Appeal-Based Distributed Trust Management Model in VANETs Concerning Untrustworthy RSUs

Yu Wang[1], Yu'ang Zhang[1], Yujie Song[1], Yue Cao[1*], Lei Zhang[2], and Xuefeng Ren[3]

[1]School of Cyber Science and Engineering, Wuhan University, China. yue.cao@whu.edu.cn (corresponding email)
[2]School of Engineering, University of Glasgow, Glasgow, Scotland, UK. Lei.Zhang@glasgow.ac.uk
[3]Huali iSmartWays Technology Inc, China. jackren@huali-tec.com

***Abstract*—Vehicular Ad-hoc Networks (VANETs) play an essential role in traffic safety and travel efficiency. However, due to the variable network topology of VANETs, malicious vehicles can easily invade the network to disrupt the network integrity. Moreover, compromised Roadside Units (RSUs) may pose a tremendous threat to network. Thus, we propose a distributed trust model to resist malicious vehicles and compromised RSUs by a mutual supervision mechanism between vehicles and RSUs. Three stages of this model ensure the trustworthiness of participants, including trust evaluation, adjudication, and vehicle appeal mechanism. In the trust evaluation stage, message receivers calculate three types of trust values (i.e., direct, indirect, and combined trust values) and upload them to RSUs. Then, RSUs dynamically update the trust threshold by aggregating vehicular trust values. In the adjudication stage, RSUs punish/reward vehicles by comparing the trust threshold to aggregated trust values. In the vehicle appeal stage, vehicles appeal to other RSUs if they have received the undesired punishment by an RSU. Then, multiple RSUs jointly judge whether a vehicle is successfully appealed, and the misjudging RSU will be punished Extensive simulations show that the proposed model effectively identifies malicious vehicles with the presence of compromised RSUs.**

***Index Terms*—Vehicular ad-hoc networks, Internet of vehicles, Trust management, Dynamic trust threshold, Appeal mechanism**

I. Introduction

With the development of communication technologies, Vehicular Ad-hoc Networks (VANETs) have been widely employed in Intelligent Transportation Systems (ITS). VANETs integrate intelligent traffic management with information services via the real-time interconnection perception, which can provide safe, efficient, environmentally friendly, and comfortable travel for the transportation industry.

However, due to the inherent characteristic of VANETs, there is uncertainty in the message transmission process. For example, attackers may tamper with messages to mislead driving decisions. Attackers can also generate a large number of redundant messages, resulting in network congestion that delays exchange of critical traffic information.

Encryption and authentication algorithms are usually utilized to ensure the confidentiality, integrity, and unforgeability of data [1], whereas the internal trust problem cannot be solved. For example, an authenticated attacker with a valid certificate can pass the authentication and generate false messages. When attackers send false messages to other vehicles, it will cause traffic jams and even accidents. To ensure robustness to malicious attacks and maintain a trustworthy relationship between vehicles, a reliable trust management model is the cornerstone to address the above problems [2].

According to the target of trust evaluation, trust management models are usually classified into entity-centric, data-centric, and hybrid trust models. Specifically, the entity-centric trust model aims to evaluate the trust value of entities (such as vehicles) [3]. Furthermore, the data-centric trust model aims to evaluate the trust of received messages [4]. The model determines whether the received data is trustworthy based on the similarity of received data. Finally, the hybrid trust model combines the above two models to evaluate the trust of both vehicles and messages [5], [6].

Nevertheless, trust management models in recent works still need improvement in terms of accuracy and real-time reliability. On the one hand, the dynamics of trust threshold are ignored, leading to a decrease in the precision of malicious detection. On the other hand, the trustworthiness of RSUs is ignored which may cause tremendous damage to VANETs, e.g., revoking the certificate of good vehicles. To solve above problems, we propose an appeal-based distributed trust management model in VANETs concerning untrustworthy RSUs. The main contributions can be summarized as follows:

- Recent works set a constant trust threshold that cannot be adapted to dynamic network status. To improve the real-time nature of trust model, we propose an adaptive trust threshold update mechanism, which dynamically updates the trust threshold with vehicular trust values.
- In addition, vehicles may suffer from unreasonable punishment of compromised RSUs, resulting in a reduction in the proportion of benign vehicles, thereby wasting network communication resources. We present a vehicle appeal mechanism to protect the legitimate interests of benign vehicles. Such mechanism provides vehicles with a channel to appeal to other RSUs while being wrongly punished by a compromised RSU.

