted information in the network. These are (1) event certainty, (2) robustness against attacks, (3) managing end-to-end delays, (4) promoting node trustworthiness, (5) operating in presence of malicious vehicles, (6) benchmarking against other TMs, (7) detecting false positives and false negatives, and (8) operating in various contexts.

IV. SIMULATION ENVIRONMENT

A. SIMULATION SETUP

The core objective of our simulation is to study the performance of TMs in presence of malicious vehicles in the network. To facilitate our simulations, we used Veins [43], [44], an open source framework used widely for the simulations of vehicular networks. Veins is built on top of two popular simulators: SUMO (traffic simulator) [45], [46] and OMNET++ (discrete event simulator) [47]. SUMO provides mobility and traffic patterns for a map which can be imported from OpenStreetMap while OMNET++ provides various modules (application layer, DSRC and physical layer) to ensure realistic network behavior. A small patch "Traffic Control Interface (TraCI)" is used for communication between OMNET++ and SUMO [48]. Whenever, an event (accident information) is triggered in OMNET++, TraCI enables the vehicles in SUMO to change their route by sending out respective commands.

In order to identify the behavior and performance of TMs, we imported two maps from the city of Derby, United Kingdom using OpenStreetMap [49], [50]. One map represents a city center scenario while other shows the rural area of Derby as depicted in Figure 4. The vehicles in the city center have low mobility while rural area contain vehicles with high mobility. Moreover, all vehicles are equipped with standard wireless communication interface, i.e., IEEE 802.11p protocol. In order to facilitate attackers in the network, we considered mobile attackers in scenario 2 & 4. These attackers have the ability to launch attacks while on the move, thus creating impact on different regions of the network. For scenario 1 & 3, static attackers are randomly placed throughout the network.

According to [51], majority of the vehicles in the network are legitimate and performs their task honestly. Therefore, to study the behavior of the TMs in presence of malicious vehicles, we kept the number of legitimate vehicles constant and increases the presence of adversaries in the network from 10% to 50%.

Table 5 provide the details of various parameters used for the evaluation of TMs. We used a condition that ($\beta = 10 \times \alpha$) based on logic that trust cannot be established easily, i.e, trust is very rare and easy to break. In our simulations, we also kept the initial trust value to 0.5 to avoid the cold start problem [52], [53].

B. ADVERSARY MODEL

An adversary is a node which have the ability to launch an attack to gain unauthorized entry into the system for their own interest [37]. In order to evaluate performance of TMs in presence of attackers, we considered man-in-the-middle attacks (MITM) as an adversary model for TEAM framework which is identified via threat model (module 1) and

TABLE 5. Simulation details.

Parameter		Value
Simulation Framework	Network Simulator	OMNET++ 5.0
	Traffic Simulator	SUMO 0.25.0
	V2X Simulator	VEINS 4.4
Simulation Details	Simulation Area (Urban)	4 km × 2.5 km
	Simulation Area (Rural)	10 km × 8 km
	Simulation Time	1000 secs
	Event Start Time	75 sec
	Event Duration	50 secs
	No. of Legitimate Vehicles	100
	No. of Malicious Vehicles (%)	10, 20, 30, 40, 50
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 Details	Initial Trust	0.5
	Trust Threshold	0.5
	Honesty Factor (α)	0.01
	Dishonesty Factor (β)	0.1
Attacker Model	Actions	1) Content Alter 2) Content Delay
	Delay (d)	2 secs

risk assessment (module 2) of the framework. According to risk assessment, MITM poses critical risk in VANET, therefore, we considered MITM attack with the ability to alter and delay sensitive (i.e., accident) information by a factor of "d" seconds. Since, very sensitive information (such as collision avoidance) is shared among vehicles in VANET, therefore, tempering such data can have severe impact on the network. Further, delaying such sensitive data prohibits the legitimate vehicles to receive information on-time. The designed adversary model is equipped with both of these capabilities. In order to demonstrate TEAM framework, three trust models are evaluated in presence of such MITM attackers. The high-level pseudo code of considered adversary model is depicted in algorithm 1. It can be seen that whenever message arrives at the MITM attacker, the attacker first creates an attacked message M_A, where the content is first altered using specific alteration function. In the next phase, delay is calculated at the attacker node which is then appended to the altered message. At this stage, the attacker broadcast the message which is then received by the legitimate vehicles in its vicinity.

Algorithm 1 Adversary Model

Input: Legitimate Message M_G
Output: Attacked Message M_A

```
if (received message == M_G) then
    Check 'content' of M_G
    if (content == "data") then
        Create Attacked Message "M_A"
        Message_alteration(M_A)
        Message_delay(M_A)
    end if
    Transmit M_A at time (t_send + d)
end if
```

C. EVALUATION METRICS

We defined following metrics to evaluate the efficiency of TMs using TEAM in terms of security and Quality of Service (QoS).

1) END-TO-END DELAY (E2ED)

This metric relates to QoS of TM; depicting the total delay caused to packets generated by legitimate vehicle to be shared with neighboring vehicles. As our attacker model is constantly delaying messages, therefore, E2ED is an important metric to understand the behavior of TM when packets are delayed by such malicious vehicles. Ideally, TM with low E2ED is desirable in the network. E2ED is the difference of packet generation time (T_G) and packet reception time (T_R) which is calculated as follows:

$$E2ED = T_R - T_G \tag{12}$$

2) EVENT DETECTION PROBABILITY (EDP)

We defined this metric to identify true events in the network. As the attack model in our simulator can change true information with garbage information, therefore, this metric (EDP) will correctly identify true and bogus events in the network. Let E_{Tot} represents total events generated in the network, out of which E_T and E_M are true and malicious events respectively, then probability to detect true event (EDP) can be mathematically given by:

$$EDP = \frac{\sum(E_{Tot} - E_M)}{E_{Tot}} \tag{13}$$

The TM is considered to be effective and efficient, if it has high event detection rate.

