VTrust: A Robust Trust Framework for Relay Selection in Hybrid Vehicular Communications

Hao Hu†, Rongxing Lu†, and Zonghua Zhang‡

†School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798
‡Institut Mines-Télécom/TELECOM Lille and CNRS UMR 5157 SAMOVAR, France

Email: hhu002@e.ntu.edu.sg; rxlu@ntu.edu.sg; zonghua.zhang@telecom-lille.fr

Abstract—As one of the essential components of Intelligent Transport Systems (ITS), Vehicular Ad Hoc Network (VANET) plays a significant role in enabling various on-road applications, most of which primarily rely on two-hop Vehicle-to-Vehicle communications. To make such communications reliable and secure, it is significant to ensure that the trustworthy vehicles are selected as relays. To tackle this challenge, this paper proposes a robust trust framework, called VTrust, which systematically integrates a set of unique features of VANET, e.g., hybrid architecture, high dynamics, social attributes, into the traditional reputation system, with an objective to effectively differentiate the trust levels of the vehicles meanwhile preserve high scalability and robustness. The digital signature and multisignature techniques are also applied to enhance the security of VTrust. To validate the performance of the framework, an in-depth security analysis is conducted, which shows that it is secure and robust against several sophisticated attacks in VANETs. Also, a set of extensive simulations is carried out, demonstrating its effectiveness, accuracy, and scalability.

Keywords: VANET, Relay selection, Trust, Reputation system

I. INTRODUCTION

Vehicular Ad Hoc Network (VANET) has drawn great attention recently in both industry and academia due to its promising applications on the road [1]. As shown in Fig. 1, an envisioned VANET architecture is composed of some heterogeneous nodes, including mobile vehicles, stationary Road Side Units (RSUs), and remote servers. Each vehicle is equipped with On-Board Unit (OBU) device, allowing vehicles not only to communicate with each other (V-2-V) but also to interact with RSUs along the road (V-2-I). When RSU serves as a relay, a vehicle can also communicate with a remote server on the road. Due to its hybrid architecture, VANET provides us with not only safety-related applications (e.g., accident warning) but also non safety-related applications (e.g., infotainment). Because of these promising applications, auto industries tend to study VANET for providing new valued-added services on their new-fabricated vehicles in future. Meanwhile, since VANET is a special instantiation of traditional mobile ad hoc network (MANET), the academia also shows strong interest in it to test those previously-developed protocols for MANET.

Although VANET has been studied a lot, the trust and reputation models tailored to VANETs have not been fully exploited, because the hybrid architecture of VANET makes it different from traditional MANET, so the trust and reputation models developed in MANET cannot be applied in VANET directly. For example, Patwardhan et al. [2] propose a data intensive reputation management scheme for VANET, however, it does not really utilize the hybrid infrastructure of VANET and take advantages of RSUs. Raya et al. [3] introduce data-centric trust establishment in ephemeral VANET, while their work does not discuss how to generate and share data in VANET environment. Gomez et al. [4] propose a trust and reputation infrastructure-based proposal (TRIP) for VANET. Although the role of RSU in the trust and reputation model is considered, the data collection and spreading in VANET environment is out of concern. Therefore, many research challenges still remain in building trust and reputation models in VANET environment, thereby deserving our further investigation.

As one of the attempts to tackle the identified challenges, we present a robust trust framework, called VTrust, for relay selection in hybrid vehicular communications. The proposed VTrust framework integrates a set of unique features of VANET, e.g., hybrid architecture, high dynamics, social attributes, into the traditional trust and reputation system. In doing so, the framework can not only effectively differentiate various trust-level vehicles, but also preserve the scalability and robustness. As such, the vehicles can always choose highly-reliable and relevant vehicles as relays in two-hop V-2-V communications.