II. Related Work

A. Entity-Centric Model

The entity-centric trust model evaluates vehicular trustworthiness through their behavior. Xiao et al. [7] established an implicit web of trust. Then the direct trust was calculated with an algorithm named BayesTrust, and the global trust was calculated by the VehicleRank algorithm. Xia et al. [8] proposed a lightweight trust-aware routing protocol, integrating the Markov prediction algorithm with direct trust calculation. Furthermore, a feedback mechanism was proposed to evaluate the recommendation trust. Wang et al. [9] proposed a context-aware trust model that vehicles were classified as service providers and requesters. Then, the trust of vehicles was evaluated by a linear logistic regression model based on context variables. After that, a recommendation filtering mechanism was introduced to identify malicious vehicles. In above works, the main difficulty is to evaluate the trust value of vehicles in the data sparsity issue (i.e., the problem of inaccurate evaluation caused by less trust evidence).

B. Data-Centric Model

The data-centric trust model collects messages from various entities (neighbors and RSUs), and filters out untrustworthy messages. Huang et al. [10] proposed a distance-based voting mechanism. The voting weight is proportional to the distance between a vehicle and the event location. Rawat et al. [11] designed a data-centric model which integrated Received Signal Strength (RSS) and Vehicle Geographic Location (GPS). Dai et al. [4] proposed a provenance-based model to evaluate the data trust. A clustering algorithm was utilized to group data items that described the same event. This work analyzed four attributes that affect data trust: data similarity, path similarity, data conflict, and data deduction. However, recent data-centric models do not establish a trust relationship between vehicles, so malicious vehicles cannot be accurately identified. In addition, if there are few interactions between vehicles, the trustworthiness of messages cannot be accurately evaluated.

C. Hybrid Model

By combining above two trust models, the hybrid trust model evaluates the trustworthiness of both vehicles and messages. ART [5] utilized the Dempster Shafer theory to aggregate trust evidence. An attack-resistant trust management scheme ensures the feasibility and dependability of ART. Then, a collaborative filtering algorithm was introduced to evaluate the trustworthiness of vehicles and messages. F. Ahmad et al. [12] proposed a trust model to defend against man-in-the-middle attacks. The trust value of message sender was evaluated by the height of vehicular antenna and position. Once the message sender's trustworthiness was determined, the message's authenticity was evaluated by direct and indirect trust calculations. The combined trust model inherits the advantages and disadvantages of entity-centric and data-centric trust models. However, the combined model also suffers from problems such as data sparsity.

III. System Model

A. Network Model

As shown in Fig. 1, entities in VANETs are divided into two categories: (i) vehicles and (ii) RSUs. The detailed introduction of them is illustrated as follows.

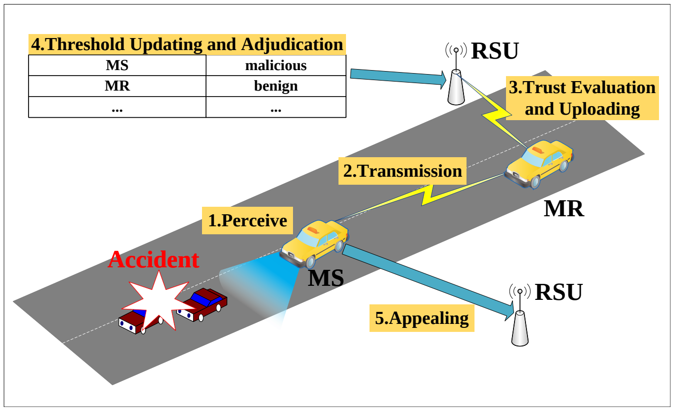


Fig. 1. System model.

