# MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles

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



**Original citation & hyperlink:**
Ahmad, F, Kurugollu, F, Adnane, A, Hussain, R & Hussain, F 2020, 'MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles', IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3310-3322.
https://dx.doi.org/10.1109/JIOT.2020.2967568

DOI 10.1109/JIOT.2020.2967568
ESSN 2327-4662

Publisher: Institute of Electrical and Electronics Engineers

# MARINE: Man-in-the-middle Attack Resistant trust model IN connEcted vehicles

Farhan Ahmad*, Fatih Kurugollu*, Asma Adnane†, Rasheed Hussain‡, and Fatima Hussain§
*Cyber Security Research Group, College of Engineering and Technology, University of Derby, United Kingdom
†Networks and System Research, Department of Computer Science, Loughborough University, United Kingdom
‡Networks and Blockchain Lab, Institute of Information Security and Cyber-Physical Systems, Innopolis University, Innopolis, Russia
§API Delivery & Operations, Royal Bank of Canada, Toronto, Canada
Email: *{f.ahmad, f.kurugollu}@derby.ac.uk; †a.adnane@lboro.ac.uk;
‡r.hussain@innopolis.ru; §fatima.hussain@rbc.com

***Abstract*—Vehicular Ad-hoc NETwork (VANET), a novel technology holds a paramount importance within the transportation domain due to its abilities to increase traffic efficiency and safety. Connected vehicles propagate sensitive information which must be shared with the neighbors in a secure environment. However, VANET may also include dishonest nodes such as Man-in-the-Middle (MiTM) attackers aiming to distribute and share malicious content with the vehicles, thus polluting the network with compromised information. In this regard, establishing trust among connected vehicles can increase security as every participating vehicle will generate and propagate authentic, accurate and trusted content within the network. In this paper, we propose a novel trust model, namely, Man-in-the-middle Attack Resistance trust model IN connEcted vehicles (MARINE), which identifies dishonest nodes performing MiTM attacks in an efficient way as well as revokes their credentials. Every node running MARINE system first establishes trust for the sender by performing multi-dimensional plausibility checks. Once the receiver verifies the trustworthiness of the sender, the received data is then evaluated both directly and indirectly. Extensive simulations are carried out to evaluate the performance and accuracy of MARINE rigorously across three MiTM attacker models and the bench-marked trust model. Simulation results show that for a network containing 35% MiTM attackers, MARINE outperforms the state of the art trust model by 15%, 18%, and 17% improvements in precision, recall and F-score, respectively.**

***Keywords*—Connected Vehicles, Trust Management, Trust Model, Smart Cities, Man-in-the-middle Attack, VANET**

## I. Introduction

Vehicular Ad-hoc NETwork (VANET) has emerged as a promising solution to address the current challenges faced by the transportation systems and vehicles. VANET increases traffic safety as well as offers other infotainment services to passengers. In VANET, the connected vehicles equipped with numerous sensors share critical information such as traffic accident-avoidance or black-ice warnings through different modes of communications, i.e., Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside Unit (V2R) and hybrid [1]–[3]. Fig. 1 highlights the realization of VANET within a smart city. The data generated by the vehicular nodes is usually shared with central servers (depending on the service provider) to generate traffic management-related messages as well as with the neighbors to generate short-range traffic view [4].

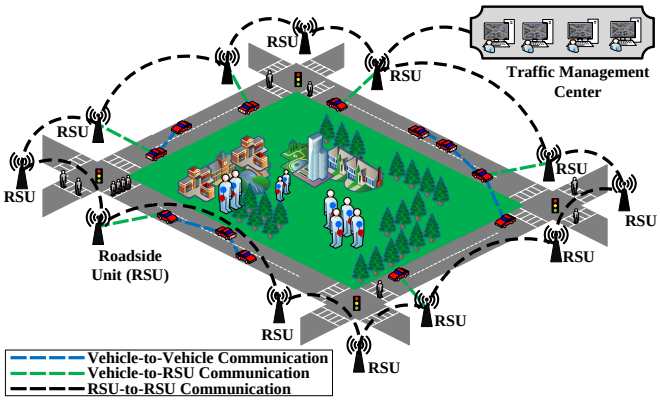



Fig. 1: Realization of VANET in Smart City

Abstractly, VANET constitutes safety messages, therefore, ensuring security of both communication and content is essential. Due to the intermittent communication among vehicles in VANET, providing such secure environment for message propagation is challenging in the presence of possibly dishonest nodes with the aim to launch a wide range of attacks including Man-in-the-Middle (MiTM), black-hole, Sybil, malware injections and Denial-of-Service (DoS) etc [5]–[7]. These dishonest nodes pollute the network with compromised messages which are then shared with other neighbors. The high mobility of the connected vehicles further increases the network complexity. Over the past decade, VANET security was the main theme of various notable projects including EVITA [8], PRESERVE [9], CONVERGE [10], and UKCITE [11] etc., to name a few, where various solutions are suggested to secure VANET.

Most of the current security solutions rely on traditional cryptography and Public Key Infrastructure (PKI). These solutions address most of the security challenges to some extent, for instance, they can easily identify outsider attackers. However, PKI-based solutions fail to detect attacks launched by insider attackers due to the fact that they are legitimate members as they possess valid credentials.

In order to address the shortcoming of the PKI-based security solutions, the concept of *trust* is introduced as a security parameter in VANET which has the ability to identify

insider attackers by mutually evaluating the shared messages. In the context of VANET, *trust* is defined as the faith which one vehicle places in other vehicle(s) for sharing reliable, trusted, accurate, and authentic messages [12], [13]. However, evaluating trust on the basis of the received information in a limited time among vehicles is extremely challenging as the vehicles only communicate for a short period of time.

Trust models are generally categorized into entity-centric, data-centric, and combined models based on their revocation targets. To secure VANET from trust perspective, a wide range of metrics are introduced including mutual interaction evaluations, neighbour recommendations and messages scrutiny, to name a few. Further, current trust management solutions rely on different similarity measurement techniques, which add a considerable amount of undesired overhead to the original shared messages, to compare the generated messages. In addition, the focus of most of these solutions are on revoking dishonest vehicles or their malicious content based on either identity related or messages analysis metrics. Even combined trust models consider only one category of metrics, where, a genuine node generates fake or malicious message due to compromised sensor, and an attacker generates true messages about an occurring event. Therefore, both nodes honesty and true messages are pre-requisite for an efficient trust management scheme for these solutions.

To fill the security gaps in VANET, in this paper, we propose an efficient and light-weight trust management model that enables the vehicular nodes to evaluate the entity (sender) trust and content (the shared information) trust in an intelligent manner. The main contributions of this paper are summarized below:

- A new trust management model (MARINE), that evaluates and manages trust among the communicating vehicles in VANET, is proposed.
- In MARINE, we incorporate both entity trust and content trust where entity trust is evaluated through extensive plausibility checks and the content trust is evaluated through neighbors recommendation. This two-step trust management solution helps eradicating the problem of insiders attacks where one solution is not enough to mitigate the attacks.
- We propose a Man-in-The-Middle (MiTM)-resistant trust framework to stop the dishonest nodes from sharing malicious information.
- We carry out extensive simulations to validate the proposed scheme and evaluate the efficiency of MARINE from accuracy and trust standpoints.

The remainder of this paper is organized as follows: In Section II, we present related work on trust management in VANET. Next, Section III provides details of our proposed MARINE scheme. Afterwards, the simulation environment is explained in Section IV including simulation results of MARINE. Finally, we conclude the paper in Section V.

## II. Related Work

The main motivation of the trust models in VANET is to disseminate accurate, authentic and up-to-date trusted content among the network entities. However, due to the highly intermittent and mobile nature of vehicular nodes, establishing and evaluating trust for the received information is a challenging task. [14], [15].

