HDRS: A Hybrid Reputation System With Dynamic Update Interval for Detecting Malicious Vehicles in VANETs

Xuejiao Liu, Oubo Ma, Wei Chen, Yingjie Xia, *Member, IEEE*, and Yuxuan Zhou

*Abstract***—The reputation-based scheme is a promising solution to prevent malicious behaviors in Vehicular Ad-hoc Networks (VANETs). However, traditional centralized reputation schemes are not suited for distributed networks, while decentralized reputation schemes are vulnerable to malicious vehicles spreading false messages. Most of these schemes assume that the behavior of vehicles can be accurately measured as reputation from the communication, ignoring that malicious vehicles may behave intelligently to avoid being detected. In this paper, we propose a hybrid reputation system (HDRS) which allows vehicles and roadside units (RSU) to complete reputation evaluations separately and provide references to each other. HDRS utilizes a reliability evaluation module to filter out unreliable calculation results and reference records. Furthermore, HDRS includes a dynamic adjustment mechanism for the reputation update interval, employing Analytic Hierarchy Process (AHP) and reliability evaluation results to resist intelligent attacks. Simulation results illustrate that HDRS can maintain a high detection rate and low false-positive rate for detecting malicious vehicles in different environments. Compared with existing schemes, HDRS increases the detection rates of collusion and intelligent attacks by 30% and 16%, respectively.**

*Index Terms***—VANETs, reputation system, hybrid architecture, reliability evaluation, dynamic adjustment.**

I. Introduction

OWING to open, distributed, and highly dynamic characteristics, VANETs are vulnerable to attacks by malicious vehicles [1], [2]. Attackers can spread false messages or launch malicious attacks, causing congestion or even traffic accidents in scenarios with dense traffic or sparse traffic, or blind zones of infrastructure [3]. Therefore, it is challenging to establish the trust of vehicles accurately based on the communications while detecting malicious vehicles in VANETs.

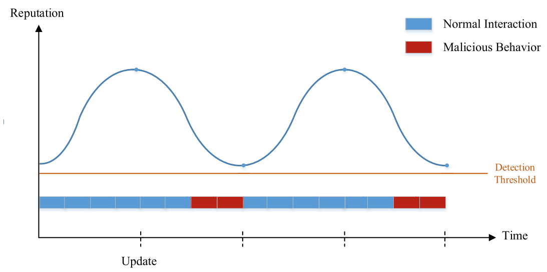


Fig. 1. **Intelligent attacks.** For reputation systems with the fixed reputation update interval, malicious vehicles can stabilize the reputation fluctuation above the detection threshold by controlling the ratio of their malicious behavior to legal behavior for a while.

The reputation-based scheme is one of the important research directions to ensure secure and reliable communication [4], [5]. Based on *reputation*, which is defined as the confidence of one node on the other for performing a specific information interaction in VANETs [6], each vehicle can measure the credibility of others before taking action on the received message to avoid serious consequences caused by false messages [7].

Reputation systems can be divided into centralized and distributed based on the architecture. The centralized scheme relies on the center to evaluate the global reputation of the vehicle, but it is not suitable for the blind zones of infrastructure [8]. The distributed scheme relies on vehicles to self-organize to update each other's reputation. However, the evaluation results may be inaccurate due to insufficient references [9].

In VANETs, malicious vehicles can ally to achieve collusion attacks [10]. They improve their reputation at a low cost and give unreasonable low scores to a target vehicle. If the evaluator does not verify whether the result is reliable when updating a target's reputation, it is easy for malicious vehicles to implement collusion attacks by providing false opinions. Therefore, in addition to using references to calculate the trust value, a reputation system should also evaluate the reliability of these references and the likelihood of the target vehicle reaching the expected trust value [11].

Furthermore, intelligent malicious vehicles in VANETs may switch between malicious and legitimate. As depicted in Fig.1, these vehicles control the ratio of their malicious behavior to legal behavior for a while. Kerrache *et al.* [12] pointed out that intelligent malicious vehicles can bypass the detection of the reputation system in the manner described above. They proposed to evaluate the trust among vehicles for independent

Manuscript received 10 October 2020; revised 27 May 2021 and 8 August 2021; accepted 15 September 2021. Date of publication 8 October 2021; date of current version 9 August 2022. This work was supported in part by Zhejiang Province Natural Science Foundation under Grant LY19F020021, in part by the National Natural Science Foundation of China under Grant 61873232, in part by the New Talent Plan of Zhejiang Province under Grant 2020R427062, and in part by the Opening Project of Key Laboratory of Ministry of Public Security (Public Security Information Application Based on Big-data Architecture) under Grant 2020DSJSYS005. The Associate Editor for this article was R. Malekian. *(Corresponding author: Yingjie Xia.)*

Xuejiao Liu, Oubo Ma, and Yuxuan Zhou are with the School of Information Science and Technology, Hangzhou Normal University, Hangzhou 311121, China.

Wei Chen is with the School of Information Science and Technology, Hangzhou Normal University, Hangzhou 311121, China, and also with MacroSAN Technologies Company Ltd., Hangzhou 310053, China.

Yingjie Xia is with the College of Computer Sciences, Zhejiang University, Hangzhou 310058, China, and also with Hangzhou Yuantiao Technology Company, Hangzhou 311121, China (e-mail: xiayingjie@zju.edu.cn).

Digital Object Identifier 10.1109/TITS.2021.3117289

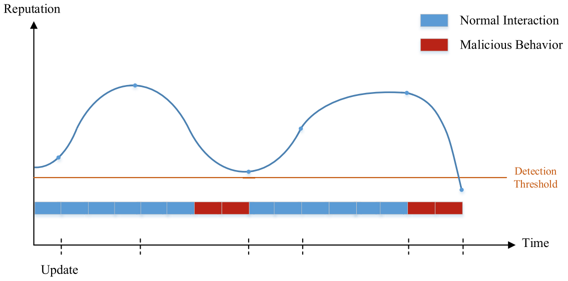


Fig. 2. **Dynamic update interval.** If the reputation update interval changes dynamically, it will be difficult for malicious vehicles to switch behavior patterns to maintain stable reputation fluctuations.

periods and compute the behavior variation of the target vehicle between smaller, consecutive periods to prevent intelligent attackers from attempting to bypass the reputation system [13]. Later, they proposed a new mechanism for detecting intelligent attacks based on an adaptive detection threshold [14], the essence of which is to amplify the punishment for malicious behavior. According to theoretical analysis and simulation experiments, we find that this mechanism will produce a particular amount of false alarms. In addition, the detection rate of this mechanism decreases significantly when the proportion of malicious behavior of the attacker is low.

This paper proposes a hybrid reputation system (HDRS) to solve the above problems, in which the vehicle and the RSU update target's V2V reputation and global reputation separately and provide a reference to each other. We utilize the reliability evaluation module to filter out the unreasonable results obtained by the trust calculation module by measuring the expected value and the deviation value. In addition, we propose adjusting the update interval of the evaluator dynamically by quantifying the security of the communication environment (see Fig.2). The main contributions of this paper are as follows.

1) We propose a hybrid reputation system (HDRS), in which V2V reputation and global reputation are evaluated through multiple reference sources, respectively, which effectively balances the infrastructure dependence with a comprehensive evaluation of multiple reference sources.

2) We utilize a reliability evaluation module to evaluate the creditability of the trust value calculated from multiple references, which can mitigate collusion attacks by filtering unreasonable results.

3) We propose a dynamic mechanism for adjusting the reputation update interval based on the communication security of the evaluator to avoid malicious vehicles bypassing detection.

The rest of the paper is organized as follows: Section II reviews related works. Section III introduces the entities and hybrid architecture of HDRS and the attack model of malicious vehicles. In Section IV, we provide the design details of our scheme. In Section V, we analyze the detection performance of HDRS in simulation. Finally, we summarize our work in Section VI.

II. Related Work

In this section, we review the trust management schemes in VANETs.