1) Vehicles: Each vehicle is equipped with an On-Board Unit (OBU) to detect traffic events and collect trust evidence. Furthermore, vehicles have certain data storage and computing capabilities. Necessary functions of vehicles fundamentally support the trust calculation and judgment, including (i) traffic-related message sharing with neighbors, (ii) local trust evidence uploads, and (iii) undesired punishment appeals.

In addition, the trust evidence format is shown as follows:

$$TE_{i,j} = \{ID_j, DT_{i,j}, RT_j, IT_{i,j}, CT_{i,j}, \alpha, \beta, t\}, \tag{1}$$

where i and j denote the Message Receiver (MR) and Message Sender (MS), respectively. ID_j denotes the unique identifier of vehicle j. $DT_{i,j}$, $IT_{i,j}$ and $CT_{i,j}$ are direct, indirect, and combined trust values calculated for vehicle j, from the view of vehicle i, respectively. RT_j represents the recommendation trust values of vehicle j issued by RSUs. α and β denote the historically benign and malicious message forwarding behavior of vehicle j, respectively.

2) RSUs: RSUs are fixed infrastructures deployed along the road. They are responsible for relaying messages to vehicles or other RSUs, to expand the communication range of VANETs. In addition to the essential functions of vehicles, RSUs have advanced functions, including (i) collecting trust evidence and aggregating trust values, (ii) updating the trust threshold according to aggregated trust values, and (iii) punishing/rewarding vehicles according to aggregated trust values.

B. Adversary Model

This study implements three adversary models: Simple Attack (SA), Bad Mouth Attack (BMA), and RSU Attack (RA). SA and BMA attacks are conducted by authenticated vehicles, and RA attack is conducted by RSUs. A compromised RSU has the potential to revoke the certificates of benign vehicles, to decrease the transmission efficiency of messages. In addition, a compromised RSU may send the false trust threshold with vehicles, resulting in the vehicle being unable to select a trustworthy neighbor for message transmission. The details of three attack models are illustrated as follows:

- **Simple Attack (SA):** Attackers tamper with the received messages, i.e., modifying the contents of messages.

- **Bad Mouth Attack (BMA):** Attackers tamper with messages similar to attackers in SA. When a vehicle requests recommendations from a BMA attacker, the attacker will send false recommendations, resulting in the inaccuracy of trust evaluation and misjudged decision.
- **RSU Attack (RA):** Compromised RSUs will carry out RA, they provide false trust threshold and false aggregated trust values to vehicles. Moreover, they can also revoke the certificate of benign vehicles arbitrarily.

TABLE I
LIST OF NOMENCLATURES

Notations	Explanation
i	The vehicle that receives messages
j	The vehicle that sends messages
k	The vehicle that provides recommendations
α	The number of benign forwarding behaviors
β	The number of malicious forwarding behaviors
α', β'	The updated values of α and β
$x_{i,j}$	The current benign forwarding behaviors of j observed by i
$y_{i,j}$	The number of total forwarding behaviors of j observed by i currently
$\mathcal{V}$	The set of all vehicles in network
$\mathcal{V}_i$	The set of vehicles that have interacted with vehicles i
$DT_{i,j}$	The direct trust value evaluated by i on j
$IT_{i,j}$	The indirect trust value evaluated by i on j
$CT_{i,j}$	The combined trust value evaluated by i on j
AT_i	The aggregated trust value of vehicle i
$\overline{AT}$	The average trust value of all vehicles in the network
$\mathcal{T}$	The old trust threshold
$\mathcal{T}'$	The updated trust threshold
λ	The actual number of interactions between vehicles
Θ	The minimum number of interactions to evaluate trust accurately
P	The precision of detection
R	The recall of detection

IV. DESIGN OF THE PROPOSED TRUST MODEL

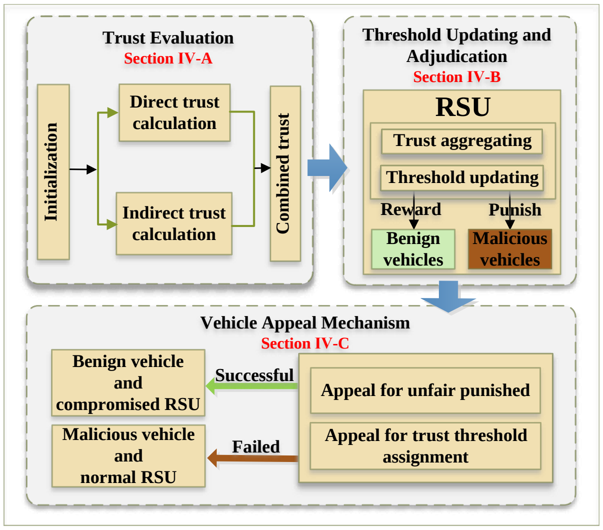


Fig. 2. Architecture of the proposed model.