More specifically, our contributions delivered in this paper are three-fold,

- We firstly formulate the system model, as well as the trust model, for hybrid VANETs, which are given in Section II and taken as the design basis for our trust framework VTrust. It is worth noting that one of the salient features of VTrust is that it fully considers the unique features of VANETs, i.e., hybrid infrastructure, high dynamism, ephemeral link, and social connectivity, making it very applicable in hybrid vehicular communications. The design details are presented in Section IV.
- We further apply digital signature and multisignature
techniques, which are briefly introduced in Section III, to enhance the security of VTrust, especially to defend against the sophisticated attacks targeting at reputation systems, one of the core component of VTrust. The detailed analysis can be found in Section V.

- Finally, we develop a customized simulator built in Java, which is used to experimentally validate the performance of VTrust on efficiency, accuracy, and scalability. The results are reported in Section VI.

II. MODELS AND DESIGN GOALS

In this section, we formalize the system model, trust model and identify our design goals.

A. System Model

Our system model considers a scenario in urban area where Road Side Units (RSUs) are deployed at the crossroads and a set of vehicles $V$ are moving in the area, as shown in Fig. 2. In addition to RSUs and vehicles, a Trust Authority (TA) is also included in the system.

**TA**: Trust Authority plays a key role, which is powerful and highly trusted to take charge of the system initialization, the registration of subordinate RSUs and vehicles in our model. In addition, TA also maintains the trust and reputation scores for all vehicles as well as profiles of vehicles which store their social attributes. Due to its high capability of computation, TA can efficiently calculate and update the reputation scores for each vehicle.

**RSU**: Road side units (RSUs) are deployed at many crossroads which are equipped with more powerful wireless devices. With 802.11p protocol, they can exchange data with passing-by vehicles. In general, RSUs are subordinated to TA and connected with a remote server through high bandwidth, low delay and low bit error rates’ wires. Thus, RSUs function as a transit between vehicles and TA. Due to the high cost of RSU installment and maintenance, especially in the early stage of VANET, only a limited number of RSUs are deployed at crossroads where the traffic flow is very large.

**Vehicles**: The vehicles $V$ are highly mobile nodes, they are travelling along the road in a specific speed, hence it can be assumed that some vehicles are relatively static to each other for some periods on the road. Vehicles $V$ can be classified into private cars, buses, police cars, taxi cabs and trucks, whatever their functions in real life are, they are regarded the same in our model when performing as relays. Each vehicle is equipped with on board unit (OBU) which allows the vehicle to communicate with each other (V-2-V) and also to connect to RSUs along the road (V-2-I). In general, OBUs have no power restriction since they’re directly fed by the power of vehicles.

B. Trust Model

In our trust model, we define the trust level of each role in our system as follows:

**TA**: TA is a powerful entity, which cannot be compromised and is always trusted by other entities in our model. TA maintains the trust and reputation scores for all vehicles in VANET.

**RSU**: RSUs are deployed at road side but also subordinated to TA via reliable communication. Therefore, all these RSUs are also trusted in our model. However, it is possible for attackers to deploy some rogue RSUs at road side, thus we also need to adopt some efficient authentication mechanisms to detect and exclude these rogue RSUs in our system.

**Vehicles**: The behaviors of vehicles are actually the behaviors of drivers. The selfish or bad drivers always exist, they may be reluctant to cooperate if there is no benefit for them or deliberately do harmful things to the network, e.g., simply dropping the packets. In our trust model, we differentiate those vehicles from the normal vehicles by using our proposed VTrust framework. Specifically, two types to vehicles will appear in our model: one is White Vehicles who always relay the messages to the next hop once they receive some. To the opposite, the other type of vehicles which we call them Grey Vehicles have a certain possibility of dropping packets either because they’re selfish or they deliberately vandalize the network. Since Grey Vehicles are harmful to VANET, we need to figure them out.