3) ANOMALY RATIO (AR)

AR is defined to identify malicious activity in the network. The transmitting vehicle performs two types of activities in the network, i.e., either legitimate or malicious. Based on this metric, E_V can identify the behavior of transmitting node. Upon detection of malicious activity by E_V, this information is shared with the neighboring vehicles. Higher the AR ratio, higher the node have ability to detect malicious node in the network [54]. AR is defined as the ratio of malicious packets to the total generated messages. Let sender 'S' generates total $M_T(S)$ messages, $M_M(S)$ represents those packets which are tempered and compromised by the sender, then, AR ($\eta(S)$) can be represented as follows.

$$\eta(S) = \frac{M_M(S)}{M_T(S)} \tag{14}$$

4) FALSE POSITIVE RATE (FPR)

FPR represents the effectiveness of TM to identify compromised messages which are incorrectly labeled and identified as legitimate vehicles. Ideally, the TMs should have low FPR values. Let $P_{M|L}$ represents the probability of detecting node as malicious, given the node is legitimate, and $P_{L|L}$ is

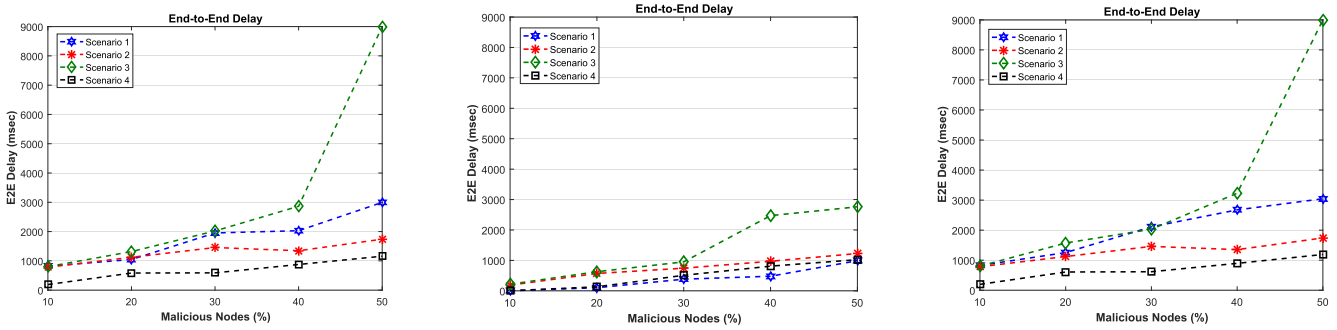

FIGURE 5. End-to-End Delay (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM.

the probability of detecting node as legitimate, given the node is legitimate, then FPR is mathematically written as:

$$False\ Positive\ Rate = \frac{P_{M|L}}{P_{L|L} + P_{M|L}} \tag{15}$$

5) TRUSTED & UNTRUSTED PACKETS

These metrics are defined to identify the amount of trusted and untrusted packets in the network. Let N_{Total} is the total packets generated in the network. Out of N_{Total} packets, $N_{Trusted}$ are the trusted packets and $N_{Untrusted}$ are the untrusted packets. Then we calculate trusted and untrusted packets as follows:

$$N_{Trusted} = \sum (N_{Total} - N_{Untrusted}) \tag{16}$$

$$N_{Untrusted} = \sum (N_{Total} - N_{Trusted}) \tag{17}$$

V. RESULTS AND DISCUSSION

In this section, we first present the simulation results of different TMs using our proposed TEAM framework. Then, we focused on the discussion of the performance of TEAM framework.

A. EVALUATION OF TRUST MODELS

We evaluated the performance of three TMs (data-oriented trust model, entity-oriented trust model, hybrid trust model) using various evaluation criteria which mainly focused on the security and QoS of the network as mentioned in section IV-C. Figures 5 to 10 depict that the presence of malicious vehicles deteriorate the performance of TMs in terms of high end-to-end delays, false positive rates and high number of untrusted packets in the network. Moreover, the existence of adversaries also reduces the probability to detect true events, anomalies and generation of trusted packets in the network.

1) END-TO-END DELAY

Figure 5a shows E2ED of data-oriented trust model in four scenarios. It can be seen that scenario 4 outperforms other scenarios by achieving lowest end-to-end delay (E2ED). Moreover, static attackers affect the network more rather than mobile attackers. As the impact created by static attackers is limited to a specific geographical location, therefore, increasing such malicious vehicles results in delaying more packets in the network, ultimately increasing the overall E2ED. On the other hand, the scope of attack by mobile attacker is not limited to specific location due to their constant mobility. It is quite possible that legitimate vehicles might receive messages from neighborhood in that specific location. Comparing all scenarios for DOTM, for a network with 50% malicious vehicles, we observed that scenario 1, 2 & 3 attains 61.33%, 96.47% & 98.92% high E2EDs respectively as compared to scenario 4.

Figure 5b highlights E2ED for entity-oriented trust model, where network with low mobility is affected significantly by static malicious entries. These malicious vehicles introduce massive delay in the attack-prone area which prohibits the legitimate vehicles to receive messages on time. Increasing static attackers in the network increases the attack vector which results in higher message delay. On the other hand, mobile attackers have high influence on the network with high mobility. Attack vector of such attackers continuously change due to their mobility, thus the impact caused by mobile malicious vehicles is different from static malicious vehicles. From Figure 5b, we observe that when a network contains 50% malicious vehicles, scenario 1 performs 19.31%, 64.16% and 3.3% better than scenario 2, 3 and 4 respectively by achieving low E2E delays.