Fig. 2 depicts the overall architecture of proposed model. In the trust evaluation stage, the message receiving vehicle calculates the direct, indirect and combined trust values. Then, the vehicle uploads trust values to RSUs, at which point it enters the threshold updating and adjudication stage. Here, RSUs will aggregate the received trust values to update the trust threshold, and punish/reward vehicles according to the trust threshold. When a vehicle receives a reward or punishment from RSUs, it enters the vehicle appeal stage. If the vehicle believes that an RSU's punishment is unreasonable, it will appeal to other RSUs to avoid a misjudgment. In general, vehicles are responsible for trust evaluating, uploading, and appealing. RSUs are responsible for trust aggregation, trust threshold updating, and reward/punish vehicles.

A. Trust Evaluation

Vehicle i maintains local trust evidence $TE_i = \{TE_{i,1}, TE_{i,2}, ..., TE_{i,x}\}$. When vehicle i receives the message from vehicle j, it first queries whether there is trust evidence locally ($TE_{i,j}$). If $TE_{i,j}$ does not exist, vehicle i initializes the trust evidence according to Eq. (1). Then, vehicle i calculates the direct trust value of vehicle j by the Bayesian method [7]. The direct trust value $DT_{i,j}$ is depicted as follows:

$$DT_{i,j} = \frac{\alpha + x_{i,j}}{\alpha + \beta + y_{i,j}}, \tag{2}$$

where α and β represent the historical benign message forwarding behavior and malicious message forwarding behavior of vehicle j, respectively. $x_{i,j}$ and $y_{i,j}$ are benign and malicious message forwarding behaviors vehicle j in the current interaction, respectively.

The message forwarding behavior is judged by the integrity of message. Specifically, when vehicle i receives the message, vehicle i can determine whether the received message has been tampered with through verification or authentication (if the message is tampered with, the forwarding behavior is considered malicious). Furthermore, α and β are updated and the equations are shown as follows:

$$\begin{cases} \alpha' = \alpha + x_{i,j}, \\ \beta' = \beta + y_{i,j} - x_{i,j}, \end{cases} \tag{3}$$

where α' and β' are the values after the iterations and their initial value is set to 1.

Moreover, vehicle i calculates the indirect trust value of vehicle j according to the recommendation from its neighbors. The indirect trust value $IT_{i,j}$ is given by:

$$IT_{i,j} = \frac{\sum_{k=1}^{\mathcal{V}_i} DT_{i,k} \times DT_{k,j}}{|\mathcal{V}_i|}, \tag{4}$$

where $\mathcal{V}_i$ represents the set of neighbors for vehicle i, $|\mathcal{V}_i|$ is the number of $\mathcal{V}_i$. $DT_{i,k}$ represents the direct trust value evaluated by vehicle i on k. Similarly, $DT_{k,j}$ represents the direct trust value evaluated by vehicle k on j.

Based on this, vehicle i aggregates the direct and indirect trust value into a combined trust $CT_{i,j}$, which is given by:

$$CT_{i,j} = \begin{cases} \frac{\lambda}{\theta} DT_{i,j} + (1 - \frac{\lambda}{\theta}) IT_{i,j} & \text{if } \lambda < \theta, \\ DT_{i,j} & \text{if } \lambda \geq \theta, \end{cases} \tag{5}$$

where λ denotes the number of interactions between vehicle i and vehicle j. θ is a preset fixed value, representing the minimum number of interactions with witch vehicle i can accurately evaluate the trust value. $DT_{i,j}$ represents the direct trust value evaluated by vehicle i on j, and $IT_{i,j}$ represents the indirect trust value evaluated by vehicle i on j. Specifically, the weight of direct and indirect trust aggregation depends on the number of interactions between vehicles i and j. When there are enough interactions, it can be considered that the direct trust of vehicle i is trustworthy. Therefore, the neighbors' recommendations required by vehicle i are unnecessary.