VANET involves two revocation targets, i.e., (1) participating network entities, and (2) data exchanged among these nodes, resulting in fully distributed trust management schemes [16]. Further, the data can be exchanged through connected infrastructure (i.e., Road-Side Unit - RSU) adjacent to the road with the aim to disseminate trusted content to a large geographical location. The RSU-based trust management schemes are the centralized trust models. Based on this information, the resultant trust models can further be categorized into three classes, i.e., (1) entity-centric trust models, (2) data-centric trust models, and (3) combined trust ( hybrid) models [17]–[19] as shown in Fig. 2.

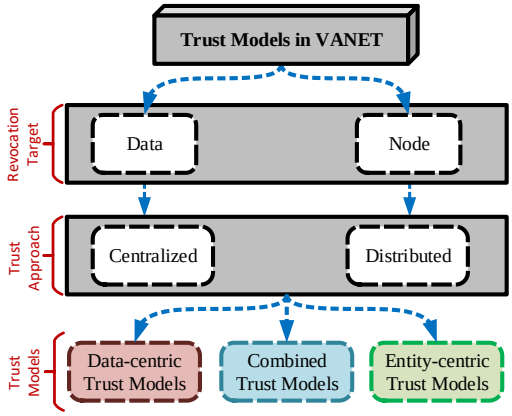



Fig. 2: Categories of Trust Models in VANET

### A. Entity-centric Trust Models (ECTM)

The major aim of entity-trust is to identify the presence of dishonest nodes within the pool of legitimate vehicles. These trust models rely on the opinions provided by its neighbours where a reputation-based trust evaluation methodology is employed to evaluate the trustworthiness of the sender. Currently, various ECTMs are proposed in the literature. Marmol et al. [20], proposed a centralized entity-centric trust model where vehicular reputation is evaluated by the message evaluator ($M_{Eval}$) with the help of adjacent RSU. Upon reception of the messages, a fuzzy-based trust score is generated by the $M_{Eval}$ which depends on the information received via three sources, i.e., recommendation shared by RSU, recommendation provided by nearby vehicles, and previous reputation of the sender. Once, the trust-score is generated, $M_{Eval}$ takes one of the following decision, i.e., (1) *drop* the message if not trustworthy, (2) $M_{Eval}$ accepts the message but do not forward it, and (3) *accept and forward* the message. The main drawback of this trust model is the extra overhead generated by multiple sources in order to provide reputation of the sender.

Another approach for revoking dishonest nodes from the network was proposed by Khan et al. [21], where a cluster-based mechanism is introduced in the network. First, a cluster

head ($CH$) is selected by the nodes, which employs a watchdog mechanism in its neighbourhood. Honest nodes report to $CH$ by providing its recommendation about the presence of misbehaving entity in its vicinity. Once, the dishonest nodes are detected, $CH$ informs the central trusted authority ($CTA$) which eliminates them from the pool of trusted nodes. However, this approach requires high amount of overheads generation due to continuous reports exchange between nodes which reduces the overall network efficiency.

A similar cluster-oriented trust model was presented by Jesudoss et al. [22], where every node follows a truth-telling approach to disseminate true content to get better reputation. Further, these nodes must participate in the election of $CH$ in the network, which provides incentives in the form of weights to these nodes. $CH$ only trusts the information if the participating node gains sufficient weights in $CH$ election. This solution fails in a highly mobile and rural scenario due to limited number of neighbouring vehicles. As a result, the presence of dishonest nodes in such location may result in the biased selection of $CH$.

A centralized entity-centric trust model namely Reputation-based Global Trust Establishment (RGTE) was proposed by Li et al. [23]. In this model, the vehicles compute reputation of the vehicles in theirs close vicinity and share their opinions with the centralized Reputation Management Center (RMC) via RSUs. RSUs are responsible to calculate the overall trust of the sender. Further, RMC updates the node reputation, and shares the updated list with the neighbouring vehicles after a short interval of time. The major limitation of this model are: (1) the overheads caused by the neighbouring vehicles by sharing their opinions with RMC, and (2) the delay which RMC takes to inform participating vehicles about the trustworthiness of the sender node.

Haddadou et al. [24], on the other hand, adapted a different approach where an economic incentive model was introduced to exclude dishonest nodes from the network. Every participating node is bootstrapped with a specific credit value, which is incremented and decremented based on the behaviour of the node. For a good behaviour, credit of the node is incremented by the $M_{Eval}$, while, in case of an attack, it is decreased for its misconduct in the network. If the credit of the node falls to 0, the node is classified as malicious and is revoked from the network. The major constraint of this trust model is its inability to differentiate between direct or indirect trust.

### *B. Data-centric Trust Models (DCTM)*

Data-centric trust mechanism evaluates the trustworthiness of the received messages, rather than the evaluating the trust of the message sender. To date, various data-centric trust solutions have been proposed in the literature. For instance, Lo et al. [25] proposed a trust evaluation mechanism namely Event-based Reputation System (ERS) to prevent the vehicles to disseminate compromised and malicious warning messages in the network. In this method, a cooperative event observation mechanism and reputation scheme is employed to share the event confidence and reputation thresholds with the $M_{Eval}$. Based on the evaluation results, $M_{Eval}$ determines whether to broadcast and disseminate traffic warning messages or not. The main limitation of this approach is the time taken by the $M_{Eval}$ to decide and share the trusted information with the neighbors in time.

To assess the information generated by malicious nodes, Shaikh et al. proposed an intrusion-aware data trust model, where four distinct sources including location closeness, time closeness, location verification, and time-stamp verification are utilized to compute a confidence value for every received message [26]. While preserving identity of vehicle, this scheme suffers from a wide number of geographical problems including the generation of high number of messages describing the same event. Further, safety-related messages are delay-sensitive, therefore, processing time to compute confidence value can lead to unwanted situations such as late accident notification.

Unlike [26], Rawat et al. [27] introduced combined opportunistic/deterministic approaches, where $M_{Eval}$ computes the similarity between the messages representing same events. Thus, this trust model filters out the different minority of messages from the pool of the received messages. Next, a deterministic approach based on coordinates of vehicles position and received signal strength estimation is ensured by comparing malicious vehicles and their transmitted messages. Similar to [26], this proposal is also time consuming and as a result, it fails to provide expected level of security in critical and extreme cases. Further, this trust model requires a large number of communicating vehicles, thus it fails to operate in rural scenarios.

To address the dynamics (high mobility and random distribution) of VANET, Liu et al. presented a lightweight data-centric trust model, namely LSOT which operates in a fully distributed manner [28]. To accurately determine the overall trust evaluations, three factors (number weight, time decay weight and context weight) are integrated for the trust-based evaluations. On the other hand, LSOT also relied on recommendation-based evaluations to identify and maintain its neighbourhood by creating a trusted environment. The main shortcoming of this scheme is its failure to distinguish among the trust of node and the message. If any sensor of the legitimate vehicle is faulty or impersonated by an attacker, then compromised messages will be transmitted from that vehicle, which ultimately pollutes the network with wrong information.

### *C. Combined Trust Models (CTM)*

Combine trust models aggregate the properties of both entity-centric and data-centric trust management schemes, where node trust is calculated based on the trust evaluations of the received messages. Recently, different studies have been conducted where trust is established based on the characteristics of both data and entity. For instance, Ahmed et al. proposed a logistic-based trust computation technique to quickly identify the nodes transmitting compromised and malicious messages [29]. In this technique, $M_{Eval}$ closely observes the events occurring within its vicinity, thus information shared by neighbouring vehicles directly depicts the behaviour of the sender which is calculated through weighted voting and