C. Design Goals

The primary design objective of our framework is to provide an efficient trust model to distinguish white vehicles from grey vehicles, so that the vehicles with high trust score can be always selected as the relays, eventually increasing the efficiency and reliability of VANET. Specifically, there are four sub-goals to be achieved: i) **Ranking.** The proposed framework should be able to classify the grey vehicles and white vehicles into different clusters by ranking them in the reputation system; ii) **Improved relay ratio.** The proposed framework should also be helpful for improving the two-hop relay ratio in VANET; iii) **Scalability.** The proposed framework should be scalable, i.e., the framework still functions well when the number of vehicles significantly increases; and iv) **Robustness.** The proposed framework should be resistant against malicious attacks, e.g., repudiation attack, rogue RSU attack, badmouth attack, and packet dropping attack, etc.

III. PRELIMINARIES

In this section, we first recall the bilinear pairing technique and an efficient ID-based multisignature scheme [5], which serve as the basis of the proposed VTrust framework for ensuring its robustness.
A. Bilinear Pairing

Let \((G, \times)\) and \((G_T, \times)\) be two multiplicative cyclic groups of the same prime order \(q\). Then, a bilinear pairing \(e: G \times G \rightarrow G_T\) will satisfy the following properties: i) Bilinear: Let \(g, h \in G\) and \(a, b \in \mathbb{Z}_q^\ast\), then \(e(g^a, h^b) = e(g, h)^{ab}\). ii) Non-degenerated: Let \(g \in G\) be a generator in \(G\), then \(e(g, g) \neq 1_{G_T}\). and iii) Computable: Let \(g, h \in G\), then \(e(g, h)\) can be efficiently computed.

**Definition 1 (Bilinear Parameter Generator):** A bilinear parameter generator \(\text{Gen}\) is a probabilistic algorithm that takes a security parameter \(\kappa\) as its input, and outputs a 5-tuple \((q, g, G, G_T, e)\), where \(q\) is a \(\kappa\)-bit prime number, \((G, G_T)\) are two multiplicative groups of the same order \(q\), \(g \in G\) is a generator, and \(e: G \times G \rightarrow G_T\) is a non-degenerated and efficiently computable bilinear map.

B. ID-based Multisignature Scheme

Gentry and Ramzan [5] proposed an efficient ID-based multisignature scheme in 2006, which consists of five parts (Setup, Private key extraction, Individual signing, Aggregation, Verification), and each part will be detailed as follows.

**Setup:** Given a security parameter \(\kappa\), the private key generation (PKG) generates \((q, g, G, G_T, e)\) by running \(\text{Gen}(\kappa)\). PKG also chooses a random number \(s \in \mathbb{Z}_q^\ast\) as the master key, and computes \(h = g^s\). In addition, PKG chooses two cryptographic hash functions \(H_i : \{0, 1\}^\ast \rightarrow G\) with \(i \in \{0, 1\}\). Thus, the system public key is \((g, h, G, G_T, e, H_0, H_1)\).

**Private key extraction:** Given an identity ID, PKG can generate the corresponding private key \(S_i = H_0(0(\text{ID}))\).

**Individual Signing:** To sign a message \(m\), the signer with identity \(ID\) chooses a random number \(r_i \in \mathbb{Z}_q^\ast\), and computes \((S'_i = H_1(m)^{r_i} \cdot S_i, T'_i = g^{r_i})\) as its signature on \(m\).

**Aggregation:** Anyone can aggregate a collection of individual signatures \((S'_i, T'_i)\), for \(i = 1, 2, \cdots, n\), on the same message \(m\). In particular, the multisignature \((S_n, T_n)\) can be generated as \(S_n = \prod_{i=1}^{n} S'_i,\ \ T_n = \prod_{i=1}^{n} T'_i\). If it holds, the multisignature can be accepted; and rejected otherwise. Its correctness and security can be referred to [5].

IV. Proposed VTrust Framework

In this section, we describe our proposed VTrust framework for VANETs, which mainly consists of three parts: system initialization, relay selection, and trust update.