B. Trust Threshold Updating and Adjudication

When vehicle i is within the communication range of an RSU, its local trust evidence is uploaded. Then the RSU aggregates the trust evidence collected by vehicles to obtain an aggregated trust value AT_i:

$$AT_i = \frac{\sum_{x=1}^{\mathcal{V}_R} CT_{x,i}}{|\mathcal{V}_R|}, \tag{6}$$

where $\mathcal{V}_R$ is the set of vehicles that have communicated with the RSU, $|\mathcal{V}_R|$ is the size of set $\mathcal{V}_R$, and $CT_{x,i}$ represents the combined trust value of vehicle x to vehicle i. The RSU locally stores the aggregated trust value of multiple vehicles, $AT = \{AT_1, AT_2 ..., AT_n\}$.

Finally, aggregated trust values are shared between RSUs periodically. The trust threshold is updated according to the aggregated trust value, which is given by:

$$\mathcal{T}' = \begin{cases} \mathcal{T} + (\overline{AT} - \mathcal{T}) * exp\left\{\frac{1}{\mathcal{T} - \overline{AT}} - \frac{\overline{AT}}{\mathcal{T}}\right\} & \text{if } \overline{AT} > \mathcal{T}, \\ \mathcal{T} - (\mathcal{T} - \overline{AT}) * exp\left\{\frac{1}{\overline{AT} - \mathcal{T}} - \frac{\mathcal{T}}{\overline{AT}}\right\} & \text{if } \overline{AT} \leq \mathcal{T}, \end{cases} \tag{7}$$

where $\mathcal{T}$ represents the historical trust threshold. $\overline{AT}$ represents the average of total aggregated trust values, denoted as:

$$\overline{AT} = \frac{\sum_{i=1}^{\mathcal{V}} AT_i}{|\mathcal{V}|}, \tag{8}$$

where $\mathcal{V}$ is the set of vehicles. $|\mathcal{V}|$ is the total number of vehicles in the network, and AT_i is the aggregated trust value of vehicle i calculated by RSUs. If the aggregated trust value is lower than the trust threshold, the RSU will punish the corresponding vehicle, revoke its network certificates, and prohibit that vehicle from communicating with others.

C. Vehicle Appeal Mechanism

A compromised RSU has the potential to revoke the certificates of benign vehicles, to decrease the transmission efficiency of messages. Furthermore, a compromised RSU may send the false trust threshold with vehicles, resulting in the vehicle being unable to select a trustworthy neighbor for message transmission. Therefore, a vehicle appeal mechanism is proposed to supervise RSUs and resist the effect of untrustworthy participants, i.e., compromised RSUs.

The vehicle appeal mechanism details are shown in Algorithm 1. Two cases can trigger this mechanism: (i) a vehicle is punished, and (ii) a vehicle receives two trust thresholds with a significant difference within a short time interval.

Algorithm 1: Vehicle Appeal Algorithm

```
Input: vehicle's ID
Output: success or failure
vehicle $i$ appeals to TA;
if vehicle $i$ is wrongly punished then
    for other RSUs do
        global trust calculation, Eq. (6);
    end
    if $GT_i$ of most RSUs is higher than the threshold then
        vehicle $i$ is trustworthy, and restore its credentials;
        the misjudging RSU's ID is recorded, Eq. (9);
        Result: success
    end
    Result: failure
end
if the difference of trust threshold between two RSUs is out of range then
    for suspicious RSUs do
        The TA collects the RSU's threshold $\mathcal{T}'_{RSU}$;
        if $\mathcal{T}'_{RSU}! = \mathcal{T}'_{TA}$ then
            the misjudging RSU's ID is recorded, Eq. (10);
            Result: success
        end
    end
    Result: failure
end
```