A. Cryptography-Based Schemes

Many latest studies utilize cryptography to help trust establishment in VANETs. Hu *et al.* [15] proposed a reliable trust-based platoon service recommendation (REPLACE) to compute the trust value of the platoon head in a platooning application. The security of this scheme is based on establishing a secure session key between the RSU and the vehicle using public-key cryptography and certificates. The use of the established non-interactive session key prevents malicious vehicles from launching attacks. Kerrache *et al.* [16] proposed a social-driven trust management scheme for the Internet of Vehicles (IoV) which utilizes chaotic maps-based PKI for establishing trust among communicating nodes. Azad *et al.* [17] proposed a collaborative crowdsourcing-based vehicle reputation system (TrustVote) in which the RSU utilizes homomorphic encryption to hide vehicles' weighted aggregated credibility scores and the list of interacted vehicles.

B. Reputation-Based Schemes

Reputation computation is considered to be a computationally cheaper alternative to cryptography [2]. There are two main categories of existing reputation schemes in VANETs: centralized and distributed schemes. The centralized reputation scheme relies on infrastructure to centrally update and maintain the global reputation of vehicles. Li *et al.* [18] pointed out that a centralized scheme is easier to manage, control, and secure. They designed a reputation-based announcement scheme for VANETs based on these characteristics. Cui *et al.* [19] proposed a centralized-based reputation scheme suitable for highways and urban roads in which the Trusted Authority (TA) weights the feedbacks from different vehicles and update the target's reputation score. TA adds a target to the blacklist and announces its true identity when its reputation is below the threshold. Kadadha *et al.* [20] utilized RSUs to form a blockchain and designed a smart contract to hold and update the reputations of registered vehicles transparently and in a trusted manner on-chain. Khalid *et al.* [21] proposed an incentive provisioning scheme in which the RSU updates the initiator's reputation based on the event validations provided by the witnesses, and the initiator rewards the witnesses afterwards.

The distributed reputation scheme does not depend on the infrastructure, and the vehicles maintain and update the V2V reputation through self-organization. El *et al.* [9] developed a reputation model that can evaluate the trustworthiness of both vehicles and messages. To reduce the overhead during propagation, the single-hop nodes, which are close to each other and similar in their mobility pattern, are clustered into individual platoons. Kudva *et al.* [22] proposed to build a blockchain by self-organization of vehicles and filter the malicious miner vehicles based on service standard score. Xu *et al.* [23] proposed a trust-based probabilistic broadcast scheme (TPB). TPB has a lightweight trust management model based on direct and recommended trust evidence to obtain vehicles' trust levels. Kerrache *et al.* [24] proposed a scheme called T-VNets, in which the vehicles follow a centralized reputation method within the transmission range of the RSU and update the V2V reputation through self-organization in the blind zone.

There are two ways to trigger an update in reputation systems: interaction-based and time-based. The interaction-based method requires setting a critical value for the number of interactions to trigger the update. Ahmad *et al.* [6] proposed a novel trust evaluation and management (TEAM), in which vehicles will update each other's reputation every time they complete an interaction. Dias *et al.* [25] proposed a cooperative watchdog system in which vehicles evaluate the target vehicle based on a particular number of interaction records. In these schemes, the target vehicle can control when its reputation is updated by the evaluator by adjusting the number of interactions, thereby achieving reputation manipulation. The time-based triggering method needs to set a trigger period. Kerrache *et al.* [13] proposed a risk-aware trust-based architecture for collaborative multi-hop vehicular communications. In this scheme, the evaluator maintains a fixed reputation value of the target vehicle until the timer triggers the next update. In the time-based method, the evaluator occupies a dominant position and can decide when to update the reputation of a target vehicle. However, it is challenging to set a reasonable fixed update interval in the complex and variable environment of VANETs.

C. Machine Learning-Based Schemes

Recently, scholars have tried to combine machine learning to assist in the detection of malicious vehicles. Fan *et al.* [26] proposed an attribute-weighted k-means clustering algorithm to identify legitimate messages among messages with possibly contradictory contents received during a short period. Shams *et al.* [27] proposed a trust-aware intrusion detection and prevention system, including a support vector machine (SVM) module to detect malicious behaviors. Magaia and Sheng [28] proposed a novel reputation framework ReFIoV for information-centric vehicular applications leveraging on machine learning and the artificial immune system. This scheme uses the k-means clustering algorithm to cluster nodes and integrates other nodes' recommendations to make the framework resilient against false accusations and praise as a result of unpredictable nodes' behavior. Xiao *et al.* [29] proposed a hotbooting policy hill climbing (PHC)-based UAV relay strategy with reinforcement learning to help the VANET resist smart jamming in the dynamic game without being aware of the VANET model and the jamming model.

III. The Hybrid Architecture of HDRS

This section introduces the entities in HDRS and the hybrid architecture of HDRS and the attack model of malicious vehicles.

A. System Model

As depicted in Fig.3, there are two main types of entities in HDRS: vehicles and RSUs.

1) Vehicles: In a V2V reputation evaluation process, vehicles are divided into three roles: evaluator, target, and neighbor. The vehicles that realize information interaction are evaluators and targets of each other. Vehicles within the evaluator's transmission range are its neighbors. The evaluator updates the V2V reputation of a target vehicle based on the records of multiple reference sources and shares this information with neighbors and RSUs. Neighbors provide the evaluator with the historical V2V reputation of a target vehicle. Since multiple reputation evaluation processes may exist parallel in VANETs, a vehicle may play different roles simultaneously.

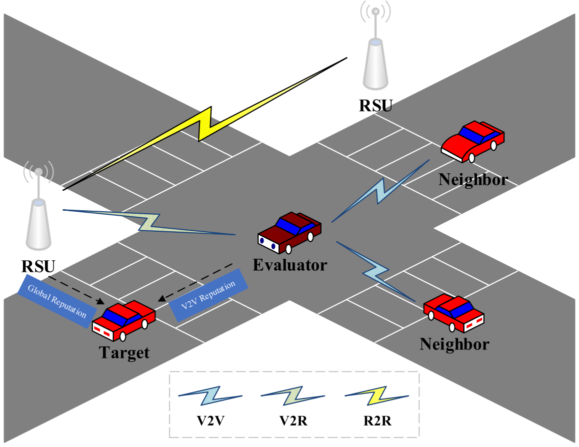


Fig. 3. System model.

2) RSUs: RSUs receive the V2V reputation of vehicles within their transmission range and update the global reputation of all vehicles. Then, they punish malicious vehicles and update the global blacklist. Finally, RSUs announce the updated information to all vehicles within their transmission range and one-hop neighbor RSUs.

B. Our Reputaiton System

HDRS contains V2V reputation and global reputation, updated by the evaluator and RSU, respectively. A target vehicle may have multiple V2V reputations due to the presence of multiple evaluators, but its global reputation is unique.

1) V2V Reputation: Four reference sources are required for the calculation of V2V reputation.

- *Direct experience:* The evaluator stores all records of direct interactions with the target.
- *Opinion of neighbor:* The evaluator receives and stores the target's V2V reputations updated by neighbors.
- *Role-based rule:* The evaluator formulates trust rules based on different identities of vehicles.
- *Global reputation:* The evaluator receives and stores the target's global reputation, regularly updated and published by the RSU.

The evaluator calculates the target's trust value based on the above four reference sources and evaluates the reliability of the result. If the trust value passes the reliability test and is higher than the detection threshold, it will be updated as the target's V2V reputation. Otherwise, the target is added to the evaluator's local blacklist.

2) Global Reputation: Three reference sources are required for the calculation of global reputation.

- *V2V reputation:* the RSU receives and stores vehicles' V2V reputations within the transmission range.
- *Opinion of RSU:* the RSU receives and stores the reputation opinions provided by neighbor RSUs.
- *Historical reputation:* the RSU stores the global reputation of all vehicles calculated for each round.

The RSU calculates the vehicle's trust value based on the above three reference sources and evaluates the reliability of the result. Then, by comparing the historical reputation, RSU determines whether the vehicle needs to be punished. If the trust value is higher than the detection threshold, it will be updated as the vehicle's global reputation. Otherwise, the vehicle is added to the global blacklist.

C. Attack Model

HDRS considers the following five malicious behaviors.

