DCACA: Dual-Model Consensus-Based Anti-Risk Confidence Allocation Trust Management in IoVs

Chaklam Cheong, Yujie Song, Yue Cao, *Senior Member, IEEE,* Yu'ang Zhang, Haoxiang Wang, Qiang Ni, *Senior Member, IEEE*

***Abstract*—With the development of Internet of Vehicles (IoVs), data security emerges as a significant challenge, especially regarding data tampering and the spread of false information. While cryptography technologies tackle external security threats, they fall short in addressing internal security threats, such as authorized malicious vehicles tampering with and spreading false information. Consequently, trust management becomes a crucial technology, focusing on the analysis and identification of internal inappropriate behaviors to ensure safe interactions among vehicles. This paper explores the effective integration of trust opinions provided by Roadside Units (RSUs) into trust evaluations in IoVs, ensuring the comprehensiveness and accuracy of trust evaluations. We propose a Dual-model Consensus-based Anti-risk Confidence Allocation trust management scheme (DCACA) in IoVs. Specifically, DCACA utilizes direct trust, indirect trust, and global trust, to evaluation the trustworthiness of vehicles. Furthermore, to address the potential untrustworthiness of network entities (RSUs and vehicles), DCACA employs a dual-model consensus mechanism operates two processes of reaching consensus, including Real-time Collection Consensus Mechanism (RCCM) and Matrix-based Consensus Mechanism (MCM). RCCM is based on real-time collected trust opinions, reaching consensus to identify potential malicious trust opinions. MCM utilizes trust opinion matrices to collect trust opinions and achieves consensus through the elements in these matrices, identifying the sources of malicious trust opinions. Additionally, DCACA utilizes an anti-risk confidence allocation mechanism assigns confidence levels based on risk assessments, to mitigate the impact of malicious entities. Extensive experiments demonstrate that our scheme significantly outperforms other baseline schemes, exhibiting high levels of precision, recall, and F-Measure.**

***Index Terms*—IoVs, Trust Management, Consensus, Anti-Risk Confidence Allocation.**

I. Introduction

With rapid technological advancements, the Internet of Vehicles (IoVs) has garnered widespread attention for its immense potential in reducing the energy costs of autonomous driving vehicles [1], [2]. By enabling smart vehicles to share sensitive information with others, the safety, efficiency, and fluidity of road transport are greatly enhanced through the IoVs [3]. However, the open environment of IoVs and the characteristic of high-speed mobility of vehicles pose challenges to the reliability of data sharing [4]–[6]. Particularly, the open architecture makes IoVs susceptible to potential authorized malicious vehicles, thus facing various internal and external security threats[1] [7].

Some existing solutions in the field of IoVs focus on safeguarding communication channels, by utilizing traditional cryptographic technologies. A key approach involves providing vehicles with unique key pairs (private and public keys) and digital signatures, aimed at enhancing the security and integrity of data exchanges between vehicles [8]. Although these cryptographic methods are effective against external attacks, they are limited in countering internal attacks. Since cryptographic methods primarily validate the identity and integrity of data source, they are less effective in detecting malicious behavior from authenticated internal sources [9]. Consequently, research endeavors have shifted to security solutions based on trust management [10]. Its basic idea is to establish a trust framework in IoVs, where the receiver (vehicle) only accepts broadcast messages from senders (vehicles) with high trust values. Thus, receivers can filter out potential malicious senders with a low trust value, combating internal security threats and enhancing the effectiveness of overall network security.

Most existing works [11]–[14] focus on analyzing historical records to establish direct trust, while also incorporating indirect trust opinions[2] from neighbors (vehicles) to enhance trust evaluation accuracy. However, these schemes often demonstrate poor effectiveness in situations with insufficient data, because neighbors may be unable to provide accurate indirect trust opinions, leading to incomplete trust evaluations. Particularly, when interaction is insufficient, the resulting evaluation may not be as accurate. Moreover, existing solutions have not fully utilized trust opinions from other perspectives, such as Roadside Units (RSUs), limiting the comprehensiveness and accuracy.

In addition, previous works for the trust management field of IoVs often focus solely on the trust evaluation of vehicles. However, some schemes [15], [16] utilize RSUs to assist in trust evaluation, they often neglect to consider the potential unreliability of RSUs. Previous works related to malicious RSUs are relatively scarce in IoVs, lacking an in-depth analysis of the potential risks these units may pose. If RSUs provide malicious opinions to vehicles, it will lead to distorted trust

C. Cheong, Y. Song, Y. Cao (corresponding author), Y. Zhang, and H. Wang are with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430000, China. (e-mail: cheongchaklam@163.com, Y.Song@whu.edu.cn, yue.cao@whu.edu.cn, yuang.zhang@whu.edu.cn, 2023182210043@whu.edu.cn).

Q. Ni is with the School of Computing and Communications, Lancaster University, U.K. (e-mail: Q.Ni@lancaster.ac.uk).

[1] Internal security threats typically refer to attacks originating from within the network, such as data tampering or fraudulent activities carried out by network participants. External security threats involve external attackers, who may attempt to infiltrate the network, and disrupt the normal functioning of the network.

[2] Trust opinions refer to assessments made by vehicles about the reliability and credibility of other vehicles according to their previous interactions.

evaluation results, posing a significant threat to security and reliability of IoVs.

Motivated by above considerations, we propose a Dual-model Consensus-based Anti-risk Confidence Allocation trust management scheme (DCACA), aiming to enhance the completeness and accuracy of trust evaluations. Different from previous models, DCACA integrates the global trust provided by RSUs to strengthen trust evaluations, addressing the data scarcity problem. Furthermore, DCACA incorporates a dual-model consensus mechanism and an anti-risk confidence allocation mechanism. The former mechanism effectively identifies network entities (RSUs and vehicles) providing malicious trust opinions. The latter mechanism enhances the accuracy of evaluation results by filtering out these malicious opinions. Together, these mechanisms provide a robust response to the potential threats posed by malicious RSUs, which have been historically underexplored in the field of IoVs trust management. Overall, the main contributions of DCACA are as follows:

(1) Most of previous works [11]–[14] primarily focus on trust evaluations based on the historical interactions among vehicles. They cannot effectively operate trust evaluations in a data-scare scenario, reducing the accuracy of trust evaluations. In contrast, DCACA evaluates trust values by a comprehensive approach, i.e., operating trust evaluations and incorporating trust opinions from vehicles and RSUs. It is particularly vital in data-scarce environments, guaranteeing the completeness of evaluation. Moreover, DCACA introduces an innovative dual-model consensus mechanism to identify network entities providing malicious trust opinions. The dual-model consensus mechanism significantly improves the detection of malicious activities, by collecting and analyzing trust opinions provided by various entities.