Figure 5c represents the E2E delay of the network utilizing hybrid trust model. The performance of HTM is similar to DOTM, where, network achieves highest end-to-end delays in scenario 3 and lowest in scenario 4. HTM integrates both sender reputation and data correctness, thus the evaluator node requires more time to calculate and evaluate trust as these are time intensive processes. From Figure 5c, scenario 4 performs 31.6%, 60.9% and 86.7% better than scenario 2, 1 and 3 respectively by achieving lower E2ED.

Figure 5 presents the simulation results of three trust models in terms of end-to-end delay. It can be seen that the network achieves low E2ED in presence of EOTM, rather

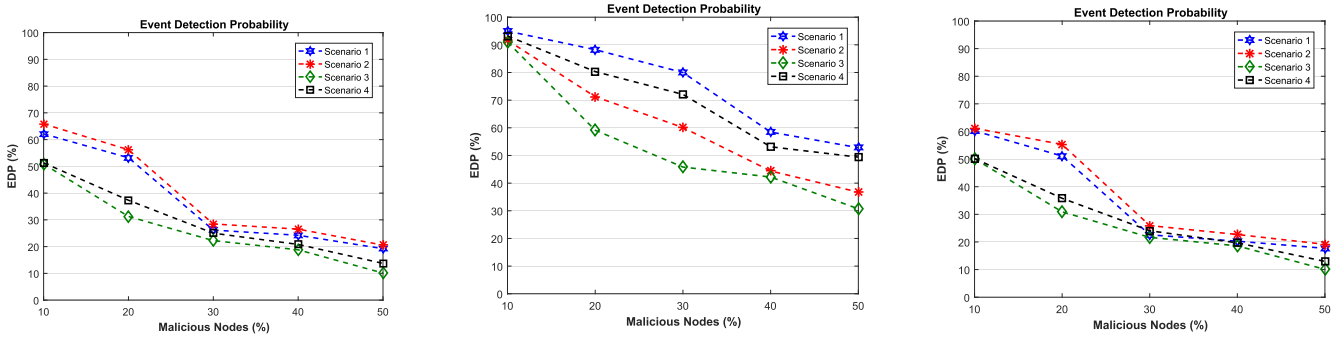

FIGURE 6. Event Detection Probability (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM.

than DOTM and HTM. This is due to the existence of role-based and highly experienced vehicles which can detect and eliminate dishonest vehicles from the network. On the other hand, DOTM and HTM depends on data for trust evaluation, which is continuously delayed by the malicious vehicles. As a result, legitimate vehicles are unable to receive messages in-time, thus creating a strong impact on the network in terms of high E2E delay.

2) EVENT DETECTION PROBABILITY

Figure 6a depicts the probability of data-oriented trust model to detect true events in four scenarios. It can be seen that highest EDP is achieved when the network contains mobile attackers. The attack vector of the mobile attacker constantly changes. As a result, probability of vehicles to detect true event increases as they might receive true events from other honest vehicles in its vicinity. On the other hand, static attackers decreases the ability of legitimate vehicles to detect true events due to constant attack-vector in geographical location. For a network with 20% malicious nodes, scenario 2 achieves 5.3%, 44.3% & 33.5% high EDP than scenario 1, 3 & 4 respectively.

Event detection probability of entity-oriented TM is shown in Figure 6b, highlighting that high mobility networks are affected to a greater extent with mobile attackers, where the detection of true events decreases massively in the network. Static attackers, on the other hand, create high impact on the network with low mobility (such as city center), where increasing such vehicles increases the generation of compromised messages in the network. This limits the scope of the legitimate vehicles to correctly detect true events in the network. Among all the considered scenarios, highest EDP is achieved in scenario 1 and lowest EDP in scenario 3. When the network is injected with 20% malicious nodes, scenario 1 achieves 8.9%, 19.2% & 32.9% better EDP than scenario 4, 2 & 3 respectively.

Figure 6c shows the true event detection probability of hybrid trust model in four scenarios. HTM performs similar to DOTM where highest EDP is achieved in scenario 2 and lowest in scenario 3. The vehicles incorporating HTM integrates trust evaluation on the received data, which may be tempered by malicious vehicles. Increasing such vehicles which disseminates compromised data will limit the vehicles to correctly identify true events, thus decreasing network efficiency. For a network having 20% malicious vehicles, scenario 2 achieves 7.5%, 44.1% & 35.2% high EDP than scenario 1, 3 & 4 respectively.

Figure 6 depicts that the event detection probability of entity-oriented trust model is better than other trust models. EOTM integrates role-based trust mechanism which ensures the propagation of true events in the network. As a result, the scope of vehicles to detect true events increases in the network in presence of malicious vehicles.

3) ANOMALY RATIO

Figure 7a depicts the capability of data-oriented trust model to detect anomalies in the network. It shows that scenario 4 outperforms other scenarios by detecting maximum number of anomalies. This is due to the fact that mobile attackers affect the high number of vehicles as a consequence of their low mobility. On the other hand, less anomalies are detected in scenario 1, as the vehicles communicate for a very short span of time for highly mobile legitimate vehicles and static attackers. For 50% malicious vehicles, scenario 4 can detect 31.1%, 77.5% & 86.13% better anomalies than scenario 2, 3 & 1 respectively.

Figure 7b shows the anomaly ratio of the network incorporating entity-oriented trust model, highlighting that scenario 4 can detect high number of anomalies in the network as in DOTM. The low mobility and high number of legitimate vehicles (e.g., city center) can detect malicious activity in the network. When the network contains 50% malicious vehicles, scenario 4 detects 81.1%, 2.16% and 84.88% more anomalies than scenario 1, 2 and 3 respectively.