- *False message:* Malicious vehicles send false messages to deceive other vehicles.
- *Value imbalance attacks:* Malicious vehicles send genuine infotainment information to enhance their reputation and then send false road safety information or traffic efficiency and management information to deceive other vehicles.
- *Selfish behavior:* Selfish vehicles utilize the resources transmitted in VANETs while not providing services to others [25].
- *Collusion attacks:* Malicious vehicles ally to enhance their reputation at a low cost and jointly give unreasonable low scores to target vehicles.
- *Intelligent attacks:* Malicious vehicles control their behavior for a period of time to keep the reputation above the detection threshold, thereby bypassing reputation detection.

IV. Proposed Details

This section presents the trust calculation and reliability evaluation modules and then describes how the evaluator and RSU update the V2V and global reputations. Finally, we introduce how to adjust the update interval dynamically. The main notations in this section are given in Table I.

A. Trust Calculation Module

The basis of the reputation update is to calculate the trust value. The trust calculation module calculates the target's trust value by weighted averaging the rating values in the records from different reference sources. To defend against value imbalance attacks, we set three reputations of the target vehicle based on information types.

The trust value is calculated by

$$T_X(m,n,c)=\frac{\sum_{h\in\Re_X(m,n,c)}\omega_X(h)\ \cdot s}{\sum_{h\in\Re_X(m,n,c)}\omega_X(h)},\qquad(1)$$

where T_X denotes the trust value calculated utilizing the records provided by the reference source X; X is one of D, O, R, and G standing for direct experience, opinion of neighbor, role-based rule, and global reputation, respectively; m denotes the evaluator; n denotes the target vehicle; c denotes the information type, such as road safety information (rs), traffic efficiency and management information (tm), and infotainment information (in) [30]; $\Re_X(m,n,c)$ denotes the set of all records associated with X; h denotes the historical behavior record of the target, and its storage form is determined by X; $\omega_X(h)$ denotes the weight function of the record ($\omega_X(h)\ \in$ [0, 1]); s denotes the rating value stored in the record.

TABLE I
Notations

Notation	Description
T	Trust value
X	Reference source
D, O, R, G	Direct experience, opinion of neighbor, role-based rule, and global reputation
m, n, c	Evaluator, target, information type
rs, tm, in	Road safety information, traffic efficiency and management information, and infotainment information
h	Historical behavior record
$\Re_X(m,n,c)$	Set of all records
ω	Weight function
t	Recorded time
s	Rating value
ρ	Reliability evaluation value
ρ_{RX}, ρ_{DX}	Rating reliability and deviation reliability
Rv, Rg	V2V reputation and global reputation
τ_D, τ_R	Detection threshold and reliability threshold
β	Fixed weight coefficient

B. Reliability Evaluation Module

Evaluators may face insufficient references or significantly deviations in neighbors' opinions. These cause the trust value obtained by the trust calculation module to be unreliable. Therefore, we utilize the reliability evaluation module to mitigate those adverse effects.

The reliability value of $T_X(m,n,c)$ is defined as

$$\rho_X(m,n,c)=\rho_{RX}(m,n,c)\cdot\rho_{DX}(m,n,c),\qquad(2)$$

where $\rho_{RX}(m,n,c)$ denotes the rating reliability; $\rho_{DX}(m,n,c)$ denotes the deviation reliability. $\rho_X(m,n,c)\in$ [0, 1], where 0 indicates the result of the trust calculation is entirely unreliable, and 1 indicates it is entirely reliable.

Rating reliability is similar to the expected value in statistics and is used to measure the number and credibility of records.

$$\rho_{RX}(m,n,c)=1-e^{-\gamma_X\cdot(\sum_{h\in\Re_X(m,n,c)}\omega_X(h))},\qquad(3)$$

where γ_X is the control factor, which can be adjusted based on the value of X. Since there is usually more than one direct interaction record and neighbor's opinion, we tend to make γ_D and γ_O smaller than γ_R and γ_G. $\rho_{RX}(m,n,c)$ increases from 0 to 1 when the sum of weights increases from 0 to $+\infty$.

Deviation reliability is similar to the deviation in statistics and is used to measure the difference between rating values in records.

$$\rho_{DX}(m,n,c)=1-\frac{\sum_{h\in\Re_X(m,n,c)}\omega_X(h)\ \cdot|s-T_X(m,n,c)|}{\sum_{h\in\Re_X(m,n,c)}\omega_X(h)}.\qquad(4)$$

When $\rho_{DX}(m,n,c)$ is 1, it indicates that the deviation does not exist.

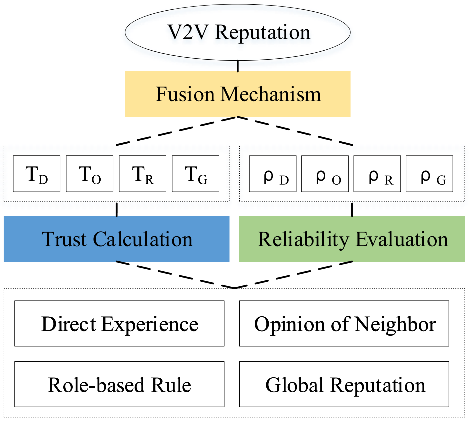


Fig. 4. The update process of V2V reputation.

C. Update Process of V2V Reputation

As shown in Fig.4, the evaluator utilizes the trust calculation module to calculate the direct trust (T_D), indirect trust (T_O), role-based trust (T_R), and global trust (T_G) of the target vehicle based on the records provided by the four reference sources and utilizes the reliability evaluation module to obtain the corresponding reliability values ρ_D, ρ_O, ρ_R, and ρ_G. Then, the evaluator utilizes the fusion mechanism to fuse the obtained trust values and reliability values respectively to update the target's V2V reputation and reliability value. Algorithm 1 illustrates this process. The specific update process of the update interval $Time$ is given in Section IV-E.

1) Direct Trust: The evaluator calculates the direct trust T_D and its reliability ρ_D based on direct interaction experience with the target vehicle. Specifically, the evaluator m records every interaction with the target n. The evaluator stores all interaction records locally in the form of $h = (D, m, n, c, t, s)$, where t denotes the recorded time when the interaction occurred; s is the satisfaction of the evaluator m with this interaction, and the possible values of s are $\{0, 0.5, 1\}$, where 0 indicates that m determines that n provides false information, 0.5 indicates that m does not use the information provided by n, and 1 indicates that m determines that n provides correct information. Therefore, if the malicious vehicles send false messages, they will be blacklisted by other vehicles.

New interaction records have higher reference values, so the weight function of direct trust is defined as

$$\omega_D(h) \ = e^{-\frac{\Delta t(h)}{\lambda}}, \tag{5}$$

where $\Delta t(h)$ is the difference between the current time and the recorded time of h; λ is the control factor, which can be adjusted depending on the time unit. For instance, if the time unit is in the order of seconds and we want a record obtained ten seconds earlier to only have half the effect of a new record obtained, we can set $\lambda = -10/\ln 0.5$.

When calculating direct trust, the evaluator picks all records h of $X = D$ to form a set $\Re_D(m, n, c)$ first; then, the evaluator calculates the weight function $\omega_D(h)$ based on recorded time t and Eq.(5); finally, the evaluator calculates $T_D(m, n, c)$ and $\rho_D(m, n, c)$ based on $\omega_D(h)$, rating value s, and Eq.(1)-(4).

2) Indirect Trust: The evaluator calculates the indirect trust T_O and its reliability ρ_O based on neighbors' opinions.