(2) Most of literatures in trust management assume that RSUs are completely trustworthy, overlooking the impact of potential malicious RSUs in IoVs. Inevitably, some RSUs are considered as malicious entities to provide false trust opinions in DCACA. Then, DCACA introduces an innovative anti-risk confidence allocation mechanism to filter out negative trust opinions provided by malicious entities. Moreover, in the step of multi-trust (direct, indirect, and global trust) fusion, DCACA employs a confidence-based weighting method to ensure the accuracy of evaluation results.

II. Related Works

A. Traditional Trust Models

Traditional trust management models, regarded as widely recognized frameworks, focus on enhancing resistance to simple attack types rather than relying on complex data processing or statistical inference techniques. The model presented in the literature [17] utilized a user-post credibility network to differentiate between true and false alarm information. It calculated trust scores based on the social utility, behaviors, and contributions of vehicles. The work [15] proposed a hybrid trust model named MARINE, designed to combat man-in-the-middle attacks. MARINE considers various trust aspects, including node trust, data trust, vehicle-to-vehicle trust, and infrastructure-to-vehicle trust. The work [18] established a trust reasoning mechanism, emphasizing its effectiveness in addressing black hole and gray hole attacks. However, traditional models typically handle simple attacks well, such as black hole and message tampering attacks, but often struggle with multiple types of mixed attack patterns.

B. Trust Model based on Blockchain

Thanks to the advantage of blockchain technologies in ensuring data integrity and decentralization, it is increasingly being introduced into the field of trust management. Lahbib *et al.* [19] proposed a blockchain-based trust management scheme. Its core architecture includes trust managers, authenticators, and miners, all embedded in the management layer. The trust manager calculates the overall trust score by averaging direct and indirect subjective trust weights. Then, it sends these scores to miners for transaction processing (such as trust scores and interaction records). The work [20] introduced a dual-layer trust scoring system based on blockchain. In the first layer, vehicles independently calculate the trust score of neighbors based on the number of matched data packets, and upload transactions containing these trust scores to the nearest RSU. In the second layer, authorized RSUs aggregate the trust score of vehicles based on a weighted average method. Yang *et al.* [21] proposed a decentralized trust management model employing blockchain technology, where vehicles assess received messages and inform RSUs of assessment results. Subsequently, RSUs calculate entity-based trust values for vehicles and create trust blocks. The work [22] proposed a blockchain-based decentralized trust management scheme that utilizes smart contracts, ensuring reliable and consistent trust values are maintained. However, blockchain is not incorporated into our scheme due to its high computational and financial costs. Additionally, the potential integration of blockchain with trust mechanisms raises significant concerns, particularly regarding vulnerabilities to bad-mouth and first-rating advantage attacks [23]. Addressing malicious trust opinions has become a critical priority. Therefore, our proposed dual-model consensus mechanism offers a different way. It consists of real-time collection and matrix-based consensus mechanisms (discussed in Section III-B1 and III-B2).

Different from blockchain consensus, which relies on miners validating transactions and adding them to a decentralized ledger, the dual-model consensus utilizes trust opinion matrices and real-time collection to facilitate evaluations, allowing dynamic updates and adaptability to network conditions. Several key differences between blockchain and the dual-model consensus mechanism are shown as follows: i) The dual-model consensus mechanism adjusts consensus thresholds based on real-time network parameters, enabling quick responses to changes in IoVs. However, blockchain consensus mechanisms operate on fixed algorithms and periodic updates. ii) The dual-model consensus mechanism is more cost-efficient as it avoids the high computational and financial costs associated with blockchain mining and transaction validation. iii) While blockchain consensus ensures data integrity and immutability, the dual-model consensus mechanism specifically targets the detection and mitigation of malicious trust opinions.

C. Trust Model based on Probability Theory

Probability-based inference trust models employ probability distributions and density functions for calculating trust values, enabling trust reasoning. These models incorporate the likelihood of events into their evaluations. Bayesian inference and Dempster-Shafer (D-S) evidence theory fall under this category, assessing the credibility of vehicle based on probability values. The work [16] proposed a trust management scheme namely MEFPB combining path-backtracing mechanism and trust evidence fusion. MEFPB detects malicious behaviors on the transmission path of messages based on a path-backtracing mechanism. It also fuses trust evidences from various dimensions based on D-S evidence theory. However, MEFPB does not consider the presence of malicious RSUs, which could significantly impact the performance when RSUs provide malicious trust evidences.

In addition, Bhargava *et al.* [13] proposed an uncertainty-based trust model using D-S evidence theory to address the scarcity of information. This model integrates direct and indirect trust values of the message sender to establish new trust opinions. Xiao *et al.* [14] combined the Bayesian method with the PageRank algorithm to construct an implicit network. It distinguishes between malicious and normal vehicles by merging local trust evaluations into a global trust value. The work [24] focused on trust node management, proposing a composite trust model (e.g., direct and recommendation trust). The direct trust is dynamically calculated based on historical interaction records and Bayesian reasoning. The recommendation trust is derived from the trust evaluations and reputations provided by neighbors. The work [11] proposed a recommendation-based trust model, characterized by an adaptive weighting mechanism used in processing recommendations. This model dynamically adjusts weights based on the balance between positive and negative recommendations received. However, above models rely on direct trust and indirect trust provided by neighbors to assess the credibility of vehicles. They may lead to incomplete trust assessments in the absence of data, thereby failing to effectively address the complex and variable environments. Table I summarizes the exiting trust models.

D. Motivation

Based on above concerns, to ensure a comprehensive trust evaluation, DCACA encompasses not only direct trust and indirect trust provided by neighbors but also trust opinions offered by RSUs. To prevent malicious opinions from distorting the evaluation results, we introduce an anti-risk confidence allocation mechanism. It excludes trust opinions from entities whose confidence levels fall below a predetermined threshold. Furthermore, we employed a dual-model consensus mechanism to identify and appeal against entities with malicious behaviors. We also designed various response measures based on the frequency of appeals against entities. Malicious vehicles that repeatedly and persistently engage in malicious behavior are subjected to strict penalties. Based on above mechanisms, DCACA effectively counters various complex attacks, ensuring the accuracy and integrity of trust evaluations in IoVs.