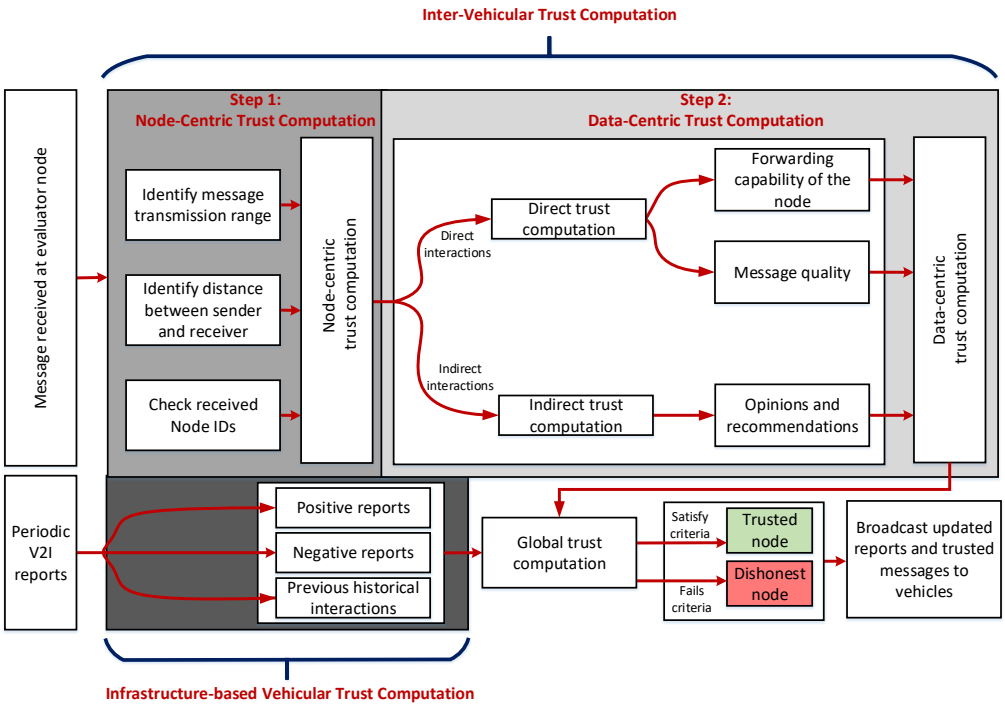



Fig. 3: Operation of the Proposed Trust Model

logistic trust function. Since the trust is evaluated based on weighted voting, the trust computation can be biased if $M_{Eval}$ is surrounded by dishonest nodes.

Li et al. introduced an attack-resistant combined trust model, where $M_{Eval}$ estimates the trust on the received information by evaluating both node and data-centric trust [30]. The data trustworthiness is calculated based on Bayesian Inference (BI), where $M_{Eval}$ relies on the information received from multiple neighbours. Furthermore, $M_{Eval}$ integrates Functional Trust (FT) and Recommendation Trust (RT) to evaluate node-centric trustworthiness. FT ensures that the participating node behaves properly while communicating with $M_{Eval}$, while RT maintains a certain level of trust before the node can be trusted. This scheme does not take data sparsity into account, which is pervasive in VANET.

To quickly revoke the malicious nodes from the network, Chen et al. proposed a novel evidence-based trust management scheme which integrates both direct and indirect trust [31]. $M_{Eval}$ establishes direct trust at a local level, while indirect trust is computed using BI to filter out the malicious information received from the neighbouring vehicles. This approach aims to compute a global trust value on the received information, which is then shared with the neighbouring vehicles directly and via RSU. Although this trust model is efficient as it evaluates the trust on the received information in a small interval of time; however, a high number of neighbours are required around $M_{Eval}$ to compute indirect trust.

Recently, Mahmood et al. presented a novel combined trust model which relies on traditional clustering mechanism to evaluate trust of the network nodes [32]. In this trust model, cluster head ($CH$) is elected in the network based on the trust of the participating nodes and their available resources. $CH$ is responsible for transmitting trusted messages within the network. However, the main drawback of this approach is the biased election of $CH$, if majority of the nodes are dishonest in the network.

In a nutshell, various trust models have been proposed in VANET that ensure the propagation of trusted content in the network. According to our literature review, most of these trust models operate only at the application layer, arising technical challenges including higher network delays. In this paper, we propose a novel combined trust model which operates at the two layers, i.e., network and application layers. Further, RSU is utilized to compute the global trust value with the aim to share trusted content with neighbouring vehicles at a large geographical location.

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

## III. Proposed MARINE Trust Management Model

In this section, we provide the details of our proposed trust model, i.e, MARINE. First, we abstractly describe MARINE, followed by its operation and trust evaluation. The detailed proposal is highlighted in Fig. 3, suggesting that MARINE involves various steps in order to trusts the information from sender by evaluating it in two dimensions including, node-centric trust computation and data-centric trust computation. Further, MARINE integrates both inter-vehicular and infrastructure-based trust computation in order to provide higher accuracy of detecting malicious content in large geographical locations.

### A. Baseline of MARINE

The MARINE is a novel and efficient mechanism to evaluate the trust in VANET, which not only integrates the information and opinion shared by vehicles, but also takes the suggestions provided by nearby RSU. MARINE is a lightweight trust model that operates in two stages to evaluate inter-vehicular trust. First, it evaluates the sender node to identify its trustworthiness. This is achieved via previous interactions and the recommendations provided by the neighbouring vehicles. Second, once node-centric trust is calculated, the received data is evaluated in three distinct dimensions, i.e., (1) information quality, (2) node's message forwarding capability, and (3) opinions from neighbours. Data from the sender node is accepted only if both node and data-centric trust is computed successfully. Otherwise the evaluator node will drop the data.

MARINE relies on both vehicles *(inter-vehicular trust computation)* and RSU *(infrastructure-based trust computation)* to compute the overall trust on the sender and the received information.

### B. Inter-vehicular Trust Computation

In order to trust the received information, MARINE involves the following two steps, i.e., (1) node-centric trust computation, and (2) data-centric trust computation.

*1) Step 1: Node-centric trust computation:* In the first step, MARINE evaluates trust on sender transmitting the safety messages. The communication module embedded in the vehicles enables them to share messages with the neighbouring vehicles in a specific range, which directly depends on the height and position of the antenna on the transmitting vehicle [33], [34]. A slight change in the antenna position and height can distort the signal strength, which ultimately results in a signal loss. This impacts the message transmission range and the neighbouring vehicles may be unable to receive the transmitted messages. In this regard, we define "$M_{Range}$" as a function of (1) distance ($D_{M_S<->M_R}$) between $M_S$ and $M_R$, (2) sender antenna height ($A_{Sender}$), and (3) receiver antenna height ($A_{Receiver}$) as follows.

$$M_{Range} = \sqrt{(D_{M_S<->M_R})^2 + (A_{Sender} + A_{Receiver})^2} \quad (1)$$

$M_R$ upon receiving message, performs various plausibility checks that depend solely on the $M_{Range}$. $M_R$ classifies message as malicious if it is received outside its range. However, if the message is received from the vehicle located within its $M_{Range}$, then $M_R$ first checks its existing database for previous interactions. For every encounter, the vehicles keep track of each other (i.e., $Veh_{ID}$) along with its trust values. The existence of non-zero entry within the database of $M_R$ depicts that the sender vehicle has been encountered previously as vehicles in the network are assigned with unique identities (IDs). In case the vehicles are communicating with each other for the first time, the database will have no entry within its database. Next, $M_R$ checks the trust value of the encountered vehicle. Every vehicle assigns two trust ratings for every encountered vehicle, i.e., (1) *positive trust rating* ($Rating_{Pos}$) for sharing true and trusted message, and (2) *negative trust rating* ($Rating_{Neg}$) for malicious messages. $M_R$ will trust the node only, if the resultant trust level ($TL$) is higher than the pre-defined trust threshold ($TR_{Threshold}$). In this case, $M_R$ assigns partial reward ($\alpha_1$) to the $M_S$ and forwards the message to Step 2 for evaluating the content of the received message. However, if $TL$ is less than $TR_{Threshold}$, $M_R$ discards the received message directly and provides penalty ($\beta$) to the $M_S$.

In order to allow the communication among vehicles for the very first time, $M_R$ creates an entry within its database along with the default minimum ($TL_{Min}$). To gain the trust of ($M_R$), the new vehicle must ensure to provide true content, otherwise, the messages shared from such vehicles are classified as malicious. We summarize the checks performed in this step in Algorithm 1.