The ability of hybrid trust model to detect anomalies is shown in figure 7c. HTM behaves similar to DOTM where low mobility of legitimate vehicles detects high number of anomalies in the network in the presence of mobile malicious attackers. These attackers provide an opportunity of window to the vehicles to communicate and detect anomalies

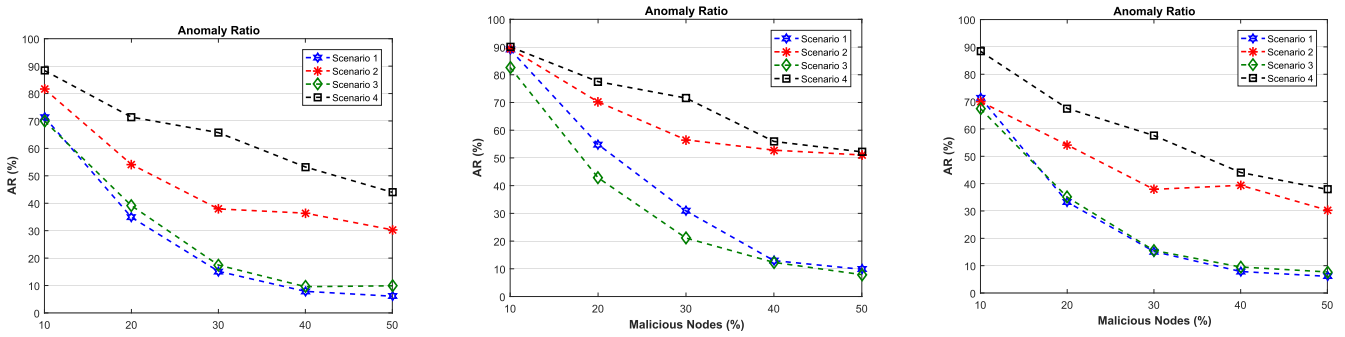

FIGURE 7. Anomaly Ratio (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM.

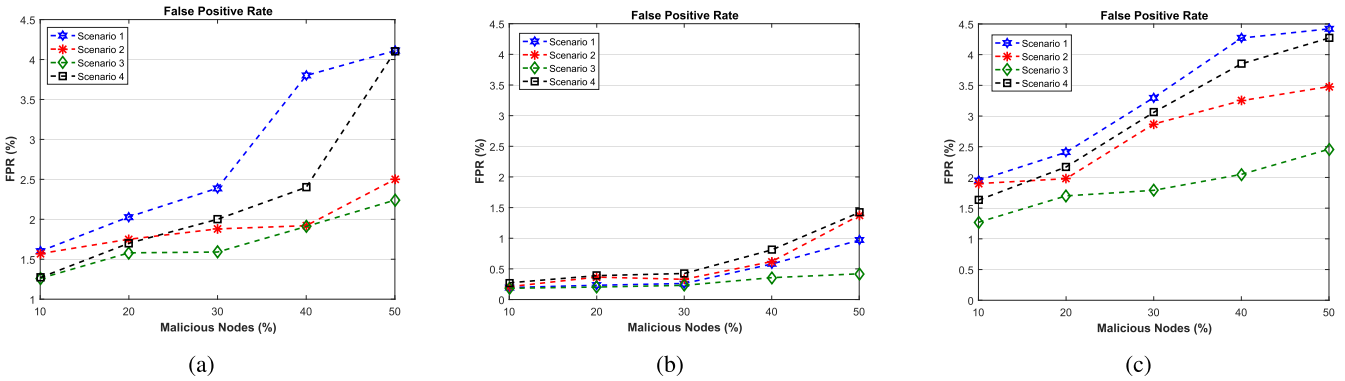

FIGURE 8. False Positive Rate (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM.

in the network. For a network injected with 50 % malicious vehicles, scenario 4 provides 83.9%, 20% and 79.6% better results than scenario 1, 2 and 3 respectively by detecting more anomalies.

In short, figure 7 clearly depicts that entity-oriented trust model can detect high number of anomalies than data-oriented and hybrid trust model. EOTM relies on trusted and experienced vehicles which are classified as trusted members of the network by the higher authorities, thus, the ability of the vehicles to detect malicious activity in the network increases.

4) FALSE POSITIVE RATE

False positive rate illustrate the error margin of the TM where malicious entity and its content is incorrectly identified as legitimate. FPR of the data-oriented and hybrid trust models is shown in Figures 8a & 8c, emphasizing that network attains high FPR in scenario 1 & 4 where it increases almost exponentially as compared to scenario 2 & 3. Moreover, DOTM & HTM achieves high FPR for a network containing high mobility and static attackers. These attackers provide limited window of opportunity for legitimate vehicles to communicate with each other. Increasing such malicious vehicles in the network increases the probability of incorrectly labeling valid data as malicious. DOTM and HTM achieves low FPR in urban scenario where high density of legitimate vehicles can correctly identify valid messages. For a network incorporating DOTM and containing 30% malicious vehicles, scenario 3 achieves 50.3%, 18.23% and 25.78% low FPR than scenario 1, 2 and 4 respectively. In case of HTM, scenario 3 achieves 45.7%, 37.6% and 41.5% low FPR than scenario 1, 2 and 4 respectively.