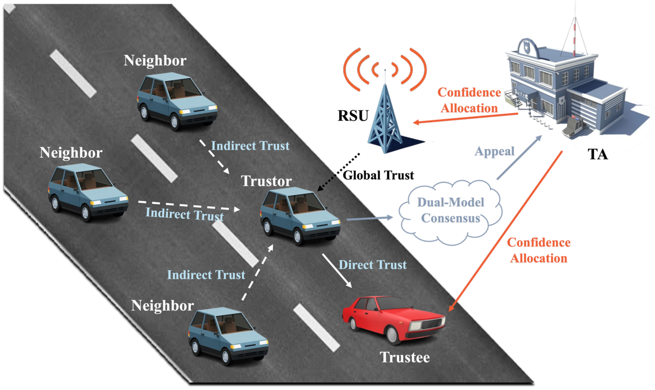


Fig. 1. The System Architecture of DCACA.

III. Trust Evaluation of DCACA

A. Preliminaries

1) System Architecture: As depicted in Fig. 1, the system consists of three components, i.e., vehicles, RSUs, and the Trust Authority (TA). Wireless communication channels are considered based on the 802.11p standard [25]. TA is the highest administrative authority within the network. In practical scenarios, such as hospitals, fire stations, and police stations can all serve as the TA [26]. In DCACA, the TA is considered an absolutely trustworthy central entity, whereas vehicles and RSUs are viewed as untrusted entities.

2) Trust Mechanism of DCACA: Trust evaluation occurs in a distributed manner, with each vehicle evaluating the trustworthiness of nearby vehicles. The trustor (vehicle V_i) sending messages, evaluates the trustworthiness of another vehicle and operates the consensus process as the leading vehicle. Messages received by the trustee (vehicle V_j) are utilized in the process of evaluating its trustworthiness. Furthermore, the trustworthiness of vehicles are represented by a trust value $T_{V_i} \in [0, 1]$. Specifically, T_{V_i} is a combination of three types of trust measurements: direct trust $DT^{t}_{V_i,V_j}$ (t represents the current time), indirect trust IV_{V_i,V_j}, and global trust GT_{RSU_i,V_j}. When a vehicle consistently exhibits positive behaviors, it is considered trustworthy, and T_{V_i} will approach 1. Conversely, it will near 0. Table II lists major abbreviations.

In the trust evaluation process, one of the steps involves vehicle V_i collecting trust opinions from neighbors V_k. Especially, the trust opinions originate from the previous direct trust evaluation conducted by V_k on V_j ($DT^{t_l}_{V_k,V_j}$, where t_l represents the time of the last direct trust evaluation). These opinions serve as the basis for IV_{V_i,V_j}, and are employed to evaluate the trustworthiness of V_j. To organize the above information, each vehicle maintains a vehicle trust opinion matrix $R^V_{V_i}$, and its structure is shown as follows:

$$R^V_{V_i} = \begin{bmatrix} Null & r^V_{2,1} & \cdots & r^V_{m,1} \\ r^V_{1,2} & Null & \cdots & r^V_{m,2} \\ \vdots & \vdots & \ddots & \vdots \\ r^V_{1,m} & r^V_{2,m} & \cdots & Null \end{bmatrix} \tag{1}$$

where m represents the total number of vehicles in the network. For instance, $r^V_{1,2}$ represents the trust opinion of

TABLE I
TRUST MODELS.

	Trust dimensions			Malicious entity		Attack model					
	Direct trust	Indirect trust	RSU opinions	Vehicle	RSU	Simple	Black hole	Bad mouth	Collusion	On-off	RSU bad mouth
[11]	✓	✓		✓			✓	✓		✓	
[13]	✓	✓		✓		✓				✓	
[14]	✓	✓		✓		✓	✓				
[15]	✓	✓	✓	✓		✓	✓			✓	
[16]	✓	✓	✓	✓		✓	✓			✓	
[17]	✓	✓		✓		✓		✓			
[18]	✓	✓		✓			✓	✓	✓	✓	
[19]	✓	✓		✓				✓	✓	✓	
[20]	✓	✓		✓	✓		✓	✓			
[21]	✓			✓	✓	✓		✓			
[22]	✓			✓		✓					
DCACA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

TABLE II
MAJOR ABBREVIATIONS.

Terms	**Description**
$R_{V_i}^{V}$	The vehicle trust opinion matrix of i-th vehicle
$R_{V_i}^{RSU}$	The RSU trust opinion matrix of i-th vehicle
RSU_i	The i-th RSU
E_i	The i-th entity
t_n	The current time window
$Rec_{V_i}^{t}$	Neighbor set of V_i
DT_{V_i,V_j}^{t}	The direct trust of V_j computed by V_i
IT_{V_i,V_j}	The indirect trust V_j computed by V_i
GT_{RSU_i,V_i}	The indirect trust V_j provided by RSU_i
T_{V_i}	The trust value of i-th vehicle
$TS_{CV}^{V_i}$	The consensus threshold for $R_{V_i}^{V}$
$TS_{CR}^{V_i}$	The consensus threshold for $R_{V_i}^{RSU}$
CD_{V_i}	The communication density for V_i
R_{E_i}	The risk of E_i
C_{E_i}	The confidence level of E_i
C_{V}^{ts}	The confidence threshold of all vehicles
C_{RSU}^{ts}	The confidence threshold of all RSUs
λ_{V_i,V_j}	The forgetting factor from the view of V_i to V_j
TR_{V_j}	The transmission reliability of V_j
CP_{V_j}	The cooperativeness of V_j
δ_{V_j}	The cooperativeness factor of V_j
DT_{V_k,V_j}^{tl}	The previous direct trust of V_k to V_j
CR_{V_j}	The cooperative reliability of V_j

vehicle V_1 regarding vehicle V_2. These trust opinions adhere to a defined criterion: the trust opinion from V_1 regarding V_2. If the trust opinion of V_1 regarding V_2 greater than or equal to 0.5, $r_{1,2}^{V} = Trust$. Conversely, $r_{1,2}^{V} = Distrust$.