1) Case 1: When vehicle i receives an unexpected punishment from an RSU, it appeals to RSUs (other than the one that implements punishment) for fair judgment. Then, other RSUs calculate the aggregated trust value AT_i on vehicle i. If AT_i is above the trust threshold $\mathcal{T}'$, the appeal will be successful. Furthermore, other RSUs restore the certificates for vehicle i and record the malicious value of the RSU r (denoted as M_r). The updated malicious value $M_r^{'}$ is shown as follows:

$$M_r^{'} = \begin{cases} M_r + 1 & \text{if appeal successful,} \\ M_r \times e^{-\Delta t} & \text{if appeal failed,} \end{cases} \tag{9}$$

where M_r represents the historical malicious value of RSU r, and its initial value is 0. Δt is the timestamp of the last record. If an RSU is subjected to multiple successful appeals within a short time, its malicious value will increase rapidly. When the malicious value of an RSU rises to a certain threshold, the RSU is considered a compromised RSU.

2) Case 2: If two RSUs assign two trust thresholds to a common vehicle but with large difference within short time interval, the vehicle will appeal to other RSUs (except the two suspicious RSUs). Then, other RSUs calculate the average value of the trust threshold $\overline{\mathcal{T}'}$ and compare it with the two suspicious RSUs. Then, the malicious value of the RSU is updated according to the results of the comparison:

$$M'_r = \begin{cases} M_r + 1 & \text{if } \mathcal{T}'_r \neq \overline{\mathcal{T}'}, \\ M_r \times e^{-\Delta t} & \text{if } \mathcal{T}'_r = \overline{\mathcal{T}'}, \end{cases} \tag{10}$$

where $\mathcal{T}'_r$ is the trust threshold of RSU r, and $\overline{\mathcal{T}'}$ is average trust threshold. It is observed that the vehicle appeal mechanism can prevent RSUs from providing the false trust threshold, which significantly impacts the vehicular selection of trustworthy neighbors for message transmission.

V. Performance Evaluation

A. Simulation Setup

The Opportunistic Network Environment (ONE) simulator [13] is utilized to perform experiments and analysis results. Realistic road from Helsinki city within a $4500 \times 3400 m^2$ area serves as the scenario for our simulation experiment, as shown in Fig. 3. Here, 200 vehicles and 12 RSUs are randomly generated on the digital map, and vehicles move to a random destination, following the shortest path obtained by Dijkstra algorithm. Furthermore, the transmission range, transmission rate and buffer size is set to $100m$, $900kbps$, and $10MB$.

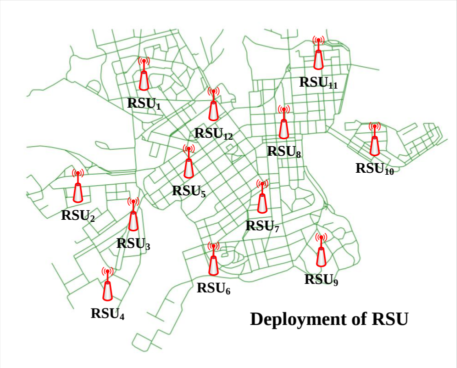


Fig. 3. The Helsinki City Scenario.

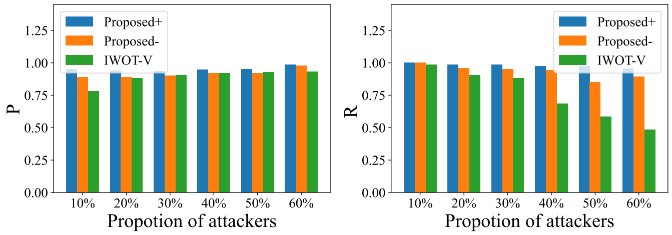
In addition, we introduce malicious vehicles and compromised RSUs into the network. Three attack methods are employed in vehicles, including SA, BMA, and RA mentioned in Section III-B. Then, we set the simulation time of each round to 3600 seconds, and there will be a warm-up time of 100 seconds before the simulation starts.