FPR for entity-oriented trust model is highlighted in Figure 8b, demonstrating that efficiency of the network decreases in terms of FPR when it is flooded with mobile attackers. The attack-vector of such attacker changes continuously which increase the probability of incorrectly classifying malicious message as valid. Among 4 scenarios, EOTM performs better in scenario 3, where low FPR is achieved. The low mobility and high density of vehicles produce a massive amount of messages, which provide an extended window to legitimate vehicles to identify true and malicious events in the network. When a network is flooded with 30% malicious nodes, scenario 3 performs 11.4%, 29.6% and 45.4% better than scenario 1, 2 and 4 respectively by achieving low FPR. The main reason for achieving low FPR in EOTM and HTM is the integration of role-based and direct trust evaluation mechanism respectively, thus reducing the probability to incorrectly detect malicious nodes.

5) TRUSTED AND UNTRUSTED PACKETS

Figures 9 & 10 show the number of trusted and untrusted packets generated by a network incorporating DOTM, EOTM

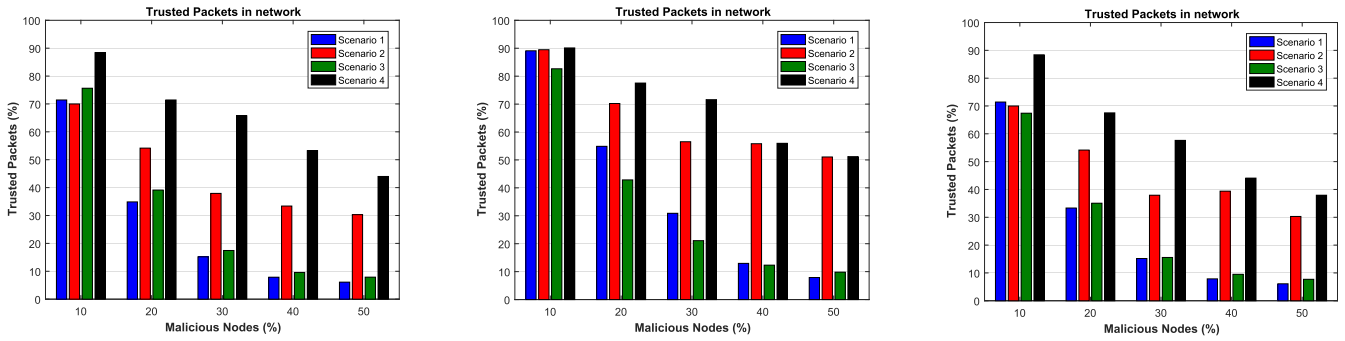

FIGURE 9. Trusted packets in the network (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM.

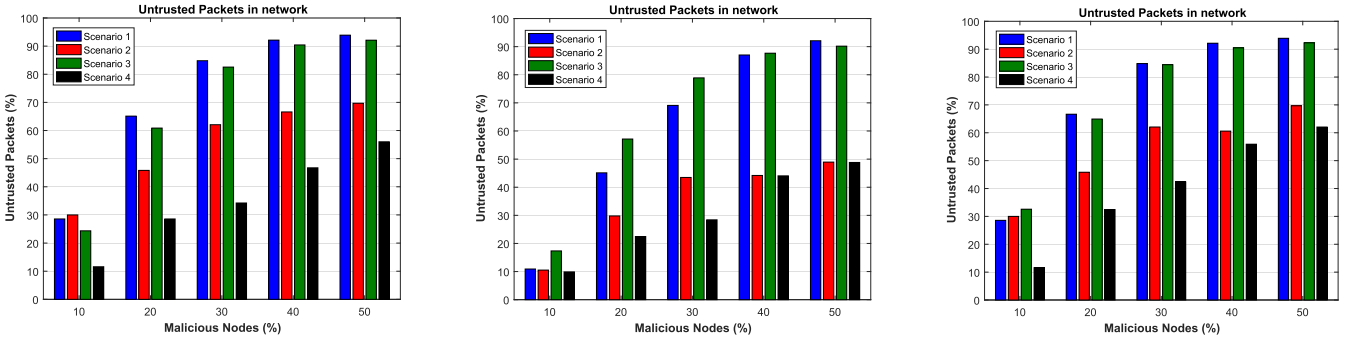

FIGURE 10. Untrusted packets in the network (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM.

and HTM respectively, demonstrating that scenario 4 outperforms other scenarios by propagating high number of trusted messages in VANET. This is due to the fact that low mobility of vehicles provide ample amount of time for legitimate vehicles to validate trust on the sender. Moreover, network is affected when it is polluted with static attackers. These attackers have a constant attack-vector in a attack-prone location, thus it is highly unlikely that vehicles receive trusted messages from legitimate vehicles in presence of these attackers. On the contrary, vehicles have the possibility to receive trusted messages in presence of mobile attackers as the attack-vector changes continuously due to their mobility.

When a network integrates DOTM and is flooded with 50% malicious vehicles, scenario 4 generates 86.12%, 31.12% and 82% more trusted packets and 67.66%, 24.45% and 64.46% less untrusted packets generated for scenario 1, 2 and 3 respectively. In case of the network with EOTM, scenario 4 generates 84.5%, 0.25% and 80.8% more trusted and 47%, 0.26%, 45.87% less untrusted packets than scenario 1, 2, and 3 respectively. Moreover, for a network incorporating HTM, scenario 4 produces 83.9%, 20.1% and 79.6% more trusted and 33.9%, 10.94%, 32.68% less untrusted packets than scenario 1, 2, and 3 respectively.

B. DISCUSSION

In this section, we focus on the discussion of TEAM framework performance in terms of its applicability, usability, scalability, security assurance and limitation.