**Algorithm 1:** Step 1: Node-centric trust computation

**Input:** Vehicle ID ($ID_{Node}$); Trust level ($TL$); Minimum trust level ($TL_{min}$); Trust threshold ($TR_{Threshold}$); Message threshold range ($M_{Range}$); Partial Reward ($\alpha_1$); Penalty ($\beta$)

```
if (Message ∈ M_Range) then
    Check Vehicle ID (Veh_ID);
    if (Veh_ID ∈ Database) then
        Check TL;
        if (TL ≥ TR_Threshold) then
            TL = TL + α1;
            (Goto Step 2: Data-centric trust computation);
        else
            Classify as dishonest vehicle;
            TL = TL - β;
            Update Database;
        end
    else
        Insert Veh_ID to Database for new vehicles;
        TL = TL_min;
    end
else
    Discard M;
    Insert ID_Node to Database;
    TL = T_Min;
end
```

*2) Step 2: Data-centric trust computation:* Once node-centric trust is calculated in Step 1, $M_R$ evaluates trust on the content of the received message. Since, messages can be delivered at the $M_R$ either directly or through intermediate neighbours, therefore, two methods of trust computation are performed in this step:

***Direct Trust Computation:*** $M_R$ computes trust on the received message directly based on two important factors: (1) quality of the received message ($M_{Quality}$), and (2) ability of the node to disseminate message.

According to ETSI, $M_{Quality}$ depends directly on the distance of the received message [35]. The greater the distance between $M_S$ and $M_R$, the higher is the probability that

message is generated from dishonest vehicle. To this end, we divide the geographical location between sender and receiver into 4 tiers ($\mu$), i.e.,

$$M_{Quality} = \begin{cases} 1 & \text{if } 0 < D_{M_S <-> M_R} \leq \mu_1 \\ 0.75 & \text{if } \mu_1 < D_{M_S <-> M_R} \leq \mu_2 \\ 0.5 & \text{if } \mu_2 < D_{M_S <-> M_R} \leq \mu_3 \\ 0.25 & \text{if } \mu_3 < D_{M_S <-> M_R} \leq \mu_4 \\ 0 & \text{if } D_{M_S <-> M_R} > \mu_4 \end{cases} \quad (2)$$

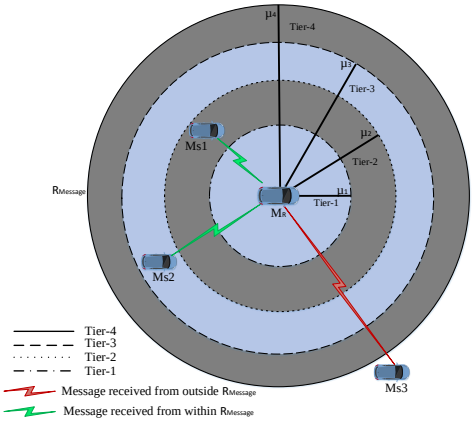



Fig. 4: Tier-based Threshold Approach

In equation 2, $\mu_1, \mu_2, \mu_3, \mu_4$ are respective boundaries of the tiers between $M_S$ and $M_R$ as depicted in Fig. 4. In this paper, we followed a tier-based approach due to the fact that $M_R$ is unable to distinguish between legitimate and malicious messages generated from $M_S$, if the distance is very large between them. As an illustration, $M_R$ receives messages from three vehicles $M_{S1}$, $M_{S2}$ and $M_{S3}$, which are located in different tiers of $M_R$. $M_{S1}$ and $M_{S2}$ are located within tier 2 and tier 3, therefore, the respective values of $M_{Quality}$ assigned by $M_R$ are 0.75 and 0.5. However, $M_R$ assigns 0 to vehicle 3 as it is received from outside of the range of $M_R$.

Next, we also take into account the ability of the vehicle to disseminate and share information with the neighboring vehicles. To this end, we define a "Message Disseminate Ratio ($MDR$)" as follows:

$$MDR = \sum_{i=1}^{n} \frac{\alpha \times PTR}{(\alpha \times PTR) + (\beta \times PDR)} \quad (3)$$

In equation 3, *PTR* is the packet transmit ratio, depicting the ability of the vehicle to transmit messages with its $n$ neighbors. $\alpha$ is the reward awarded for their honesty and transmitting messages towards other nodes. *PDR*, on the other hand, indicates the class of the dropped messages at the vehicle. PTR for the legitimate vehicles will be high as the number of messages dropped at the node are very limited. However, for MiTM attackers, this ratio will be low, as high number of messages are dropped at the node. Similarly, $\beta$ represents the penalty given to malicious vehicles, failing to transmit and share messages. As a result, MDR is mostly low for malicious nodes. Once $M_{Quality}$ and $MDR$ are identified, $M_R$ calculates direct trust ($DTR$) according to equation 4.

$$DTR = \frac{1}{2} \sum_{i=1}^{n} \left( \frac{M_{Quality} \times MDR}{M_{Quality} + MDR} \right) \quad (4)$$

***Indirect Trust Computation:*** MARINE also takes into account the opinions generated by the intermediate vehicles. Specifically, the proposed system categorizes opinions provided by '$n$' neighbor vehicles into two distinct classes, i.e., (1) positive opinions ($PO$), and (2) negative opinions ($NO$). Upon receiving an indirect message, $M_R$ computes indirect trust ($ITR$) as follows:

$$ITR = \left[ \left( \frac{\alpha}{\alpha + \beta} \times \sum_{i=1}^{n} PO \right) + \left( \frac{\beta}{\alpha + \beta} \times \sum_{i=1}^{n} NO \right) \right]^{\frac{1}{n}} \quad (5)$$

In equation 5, $\alpha$ and $\beta$ are the respective reward and penalty factors as explained earlier, $n$ represents the 1-hop direct neighbours of $M_R$ which provides respective positive opinions ($PO$) and negative opinions ($NO$) about the received messages.

Once, DTR and ITR are computed at the $M_R$, the overall inter-vehicular trust ($Trust_{Inter}$) is computed according to:

$$Trust_{Inter} = R_O \times \overline{(DTR + ITR)^{\frac{n}{Dist}}} \quad (6)$$

In equation 6, $R_O$ represents the opinions and the information provided by role-oriented vehicles ($veh_{Role}$), which are regarded as highly trusted vehicles, including law-enforcement, ambulances, public buses, taxis etc. due to the fact that they are regulated and authorized by a central authority or specific department such as local councils [36], [37]. On the other hand, the major portion of the network constitutes such vehicles which have no role in the network, i.e., traditional vehicles ($Veh_{Trad}$). Messages generated by these vehicles must be evaluated for their trustworthiness. In this paper, we modeled $R_O$ according to equation 7. Further, algorithm 2 summarizes the process of choosing values for $R_O$.

$$R_O = \begin{cases} 0.8 \leq R_O \leq 1.0 & \text{if } veh = veh_{Role} \\ R_O = 0.5 & \text{if } veh = Veh_{Trad} \end{cases} \quad (7)$$

**Algorithm 2:** $R_O$ computation

**Required:** Message ($M$); vehicle type ($veh$); Role-oriented vehicles ($veh_{Role}$); Traditional vehicles ($veh_{Trad}$);
Get vehicle type ($veh$);
**if** *(($veh$) == $veh_{Role}$)* **then**
  $0.8 \leq R_O \leq 1.0$;
**else**
  $R_O = 0.5$;
**end**

Fig. 5 depicts the high-level flow chart of inter-vehicular trust computation in MARINE.

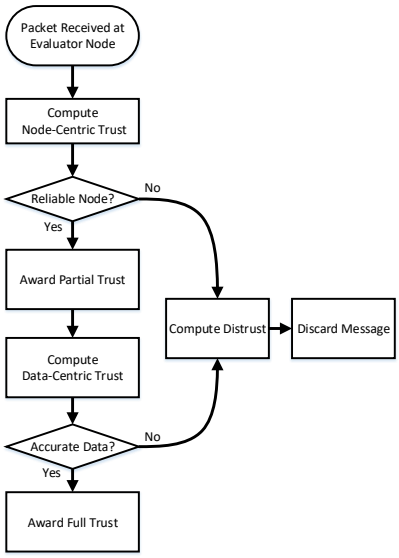



Fig. 5: Flow Chart of Inter-vehicular trust computation

### C. Infrastructure-based Trust Computation

Deploying infrastructure (such as RSU) along the road in both urban and rural areas is extremely challenging task due to (1) high cost, and (2) presence of different obstacles, thus affecting the coverage of RSU [38], [39]. However, RSU can be useful in disseminating messages by increasing the coverage area and providing the quasi global view of the overall network [40]. Therefore, from the trust management perspective, RSU can be helpful in broadcasting and sharing trusted information with large number of vehicles.