Algorithm 1 The Update Process of V2V Reputation

```
Input:
   $\Re_X(m, n, c)$, $X \in \{D, O, R, G\}$;
Output:
   $Rv(m, n, c)$;
while $Time = 0$ do
   if $\Re_D(m, n, c) \neq \varnothing$ then
      $\omega_D(h) \ \leftarrow e^{-\frac{\Delta t(h)}{\lambda}}$;
      Calculate $T_D(m, n, c)$, $\rho_D(m, n, c)$ by Eq.(1)-(4);
   end if
   if $\Re_O(m, n, c) \neq \varnothing$ then
      $\omega_O(h) \ \leftarrow \varepsilon \cdot Rv(m, p, rs)$;
      Calculate $T_O(m, n, c)$, $\rho_O(m, n, c)$ by Eq.(1)-(4);
   end if
   if $\Re_R(m, n, c) \neq \varnothing$ then
      $\omega_R(h) \ \leftarrow g$;
      Calculate $T_R(m, n, c)$, $\rho_R(m, n, c)$ by Eq.(1)-(4);
   end if
   if $\Re_G(m, n, c) \neq \varnothing$ then
      $T_G(m, n, c) \leftarrow Rg(n, c)$, $\rho_G(m, n, c) \leftarrow \rho(n, c)$;
   end if
   Calculate $Rv(m, n, c)$,$\rho_{Rv}(m, n, c)$ by Eq.(8)-(10);
   if $Rv(m, n, c) \geq \tau_D$ and $\rho_{Rv}(m, n, c) \geq \tau_R$ then
      Update the V2V reputation of the target $n$ to
      $Rv(m, n, c)$;
   end if
   Update the local blacklist;
   Update $Time$ and restart timing.
end while
```

Specifically, the evaluator m collects neighbors' opinions of the target vehicle n, which are shared between vehicles through beacons. We extend the beacon to the structure depicted in Fig.5. The extended content includes the target's ID, information type, and opinion value. The beacon packet is usually larger than 200 bytes, and the maximum payload of the MAC layer is generally above 1,400 bytes [31], so the additional overhead caused by adding 4 bytes is even negligible. In addition, adding extra information in beacons to achieve distributed protocol design is common in VANETs [14], [32], [33]. The evaluator stores all opinions locally in the form $h = (O, p, n, c, s)$, where p denotes the neighbor's identity; s denotes the opinion value, which is the V2V reputation of the target n updated by the neighbor p.

The evaluator calculates the similarity through the distance with the neighbors, and it defaults that the opinions provided by the neighbors with high similarity are valuable. The similarity ε is calculated as follows.

$$\varepsilon = \begin{cases} 1, & \Delta L \leq L \\ \dfrac{L}{\Delta L}, & \Delta L > L, \end{cases} \tag{6}$$

where ΔL denotes the distance between the evaluator and neighbor; L is the defined trusted distance, and the evaluator sets the similarity of neighbors within this range to 1.

The weight function of indirect trust is defined as

$$\omega_O(h) \ = \varepsilon \cdot Rv(m, p, rs), \tag{7}$$

Conventional payload	Target ID 2 Bytes	Type 1 Byte	Opinion 1 Byte

Fig. 5. New extended beacon format.

where $Rv(m, p, c_{rs})$ is the V2V reputation for road safety information of the neighbor p evaluated by the evaluator m.

When calculating indirect trust, the evaluator picks all records h of $X = O$ to form a set $\Re_O(m, n, c)$ first; then, the evaluator calculates the weight function $\omega_O(h)$ based on the distance to the neighbor and the neighbor's reputation; finally, the evaluator calculates $T_O(m, n, c)$ and $\rho_O(m, n, c)$ based on $\omega_O(h)$, opinion value s, and Eq.(1)-(4).

3) Role-Based Trust: The evaluator calculates the role-based trust T_R and its reliability ρ_R based on role-based rules, which are set by the evaluator or provided by a trusted center. Role-based rules are tuples of the following form: $h = (R, role_n, c, g, s)$, where $role_n$ denotes the role of n (e.g. bus, private car, and police car), c denotes the information type the rule applies, g is the belief strength of the evaluator on this rule ($g \in [0, 1]$), and s is the reference value stipulated by this rule ($w \in [0, 1]$).

When calculating role-based trust, the evaluator picks all records h of $X = R$ to form a set $\Re_R(m, n, c)$ first; then, the evaluator assigns the values of g to the weight function $\omega_R(h)$; finally, the evaluator calculates $T_R(m, n, c)$ and $\rho_R(m, n, c)$ based on $\omega_R(h)$, s, and Eq.(1)-(4).

4) Global Trust: The evaluator calculates the global trust T_G and its reliability ρ_G based on the target's global reputation and its reliability issued periodically by the RSU. Specifically, the evaluator stores the global reputation of neighbors periodically published by the RSU in the form of $h = (G, Rg(n, c), \rho(n, c))$, where $Rg(n, c)$ is the global reputation of the target on c-type information, and $\rho(n, c)$ is the reliability of $Rg(n, c)$.

When calculating global trust, the evaluator picks all records h of $X = G$ to form a set $\Re_G(m, n, c)$ first; then, the evaluator assigns the results of $Rg(n, c)$ and $\rho(n, c)$ to $T_G(m, n, c)$ and $\rho_G(m, n, c)$, respectively. The specific calculation process of global reputation is given in Section IV-D.

5) Fusion Mechanism: The evaluator fuses $T_D(m, n, c)$, $T_O(m, n, c)$, $T_R(m, n, c)$, and $T_G(m, n, c)$ to obtain the V2V reputation of the target vehicle.

$$Rv(m, n, c) = \frac{\sum_{X \in (D,O,R,G)} \alpha_X \cdot T_X(m, n, c)}{\sum_{X \in (D,O,R,G)} \alpha_X}, \tag{8}$$

where α_X denotes the weight:

$$\alpha_X = \eta_X \cdot \rho_X(m, n, c), \tag{9}$$

where η_X denotes the importance of reference source X ($\sum_{X \in (D,O,R,G)} \eta_X = 1$). η_D is maximized when the evaluator has sufficient direct interactions with the target vehicle; η_O increases when there are sufficient neighbors' opinions; η_R increases when the first two conditions are not satisfied and the evaluator is in the blind zone; η_G increases when the evaluator receives the global reputation from the RSU.

Then, the evaluator evaluates the reliability $\rho_{Rv}(m, n, c)$ of $Rv(m, n, c)$ based on $\rho_D(m, n, c)$, $\rho_O(m, n, c)$, $\rho_R(m, n, c)$, and $\rho_G(m, n, c)$.

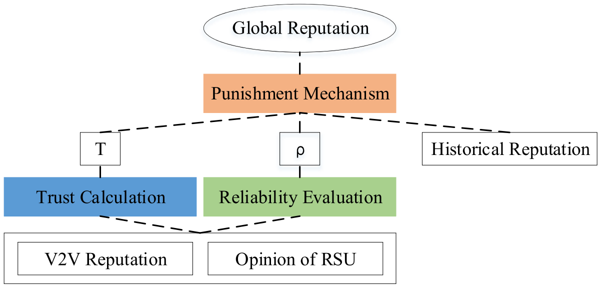


Fig. 6. The update process of global reputation.

$$\rho_{Rv}(m, n, c) = \frac{\sum_{X \in (D,O,R,G)} \alpha_X}{\sum_{X \in (D,O,R,G)} \eta_X}. \tag{10}$$

If $\rho_{Rv}(m, n, c) < \tau_R$, where τ_R is the reliability threshold, $Rv(m, n, c)$ is unreliable, and the evaluator will interrupt this update; otherwise, $Rv(m, n, c)$ is reliable, and the evaluator continues to perform subsequent judgment.

If $Rv(m, n, c) < \tau_D$, where τ_D is the detection threshold, the evaluator determines that the target is a malicious vehicle and adds it to the local blacklist; otherwise, the evaluator updates the V2V reputation of the target to $Rv(m, n, c)$.