Moreover, in the trust evaluation process, V_i not only considers trust opinions from V_k but also acquires trust opinions about V_j from RSUs. These trust opinions obtained from RSUs, denoted as global trust GT_{RSU_i,V_j}. It will be further employed in assessing the trustworthiness of V_j. Then, each vehicle maintains a RSU trust opinion matrix $R_{V_i}^{RSU}$, and its structure is shown as follows:

$$R_{V_i}^{RSU} = \begin{bmatrix} r_{1,1}^{RSU} & r_{2,1}^{RSU} & \cdots & r_{n,1}^{RSU} \\ r_{1,2}^{RSU} & r_{2,2}^{RSU} & \cdots & r_{n,2}^{RSU} \\ \vdots & \vdots & \ddots & \vdots \\ r_{1,m}^{RSU} & r_{2,m}^{RSU} & \cdots & r_{n,m}^{RSU} \end{bmatrix} \tag{2}$$

where n denotes the total number of RSUs in the network. For instance, $r_{1,2}^{RSU}$ indicates the trust opinion of the i-th RSU (RSU_1) towards vehicle V_2. Similar to the vehicle trust opinion matrix $R_{V_i}^{V}$, if the trust opinion from RSU_1 regarding V_2 exceeds or equals 0.5, $r_{1,2}^{RSU} = Trust$. Conversely, $r_{1,2}^{RSU} = Distrust$. Fig. 2 illustrates the relationship between all mechanisms in DCACA and the three types of trust.

B. Dual-Model Consensus and Appeal Mechanism

Truster V_i analyzes all collected trust opinions to identify trust patterns (i.e., $Trust$ or $Distrust$) and filtering out potential malicious trust opinions. If the majority of trust opinions by vehicles or RSUs align with a trust pattern, it can be inferred that a consensus has been formed. Specifically, two consensus mechanisms are constructed, i.e., a Real-time Collection Consensus Mechanism (RCCM) and a Matrix-based Consensus Mechanism (MCM). Both of them are founded on Practical Byzantine Fault Tolerance[3] (PBFT) [27].

1) Real-time Collection Consensus Mechanism: RCCM identifies potential malicious trust opinions provided by vehicles. The specific implementation process is as follows:

1. Initial Stage: Truster V_i establishes a connection with Trustee V_j, and broadcasts a request for trust opinions to neighbors.

2. Trust Opinions Collection: Neighbors participate in the trust evaluation, respond based on their latest direct trust of V_j, and send these trust opinions to V_i.

3. Analysis and Consensus: V_i collects all trust opinions from neighbors and updates $R_{V_i}^{V}$. V_i then analyzes the collected opinions to identify whether a prevalent trust pattern ($Trust$ or $Distrust$) can be obtained. If a majority of vehicles agree on a particular trust pattern, consensus is reached.

[3] PBFT represents an efficient fault-tolerant mechanism designed to ensure that the system processes information correctly and reaches consensus, even in the presence of faulty or malicious nodes.