In MARINE, vehicles manages two reports about the encountered vehicles, i.e., (1) positive reports ($P_R$) contain information about vehicles with positive ratings, and (2) negative reports ($N_R$) represent vehicles which are classified as malicious by the vehicles. Whenever these vehicles approach within the coverage of certain RSU, they share these reports with RSU. RSU upon receiving messages, computes Infrastructure-based trust ($Trust_{Intra}$) on the received reports using equation 8.

$$Trust_{Intra} = \frac{\alpha}{\alpha+\beta} \times \sum_{i=1}^{n} P_R \quad + \quad \frac{\beta}{\alpha+\beta} \times \sum_{i=1}^{n} N_R \tag{8}$$

Factors $\alpha$ and $\beta$ are the same reward and penalty factors as described previously. RSU shares the updated report about the trusted and dishonest vehicles with the neighboring vehicles periodically to maintain the trusted environment in the network. We summarize the data-centric trust computation within MARINE in Algorithm 3.

### D. Global Trust Computation

MARINE facilitates the vehicles to quickly identify MiTM attackers. In MARINE, every vehicle establishes a quasi global view of the network, which enables them to evaluate trust in both the presence and absence of the RSU. Let $n$ represents the neighboring vehicles within the vicinity of the RSU, then global trust ($GTC$) can be computed as follows:

$$GTC = \frac{}{Trust_{Inter} + \sqrt{Trust_{Intra}}}^{\frac{1}{n}} \tag{9}$$

If there is no RSU in the vicinity, MARINE still enables the vehicles to evaluate trust on the received information through $Trust_{Inter}$.

**Algorithm 3:** Data-centric Trust Computation in MARINE

**Required:** Message ($M$); Message Range ($M_{Range}$), Positive reports ($P_R$), Negative reports ($N_R$), Positive opinions ($PO$), Negative opinions ($NO$), Direct trust ratio (DTR), Indirect trust ratio (ITR), Message dissemination ratio (MDR), Message receiver ($M_R$), Infrastructure-based vehicular trust ($Trust_{Intra}$), Inter-vehicular trust ($Trust_{Inter}$);

```
Message dissemination across the network;
if (RSU present within M_Range of M_R) then
    Compute P_R;
    Compute N_R;
    Calculate Trust_Intra using equation 8;
else
    Compute Trust_Inter;
    if (M directly received at M_R) then
        Calculate M_Quality via equation 2;
        Identify MDR using equation 3;
        Compute DTR using equation 4
    else
        if (M indirectly received at M_R) then
            Compute PO;
            Compute NO;
            Calculate ITR using equation 5;
        else
        end
    end
end
```

## IV. Performance Evaluation

In this section, we perform extensive simulations to evaluate our proposed scheme. First we discuss the simulation model followed by discussion on the obtained results.

### A. Simulation Model

To evaluate the performance of MARINE, we exploit VEINS, an open-source simulator, designed specifically to evaluate the performance of the vehicular networks [41]. To validate MARINE, a real map from the city of Derby, United Kingdom has been extracted from OpenStreetMap [42]. Further, a real mobility trace of 100 vehicles has been generated on the extracted map using SUMO [43], which is considered enough for various urban scenarios [44]. Furthermore, ten RSUs are randomly deployed at a fixed locations across the map as shown in Fig. 6.

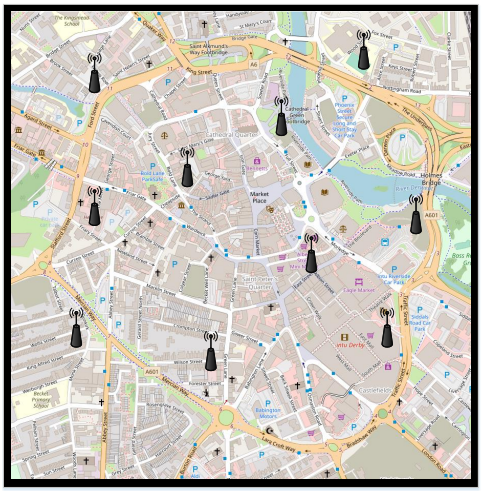


Fig. 6: Extracted Map of Derby, United Kingdom

Moreover, a safety-related event (i.e., accident) is generated at a random location within the network. The first vehicle located within the close proximity of accident generates a message regarding this event and share with its neighbours. Every vehicle within the network validates the authenticity and accuracy of the received message as they are equipped with MARINE trust model. Next, MiTM nodes are introduced within this network, whose sole aim is to either drop the received message or share the compromised message with the neighbours. Further, the quantity of these malicious nodes are increased from 5% to 40% in order to validate the efficiency of MARINE in terms of identifying malicious nodes and their compromised data.

Finally, every simulation scenario is carried out twenty-five with random seed value every time to ensure unique initial vehicle assignment within the network. Moreover, experimental results are generated by averaging over twenty-five runs. The details of the simulations are provided in Table I.

TABLE I: Simulation Parameters

| Parameters | Value |
|---|---|
| Simulation Time (secs) | 600 secs |
| Simulation Area (km × km) | 2.5km × 2.5km |
| Vehicles Distribution | Random |
| Total Number of Vehicles | 25, 50, 75, 100 |
| Role-oriented Vehicles (%) | 5 |
| Total Number of RSUs | 10 |
| Total MiTM attackers (%) | 5, 10, 15, 20, 25, 30, 35, 40 |
| MAC Protocol | IEEE 802.11p |
| Network Protocol | WAVE |
| Radio Propagation Model | Two-Ray Interference |
| Packet Data Size | 1024 bits |
| Packet Header Size | 256 bits |
| $Trust_{Initial}$ | 0.5 |
| $Trust_{Threshold}$ | 0.5 |
| $\alpha$ | 0.01 |
| $\alpha_1$ ($\alpha_1$ = 0.1 × $\alpha$) | 0.001 |
| $\beta$ ($\beta$ = 10 × $\alpha$) | 0.1 |

### B. MiTM Attacker Models

The main motivation of the trust model is to disseminate trusted information within the network. Therefore, to evaluate the performance of MARINE, we defined following three variants of MiTM attackers:

*1) Attacker Model 1:* In this model, we equipped the MiTM with the ability to tamper the legitimate messages and share compromised messages with the network nodes. Further, these nodes also intelligently share bogus trust values with the vehicles in order to gain the trust of the honest vehicles. This attacker model misleads the vehicles by sharing malicious and compromised content, thus, it is very important to evaluate the trust model under this attacker model.

*2) Attacker Model 2:* This attacker model considers a selfish MiTM attacker who deliberately drops and delay the safety messages. The attacker acts as a sink where messages are dropped or delayed intentionally, thus prohibiting the legitimate vehicles to receive safety messages in time. Dropping safety messages can have drastic impact on the network due to the sensitive nature of the messages involved within vehicular environment. Therefore, we defined this attacker model to evaluate the efficiency of MARINE in identifying true information in presence of such MiTM attackers within the network. In this attacker model, half attackers are dropping the messages, while the other half are delaying the safety messages with a factor of 'd' before broadcasting it.

*3) Attacker Model 3:* Next, an advanced version of the MiTM attackers is defined where the attackers behaves intelligently by adopting a random pattern within the network. The attacker initially behaves as a legitimate node for short span of time to gain the trust of the vehicles within the network. The attacker starts behaving maliciously only after becoming part of the legitimate network by gaining trust of the participating vehicles. In this defined model, the attacker specifically shares compromised messages and ratings with the neighbouring vehicles during its attack mode. Moreover, some of the attacker nodes are dropping the safety messages apart from sharing misleading compromised messages and trust ratings.