Algorithm 2 The Update Process of Global Reputation

```
Input:
  $OldRg(n, c)$, $Rv(m, n, c)$, $Rg(m, rs)$;
Output:
  $Rg(n, c)$;
while $Time = 0$ do
  Calculate $T(n, c)$ by Eq.(11);
  $\omega_G(h) \leftarrow Rg(m, rs)$, $s \leftarrow Rv(m, n, c)$;
  Calculate $\rho(n, c)$ by Eq.(2)-(4);
  if $\rho(n, c) < \tau_R$ then
    Break;
  end if
  $\varphi = \sum_{c \in (rs,tm,in)} (T(n, c) - OldRg(n, c))$;
  if $\varphi > 0$ then
    $Rg(n, c) = T(n, c)$;
  else if $\varphi = 0$ then
    $Rg(n, c) = T(n, c) - (\frac{\tau_D}{aT(n,c)^b})^{\chi}$;
  else
    $Rg(n, c) = T(n, c) - \varphi^2$;
  end if
  if $Rg(n, c) < \tau_D$ then
    Add the vehicle $n$ to the global blacklist;
  else
    Update the global reputation of the vehicle $n$ to $Rg(n, c)$.
  end if
  Start the next round of timing.
end while
```

D. Update Process of Global Reputation

As shown in Fig.6, the RSU updates the global reputation of vehicles that first enter its transmission range based on the latest opinion provided by neighbor RSUs. When a vehicle's global reputation is updated subsequently, the RSU calculates the overall trust and evaluates its reliability by referring to the V2V reputation provided by evaluators. If it passes the reliability test, the RSU implements the punishment mechanism, which calculates the global reputation based on the overall trust and the historical reputation of the vehicle in the previous round. Algorithm 2 illustrates this process.

Specifically, the RSU calculates the overall trust $T(n, c)$ of the vehicle n first.

$$T(n,c) = \frac{\sum_{\forall m \in Range(RSU)} Rg(m,rs) \cdot Rv(m,n,c)}{\sum_{\forall m \in RSU} Rg(m,rs)}, \quad (11)$$

where $Range(RSU)$ is the set of all vehicles within the transmission range of the RSU; $Rg(m, rs)$ is the global reputation for road safety information of the evaluator m; $Rv(m, n, c)$ denotes the V2V reputation for c-type information of the vehicle n evaluated by the evaluator m.

Secondly, the RSU assigns $Rg(m, rs)$ to the weight function $\omega_G(h)$ and $Rv(m, n, c)$ to the rating value s, and utilizes Eq.(2)-(4) to calculate the reliability $\rho(n, c)$. If $\rho(n, c) < \tau_R$, the RSU interrupts this update; otherwise, it continues with the subsequent steps.

Then, the RSU calculates the difference φ between the overall trust $T(n, c)$ and the historical reputation of the vehicle in the previous round $OldRg(n, c)$.

$$\varphi = \sum_{c \in (rs,tm,in)} (T(n,c) - OldRg(n,c)). \quad (12)$$

Finally, the RSU implements the punishment mechanism.

$$Rg(n,c) = \begin{cases} T(n,c), & \varphi > 0 \\ T(n,c) - (\dfrac{\tau_D}{aT(n,c)^b})^{\chi}, & \varphi = 0 \\ T(n,c) - \varphi^2, & \varphi < 0, \end{cases} \quad (13)$$

where a, b, and χ are punishment parameters for selfish behavior. If $\varphi > 0$, RSU determines the behavior of the vehicle n is normal; if $\varphi = 0$, RSU determines the behavior of the vehicle n is selfish; if $\varphi < 0$, RSU determines the behavior of the vehicle n is malicious. RSU does not punish normal behavior and adopts varying degrees of punishment for selfish and malicious behavior.

If $Rg(n, c) \geq \tau_D$, the RSU updates $Rg(n, c)$ as the new global reputation of the vehicle n; otherwise, the RSU determines that the vehicle n is malicious and adds it to the global blacklist.

E. Dynamic Adjustment Mechanism of Update Interval

1) Calculation Method of Update Interval: The evaluator calculates the update interval based on the security of its communication environment.

$$Time' = \frac{\mu \cdot Es}{M + 1}, \quad (14)$$

where μ is the initial update interval; Es is the security of the communication environment calculated by the evaluator; M is the total number of malicious interactions in this round.

In Section IV-B, we introduce that reliability can measure the number of neighbors, their reputations, and the deviation of their opinions. These factors reflect the security of the evaluator's communication environment. Therefore, we utilize the calculation results of the reliability evaluation module to quantify the security value, which is defined as

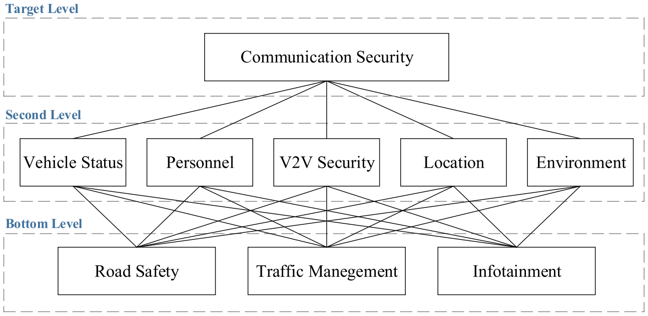


Fig. 7. **Hierarchical model.** The target level is the overall goal, the second level includes five security impact factors, and the bottom level is the three information types that interact between vehicles.

$$Es = \sum_{c \in (rs,tm,in)} \beta_c \cdot S_c, \quad (15)$$

where β_c is the fixed weight coefficient of S_c, which denotes the influence of c-type information on the security, and $\sum_{c \in (rs,tm,in)} \beta_c = 1$; S_c is defined as

$$S_{c \in (rs,tm,in)} = \sum_{\forall n \in Neigh(m)} \rho_{Rv}(m,n,c), \quad (16)$$

where $Neigh(m)$ is the set of all neighbors within the transmission range of the evaluator m.

We set the range of the update interval to $[min_t, max_t]$, so the result of $Time$ is as follows.

$$Time = \begin{cases} max_t, & \text{if } Time' > max_t \\ min_t, & \text{if } Time' < min_t \\ Time', & \text{otherwise.} \end{cases} \quad (17)$$

Each time the evaluator performs an update, the results obtained by the reliability evaluation module are different. Therefore, the update interval changes dynamically over time. Since the evaluator does not disclose the calculation results of the reliability evaluation module, malicious vehicles could not launch intelligent attacks by adapting to the update interval.

2) Calculation Method of Weights: The fixed weight coefficients $\beta_{c \in (rs,tm,in)}$ are calculated by the evaluator or a trusted center. We utilize Analytic Hierarchy Process (AHP) to quantify the impact of information type on security. AHP is a simple, flexible, and practical multi-criteria decision-making method for quantitative analysis of qualitative problems, including five steps [34].

Step 1. We establish the hierarchical structure model shown in Fig.7 according to the security impact factors and information types. Factors affecting communication security include vehicle status, personnel status, V2V security status, geographic location, and environmental status [35]. Information types include road safety information, traffic efficiency and management information, and infotainment information [30].

Step 2. Combined with Table II, we construct judgment matrices by analyzing the mutual importance of information types and impact factors. The numbers 1-9 and their reciprocals are used as scales to define the judgment matrix $A = (a_{ij})_{n \times n}$.

TABLE II
THE FUNDAMENTAL SCALE

Importance scale	Definition
1	Equal importance
3	Moderate importance of one over another
5	Essential or strong importance
7	Very strong importance
9	Extreme importance
2,4,6,8	Intermediate values between the two adjacent judgments
Reciprocal	If the ratio of the importance of factor i to factor j is a_{ij}, then the ratio of the importance of factor j to factor i is $\frac{1}{a_{ij}}$.

Step 3. We utilize the eigenvector method to calculate the weight coefficient of each matrix.

$$AW = \lambda_{max} W, \tag{18}$$

where λ_{max} is the maximum eigenvalue of the judgment matrix, which exists and is unique.

Step 4. For the constructed judgment matrix, we need to conduct a consistency test. Firstly, we calculate the consistency index CI.

$$CI = \frac{\lambda_{max} - n}{n-1}. \tag{19}$$

Then we find the random consistency index according to Table III. Finally, we calculate the consistency ratio CR.

$$CR = \frac{CI}{RI}. \tag{20}$$

If $CR < 0.1$, it is judged that the matrix passes the consistency test.

Step 5. We calculate the composite weights of the target level and assign them to the fixed weight coefficients β_{rs}, β_{tm}, and β_{in}, respectively.