A. System Initialization

For a VANET under consideration, we assume that all roles share the same parameters. Specifically, given the security parameter \(\kappa\), Trusted Authority (TA) first generates \((g, q, G, G_T, e)\) by running \(\text{Gen}(\kappa)\), sets the master key \(s \in \mathbb{Z}_q^\ast\), and publishes the public key \((g, q, h, G, G_T, e, H_0, H_1)\). Although RSUs are trusted and subordinated by the TA, TA still needs to assign a private key for each RSU deployed at roadside to prevent potential rogue RSU issue launched by malicious guys. In particular, for each deployed RSU \(RSU_j\), TA generates its private key \(S_j = H_0(RSU_j)^s\). Besides RSUs, for each vehicle \(i\) with ID \(ID_i\), TA also generates its private key \(S_i = H_0(ID_i)^s\).

In addition, each vehicle \(i \in V\) also records its interactions with other vehicle \(j \in V/i\), including the numbers of successful interactions \(\text{succ}(i, j)^{(t)}\) and total interactions \(\text{total}(i, j)^{(t)}\) in the period from 0 to time \(t\). We will describe these interactions later, but initially, both \(\text{succ}(i, j)^{(0)}\) and \(\text{total}(i, j)^{(0)}\) are obvious. Define the local trust of vehicle \(i\) towards vehicle \(j\) at time \(t\) as follows,

\[
\text{ltru}_{ij}^{(t)} = \frac{\text{succ}(i, j)^{(t)}}{\text{total}(i, j)^{(t)}}
\]

and \(\text{ltru}_{ij}^{(0)} = \lim_{t \to 0} \frac{\text{succ}(i, j)^{(t)}}{\text{total}(i, j)^{(t)}} = 1\) to indicate each vehicle trusts other vehicles in the system in the initialization stage.

Besides the local trust, TA also maintains each vehicle’s global reputation, which is defined as follows,

\[
G\text{REP}_{ij}^{(t)} = \frac{\sum_{i \in N/j} \text{succ}(i, j)^{(t)}}{\sum_{i \in N/j} \text{total}(i, j)^{(t)}}
\]

which is the global reputation of vehicle \(j\) at time \(t\). Initially, \(G\text{REP}_{ij}^{(0)} = \lim_{t \to 0} \frac{\sum_{i \in N/j} \text{succ}(i, j)^{(t)}}{\sum_{i \in N/j} \text{total}(i, j)^{(t)}} = 1\), which also indicates all vehicles in the system have the same reputation at the beginning. Note that, the detailed procedure of trust update will be described in the rest of this section.

Except for trust and reputation scores, social similarities of vehicles and messages are also considered for relay vehicle choosing since it is more possible for a vehicle to forward the message if it shares more social similarities with the message, e.g. destination. The social attributes are stored in a profile \(I\), each element of \(I\) is a binary variable indicating one specific attribute of the vehicle or message. Before a vehicle \(j\) starts its journey, it firstly declares its social attributes \(I_j\) and uploads it to the TA, the social attributes of a message \(I_m\) is stored together with the message.

B. Relay Selection

After the VANET system is established, each vehicle \(i \in V\) will run in an urban area, and make V-2-I and V-2-V communications when encountering RSUs and other vehicles. In particular, when a vehicle \(i\) meets with an RSU \(RSU_j\) at time \(t_k\), they can first use their privacy keys \((S_i, S_j)\) to negotiate a session key \(sk_{ij} = H_1(e(H_0(ID_i), H_0(RSU_j))^s)|t_k\) in a non-interactive way, i.e.,

\[
sk_{ij} = H_1(e(S_i, H_0(RSU_j))|t_k) = H_1(e(H_0(ID_i), S_j)|t_k)
\]

With the key \(sk_{ij}\), vehicle \(i\) and \(RSU_j\) can launch secure communications. During the period of V-2-I communication, \(RSU_j\) also communicates with TA to obtain the updated global reputations of other vehicles \(G\text{REP}_j^{(t_k)}\), for \(l \in V/i\), and forward these global reputations to vehicle \(i\). Note that, according to the localization feature of VANETs, most of vehicles are active in a local area, vehicle \(i\) most likely meet
other vehicle active in the same area. Therefore, vehicle \( i \) does not need to obtain the global reputations of all vehicles in the system, but only the global reputations of those vehicles moving in proximity.