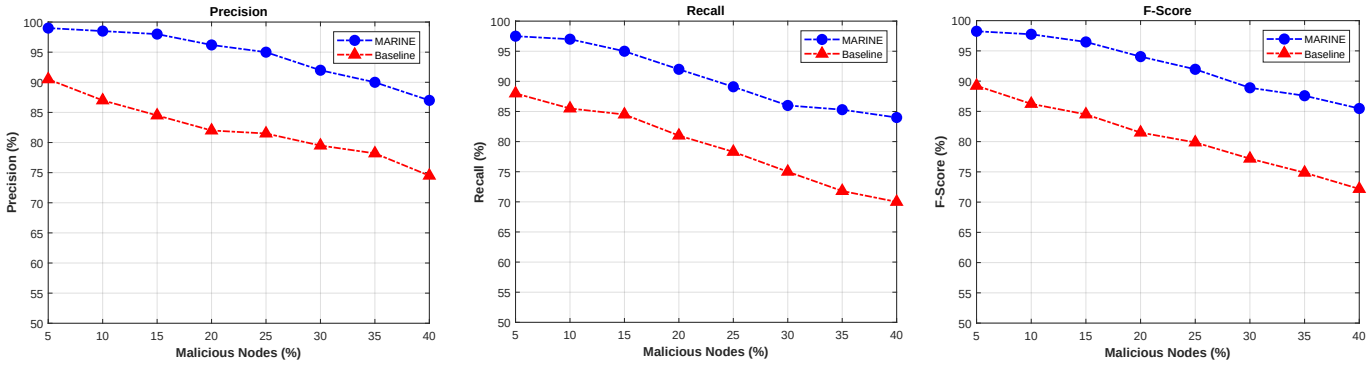
### C. Performance Evaluation Metrics

We evaluated MARINE from accuracy point of view due to the fact that the trust model aim to disseminate trusted, accurate and authentic information within the network. To this end, we considered following metrics which are categorized into two distinct classes for the evaluation of our trust model.

*1) Trust Model Accuracy:* This class of evaluation metrics is defined specifically to evaluate the accuracy of MARINE in presence of MiTM attackers. Therefore, following three metrics are used which are considered as one of the most important trust evaluation criteria within highly mobile networks like VANET [45].

(a) *Precision ($P_{rec}$)* – depicts that ability of the trust model to correctly predict the trustworthy event. Let $P_{D|H}$ illustrates the probability of the node to detect as malicious, given the legitimate node and $P_{D|D}$ represents the probability to detect node as malicious, given malicious node, then $P_{rec}$ can be given as:

$$P_{rec} = \frac{P_{D|D}}{P_{D|H} + P_{D|D}} \tag{10}$$




(a) (b) (c)

Fig. 7: Accuracy of Proposed Trust Model under Attacker Model 1 (a) Precision (b) Recall (c) F-Score

(b) *Recall ($R_{ec}$)* – depicts the trust model capability to correctly detect the nodes disseminating malicious content. Let $P_{D|D}$ presents the probability of trust model to detect node as malicious, given node is malicious and $P_{H|D}$ resents probability of detecting malicious node as legitimate node, given the node is malicious, then Recall can be mathematically expressed as:

$$R_{ec} = \frac{P_{D|D}}{P_{H|D} + P_{D|D}} \tag{11}$$

(c) *F-Score* – A weighted average of $P_{rec}$ and $R_{ec}$, depicting the accuracy of the trust model [46]. Higher the F-Score, the more accurate is the trust model. F-Score is given as:

$$F - Score = 2 \times \frac{P_{rec} \times R_{ec}}{P_{rec} + R_{ec}} \tag{12}$$

*2) Impact of Trust:* We also considered trust model related metrics, illustrating the ability and efficiency of the trust model to detect true events within the network [47]. To do so, following three metrics are defined:

(a) *Trust* – A significant evaluation metric which portray the capability of the trust model to detect and classify received messages either as legitimate or malicious.
(b) *Trust Metric Variation for Legitimate Nodes* – Illustrates the behaviour of the trust metric within honest nodes in presence of MiTM attackers sharing compromised messages and trust ratings.
(c) *Trust Metric Variation for Malicious Nodes* – Depicts the ability of the trust model to enforce the minimum trust level of MiTM attackers.

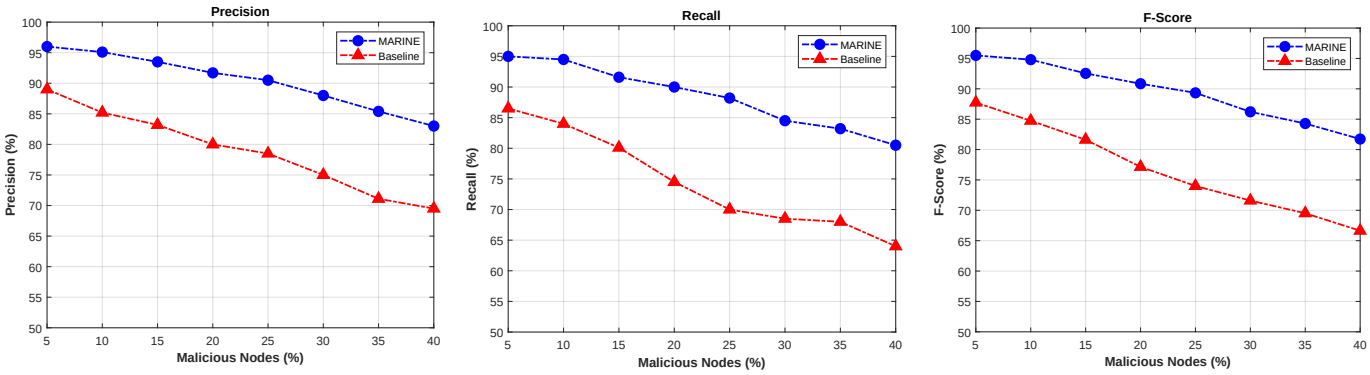
### D. Simulation Results

This section discusses the performance of MARINE trust model in VANET in presence of three variants of MiTM attacker. Further, the efficiency of MARINE is computed against a baseline trust model which evaluates trust on the received information from the vehicles via weighted voting method. We chose this method as a baseline trust model as it has been used widely in various trust management methods, such as [31], [48]–[52].