1) APPLICABILITY OF TEAM

TEAM provides a base framework for smart city planners and automobile manufacturers to design, test and validate TMs in different contexts and attacker models before integrating them within the vehicles and network. Moreover, TEAM provides various TMs for benchmarking purposes. Further, TEAM can be used by the researchers to validate their newly designed TM. Thus, a wide range of users (automobile manufacturers, researchers and smart city planners) can evaluate the efficiency of the designed TM by comparing it against benchmarked TM using an extensive set of realistic trust evaluation criteria.

2) USABILITY OF TEAM

TEAM is designed using three widely used open-source platforms, i.e., OMNET++, VEINS and SUMO. OMNET++ supports the graphical user interface, therefore, TEAM can provide the graphical representation of the network where the user can visualize the behavior of the TM. Thus, the smart city planners or users with knowledge about these

standardized platforms can validate newly designed and available TMs using TEAM. However, a small effort is required to understand the implementation and integration of various components of TM within the framework. TEAM is available to researchers upon request for research purposes.

3) SCALABILITY ANALYSIS

Scalability is one of the crucial requirement in VANET as the rate of entering and exiting vehicles in the network is not constant. Thus, the TMs should be scalable and independent of network size and vehicles mobility. TEAM is a scalable framework as it integrates scalable simulation tools such as OMNET++ [55], SUMO [56] and VEINS [57].

We tested our framework by evaluating TMs in four contexts with random vehicular mobility. However, more contexts can easily be integrated in TEAM. For example, contexts based on vehicles concentration and dispersion across the network is not considered in current framework.

Moreover, in the context of smart city, TEAM can support high number of vehicles to better understand the behavior of TMs for validation purposes. TEAM framework integrates realistic maps, imported directly from OpenStreetMap. Traffic is generated on these maps via SUMO which includes both mobile and static vehicles (attackers) in the network. However, identifying the ideal location on the map for placing static vehicles is a time intensive process as the user has to first identify the favorable place on the map and then align the vehicle in that location to utilize its capabilities. This complexity increases when the user has to place a high number of static vehicles in the network. For instance, placing 80% static attackers for a network with 1000 vehicles is challenging as the user has to identify ideal locations for implementing such high number of attackers on the map.

4) SECURITY ANALYSIS

It is eminently important for TMs to be robust against attacks which reduces the network performance by transmitting untrusted and compromised messages in the network such as MITM attacks. Threat model and risk assessment modules of TEAM identified various attacker models (AMs) with critical and high risk in the network. Our framework has the ability to provide the security perspective for the evaluation of TMs in the network as AMs with critical risks are integrated within TEAM. We tested the behavior of three TMs using TEAM in presence of MITM attackers. Simulation results indicate that the implemented EOTM is more resilient to MITM attacks than DOTM and HTM. This is due to the fact that EOTM integrates role-based and experience-based trust management schemes which ensures the propagation of trusted messages in the network. On the other hand, DOTM and HTM relies heavily on trustworthiness of data for trust calculation, which can be compromised by the attackers. Further, the absence of role-based vehicles in the network degrades the performance of DOTM and HTM in presence of MITM attacks as no trusted vehicle is present to evaluate the trustworthiness of the message. Therefore, DOTM and HTM has to rely on ordinary vehicles for trust calculation. In general, any trust model which integrates role-based trust management scheme can perform well in presence of malicious vehicles as this can ensure the presence of trusted information in the network.

5) LIMITATION OF TEAM

Simulation results showed the applicability of TEAM to accurately evaluate the TMs in VANET. However, there are certain limitations in current framework.

- Modeling human factor (driver's honesty and selfishness) accurately for trust management is a challenging task in VANET. Recently, some TMs are proposed which relies on social networks for trust management such as [58] and [59]. Currently, TEAM can only evaluate TMs for pure VANET and it cannot evaluate social-network based TMs as it is not integrated in our framework yet.
- Recently, some effort is done in adopting Content-Centric Networking (CCN) and Named Data Networking (NDN) into VANET [60], [61]. Currently, TEAM is limited to host-based communication paradigm only, and hence, it can not evaluate TMs which are developed purely on CCN and NDN-based VANET.
- We have tested the performance of our framework with up-to 300 vehicles which were generated in SUMO. Theoretically, TEAM is scalable and can support higher number of vehicles. Only complexity is placing higher number of static nodes at the micro-level on the realistic map.

VI. CONCLUSION

A secure and attack-free environment is a prerequisite in VANET for trusted message dissemination among vehicles and infrastructure. However, as various contexts are involved in VANET, ensuring trusted environment in every context is an extremely challenging task as the attackers penetrate the network and pollute it with bogus information. Therefore, the TMs should be validated in different context of VANET, and there should be a way to compare different proposed TMs.

In this paper, we presented a novel framework which can validate and evaluate the efficiency of TMs in VANET. Various attacker models are identified using threat model and risk assessment which are integrated in our framework. These attacker models can be used to evaluate TMs in presence of the malicious nodes.

In order to demonstrate our framework, we implemented three different TMs, i.e., entity-oriented, data-oriented and hybrid trust model. We conducted an extensive set of simulations to study the behavior of TMs under different contexts and attacker models. TEAM revealed an interesting result which changes the general perception that hybrid trust models perform better in VANET due to their imperative nature of evaluating trust on both vehicle and data. However, according to our framework, entity-oriented TM outperforms both data-oriented and hybrid TMs. This is due to the presence of highly

trusted and experienced vehicles in the network ensuring the dissemination of trusted messages.

As future work, we intend to extend this research by implementing and evaluating more TMs with TEAM against further attacker models and contexts.

REFERENCES

[1] E. C. Eze, S.-J. Zhang, E.-J. Liu, and J. C. Eze, "Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development," *Int. J. Autom. Comput.*, vol. 13, no. 1, pp. 1–18, 2016.

[2] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, Nov. 2011.