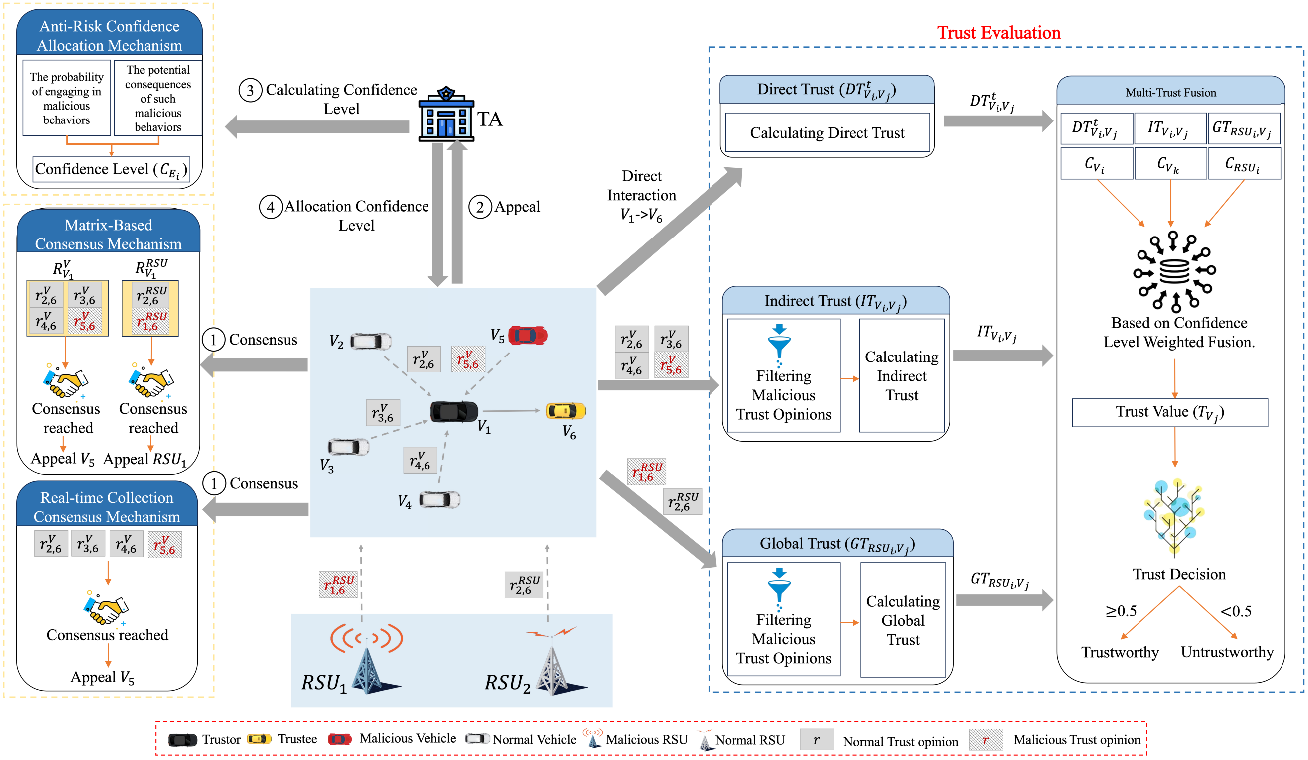

Anti-Risk Confidence Allocation Mechanism
The probability of engaging in malicious behaviors
The potential consequences of such malicious behaviors
Confidence Level (C_{E_i})
3 Calculating Confidence Level
TA
4 Allocation Confidence Level
2 Appeal
Matrix-Based Consensus Mechanism
$R^V_{V_1}$
$R^{RSU}_{V_1}$
Consensus reached
Consensus reached
Appeal V_5 Appeal RSU_1
1 Consensus
1 Consensus
Real-time Collection Consensus Mechanism
Consensus reached
Appeal V_5
V_1 V_2 V_3 V_4 V_5 V_6
$r^V_{2,6}$ $r^V_{3,6}$ $r^V_{4,6}$ $r^V_{5,6}$ $r^{RSU}_{1,6}$ $r^{RSU}_{2,6}$
RSU_1 RSU_2
Direct Interaction V_1->V_6
Trust Evaluation
Direct Trust ($DT^t_{V_i,V_j}$)
Calculating Direct Trust
$DT^t_{V_i,V_j}$
Indirect Trust (IT_{V_i,V_j})
Filtering Malicious Trust Opinions
Calculating Indirect Trust
IT_{V_i,V_j}
Global Trust (GT_{RSU_i,V_j})
Filtering Malicious Trust Opinions
Calculating Global Trust
GT_{RSU_i,V_j}
Multi-Trust Fusion
$DT^t_{V_i,V_j}$ IT_{V_i,V_j} GT_{RSU_i,V_j}
C_{V_i} C_{V_k} C_{RSU_i}
Based on Confidence Level Weighted Fusion.
Trust Value (T_{V_j})
Trust Decision
≥0.5
<0.5
Trustworthy
Untrustworthy
Trustor Trustee Malicious Vehicle Normal Vehicle Malicious RSU Normal RSU
r Normal Trust opinion
r Malicious Trust opinion

Fig. 2. The relationship between all mechanisms in DCACA and the three types of trust.

4. Execution and Appeal: Once consensus is reached, V_i identifies trust opinions significantly diverging from the consensus, and appeals to TA regarding vehicles that provided these opinions.

For instance, as shown in Fig. 2, V_i broadcasts a request to its neighbors (V_2, V_3, V_4, V_5) to gather trust opinions about V_6. Each vehicle provides its trust opinion based on its latest direct trust evaluation of V_6 and sends it to V_1. Then, V_1 conducts an analysis of received opinions, discovering opinions from V_2, V_3, and V_4 are $Trust$. In contrast, the trust opinion from V_5 stands out as $Distrust$, leading V_1 to lodge an appeal concerning V_5.

2) Matrix-based Consensus Mechanism: MCM is efficient in scenarios characterized by a high proportion of malicious vehicles. For instance, if the majority of trust opinions are provided by malicious vehicles, the importance of MCM in identifying these harmful trust opinions becomes vital.

Furthermore, with the often sparse distribution of RSUs in real-world settings, trust evaluations often involve trust opinions from only one or a few RSUs, posing challenges in achieving a consensus. MCM is aimed at addressing potential malicious trust opinions originating from RSUs.

MCM involves two types of trust opinion matrices: $R^V_{V_i}$ and $R^{RSU}_{V_i}$. They record trust opinions provided by vehicles and RSUs, respectively. To adapt to the high dynamics of IoVs, these matrices are regularly updated to remove trust opinions that have been appealed. Moreover, to ensure efficient system operation and prevent the abuse of appeal mechanism, the number of appeal for vehicles is limited to one within a time window θ (set at 300s [16]).

Vehicles can adjust the consensus threshold based on current network conditions and dynamic change to determine whether to initiate the consensus process. A consensus process is triggered when any element in a certain row of the matrix exceeds the consensus threshold. The consensus threshold consists of total number of vehicles (m), total number of RSUs (n), trust opinion change rate (TCR), and communication density (CD). The consensus thresholds for $R^V_{V_i}$ and $R^{RSU}_{V_i}$ are denoted as $TS^{V_i}_{CV}$ and $TS^{V_i}_{CR}$, respectively. Their formulas are shown as follows:

$$TS^{V_i}_{CV} = [w_{ts} * TCR^V_{V_i} + (1 - w_{ts}) * CD_{V_i}] * m, \quad (3)$$

$$TS^{V_i}_{CR} = [w_{ts} * TCR^{RSU}_{V_i} + (1 - w_{ts}) * CD_{V_i}] * n, \quad (4)$$

where w_{ts} represents the weight for TCR, usually, it is set to 0.5, which indicates TCR and CD are both important. $TCR^V_{V_i}$ and $TCR^V_{V_i}$ respectively denote the trust opinion change rate of $R^V_{V_i}$ and $R^{RSU}_{V_i}$. CD_{V_i} represents the communication density of V_i. Their formulas are as follows:

$$TCR^V_{V_i} = \frac{N^{ctv}_{V_i}}{\theta}, \quad (5)$$

$$TCR^{RSU}_{V_i} = \frac{N^{ctr}_{V_i}}{\theta}, \quad (6)$$

$$CD_{V_i} = \frac{N^{cn}_{V_i}}{\theta}, \quad (7)$$

Algorithm 1: Matrix-Based Consensus Mechanism

```
Input: RSU trust opinion matrix $R_{V_i}^{RSU}$, Vehicle trust
       opinion matrix $R_{V_i}^{V}$
Output: Appeal list
Calculate $TCR_{V_i}^{V} \leftarrow (N_{V_i}^{ctv}, \theta)$, Eq. (5);
Calculate $TCR_{V_i}^{RSU} \leftarrow (N_{V_i}^{ctr}, \theta)$, Eq. (6);
Calculate $CD_{V_i} \leftarrow (N_{V_i}^{cn}, \theta)$, Eq. (7);
Calculate $TS_{CV}^{V_i} \leftarrow (TCR_{V_i}^{V}, CD_{V_i})$, Eq. (3);
Calculate $TS_{CR}^{V_i} \leftarrow (TCR_{V_i}^{RSU}, CD_{V_i})$, Eq. (4);
for each row $ROW_i$ in $R_{V_i}^{V}$ do
    if $len(ROW_i) \geq TS_{CV}^{V_i}$ then
        Initiation of the Consensus;
        for each opinion $O$ in $ROW_i$ do
            if $O = Trust$ then
                TrustCount + 1;
            else
                DisTrustCount + 1;
        if TrustCount > DistrustCount then
            Trust pattern is $Trust$;
        else if DistrustCount > TrustCount then
            Trust pattern is $Distrust$;
        else
            Continue;
        for each opinion $O$ in $ROW_i$ do
            if $O$ is different from the trust pattern then
                Addition of vehicles providing $O$ to the
                 appeal list;
return Appeal list
```

where $N_{V_i}^{ctv}$ and $N_{V_i}^{ctr}$ represent the number of trust opinions updated in $R_{V_i}^{V}$ and $R_{V_i}^{RSU}$ within a time window θ, respectively. $N_{V_i}^{cn}$ represents the total number of communications that a vehicle engages in during the same time window.