Fig. 3. Relay selection in two-hop VANET communications

In addition to the V-2-I communications, vehicle \( i \) can also launch V-2-V communications later, in either one-hop or two-hop communications to deliver information to its following vehicles, as shown in Fig. 3. In order for the non-repudiation requirements, when vehicle \( i \) sends out a message \( m \) at time \( t_{k+1} \), it also attaches its signature \( \sigma_i(m) \mid t_{k+1} \). Thus, other vehicles can verify the source of the message \( m \) when they receive it. One-hop communication is reliable, while two-hop communication is not, because two-hop communication shall require a reliable relay vehicle for forwarding. Therefore, in order to choose a reliable relay vehicle, vehicle \( i \) should run the following steps.

Step 1: vehicle \( i \) chooses a set of candidate vehicles \( C \), for each vehicle \( j \in C \), vehicle \( i \) should compute its trust score \( TS(i, j)(t_{k+1}) \) at time \( t_{k+1} \) by considering three factors: global reputation value of the targeted vehicle \( j \), direct previous experience of \( i \) to the targeted vehicle \( j \), and the recommendations from the nearby vehicles \( B \) towards the targeted vehicle \( j \).

Global reputation value: vehicle \( i \) can obtain \( j \)'s global reputation value \( GREP_j(t_k) \) at time \( t_k \). Since the reputation value changes from time to time, it is very time sensitive. At the same time, vehicle \( i \) is not always within the scope of RSU to update \( j \)'s reputation value timely, hence an attenuation factor \( e^{-\lambda(t_{k+1}-t_k)} \) is proposed as the weight of reputation value. \( \lambda \) is a coefficient to describe the attenuating speed, in dense environment where vehicle number is quite large and reputation value updates quickly, \( \lambda \) is bigger and vice versa.

Direct previous experience: Direct previous experience comes from the local trust value \( ltru(i, j)(t_{k+1}) \) of vehicle \( i \) to vehicle \( j \). Note that, in our system, if vehicle \( i \) had never asked vehicle \( j \) to relay a message before, \( ltru(i, j)(t_{k+1}) = 1 \).

Recommendations from the nearby vehicles: Recommendations from the nearby vehicles \( B \) is described by those nearby vehicles' local trust values towards the target vehicle \( j \). Also, a weight \( \omega_l \) will be given to each of those nearby vehicle \( l \in B \) according to its global reputation value \( GREP_l(t_k) \) that vehicle \( i \) obtained from RSU at time \( t_k \). To ensure that \( \sum_{l \in B} \omega_l = 1 \), we normalize \( \omega_l \) as

\[
\omega_l = \frac{GREP_l(t_k)}{\sum_{l' \in B} GREP_l(t_k)}
\]

By integrating the above parts, vehicle \( i \) can calculate the trust scores \( TS(i, j)(t_{k+1}) \) of vehicle \( j \) as

\[
TS(i, j)(t_{k+1}) = \alpha_i \cdot GREP_j(t_k) + \beta_i \cdot ltru(i, j)(t_{k+1}) + \gamma_i \cdot \sum_{l \in B} \omega_l \cdot ltru(l, j)(t_{k+1})
\]

where \( \alpha_i = e^{-\lambda(t_{k+1}-t_k)} \), and \( \beta_i, \gamma_i \) may choose proper values to satisfy \( \alpha_i + \beta_i + \gamma_i = 1 \).