V. Performance Evaluation

In this section, we compare HDRS with other reputation schemes and perform simulation experiments.

A. Comparison

As illustrated in Table IV, we compare HDRS with the existing reputation schemes in various environments. In addition, we analyze the attacks that these schemes can resist.

1) Adaptability to Various Environments: Generally, reputation schemes are affected by traffic conditions and blind zones of infrastructure [3]. We compare and analyze the adaptability of these schemes in three different scenarios.

a) Sparse traffic: At particular times of the day (e.g., between midnight or 6 am in the morning), the traffic density may be so low that the evaluator can not accurately evaluate the reputation of the target vehicle due to the loss of opinions from neighbors. The global reputation in [14] and [9] mitigates the insufficient opinions of neighbors. However, the accuracy of the global reputation is still affected by the traffic density. In contrast, in addition to providing a global reputation, [18], [24], and HDRS can solve insufficient reference records by using role-based rules. They have strong adaptability to sparse traffic scenarios.

TABLE III
RANDOM CONSISTENCY INDICATOR RI

n	1	2	3	4	5	6	7	8
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41

b) Dense traffic: In urban areas or highways, there are scenarios with high traffic density. In these cases, the reputation system has many reference records when updating the target's reputation, and it needs to determine the influence of each record from multiple dimensions to improve the accuracy of evaluation. [9] and [24] assume that the reliability of neighbors' opinions decreases with distance. [18] and [9] utilize time decay to distinguish the availability of records. [24] distinguishes records by the information type. HDRS combines the above three ways to enhance the adaptability to dense traffic scenarios.

c) Blind zones: Due to deployment cost and geographic location issues, the infrastructure cannot achieve full coverage in VANETs. [18] and [14] are dependent on the center or UAVs, so their adaptability to the blind zones of infrastructure is relatively weak. The distributed schemes [23], [25], and [9] do not rely on any infrastructure. [24] and HDRS can update the V2V reputation normally in blind zones, so they have strong adaptability.

2) Resist Attacks: HDRS is resistant to the five attacks described in the attack model in Section III-C. In HDRS, the evaluator records and evaluates all interactions with the target, so vehicles that send false messages will be punished. HDRS sets the reputation of the target vehicle based on the information type, which can prevent malicious vehicles from launching value imbalance attacks. By referring to [25], HDRS stipulates that when RSU updates the global reputation, in addition to punishing the malicious behavior, it also appropriately punishes the selfish behavior of the target. The reliability evaluation module in HDRS can mitigate collusion attacks by filtering out unreasonable results obtained by the trust calculation module. In addition, the evaluator adjusts the update interval dynamically to resist intelligent attacks.

B. Simulation

1) Simulation Setting: To evaluate HDRS, we utilize Python in conjunction with SUMO for simulation experiments. Similar to the experiments in references [9] and [14], we utilize SUMO to simulate realistic vehicle movement. The map used in the simulation is Hangzhou Cangqian Street, imported by OpenStreetMap (see Fig.8). Table V summarizes the main simulation parameters. As with reference [6], we set the initial reputation of all vehicles at 0.5 and the detection threshold at 0.4. In order to avoid fluctuation, we get the average results from 100 times experiments. In addition, we calculate the standard deviation to reflect the dispersion of the results.

TABLE IV
COMPARISON OF HDRS WITH OTHER REPUTATION SYSTEMS

Scheme	Reference source				Adaptability in various environments			Resist attacks
	DE	ON	RB	GR	Sparse traffic	Dense traffic	Blind zones	
[23]	✓	✓			Weak	Ordinary	Strong	False message
[25]	✓	✓			Weak	Weak	Strong	Selfish behavior
[14]	✓	✓		✓	Ordinary	Weak	Ordinary	False message, intelligent attacks
[18]	✓		✓	✓	Strong	Ordinary	Weak	False message
[9]	✓	✓		✓	Ordinary	Ordinary	Strong	False message, selfish behavior
[24]	✓	✓	✓	✓	Strong	Ordinary	Strong	False message, value imbalance attacks, collusion attacks
HDRS	✓	✓	✓	✓	Strong	Strong	Strong	False message, value imbalance attacks, selfish behavior, collusion attacks, intelligent attacks

* DE—direct experience; ON—opinion of neighbor; RB—role-based rule; GR—global reputation.

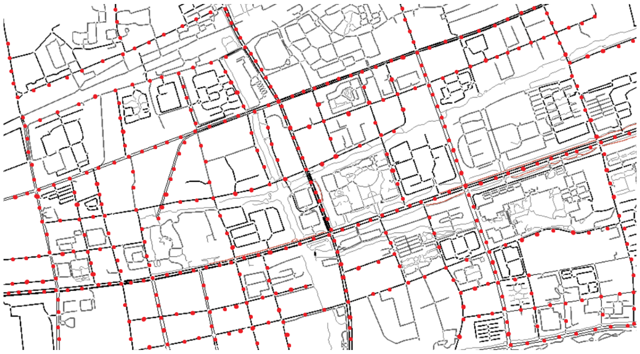


Fig. 8. **Map.** The map used in the simulation is Hangzhou Cangqian Street imported by OpenStreetMap.

2) Performence Metrics: We define two metrics to reflect the performance of the schemes.

- *Detection rate* $= N_m/N_g$, where N_m denotes the number of malicious vehicles detected; N_g denotes the number of malicious vehicles generated in the simulation.
- *False-positive rate* $= N_n/(N_n + N_m)$, where N_n is the number of vehicles erroneously determined to be malicious.

3) Detection Performance Under Different Conditions: We compare the detection rates of HDRS and the following two schemes for malicious vehicles under different conditions: the centralized reputation scheme of Li *et al.* [18] and the distributed reputation scheme of Xu *et al.* [23].

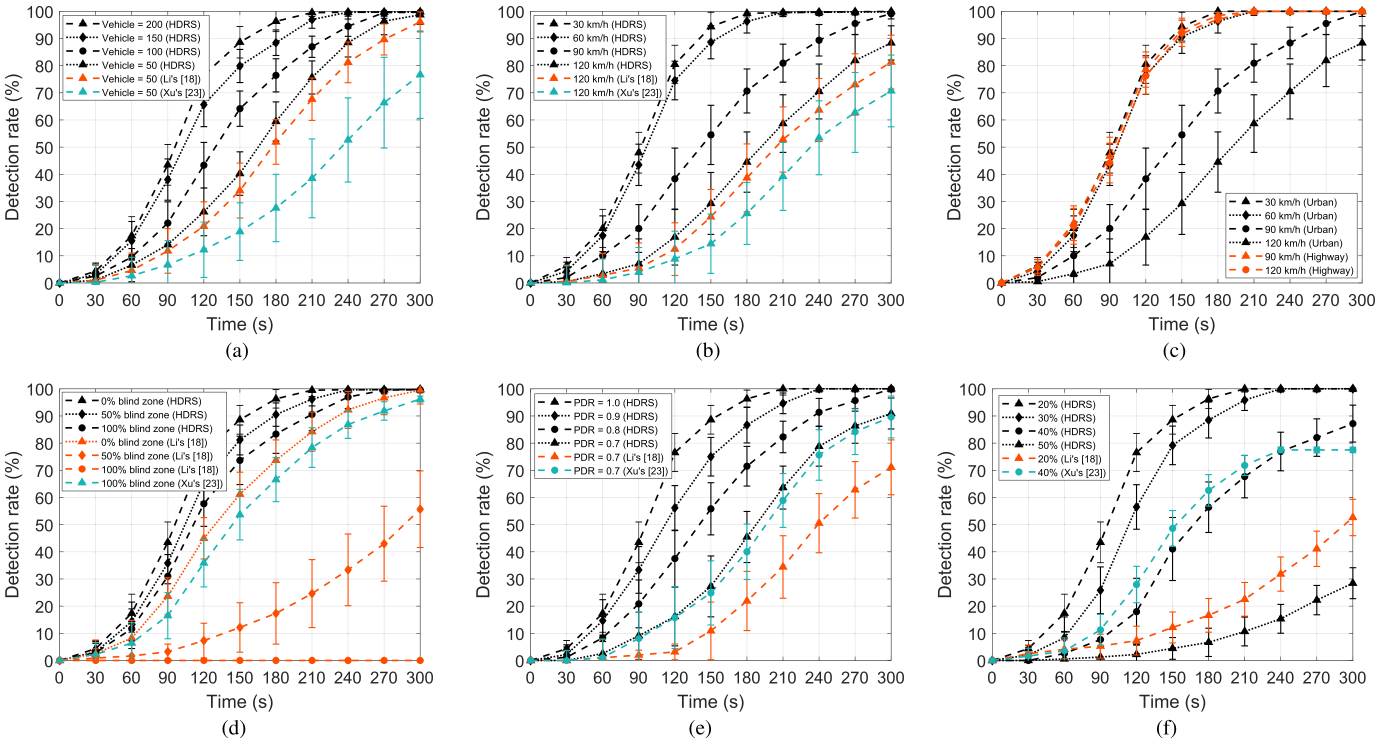
Fig.9(a) illustrates that the effect of the vehicle number on the detection rate of HDRS. We find that the decrease in the vehicle number slows down the detection speed of HDRS. However, due to the multiple reference sources of reputation evaluation, HDRS still detects all malicious vehicles within 300s. Compared with other schemes, HDRS significantly improves the detection rate when there are fewer vehicles.