For example, the first row in $R_{V_i}^{V}$ contains trust opinions from other vehicles regarding V_1. When the number of trust opinions in this row exceeds $TS_{CV}^{V_i}$, the consensus process is initiated. To illustrate, if 20 vehicles express trust in V_1 (opinions marked as $Trust$), while another 5 vehicles indicate distrust (opinions marked as $Distrust$). As the majority of opinions are $Trust$, the consensus result is determined to be $Trust$. In this case, for those 5 vehicles expressing $Distrust$, V_i will appeal to the TA. The process of the MCM is depicted in Algorithm 1, featuring the symbol $\leftarrow (*)$, where $*$ indicates data input. The function $len()$ denotes the number of elements.

3) Theoretical Analysis of RCCM and MCM: The RCCM operates on robust theoretical principles to ensure the reliable identification of malicious opinions within IoVs. In the face of vehicles providing malicious opinions, RCCM utilizes a distributed trust evaluation approach by broadcasting trust requests to multiple neighbors, mitigating the risk of single points of failure and leveraging collective network intelligence. To counteract the influence of outliers and ensure accurate trust assessments, RCCM employs majority voting as a statistical consensus method, robustly filtering out unreliable opinions. For further security, RCCM incorporates outlier detection, flagging significantly deviating trust opinions and escalating them to a higher authority (the TA) for hierarchical review and penalty imposition based on the frequency of such appeals. This layered approach effectively evaluates and manages trust, enhancing the overall security and reliability of IoVs.

The MCM implements robust methods to identify malicious opinions. By maintaining redundancy through separate trust opinion matrices for vehicles and RSUs, MCM can cross-validate trust opinions and reduce the influence of any single malicious entity. This redundancy ensures that even if one set of opinions is compromised, the overall trust evaluation remains reliable. The statistical consensus mechanism, which dynamically adjusts the consensus threshold based on factors such as the trust opinion change rate (TCR) and communication density (CD), allows MCM to adapt to real-time network conditions, ensuring resilience against varying levels of network traffic and malicious activity. Furthermore, the dynamic adaptation of consensus thresholds enables MCM to swiftly respond to changes in the network, continuously monitoring and adjusting to maintain accurate and reliable trust evaluations. This approach effectively mitigates the risks posed by malicious nodes, ensuring the stability and security of trust management within IoVs.

C. Anti-Risk Confidence Allocation Mechanism

To effectively address the potential impact of abnormal trust opinions, DCACA introduces an Anti-Risk Confidence Allocation Mechanism (ACAM) based on risk assessment. TA conducts risk assessment of these entities and calculates their confidence level accordingly, to decide whether to accept the trust opinions offered by these entities. Accurate risk assessment needs to consider various potential factors, such as weather conditions. However, acquiring this information significantly increases costs and reduces efficiency. Therefore, risk assessment is solely based on the historical behavior, vehicle density, and interaction intentions of network entities (i.e., RSUs and vehicles).

According to the definition of risk by the USA National Institute of Standards and Technology [28], risk R_{E_i} of entity i (E_i) can be quantified as follows:

$$R_{E_i} = Likelihood_{E_i} * Impact_{E_i}, \tag{8}$$

where $Likelihood_{E_i}$ represents the probability of E_i engaging in malicious behaviors, while $Impact_{E_i}$ denotes the potential consequence of such malicious behaviors caused by E_i.

Note that, $Likelihood_{E_i}$ can be estimated through an analysis focused on how often the entity has been the subject of appeals. Entities with a high frequency of appeals are viewed as high risk. The calculation for $Likelihood_{E_i}$ is based on the following formula:

$$Likelihood_{E_i} = \frac{\sum_{t=1}^{t_n} \frac{t}{t_n} H_{E_i}^{t}}{\sum_{t=1}^{t_n} \frac{t}{t_n}} * \hat{w_h}, \tag{9}$$

where t_n represents the current number of time windows, each time window is equivalent to a period, referring to the n-th period in the sequence. $H^t_{E_i}$ is the number of times E_i is appealed in each time window, and $\hat{w_h}$ is a normalization factor defined as $\hat{w_h} = \frac{1}{H_{max}}$. Here, H_{max} denotes the maximum number of appeals.

Additionally, $Impact_{E_i}$ is assessed by considering the interaction intention and vehicle density of entities. In areas where the vehicle density is high, malicious behavior tend to have a more significant impact. When there is a high intent for interaction, it suggests that malicious behaviors of an entity could have wider effects on the network. The formulas for calculating $Impact_{E_i}$ are shown as follows:

$$Impact_{E_i} = \begin{cases} N_n * \frac{N^d_{V_i}}{N^t_{V_i}}, & \text{if } E_i \text{ is vehicle} \\ N_n, & \text{if } E_i \text{ is RSU} \end{cases} \tag{10}$$

where N_n denotes the number of vehicles within a communication range, $N^t_{V_i}$ is the number of messages ever forwarded, and $N^d_{V_i}$ is the number of different vehicles messages have been forwarded.

According to Eq. (9) and Eq. (10), the confidence level C_{E_i} of E_i is inversely proportional to its R_{E_i}, with the calculation formula being:

$$C_{E_i} = 1 - R_{E_i}. \tag{11}$$

Each E_i has a C_{E_i}. If C_{E_i} meets or exceeds the designated confidence thresholds (C^{ts}_{RSU} for RSUs and C^{ts}_V for vehicles), its opinions are classified as acceptable opinions. Conversely, its trust opinions will not be considered in subsequent trust evaluation stages. These opinions will update R^V_i and R^{RSU}_i for future consensus formation and appeals in MCM. Then, C^{ts}_V and C^{ts}_{RSU} formulas are:

$$C^{ts}_V = median_V - (IQR_V \ * \gamma), \tag{12}$$

$$C^{ts}_{RSU} = median_{RSU} - (IQR_{RSU} \ * \gamma), \tag{13}$$

where $median_V$ and $median_{RSU}$ are the median C_{E_i} of all vehicles and RSUs, respectively. $IQR = Q_3 - Q_1$ represents the interquartile range, the difference between the first (Q_1) and third (Q_3) quartiles[4], quantifying the distribution range of confidence levels. γ is a scaling factor used to adjust the influence of IQR on the calculation of C^{ts}_V and C^{ts}_{RSU}, set to 1 [16], [29]. The process of the ACAM is depicted in Algorithm 2, where the function $sort()$ denotes a sort by the ascending order.

D. Direct Trust

As depicted in Fig. 3, direct trust $DT^t_{V_i,V_j}$ is a value made by V_i based on its own observations of V_j. $DT^t_{V_i,V_j}$ primarily relies on three key elements: the forgetting factor, the transmission reliability of vehicle, and its cooperativeness.