### E. Accuracy of MARINE in Presence of Attacker Model 1

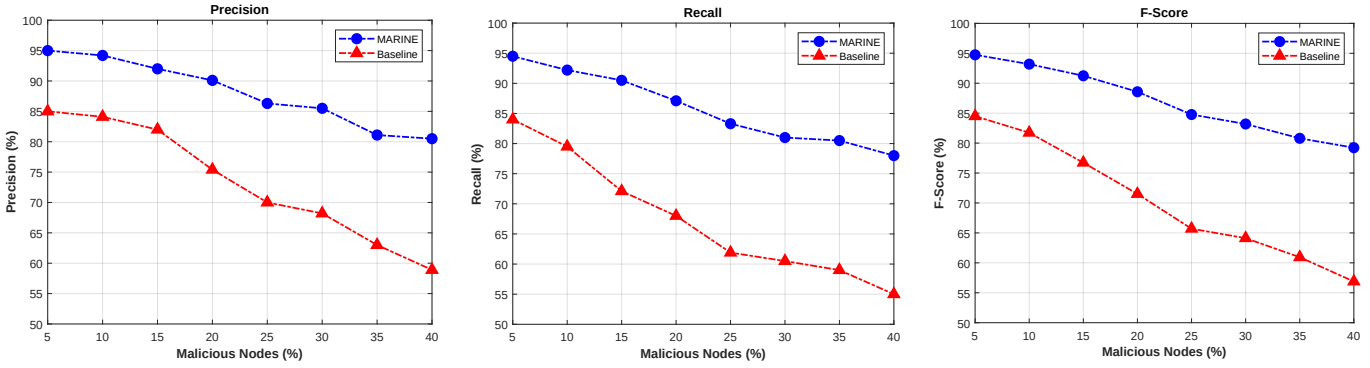
Fig. 7 shows the accuracy of MARINE under attacker model 1, where the adversary is changing the content of safety messages and tampering trust ratings before sharing it with neighbouring vehicles within its vicinity. Fig. 7a and Fig. 7b illustrates the precision and recall of our proposed trust model, depicting that the network achieves high precision and recall for low number of MiTM attackers. However, as the number of MiTM attackers with message tampering ability is increased from 5% to 40%, the corresponding precision and recall decreases. This is due to the fact that increasing MiTM attackers will result in the generation of high number of compromised messages. This limits the ability of the legitimate vehicles to classify between trusted and malicious content as the network is polluted with high number of malicious content. However, MARINE performs better in terms of identifying and classifying trusted and malicious data due to the fact that dishonest nodes are identified quickly at the lower layers, thus, enabling the vehicles to limit and revoke the data generated from malicious nodes. Next, MARINE also integrates role-oriented vehicles, thus enabling the legitimate vehicles to receive trusted information, even in presence of high number of attackers. On the other hand, baseline trust model is built upon weighted voting, which can be compromised if the legitimate vehicles are surrounded by high number of malicious nodes. Therefore, for high number of malicious nodes, baseline trust model achieves lower precision and recall values. As an illustration, precision for MARINE falls from 99% to 87% if the number of adversaries are increased from 5% to 40%, while precision for baseline trust model falls drastically from 90.5% to approximately 75%. This depicts that MARINE is efficient in dealing with MiTM attackers which are dealing with message alteration ability.

Further, comparing to baseline trust model, MARINE achieves high accuracy in terms of F-score as shown in Fig. 7c. For instance, MARINE ensures accuracy over 91.5%, while F-score for baseline trust model falls below 80% for a network with 25% MiTM adversaries, highlighting that MARINE is more accurate in identifying MiTM attackers with content alteration ability.




(a) (b) (c)

Fig. 8: Accuracy of Proposed Trust Model under Attacker Model 2 (a) Precision (b) Recall (c) F-Score




(a) (b) (c)

Fig. 9: Accuracy of Proposed Trust Model under Attacker Model 3 (a) Precision (b) Recall (c) F-Score

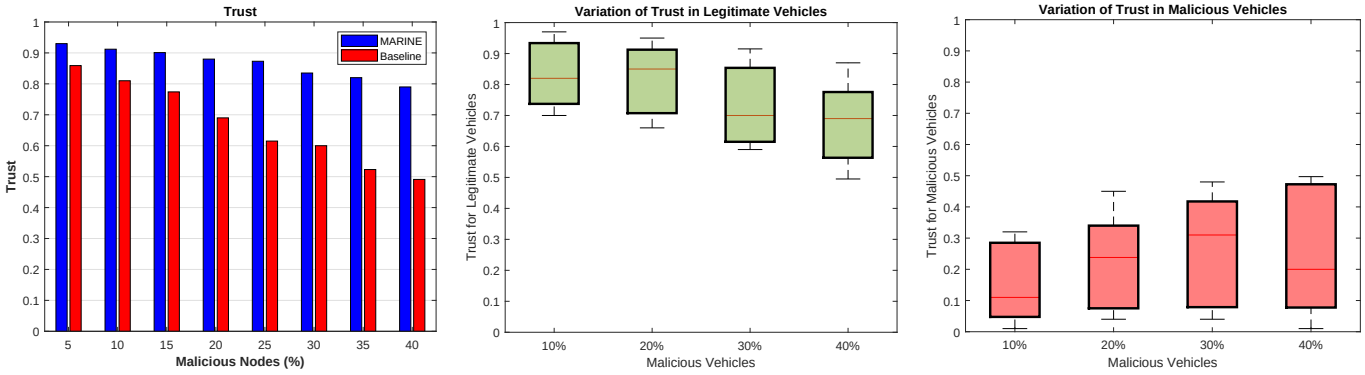
### *F. Accuracy of MARINE in Presence of Attacker Model 2*

Fig. 8 depicts the accuracy of MARINE in terms of precision, recall and F-score in presence attacker model 2, where the attackers are deliberately dropping and delaying the messages to be shared with legitimate vehicles. Dropping or delaying safety messages by the malicious nodes results in drastic impact on the network as the legitimate vehicles fails to receive significant information in time. This phenomenon is clearly highlighted in Fig 8, where the precision, recall and F-score are decreased as more and more MiTM attackers are introduced in the network. However, MARINE is efficient in detecting such malicious nodes due to the fact that the lower layers of the vehicle quickly detects the nodes implementing MiTM attacks. For a network containing high number of MiTM attackers (30 %), MARINE ensures high precision (88 %) and recall (84.5 %) values, concluding that MARINE is efficient in identifying malicious nodes in VANET. On the other hand, baseline trust model relies on weighted voting, thus the presence of malicious nodes prohibit the legitimate nodes to receive information in time. Similarly, it fails to detect the messages dropped by the MiTM attackers. Fig. 8a and Fig. 8b interprets that for a network with 30% MiTM attackers, the precision and recall falls below 75% and 70% respectively for baseline trust model.

Next, the accuracy of MARINE in terms of F-score is shown in Fig. 8c, suggesting that MARINE ensures high accuracy, thus outperforming the baseline trust model. When the number of malicious nodes are increased from 5% to 40%, accuracy of MARINE is decreased from approximately 95.5% to about 81%, comparing to baseline trust model, where accuracy falls from 87.7% to about 66%. This depicts that MARINE is an attack-resistant to MiTM attacks, where it ensures to propagate trusted information, even in presence of high number of malicious nodes.

### *G. Accuracy of MARINE in Presence of Attacker Model 3*

We also conducted a set of experiments in Fig. 9 for an advanced version of MITM attackers, which are behaving intelligently within the network to deceive legitimate nodes and pollute the network with compromised and tampered messages. Fig. 9a and Fig. 9b depicts that introducing such MiTM attackers with zig-zag attack pattern have severe impact on the network, where introducing such malicious attack activity reduces precision and recall of the network. As the attackers are behaving and launching attacks in the network intelligently, therefore, it is very difficult for legitimate vehicles to identify such MiTM attackers. However, MARINE enables the vehicles to detect such MiTM attackers with random attack pattern, which is depicted clearly in Fig. 9a and Fig. 9b. This is due to the following reasons: (1) The node-centric trust establishment at the lower layers results in the early identification of MiTM attackers, (2) The inter-vehicular trust module where trust is




(a) (b) (c)

Fig. 10: Impact of Trust (a) Trust Metric (b) Trust Variation for Legitimate Nodes (c) Trust Variation for Malicious Nodes

established based on the message quality enables the legitimate vehicles to verify the received messages from MiTM attacker, and (3) the presence of role-based trust vehicles ensures the propagation of trusted information in the network, thus enabling the legitimate vehicles to receive trusted information. For a network with 30% MiTM attackers, MARINE achieves approximately 85% precision and 80% recall, while it falls below 70% and 60% respectively for baseline trust model, highlighting that MARINE is efficient in disseminating trusted information in presence of MiTM attackers with zig-zag attack pattern.

Finally, Fig. 9c highlights the F-score of MARINE which is one of the significant metric to measure the accuracy of the trust model. As shown in Fig. 9a and Fig. 9b, varying the MiTM nodes with random attack pattern affects the overall performance of VANET, where the precision and recall falls drastically. Therefore, F-score can depict that how accurate is the trust model in detecting MiTM attackers and malicious content. The results suggest that compared to baseline trust model, our proposal achieves high accuracy in terms of F-score, i.e., in presence of 35% malicious nodes, our trust model ensures accuracy over 80%, while the baseline trust model achieve accuracy approximately 60%.