Step 2: After getting the candidate vehicle \( j \)'s trust score, vehicle \( i \) then computes the corresponding similarity score \( sim(j, m) \) of the that candidate vehicle \( j \) and the attempted deliver message \( m \) sent by \( i \). It describes the probability of the message \( m \) being forwarded by a vehicle \( j \) where \( sim(j, m) \in [0, 1] \). Specifically, to compute the similarity score, let \( I_k = \{I_{i,j,k}\}_{1 \times n} \) and \( I_m = \{I_{m,k}\}_{1 \times n} \) denote the social attributes vector of vehicle \( j \) and message \( m \) respectively, where the dimension of the social attributes vector, \( n \), is the same to all vehicles and messages, and \( I_{i,j,k} \in \{0, 1\} \) for each \( i \leq i \leq n \) [6]. The similarity score between candidate vehicle \( j \) and the attempted deliver message \( m \) is evaluated as:

\[
sim(j, m) = \frac{\sum_{k=1}^{n} I_{j,k} \cdot I_{m,k}}{\sqrt{\sum_{p=1}^{n} I_{j,p}^2} \sqrt{\sum_{q=1}^{n} I_{m,q}^2}} \in [0, 1]
\]

Step 3: Relay node is chosen according the relay score of a specific vehicle \( j \), denoted by \( RS(i, j)(t_{k+1}) \) where

\[
RS(i, j)(t_{k+1}) = TS(i, j)(t_{k+1}) \times sim(j, m)
\]

The vehicle with the highest relay score will serve as the relay vehicle. By using the watchdog mechanism [7], vehicle \( i \) can observe whether vehicle \( j \) forwards or drops the message. If vehicle \( j \) forwards the message, both \( succ(i, j)(t_{k+1}) \) and \( total(i, j)(t_{k+1}) \) increase 1. Otherwise, only \( total(i, j)(t_{k+1}) \) increases 1. Note that, due to the watchdog mechanism, other neighboring vehicles can also observe the vehicle \( j \)'s forward/drop event.

Step 4: Vehicle \( i \) contacts all neighboring vehicles who also observed the vehicle \( j \)'s forward/drop event. For vehicle \( j \)'s forward/drop event, vehicle \( i \) and these neighboring vehicles cooperatively generate a multisignature (described in section III-B) on the event, which will be used as an evidence for vehicle \( j \)'s trust update at TA.

As we discussed in our trust model, if a vehicle is white, it will always try its best to forward message. If a vehicle is grey, it could drop the message. Therefore, with the information \( succ(i, j)(t_{k+1}) \) and \( total(i, j)(t_{k+1}) \), we can gradually distinguish white vehicles from grey vehicles through trust update.

C. Trust Update

When vehicle \( i \) encounters an RSU later, e.g., at time \( t_{k+2} \), it can establish a secure channel with TA via the RSU as discussed above. For each vehicle \( j \) who is encountered by \( i \) and its \( succ(i, j)(t_{k+1}) \) and \( total(i, j)(t_{k+1}) \)
are changed at vehicle \( i \), vehicle \( i \) submits \( succ(i,j)^{\delta_{k+1}} \) and \( total(i,j)^{\delta_{k+1}} \) together with the multisignature to TA. If the multisignature is valid, and at least one signer in the multisignature has its global reputation value higher than a threshold \( Th \), TA updates vehicle \( j \)'s global reputation value as \( GREP^j_{\delta_{k+2}} = \sum_{i \in N/j} succ(i,j)^{\delta_{k+2}} \), where all \( succ(i,j)^{\delta_{k+2}} \) and \( total(i,j)^{\delta_{k+2}} \) are the latest updated values that TA got from each vehicle \( i \). Otherwise, due to all signers’ global reputation values are low, TA won’t accept this update for preventing the badmouth attack. Finally, when vehicle \( i \) leaves the RSU, it also obtains the newest global reputation values of other vehicles from TA.

V. Security Analysis

In this section, we analyze the security, especially the robustness of proposed VTrust framework in the presence of adversaries with respect to the following attacks.