Fig.9(b) illustrates that the detection rate of HDRS is negatively correlated with vehicle speed in urban areas. This effect is more pronounced when the vehicle speed reaches above 90 km/h. The reason is that the average connection time between vehicles decreases as the vehicle speed increases in urban areas. Short connection time means fewer interactions which increase the convergence time of detection. Fig.9(c) illustrates that vehicle speed on the highway does not significantly affect the detection rate of HDRS, because the vehicles on the highway travel in a single direction and their interactions are more stable than in the urban areas, which allows sufficient direct interaction for the evaluator.

TABLE V
THE MAIN SIMULATION PARAMETERS

Parameters	Value
Simulation area (km × km)	2.5 × 2.5
V2R transmission range (m)	500
V2V transmission range (m)	300
Simulation time (s)	300
Vehicle speed (km/h)	[30,120]
Number of vehicles	[50,200]
RSU update interval (s)	50
Vehicle update interval (s)	[5,100]
Initial reputation	0.5
Detection threshold	0.4
Reliability threshold	0.8

Fig.9(d) illustrates that the detection rate of HDRS is negatively correlated with the proportion of blind zones. The reason is that the vehicles in the blind zones cannot receive the updated global reputation from RSU. When the proportion of blind zones reaches 100%, HDRS changes from a hybrid scheme to a distributed scheme. However, due to the consideration of role-based rules, the detection rate of HDRS is still better than the distributed scheme [23] that only considers direct trust and indirect trust. Compared with the centralized scheme [18], HDRS reflects the adaptability to blind zones.



(a) (b) (c)

(d) (e) (f)

Fig. 9. **Detection performance under different conditions.** (a) Vehicle number; (b) vehicle speed; (c) urban areas and highways; (d) the proportion of blind zones of RSU; (e) packet delivery ratio; (f) the proportion of malicious vehicles.

Fig.9(e) illustrates that the effect of the packet loss on the detection rate of HDRS. We simulate packet loss by controlling the packet delivery ratio (PDR). Lyu *et al.* [31] pointed out that the value of PDR in urban areas is mainly between 0.7 and 1.0, so we set the range of PDR to [0.7, 1.0]. The results show that packet loss slows down the detection rate of malicious vehicles. However, as long as the simulation time is enough, HDRS can still detect all malicious vehicles.

Fig.9(f) illustrates that the detection rate of HDRS is negatively correlated with the proportion of malicious vehicles. When the proportion reaches 40%, the detection rate of HDRS decreases significantly, but it still detects 100% malicious vehicles when the simulation time is enough (about 600s). In contrast, the other two schemes cannot detect all malicious vehicles. When the proportion reaches 50%, HDRS cannot detect all malicious vehicles.

4) Punishment of Selfish Behavior: The number of rounds of reputation update required to reduce the reputation of a selfish vehicle below the detection threshold is called the elimination point. As illustrated in Fig.10(a), the punishment parameters in Eq.(13) affect the result of the elimination point. If the elimination point is too small, the false-positive rate increases. If the elimination point is too large, it is not conducive to motivate selfish vehicles to communicate with others. As illustrated in Fig.10(b), the punishment value increases exponentially with the number of rounds, which means that vehicles that behave selfishly for a long time will be punished more.

5) Detection Performance of Collusion Attacks: Fig.11 illustrates that the reliability evaluation is an effective way to resist collusion attacks, in which τ_R is the reliability detection threshold. We set τ_R to 0.5, 0.3, and 0, respectively. When $\tau_R = 0$, reliability evaluation is not performed during the reputation update process. The abscissa is the proportion of malicious vehicles launching collusion attacks. The results show that the detection rate of HDRS decreases with the increase of the proportion of collusion attacks. However, reliability evaluation improves the detection rate, and this effect is positively correlated with the proportion of malicious attacks. When collusion in attacks is 90% and $\tau = 0.5$, it improves the detection rate by about 30%.

6) Detection Performance of Intelligent Attacks: In this part, we utilize AHP to determine the weight of the parameters in Eq.(15). The specific calculation process can refer to Section IV-E.

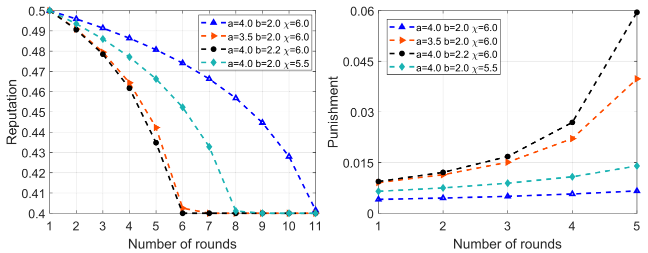
The constructed evaluation factor matrix A, vehicle state matrix B_1, personnel state matrix B_2, V2V security matrix B_3, location matrix B_4, and environment matrix B_5 are

$$A = \begin{bmatrix} 1 & 7 & 2 & 4 & 5 \\ 1/7 & 1 & 1/5 & 1/4 & 1/3 \\ 1/2 & 5 & 1 & 3 & 4 \\ 1/4 & 4 & 1/3 & 1 & 2 \\ 1/5 & 3 & 1/4 & 1/2 & 1 \end{bmatrix} \quad B_1 = \begin{bmatrix} 1 & 4 & 7 \\ 1/4 & 1 & 3 \\ 1/7 & 1/5 & 1 \end{bmatrix}$$

$$B_2 = \begin{bmatrix} 1 & 1 & 1/5 \\ 1 & 1 & 1/5 \\ 5 & 5 & 1 \end{bmatrix} \quad B_3 = \begin{bmatrix} 1 & 3 & 7 \\ 1/3 & 1 & 5 \\ 1/7 & 1/5 & 1 \end{bmatrix}$$

$$B_4 = \begin{bmatrix} 1 & 1/5 & 3 \\ 5 & 1 & 8 \\ 1/3 & 1/8 & 1 \end{bmatrix} \quad B_5 = \begin{bmatrix} 1 & 1 & 5 \\ 1 & 1 & 5 \\ 1/5 & 1/5 & 1 \end{bmatrix}$$

We utilize the constructed matrices to calculate the combined weights and perform a consistency test. Finally,



(a) (b)

Fig. 10. **Punishment of selfish behavior.** (a) Changes in the reputation of selfish vehicles; (b) the punishment for selfish behavior gradually increases.