Algorithm 2: Anti-Risk Confidence Allocation Mechanism

```
Input: Entity $E_i$
Output: Confidence level $C_{E_i}$
Calculate $Likelihood_{E_i} \leftarrow (t_n, H^t_{E_i}, H_{max})$, Eq. (9);
if $E_i$ is vehicle then
    Calculate $Impact_{E_i} \leftarrow (N_n, N^d_{V_i}, N^t_{V_i})$, Eq. (10);
else
    Calculate $Impact_{E_i} \leftarrow (N_n)$, Eq. (10);
Calculate $R_{E_i} \leftarrow (Likelihood_{E_i}, Impact_{E_i})$, Eq. (8);
Calculate $C_{E_i} \leftarrow (R_{E_i})$, Eq. (11);
for each vehicle $V_i$ in Network do
    Add $C_{E_i}$ of $V_i$ to vehicle confidence list;
$sort$(vehicle confidence list);
for each RSU $RSU_i$ in Network do
    Add $C_{E_i}$ of $RSU_i$ to RSU confidence list;
$sort$(RSU confidence list);
Calculate $C^{ts}_V \leftarrow (median_V, IQR_V, \gamma)$, Eq. (12);
Calculate $C^{ts}_{RSU} \leftarrow (median_{RSU}, IQR_{RSU}, \gamma)$,
  Eq. (13);
if $E_i$ is vehicle then
    if $C_{E_i} \geq C^{ts}_V$ then
        Trust opinion provided by $E_i$;
    else
        Untrusted opinion provided by $E_i$;
else
    if $C_{E_i} \geq C^{ts}_{RSU}$ then
        Trust opinion provided by $E_i$;
    else
        Untrusted opinion provided by $E_i$;
return $C_{E_i}$
```

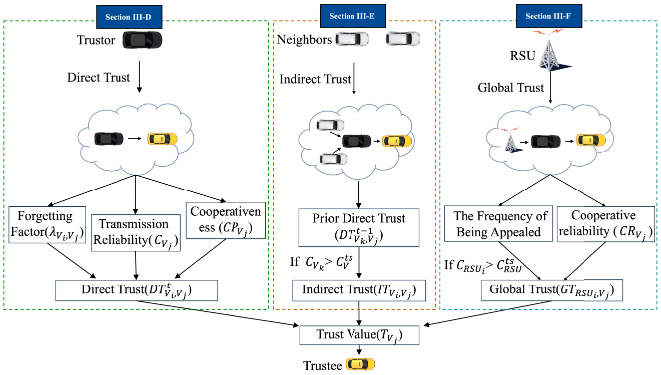

Section III-D
Trustor
Direct Trust
Forgetting Factor(λ_{V_i,V_j})
Transmission Reliability(C_{V_j})
Cooperativeness (CP_{V_j})
Direct Trust($DT^t_{V_i,V_j}$)
Section III-E
Neighbors
Indirect Trust
Prior Direct Trust ($DT^{t-1}_{V_k,V_j}$)
If $C_{V_k} > C^{ts}_V$
Indirect Trust(IT_{V_i,V_j})
Section III-F
RSU
Global Trust
The Frequency of Being Appealed
Cooperative reliability (CR_{V_j})
If $C_{RSU_i} > C^{ts}_{RSU}$
Global Trust(GT_{RSU_i,V_j})
Trust Value(T_{V_j})
Trustee

Fig. 3. Three types of trust calculation process.

1) Forgetting Factor (λ_{V_i,V_j}): The forgetting factor plays a crucial role in modulating the rate of trust value increase for vehicles that have not interacted for a long period. It helps prevent errors in trust evaluation caused by low interaction fre-

[4] Quartiles are statistical measures utilized to gauge the distribution of data. The Q_1 is the value at the 25% position when all data is arranged in ascending order, while Q_3 is at the 75% position.

quency[5]. Without the forgetting factor, the trust value of these vehicles could rise unreasonably fast, negatively impacting the overall accuracy of trust evaluations. Specifically, if V_j does not participate in any interaction within a time window θ, its $DT^t_{V_i,V_j}$ will decrease. The formula of forgetting factor λ_{V_i,V_j} is shown as follows:

$$\lambda_{V_i,V_j} = \frac{t - t_f}{\theta}, \tag{14}$$

where t represents the current time, and t_f is the last time V_j participated in an interaction.

2) Transmission Reliability (TR_{V_j}): Transmission Reliability serves as a crucial metric for evaluating whether V_j is trustworthy during the process of message transmission. A higher transmission reliability indicates that the vehicle is more reliable, thus warranting a higher degree of direct trust. Specifically, TR_{V_j} is calculated based on the frequency of V_j forwarding normal and malicious messages. When a vehicle receives a message, it employs verification or authentication to verify whether the message content has been tampered with. Messages found to be tampered with are immediately discarded to maintain the integrity and reliability of communication. The formula for calculating TR_{V_j} is shown as follows:

$$TR_{V_j} = \begin{cases} \frac{N^{sv}_{V_j}}{N^{sv}_{V_j} + N^{fv}_{V_j}}, & \text{if } N^{sv}_{V_j} > 0 \\ 0, & \text{if } N^{sv}_{V_j} = 0 \end{cases} \tag{15}$$

where $N^{sv}_{V_j}$ represents the number of times V_j has forwarded unaltered messages. $N^{fv}_{V_j}$ denotes the number of times V_j has forwarded altered messages.

3) Cooperativeness (CP_{V_j}): Cooperativeness assesses the willingness of V_j to exchange information with other vehicles. A high level of cooperativeness indicates a greater propensity for sharing information with others. Specifically, a vehicle that has interacted with a larger number of other vehicles is considered to have a high level of cooperativeness. Conversely, limited interaction with other vehicles implies a low level of cooperativeness. The formula to calculate CP_{V_j} is shown as follows:

$$CP_{V_j} = \frac{N_d}{m - 1} * \delta_{V_j}, \tag{16}$$

where N_d represents the nubmer of different vehicles, that V_j has forwarded messages to, and δ_{V_j} denotes the cooperativeness factor is shown as follows:

$$\delta_{V_j} = \frac{N^t_{V_j}}{max(N^t_{V_j})}, \tag{17}$$

where $N^t_{V_j}$ denotes the total number of messages forwarded by V_j, while $max(N^t_{V_j})$ represents the maximum number of messages forwarded by any vehicle that has interacted with V_j.