**Resilience to repudiation attack:** In the proposed VTrust framework, when a message is sent out, the sender will also attach either a single signature or a multisignature on the message, which not only fulfills the requirements of source authentication and data integrity, but also achieves the non-repudiation. Therefore, repudiation attack can be resisted in the VTrust frameworks. That is, if a vehicle sends out a message, it cannot deny this action later, so that the robustness of VTrust can be enhanced.

**Resilience to Rogue RSU attack:** Although all deployed RSUs are trusted in the proposed VTrust framework, if there is no authentication mechanism, an adversary could place a rogue RSU to degrade the trustworthy environment of VANET. In the proposed VTrust framework, V-2-I communication actually implicitly achieves mutual authentication by establishing the non-interactive session key. If an RSU is a rogue RSU, it cannot successfully generate the session key. Therefore, rogue RSU attack can be resisted in the VTrust frameworks.

**Resilience to badmouth attack:** In the proposed VTrust framework, a badmouth attack means that a colluding collective gives false information regarding trust update and uploads it to the TA for disrupting the system. For example, a grey vehicle colluding with other grey vehicles on the multisignature may cheat TA that a relay interaction is unsuccessful even though the relay vehicle helped forward the message, or on the other hand, they may also give higher local rank to the other colluding vehicles. To address this badmouth attack, the proposed VTrust framework requires that at least one vehicle with reputation score higher than a threshold \( Th \) should be involved in the multisignature, which can stop the collusion to some extent. Since the majority of vehicles in the system are normal, our countermeasure is workable, which can help the TA to decide whether or not accept the trust update.

**Resilience to packets dropping attack:** In the proposed VTrust framework, those malicious vehicles who drop packets deliberately will be given a lower reputation score in Trust Authority (TA). By choosing a highly reputable vehicle for the next hop, those malicious vehicles can be isolated, thus a reliable two-hop message relay can be achieved.

From the above analysis, we can see that our proposed VTrust framework is indeed secure and robust against the above attacks.

VI. Performance Evaluation

In this section, we study the performance of VTrust using a custom simulator built in Java. The performance metrics used in our trust framework are: i) Relay ratio, which is defined by a ratio of the number of messages that are successfully relayed to the total number of messages generated in the network in a specific time period, ii) Accuracy, which is defined by the ratio of the number of detected grey vehicles to the total number of grey vehicles in a specific time period; and iii) Scalability, which is measured by the convergence time of delivery ratio varying with different numbers of vehicles.

![Simulation results results on relay ratio, accuracy and scalability of VTrust](image)

(a) Map for simulation  
(b) Effectiveness  
(c) Accuracy  
(d) Scalability

Fig. 4. Simulation results on relay ratio, accuracy and scalability of VTrust

A. Simulation Setup

In our simulation, total \( n \) vehicles with transmission radius of 300 m and total \( N = 4 \) RSUs with transmission radius of 1000 m are deployed in an urban area of \( 10000m \times 10000m \), as shown in Fig. 4(a). Each vehicle follows the shortest path map based movement routing [1], i.e., the vehicle randomly chooses a destination and gets there in the shortest path with an constant speed of \( v \). After 5-minute pause, the vehicle repeats the process until the end of simulation time. For each vehicle \( j \) at interval of 1 minute, if the situation in Fig. 3 appears, \( j \) will send out a message. For total \( n \) vehicles, we define \( \rho = 30\% \) of the vehicles are grey vehicles. Different from the white vehicles who always relay the message, grey vehicles will drop the packets with a probability of 50%.