[3] R. G. Engoulou and M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[4] J. Liu, J. Wan, Q. Wang, B. Zeng, and S. Fang, "A time-recordable cross-layer communication protocol for the positioning of vehicular cyber-physical systems," *Future Gener. Comput. Syst.*, vol. 56, pp. 438–448, Mar. 2016, doi: 10.1016/j.future.2015.08.014.

[5] A. M. Vegni, M. Biagi, and R. Cusani, "Smart vehicles, technologies and main applications in vehicular ad hoc networks," in *Vehicular Technologies—Deployment and Applications*, L. G. Giordano and L. Reggiani, Eds. Rijeka, Croatia: InTech, 2013, ch. 1. [Online]. Available: http://dx.doi.org/10.5772/55492

[6] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-based smart cities: Recent advances and challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16–24, Sep. 2017, doi: 10.1109/MCOM.2017.1600514.

[7] G. S. Khekare and A. V. Sakhare, "A smart city framework for intelligent traffic system using VANET," in *Proc. Int. Mutli-Conf. Autom., Comput., Commun., Control Compressed Sens.*, Mar. 2013, pp. 302–305.

[8] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proc. 6th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2012, pp. 1–9.

[9] I. A. Sumra, I. Ahmad, H. Hasbullah, and J.-L. B. A. Manan, "Classes of attacks in VANET," in *Proc. Saudi Int. Electron., Commun. Photon. Conf. (SIECPC)*, Apr. 2011, pp. 1–5.

[10] F. Ahmad, M. Kazim, A. Adnane, and A. Awad, "Vehicular cloud networks: Architecture, applications and security issues," in *Proc. IEEE/ACM 8th Int. Conf. Utility Cloud Comput. (UCC)*, Dec. 2015, pp. 571–576.

[11] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Commun. J.*, vol. 4, no. 7, pp. 894–903, 2010.

[12] J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, and Y. Qiao, "A survey on position-based routing for vehicular ad hoc networks," *Telecommun. Syst.*, vol. 62, no. 1, pp. 15–30, 2016, doi: 10.1007/s11235-015-9979-7.

[13] J. Grover, M. S. Gaur, and V. Laxmi, "Trust establishment techniques in VANET," in *Wireless Networks and Security* (Signals and Communication Technology). Berlin, Germany: Springer, 2013, pp. 273–301.

[14] F. Li and Y. Wang, "routing in vehicular ad hoc networks: A survey," *IEEE Veh. Technol. Mag.*, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[15] J. Zhang, "A survey on trust management for VANETs," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Singapore, Mar. 2011, pp. 105–112.

[16] 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, doi: 10.1109/ACCESS.2016.2645452.

[17] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2013, pp. 1–6.

[18] J. Zhang, "Trust management for VANETs: Challenges, desired properties and future directions," *Int. J. Distrib. Syst. Technol.*, vol. 3, no. 1, pp. 48–62, 2012.

[19] Q. Alriyami, A. Adnane, and A. K. Smith, "Evaluation criterias for trust management in vehicular ad-hoc networks (VANETs)," in *Proc. 3rd Int. Conf. Connected Veh. Expo (ICCVE)*, 2014, pp. 118–123.

[20] S. Ahmed, S. Al-Rubeaai, and K. Tepe, "Novel trust framework for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9498–9511, Oct. 2017.

[21] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[22] T. Gazdar, A. Belghith, and H. Abutair, "An enhanced distributed trust computing protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, 2017.

[23] T. Biswas, A. Sanzgiri, and S. Upadhyaya, "Building long term trust in vehicular networks," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.

[24] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 39–68.

[25] S. Gurung, D. Lin, A. C. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. 7th Int. Conf. Network Syst. Secur. (NSS)*. Madrid, Spain: Springer, Jun. 2013, pp. 94–108.

[26] R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 1652–1669, 2014.

[27] U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks," in *Proc. Int. Conf. Inf. Commun. Technol. (ICICT)*, Dec. 2014, pp. 965–972.

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

[29] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in Vehicular Ad Hoc Networks: An economic incentive model based approach," in *Proc. Comput., Commun. IT Appl. Conf. (ComComAp)*, Apr. 2013, pp. 13–18.

[30] 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 Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407–420, May 2011.

[31] N. Yang, "A similarity based trust and reputation management framework for VANETs," *Int. J. Future Gener. Commun. Netw.*, vol. 6, no. 2, pp. 25–34, 2013.

[32] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Comput. Elect. Eng.*, vol. 43, pp. 33–47, Apr. 2015.

[33] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Securing vehicular networks: A reputation and plausibility checks-based approach," in *Proc. IEEE Globecom Workshop Web Pervas. Secur.*, Dec. 2010, pp. 1550–1554.

[34] K. C. Abdelaziz, N. Lagraa, and A. Lakas, "Trust model with delayed verification for message relay in VANETs," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2014, pp. 700–705.

[35] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust modeling framework for message propagation and evaluation in VANETs," in *Proc. 2nd Int. Conf. Inf. Technol. Converg. Services*, Aug. 2010, pp. 1–8.

[36] J. Oluoch, "A theoretical framework for trust management in vehicular ad hoc networks," *Int. J. Trust Manage. Comput. Commun.*, vol. 3, no. 2, pp. 147–167, 2015.

[37] F. Ahmad, A. Adnane, and V. N. L. Franqueira, "A systematic approach for cyber security in vehicular networks," *J. Comput. Commun.*, vol. 4, pp. 38–62, Dec. 2016.

[38] "Information technology—Security techniques—Information security risk management," BSI Standard Publication, ISO, Cham, Switzerland, Tech. Rep. BS ISO/IEC 27005:2011, Jun. 2011.