In the experiment, the proposed model is named 'Proposed+'. We measure the performance of proposed model with the 'Proposed-', which is without a vehicle appeal mechanism. Furthermore, we integrate IWOT-V [7] into the scenario of this paper. IWOT-V established an implicit web based on Bayes which identifies benign and malicious vehicles by aggregating local trust values into global trust values. The above three models are based on the spray and wait routing protocol [14] [1]. Metrics in Table II are evaluated for comparison:

TABLE II
Comparison Metrics

Metric	Calculation	Explanation
P	$\frac{The\ Detected\ malicious\ vehicles}{Detected\ as\ malicious\ vehicles}$	The accuracy of detecting malicious nodes
R	$\frac{The\ Detected\ malicious\ vehicles}{Total\ number\ of\ malicious\ vehicles}$	The recognition rate of malicious nodes
MDR	$\frac{Number\ of\ authentic\ messages}{Total\ number\ of\ messages}$	The accuracy of messages delivered in the network

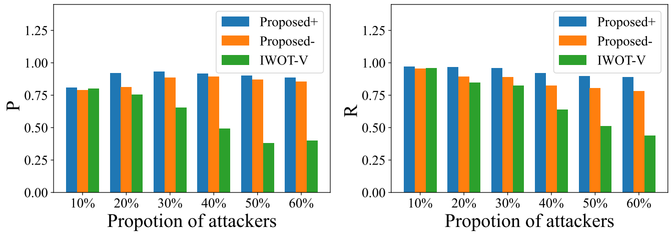
B. Result Analysis



(a) Precision (b) Recall

Fig. 4. Under SA attack, the impact of malicious vehicles' proportion.

1) Impact of SA: In Fig. 4(a), the precision of three models is improved with the increase of malicious vehicles, and the precision of 'Proposed+' is the best among three models. This is because when a minority of malicious vehicles exist, the IWOT-V inevitably misjudges benign vehicles. Due to the dynamic trust threshold mechanism, the 'Proposed+' reduces the false positive rate when there are few malicious vehicles. In addition, the misjudged vehicle can be corrected since the 'Proposed+' model utilizes the vehicle appeal mechanism to rejudge that vehicle. Therefore, the accuracy of the 'Proposed+' model outperforms others. In Fig. 4(b), with the increase in the proportion of malicious vehicles, the recall of IWOT-V decreases (from 98.4% to 48.5%). Specifically, IWOT-V only identifies roughly half of the attackers when malicious vehicles account for more than 35%.



(a) Precision (b) Recall

Fig. 5. Under BMA attack, the impact of malicious vehicles' proportion.

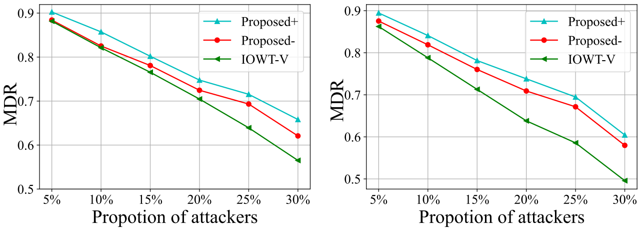
2) Impact of BMA: Fig. 5(a) shows the precision of three models. Specifically, when the number of attackers is limited, i.e., 10%, they have a subtle influence on the network. However, with the increase of attackers (from 10% to 60%), IWOT-V fails to eliminate the impact of attackers, and its

[1] Specifically, Spray and Wait algorithm is designed to work where paths may be unknown and may frequently change, for example, wildlife tracking sensor networks, military networks, inter-planetary networks, etc. In this context, conventional routing schemes would fail.

TABLE III
UNDER RA ATTACK, THE IMPACT OF COMPROMISED RSUS

Number of compromised RSUs	1	2	3	4	5	6
Precision	1	1	1	1	0.8	0.66

precision rate decreases sharply (from 79.9% to 39.8%). On the contrary, the precision of 'Proposed+' is maintained at a high level (from 80.7% to 93.1%). This is because 'Proposed+' considers weights for trust aggregations. When referring to recommendations from BMA attackers, their weights are too low to affect the trust evaluation. Fig. 5(b) shows the recall of three models. We can observe that the precision of proposed model is better against BMA than others. When the proportion of malicious vehicles is increased from 10% to 60%, the recall of three models decreases. This is because with the increase of attack probability, the probability of false recommendations from neighbors increases, resulting in the misjudgment of its final weighted average trust value. The recall of 'Proposed+' is always at the highest level because the weight of trust is considered in the trust aggregation.