The detailed settings of the simulation are shown in the Table 1. We perform the simulation for specific period varying from 5 minutes to 1 hour with an increment of 5 minutes. For
each case, we run the simulation 10 times, and the average relay ratio, accuracy, and scalability are reported in Fig. 4.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area, duration</td>
<td>$10000 \times 10000\text{m}^2$, 1 hour</td>
</tr>
<tr>
<td>RSU Number, Transmission</td>
<td>$N = 4$, 1000m</td>
</tr>
<tr>
<td>Vehicles</td>
<td></td>
</tr>
<tr>
<td>number</td>
<td>$n = 50, 100, 150$</td>
</tr>
<tr>
<td>transmission range</td>
<td>$\nu = 300\text{m/s}$</td>
</tr>
<tr>
<td>velocity</td>
<td>$v = 40\text{km/h}$</td>
</tr>
<tr>
<td>Message generate/vehicle</td>
<td>1 piece/4 min</td>
</tr>
<tr>
<td>Grey vehicles ratio</td>
<td>$\rho = 30%$</td>
</tr>
<tr>
<td>Dropping probability</td>
<td>50%</td>
</tr>
</tbody>
</table>


table I

B. Simulation Results

1) Effectiveness: Firstly, we compare the relay ratio of our proposed VTrust framework with a random selection method. From Fig. 4(b) we observe that the relay ratio can be improved gradually to 90% using our VTrust framework while it keeps in lower level in the random selection method. Hence we can conclude that the VTrust framework is more effective for improving relay ratio than random selection.

2) Accuracy: Fig. 4(c) depicts the detection ratio of VTrust when the number of vehicles is 50, 100, and 150, respectively. From the figure, we can observe that after a time period, VTrust framework shows a very high detection ratio for grey vehicles. That’s because it takes time for messages to be generated and relayed to distinguish the grey vehicles from white vehicles, but after a few minutes, VTrust achieves high accuracy for grey vehicles detection.

3) Scalability: Fig. 4(c) and Fig. 4(d) show that both the detection ratio and relay ratio of VTrust framework are very convergent, especially when the vehicle number is large. The reason is that when more vehicles are present in VTrust framework, more messages and relay requirements are generated so the grey vehicles are more easily exposed and hence distinguished in VTrust. Therefore, we can be sure that the proposed VTrust framework is scalable.

VII. Related Works

Recently, trust and reputation models in VANET have been studied by a few researchers [2]–[4], [8], [9], which are closely related to our proposed VTrust framework. Patwardhan et al. [2] present a distributed reputation management scheme for VANET, which enables vehicles to quickly adapt to changing local conditions and provides a bootstrapping method for establishing trust relationships. However, their scheme is not quite scalable and robust. Different from traditional entity-based trust model, Raya et al. [3] suggest a data-oriented trust establishment framework. By combining trust values of each piece of data together, their framework deals well with ephemerality and functions well in sparse areas. However, in dense urban area, due to large amount of data, their framework is less efficient. In 2012, Gomez et al. [4] develop a trust and reputation infrastructure-based proposal, called TRIP, which uses direct previous experiences and recommendation from nearby vehicles and central authority to compute trust scores. However, it doesn’t consider time factor in reputation system, neither does it adopt a punishment or isolation mechanism for low reputation vehicles. Chen et al. [8] propose a trust-based message propagation and evaluation framework in VANET, however, it does not consider the robustness. Zhang et al. [9] propose a reputation-driven anomaly detection system to detect and handle anomalous mesh nodes in wireless mesh networks.

Distinct from above works, our proposed VTrust framework is efficient and effective in distinguishing grey vehicles from white vehicles, it not only solves the relay selection problem by isolating grey vehicles, but also shows good scalability and robustness against a few malicious attacks like badmouth attack, repudiation attack and packets dropping attack.

VIII. Conclusions

In this paper, we have proposed a robust trust framework (VTrust) for relay selection in hybrid vehicular communications. In particular, our proposed VTrust integrates some unique features of VANET into the traditional trust and reputation system so as to efficiently differentiate white vehicles from grey vehicles, meanwhile preserving high scalability and robustness. The detailed security analysis showed that VTrust is secure and robust against some well-known attacks in VANET. In addition, extensive simulations were also conducted, and the results demonstrated the efficiency and effectiveness of VTrust. In future work, we aim to integrate more features of VANET into our trust model to make it more accurate.

References