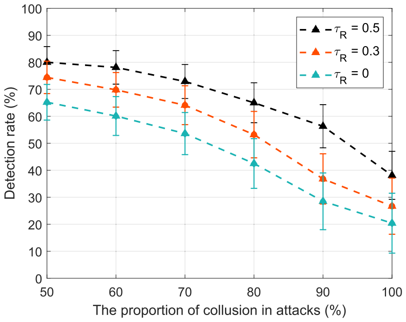
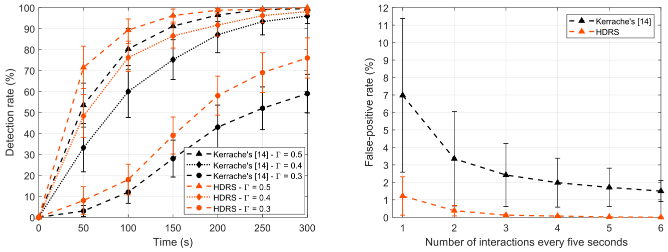


Fig. 11. Detection performance of collusion attacks.



(a) (b)

Fig. 12. **Detection performance of intelligent attacks.** (a) Detection rate; (b) false-positive rate.

we determine Eq.(14) as follows.

$$Time' = \frac{\mu \cdot (0.4269S_{rs} + 0.3658S_{tm} + 0.2073S_{in})}{M+1}$$

The object of comparison in simulation is the detection threshold adaptive control strategy [14]. As depicted in Fig.12(a), the detection rate of all schemes is positively correlated with Γ, in which Γ indicates the proportion of intelligent attacks. However, when Γ is not less than 0.4, both schemes detect all malicious vehicles within 300s; when $\Gamma = 0.3$, the detection rate of both schemes is dropped significantly. Nevertheless, the dynamic adjustment mechanism of the update interval proposed in HDRS can improve the detection rate by more than 16%. The reason is that when malicious behavior occurs, our mechanism provides more frequent reputation updates. Since the evaluator does not disclose the calculation results of the reliability evaluation module, malicious vehicles could not launch intelligent attacks by adapting to the update interval. As depicted in Fig.12(b), HDRS significantly reduces the false-positive rate compared to [14].

VI. Conclusion

This paper proposes a hybrid reputation system called HDRS, which can mitigate collusion attacks through reliability evaluation and dynamically adjust the reputation update interval to detect intelligent attacks. The simulation results show that HDRS can maintain a high detection rate and low false-positive rate for malicious vehicles under various environments in VANETs. In future work, we plan to combine reinforcement learning with HDRS to improve the detection performance for malicious vehicles.

References

[1] Z. Elrewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Veh. Commun.*, vol. 23, pp. 1–28, Jun. 2020.

[2] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2553–2571, May 2021.

[3] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, and V. Sadekar, "Broadcasting in VANET," in *Proc. Mobile Netw. Veh. Environ.*, May 2007, pp. 7–12.

[4] S. Tangade, S. S. Manvi, and P. Lorenz, "Trust management scheme based on hybrid cryptography for secure communications in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5232–5243, May 2020.

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

[6] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 28643–28660, 2018.

[7] N. J. Patel and R. H. Jhaveri, "Trust based approaches for secure routing in VANET: A survey," *Proc. Comput. Sci.*, vol. 45, pp. 592–601, Jan. 2015.

[8] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1559–1574, Jun. 2017.

[9] H. E. Sayed, S. Zeadally, and D. Puthal, "Design and evaluation of a novel hierarchical trust assessment approach for vehicular networks," *Veh. Commun.*, vol. 24, pp. 1–11, Aug. 2020.

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

[11] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "An integrated trust and reputation model for open multi-agent systems," *Auton. Agents Multi-Agent Syst.*, vol. 13, no. 2, pp. 119–154, 2006.

[12] C. A. Kerrache, A. Lakas, and N. Lagraa, "Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control," in *Proc. 5th Int. Conf. Electron. Devices, Syst. Appl. (ICEDSA)*, Dec. 2016, pp. 1–4.

[13] C. A. Kerrache, C. T. Calafate, N. Lagraa, J.-C. Cano, and P. Manzoni, "RITA: Risk-aware trust-based architecture for collaborative multi-hop vehicular communications" *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4428–4442, Nov. 2016.

[14] C. A. Kerrache, A. Lakas, N. Lagraa, and E. Barka, "UAV-assisted technique for the detection of malicious and selfish nodes in VANETs," *Veh. Commun.*, vol. 11, pp. 1–11, Jan. 2018.

[15] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.

[16] C. A. Kerrache *et al.*, "TACASHI: Trust-aware communication architecture for social internet of vehicles," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5870–5877, Aug. 2019.

[17] M. A. Azad, S. Bag, S. Parkinson, and F. Hao, "TrustVote: Privacy-preserving node ranking in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5878–5891, Aug. 2019.

[18] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.

[19] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6417–6428, Aug. 2019.

[20] M. Kadadha and H. Otrok, "A blockchain-enabled relay selection for QoS-OLSR in urban VANET: A Stackelberg game model," *Ad Hoc Netw.*, vol. 117, Jun. 2021, Art. no. 102502.

[21] A. Khalid, M. S. Iftikhar, A. Almogren, R. Khalid, M. K. Afzal, andN. Javaid, "A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs," *Inf. Process. Manage.*, vol. 58, no. 2, pp. 1–17, Mar. 2021.

[22] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Inf. Sci.*, vol. 545, pp. 170–187, Feb. 2021.

[23] H. Xu *et al.*, "Trust-based probabilistic broadcast scheme for mobile ad hoc networks," *IEEE Access*, vol. 8, pp. 21380–21392, 2020.

[24] 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," *Comput. Commun.*, vol. 93, pp. 68–83, Nov. 2016.

[25] J. A. F. F. Dias, J. J. P. C. Rodrigues, C. X. Mavromoustakis, and F. Xia, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7929–7937, Dec. 2015.

[26] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Netw.*, vol. 90, pp. 1–13, Jul. 2019.

[27] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks," *Comput. Secur.*, vol. 78, pp. 245–254, Sep. 2018.

[28] N. Magaia and Z. Sheng, "ReFIoV: A novel reputation framework for information-centric vehicular applications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1810–1823, Feb. 2019.

[29] L. Xiao, X. Lu, D. Xu, Y. Tang, L. Wang, and W. Zhuang, "UAV relay in VANETs against smart jamming with reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4087–4097, May 2018.

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

[31] F. Lyu *et al.*, "Characterizing urban vehicle-to-vehicle communications for reliable safety applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2586–2602, Jun. 2020.

[32] F. Lyu *et al.*, "MoMAC: Mobility-aware and collision-avoidance MAC for safety applications in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10590–10602, Nov. 2018.

[33] F. Lyu *et al.*, "SS-MAC: A novel time slot-sharing MAC for safety messages broadcasting in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3586–3597, Apr. 2018.

[34] W. Ho and X. Ma, "The state-of-the-art integrations and applications of the analytic hierarchy process," *Eur. J. Oper. Res.*, vol. 267, no. 2, pp. 399–414, 2018.

[35] W. B. Jaballah, M. Conti, and C. Lal, "Security and design requirements for software-defined VANETs," *Comput. Netw.*, vol. 169, pp. 1–23, Mar. 2020.

Xuejiao Liu received the Ph.D. degree in computer science from Huazhong Normal University, Wuhan, China. She is currently an Associate Professor with the School of Information Science and Technology, Hangzhou Normal University, Hangzhou, China. Her research interests include network security and cloud security.

Oubo Ma received the B.E. degree from Wenzhou University, Wenzhou, China, in 2019. He is currently pursuing the M.S. degree with the School of Information Science and Technology, Hangzhou Normal University, Hangzhou, China. His research interests include network security and vehicular ad hoc networks.

Wei Chen received the M.S. degree in software engineer from Hangzhou Normal University, Hangzhou, China, in 2021. Her research interest includes network security.

Yingjie Xia (Member, IEEE) received the Ph.D. degree from the College of Computer Science, Zhejiang University, in 2009. He was a Research Scientist at the National Center for Supercomputing Applications (NCSA), University of Illinois at Urbana–Champaign (UIUC), Champaign, IL, USA. He is currently an Associate Professor with Zhejiang University and the CEO of Hangzhou Yuantiao Technology Company. His research interests include intelligent transportation and information security.

Yuxuan Zhou received the B.E. degree from Hangzhou Normal University, Hangzhou, China, in 2021. His research interests include machine learning and network security.