(a) SA attack

(b) BMA attack

Fig. 6. Impact on message delivery rate.

3) Message delivery rate: Fig. 6(a) and Fig. 6(b) illustrate the relationship between the MDR and the percentage of attackers. It is observed that the MDR of 'Proposed+' is higher than that of the other two models. Specifically, with the increase of attackers, the MDR of three models decreases rapidly. Unfortunately, when the percentage of attackers is 30%, the maximum MDR is 65.8% that belongs to 'Proposed+'. The MDR of 'Proposed-' and IWOT-V are 62.1% and 56.5%, respectively. This is directly related to the contributions from vehicle appeal mechanism. Here, 'Proposed+' with the vehicle appeal mechanism can revoke the certificates of malicious vehicles and restore the certificates of misjudged vehicles, and improve the message transmission efficiency.

4) Impact of RA: Table III shows the detection precision of compromised RSUs. It is observed that when the number of compromised RSUs is less than half, almost all compromised RSUs can be detected (the precision rate is 100% when the number of compromised RSUs is less than 5, and 80% when the number of malicious RSUs is 5). This implies that a vehicle appeal mechanism is able to monitor RSUs' behavior to identify malicious RSUs effectively.

VI. CONCLUSION

The paper proposed a distributed trust model to resist malicious vehicles and compromised RSUs by a mutual supervision mechanism between vehicles and RSUs. Three stages of this model ensure the trustworthiness of participants, including trust evaluation, adjudication, and vehicle appeal mechanism. Specifically, the dynamic trust threshold mechanism is proposed to improve the precision and recall rate in detection of attackers. Moreover, a vehicle appeal mechanism provides vehicles a channel to appeal to other RSUs while being wrongly punished by a compromised RSU. The mechanism effectively solves the problem of compromised RSUs in the network. Extensive simulation results show that the proposed model effectively detects malicious vehicles with the presence of compromised RSUs.

VII. ACKNOWLEDGEMENT

The research is supported in part by the Wuhan Key Research and Development Program (2022012202015016).

REFERENCES

[1] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[2] Y. Liu, A. Liu, X. Liu, and M. Ma, "A trust-based active detection for cyber-physical security in industrial environments," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6593–6603, 2019.

[3] R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2013.

[4] C. Dai, D. Lin, E. Bertino, and M. Kantarcioglu, "An approach to evaluate data trustworthiness based on data provenance," in *Workshop on Secure Data Management*. Springer, 2008, pp. 82–98.

[5] W. Li and H. Song, "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2015.

[6] T. Denoeux, "A k-nearest neighbor classification rule based on dempster-shafer theory," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 25, no. 5, pp. 804–813, 1995.

[7] Y. Xiao and Y. Liu, "Bayestrust and vehiclerank: Constructing an implicit web of trust in vanet," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2850–2864, 2019.

[8] H. Xia, S.-s. Zhang, Y. Li, Z.-k. Pan, X. Peng, and X.-z. Cheng, "An attack-resistant trust inference model for securing routing in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7108–7120, 2019.

[9] Y. Wang, R. Chen, J.-H. Cho, A. Swami, Y.-C. Lu, C.-T. Lu, and J. J. Tsai, "Catrust: Context-aware trust management for service-oriented ad hoc networks," *IEEE Transactions on Services Computing*, vol. 11, no. 6, pp. 908–921, 2016.

[10] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in vanets," *Peer-to-peer networking and applications*, vol. 7, no. 3, pp. 229–242, 2014.

[11] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking." *Ad Hoc Sens. Wirel. Networks*, vol. 24, no. 3-4, pp. 283–305, 2015.

[12] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "Marine: Man-in-the-middle attack resistant trust model in connected vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310–3322, 2020.

[13] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for dtn protocol evaluation," in *Proceedings of the 2nd international conference on simulation tools and techniques*, 2009, pp. 1–10.

[14] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, 2005, pp. 252–259.