### *H. Impact of Trust on MARINE*

Figure 10 shows the efficiency of MARINE to identify and classify malicious content in terms of trust perspective. Specifically, we calculated the behaviour of trust metric for MARINE in presence of MiTM attackers in Fig. 10a. It illustrates that when the network is polluted with MiTM attackers, generating malicious content, trust of the network decreases. This is due to the fact that higher malicious nodes results in limiting the ability of the legitimate nodes to identify true events as the network is polluted with high number of malicious content. However, comparing to the baseline trust model, MARINE ensures higher trust value, depicting that MARINE is efficient in identifying and classifying the true events in presence of adversaries. This is due to the following reasons: (1) The presence of role-oriented vehicles enable the legitimate vehicles to receive true events in the network, (2) MARINE intelligently identifies node transmitting malicious content at the lower layers, thus, enabling the evaluator node to quickly distinguish between legitimate vehicle and an attacker. For a network containing 40% MiTM attackers, MARINE achieves 79% trust level, while, this level falls below 50% for baseline trust model.

Next, Fig. 10b and Fig. 10c depicts the variation of trust within legitimate and malicious nodes respectively. These metrics are very important as they depicts that how efficient the trust model is evaluating trust on the received information. Fig. 10b illustrates that trust within the legitimate nodes never falls below trust threshold, i.e., 0.5, even in presence of high number of MiTM attackers. This ensures that MARINE trust model experience very few false positives in the network. On the other hand, trust among the MiTM nodes is always below the considered threshold level as shown in Fig. 10c, thus assuming that very limited false negatives are generated via our proposal.

## V. Conclusion

In this paper, we presented MARINE, a novel trust model to increase network security by quickly detecting and revoking dishonest vehicles and their generated content. MARINE operates in two steps: First step involves early detection of malicious nodes where entity-centric trust evaluations is performed by introducing several plausibility checks within the network. Node is classified as malicious if it fails to satisfy all the evaluation criteria. Once, legitimate node is identified via step 1, the next phase involves the data-centric trust evaluation, where the trustworthiness of the data is performed. This mechanism enables the vehicles to quickly identify misbehaving vehicle along with its malicious content, which is then revoked from the pool of trusted vehicles.

Extensive simulations are carried out to the efficiency of MARINE in presence of three different flavors of MiTM attackers. Simulations results suggest that MARINE is an attack-resistant trust model which provides high accuracy in detecting trusted content in presence of MiTM attacks. Moreover, the performance of MARINE is bench-marked against a baseline trust model, which clearly shows that MARINE performs better in terms of achieving high precision, recall and F-score in presence of three MiTM attacker models. This is due to the fact that MARINE enables the participating nodes to

quickly identify dishonest nodes and prevent them to pollute the network from malicious content.

Our future step includes the integration of social networks with MARINE, which is one significant source of providing information for connected vehicles within VANET.

## REFERENCES


[1] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected Vehicles: Solutions and Challenges," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 289–299, Aug 2014, doi:10.1109/JIOT.2014.2327587.

[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] H. H. R. Sherazi, Z. A. Khan, R. Iqbal, S. Rizwan, M. A. Imran, and K. Awan, "A Heterogeneous IoV Architecture for Data Forwarding in Vehicle to Infrastructure Communication," *Mobile Information Systems*, vol. 2019, p. 12, 2019, doi: https://doi.org/10.1155/2019/3101276.

[4] R. Hussain, S. Kim, and H. Oh, "Traffic Information Dissemination System: Extending Cooperative Awareness Among Smart Vehicles with only Single-Hop Beacons in VANET," *Wireless Personal Communications*, vol. 88, no. 2, pp. 151–172, May 2016. [Online]. Available: https://doi.org/10.1007/s11277-015-3084-9

[5] T. Zhang, H. Antunes, and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 10–21, Feb 2014, doi:10.1109/JIOT.2014.2302386.

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

[7] R. Hussain and H. Oh, "On Secure and Privacy-Aware Sybil Attack Detection in Vehicular Communications," *Wireless Personal Communications*, vol. 77, no. 4, pp. 2649–2673, Aug 2014. [Online]. Available: https://doi.org/10.1007/s11277-014-1659-5

[8] EVITA, "E-Safety Vehicle Intrusion Protected Applications (EVITA)." Available online: https://www.evita-project.org/ (Accessed: December 18, 2019).

[9] PRESERVE, "Preparing Secure Vehicle-to-X Communication Systems (PRESERVE)." Available online: https://www.preserve-project.eu// (Accessed: December 18, 2019).

[10] CONVERGE, "COmmunication Network VEhicle Road Global Extension (CONVERGE)." Available online: http://www.converge-online.de// (Accessed: December 18, 2019).

[11] UK CITE, "UK Connected Intelligent Transport Environment (UK CITE)." Available online: https://ukcite.co.uk// (Accessed: December 18, 2019).

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

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

[14] S. Ilarri, T. Delot, and R. Trillo-Lado, "A Data Management Perspective on Vehicular Networks," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2420–2460, Fourthquarter 2015, doi:10.1109/COMST.2015.2472395.

[15] E. Talavera, A. Daz lvarez, and J. E. Naranjo, "A Review of Security Aspects in Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 7, pp. 41 981–41 988, 2019, doi:10.1109/ACCESS.2019.2907861.

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

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

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

[19] 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.

[20] 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.

[21] 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.

[22] A. Jesudoss, S. K. Raja, and A. Sulaiman, "Stimulating Truth-telling and Cooperation Among Nodes in VANETs Through Payment and Punishment Scheme," *Ad Hoc Networks*, vol. 24, pp. 250–263, 2015.

[23] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A Reputation-Based Global Trust Establishment in VANETs," *5th International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, 2013.

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

[25] N.-W. Lo and H.-C. Tsai, "A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 9, 2009.

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

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

[28] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: A Lightweight Self-Organized Trust Model in VANETs," *Mobile Information Systems*, vol. 2016, 2016, doi:10.1155/2016/2F7628231.

[29] 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.

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

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

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

[33] D. Eckhoff, A. Brummer, and C. Sommer, "On the impact of antenna patterns on VANET simulation," in *2016 IEEE Vehicular Networking Conference (VNC)*, Dec 2016, pp. 1–4.

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

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

[36] 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.

[37] 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.

[38] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, "T-VNets: A Novel Trust Architecture for Vehicular Networks Using the Standardized Messaging Services of ETSI ITS," *Computer Communications*, vol. 93, pp. 68–83, 2016, doi: 10.1016/j.comcom.2016.05.013.

[39] D. Kim, Y. Velasco, W. Wang, R. N. Uma, R. Hussain, and S. Lee, "A new comprehensive rsu installation strategy for cost-efficient vanet deployment," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4200–4211, May 2017.

[40] R. Iqbal, "Challenges in Designing Ethical Rules for Infrastructures in Internet of Vehicles," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 11–15, 2018.

[41] Veins, "Vehicles in Network Simulation, The Open Source Vehicular Simulation Framework," available online: http://veins.car2x.org (Accessed: August 28, 2019).

[42] OpenStreetMap, "OpenStreetMap," Available online: https://www.openstreetmap.org (Accessed: August 28, 2019).

[43] SUMO, "Simulation of Urban MObility," Available online: http://sumo.dlr.de/wiki/Simulation_of_Urban_MObility (Accessed: August 28, 2019).

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

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

[46] Y. M. Chen and Y. C. 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.

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

[48] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, April 2016, doi:10.1109/TITS.2015.2494017.

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

[50] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-centric Trust Establishment in Ephemeral Ad Hoc Networks," in *The 27th IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2008, pp. 1238–1246.

[51] R. Mühlbauer and J. Kleinschmidt, "Bring Your Own Reputation: A Feasible Trust System for Vehicular Ad Hoc Networks," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, p. 37, 2018, doi:10.3390/jsan7030037.

[52] M. A. Azad, S. Bag, S. Parkinson, and F. Hao, "TrustVote: Privacy-Preserving Node Ranking in Vehicular Networks," *IEEE Internet of Things Journal*, 2018, doi:10.1109/JIOT.2018.2880839.