[39] F. Ahmad and A. Adnane, "A novel context-based risk assessment approach in vehicular networks," in *Proc. IEEE 30th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Mar. 2016, pp. 466–474.

[40] C. A. Kerrache, C. T. Calafate, N. Lagraa, J. C. Cano, and P. Manzoni, "Trust-aware opportunistic dissemination scheme for VANET safety applications," in *Proc. Int. IEEE Conf. Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Jul. 2016, pp. 153–160.

[41] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*, document ETSI EN 302 637-3, ETSI, Sophia Antipolis, France, 2014.

[42] 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 *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Soc. Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jun. 2017, pp. 44–52.

[43] Veins. *Vehicles in Network Simulation, The Open Source Vehicular Simulation Framework*. Accessed: Jan. 11, 2018. [Online]. Available: http://veins.car2x.org

[44] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3–15, Jan. 2011.

[45] SUMO. *Simulation of Urban MObility*. Accessed: Apr. 2, 2017. [Online]. Available: http://sumo.dlr.de/wiki/Simulation_of_Urban_MObility

[46] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO—Simulation of urban mobility: An overview," in *Proc. 3rd Int. Conf. Adv. Syst. Simul.*, 2011, pp. 55–60.

[47] OMNET. *OMNET++: Discrete Event Simulator*. Accessed: Jan. 4, 2018. [Online]. Available: https://omnetpp.org/

[48] A. Wegener, M. Piórkowski, M. Raya, H. Hellbrück, S. Fischer, and J.-P. Hubaux, "TraCI: An interface for coupling road traffic and network simulators," in *Proc. 11th Commun. Netw. Simul. Symp.*, 2008, pp. 155–163.

[49] *OpenStreetMap*. Accessed: Oct. 16, 2017. [Online]. Available: https://www.openstreetmap.org

[50] M. Haklay and P. Weber, "OpenStreetMap: User-generated street maps," *IEEE Pervas. Comput.*, vol. 7, no. 4, pp. 12–18, Oct. 2008.

[51] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. Workshop Hot Topics Netw. (HOTNETs)*, 2005, pp. 1–6.

[52] T. Gazdar, A. Belghith, and A. AlMogren, "DTCF: A distributed trust computing framework for vehicular ad hoc networks," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 3, Mar. 2017.

[53] L. H. Son, "Dealing with the new user cold-start problem in recommender systems: A comparative review," *Inf. Syst.*, vol. 58, pp. 87–104, Jun. 2016.

[54] S. Ahmed and K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2016, pp. 1–6.

[55] X. Xian, W. Shi, and H. Huang, "Comparison of OMNET++ and other simulator for WSN simulation," in *Proc. 3rd IEEE Conf. Ind. Electron. Appl.*, Jun. 2008, pp. 1439–1443.

[56] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO—Simulation of urban mobility," *Int. J. Adv. Syst. Meas.*, vol. 5, nos. 3–4, pp. 128–138, 2012.

[57] C. Sommer, J. Härri, F. Hrizi, B. Schünemann, and F. Dressler, "Simulation tools and techniques for vehicular communications and applications," in *Vehicular Ad Hoc Networks*. Cham, Switzerland: Springer, 2015, pp. 365–392.

[58] D. Alishev, R. Hussain, W. Nawaz, and J. Lee, "Social-aware bootstrapping and trust establishing mechanism for vehicular social networks," in *Proc. 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.

[59] X. Chen and L. Wang, "A cloud-based trust management framework for vehicular social networks," *IEEE Access*, vol. 5, pp. 2967–2980, 2017.

[60] S. H. Bouk, S. H. Ahmed, and D. Kim, "Vehicular content centric network (VCCN): A survey and research challenges," in *Proc. 30th Annu. ACM Symp. Appl. Comput. (SAC)*, 2015, pp. 695–700.

[61] M. F. Majeed, S. H. Ahmed, and M. N. Dailey, "Enabling push-based critical data forwarding in vehicular named data networks," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 873–876, Apr. 2017.

FARHAN AHMAD received the B.Sc. degree in electronics engineering from COMSATS Institute of Information Technology, Abbottabad, Pakistan, in 2009, and the M.Sc. degree in communication and information technology from the University of Bremen, Germany, in 2014. He is currently pursuing the Ph.D. degree in computer science with the College of Engineering and Technology, University of Derby, U.K. His research focuses on cyber security, risk-assessment and trust in VANET, vehicular cloud networks, M2M communications, smart cities, and Internet-of-Things.

VIRGINIA N. L. FRANQUEIRA received the Ph.D. degree in computer science from the University of Twente, The Netherlands, in 2009, and the M.Sc. degree from the Federal University of Espirito Santo, Brazil. She was a Lecturer with the University of Central Lancashire, U.K., held a post-doctoral position at the University of Twente, and an Information Security Consultant based in the U.K. She is currently a Senior Lecturer with the University of Derby, U.K. Her topics of research interest include digital forensics, and security engineering and assessment. She is a member of the IEEE Computer Society and the British Computer Society and a fellow of The Higher Education Academy.

ASMA ADNANE received the Ph.D. degree in computer science from the University of Rennes, France. She was a Knowledge Transfer Partnership Associate with the CrowdLab, the University of Leicester, U.K., where she was also a Database and Security Expert. She joined the University of Derby, U.K., as a full-time Senior Lecturer in networks and security. She was a Research Associate/Lecturer with the University of Rennes, France, the University of Nantes, France, and ENSI-Bourges, France. She has published several papers in renowned conferences and journals focusing on ad-hoc network security and trust management. Her research interests include trust management in intelligent transport systems, smart cities, and network security.