Based on the above calculated, if $\lambda_{V_i,V_j} \leq 1$, the formula of direct trust $DT^t_{V_i,V_j}$ is as follows:

$$DT^t_{V_i,V_j} = w_D * TR_{V_j} + (1 - w_D) * CP_{V_j}, \tag{18}$$

if $\lambda_{V_i,V_j} > 1$, the formula of direct trust $DT^t_{V_i,V_j}$ is as follows:

$$DT^t_{V_i,V_j} = \frac{1}{\lambda_{V_i,V_j}} * [w_D * TR_{V_j} + (1 - w_D) * CP_{V_j}], \tag{19}$$

where w_D represents the weight of TR_{V_j} and CP_{V_j}, with $w_D = 0.5$ indicating an average taken between TR_{V_j} and CP_{V_j}, to balance the contribution of TR_{V_j} and CP_{V_j} on $DT^t_{V_i,V_j}$. The process of calculation of direct trust is expressed in Algorithm 3.

Algorithm 3: Direct Trust Calculation

```
Input: Trustor $V_i$, Trustee $V_j$
Output: Direct Trust $DT^t_{V_i,V_j}$
Calculate $\lambda_{V_i,V_j} \leftarrow (t, t_f, \theta)$, Eq. (14);
Calculate $TR_{V_j} \leftarrow (N^{sv}_{V_j}, N^{fv}_{V_j})$, Eq. (15);
Calculate $\delta_{V_j} \leftarrow (N^t_{V_j}, max(N^t_{V_j}))$, Eq. (17);
Calculate $CP_{V_j} \leftarrow (N_d, m, \delta_{V_j})$, Eq. (16);
if $\lambda_{V_i,V_j} \leq 1$ then
    $DT^t_{V_i,V_j} = w_D * TR_{V_j} + (1 - w_D) * CP_{V_j}$,
      Eq. (18);
else
    $DT^t_{V_i,V_j} = \frac{1}{\lambda_{V_i,V_j}} * [w_D * TR_{V_j} + (1 - w_D) * CP_{V_j}]$,
      Eq. (19);
return $DT^t_{V_i,V_j}$;
```

E. Indirect Trust

As depicted in Fig. 3, indirect trust involves V_i assessing the trustworthiness of V_j, utilizing the trust opinion gathered from its neighbors V_k. In this process, V_k is part of the neighor set Rec_{V_i} of V_i, and the trust opinion provided by V_k reflects its prior direct trust in V_j ($DT^{t_l}_{V_i,V_j}$). Specifically, when V_i gathers trust opinion from V_k, V_i first considers the confidence level C_{V_k} of V_k. V_i adopts the trust opinion of V_k regarding V_j only if the confidence level C_{V_k} of V_k meets or exceeds the confidence threshold C^{ts}_V. The formula of indirect trust IT_{V_i,V_j} is as follows:

$$IT_{V_i,V_j} = \frac{\sum_{k=1}^{len(Rec_{V_i})} DT^{t_l}_{V_k,V_j}}{len(Rec_{V_i})}, \tag{20}$$

where $len(Rec_{V_i})$ indicates the length of the Rec_{V_i} whose C_{V_k} are greater than or equal to C^{ts}_V.

F. Global Trust

As depicted in Fig. 3, global trust focuses on two factors, i.e., the frequency of appeals against a vehicle and its reliability in cooperative scenarios. Specifically, RSUs obtain information about the number of appeals that a vehicle send to TA. This information reflects the historical behavior patterns of vehicle and credibility.

[5] Interaction frequency refers to how often vehicles communicate or engage with each other in the network.

Furthermore, once a message successfully arrives at its destination, the destination vehicle reports to TA, noting the vehicles that participated in the transmission of message. For instance, in the transmission path $V_1 \rightarrow V_2 \rightarrow V_3 \rightarrow V_4$, V_2 and V_3 participate in the process of message delivery, they directly facilitate the forwarding of the message. To prevent malicious vehicles from unjustly elevating their trust values by continuously creating new messages, source vehicle V_1 is not considered as promoting message delivery because V_1 is a requester. Then RSUs utilize the data obtained from TA to calculate the cooperative reliability of vehicle. The formula of global trust GT_{RSU_i,V_j} of V_j is shown as follows:

Case 1: For normal vehicles that have been appealed no more than once in a time window, the formula of GT_{RSU_i,V_j} is shown as follows:

$$GT_{RSU_i,V_j} = w_{GT}(1 - \frac{\sum_{t=1}^{t_n} \frac{t}{t_n} H^t_{V_j}}{\sum_{t=1}^{t_n} \frac{t}{t_n}} * \hat{w_h}) + (1 - w_{GT})CR_{V_j}, \tag{21}$$

where t_n represents the n-th time window. $H^t_{V_j}$ represents times V_j that have been appealed by other vehicles within each time window. $\hat{w_h}$ is the normalization factor, defined as $\hat{w_h} = \frac{1}{H_{max}}$, where H_{max} is the maximum number of appeals across all time windows. $w_{GT} = 0.5$ is the weighted importance between the number of times appealed and the cooperative reliability of V_j. CR_{V_j} represents the cooperative reliability of V_j calculated as:

$$CR_{V_i} = \frac{N^{jt}_{V_j}}{N^t_{all}}, \tag{22}$$

where $N^{jt}_{V_j}$ is the number of successful transmitted messages by V_j, and N^t_{all} is the total number of messages successfully transmitted in the whole network.

Case 2: For any vehicle that receives more than one appeal in the current time window ($H^{t_n}_{V_j}$), this indicates a consensus among multiple vehicles and heightened possibility of numerous attacks, then GT_{RSU_i,V_j} is set to 0.

Case 3: For vehicles being appealed multiple times across consecutive time windows ($H^{t_n}_{V_j}$ and $H^{t_n-1}_{V_j}$), this indicates persistent and multiple malicious behaviors, TA will add these vehicles to a blacklist. The trust value T_{V_j} (to be explained in Section III-G) is set to 0.

The aforementioned global trust calculation process in DCACA is illustrated in Algorithm 4.

Algorithm 4: Global Trust Calculation

```
Input: RSU $RSU_i$, Trustee $V_j$
Output: Global Trust $GT_{RSU_i,V_j}$
Case 1:
if $H^{t_n}_{V_j} \leq 1$ then
    Calculate $CR_{V_j} \leftarrow (N^{jt}_{V_j}, N^t_{all})$, Eq. (22);
    Calculate $GT_{RSU_i,V_j} \leftarrow (t_n, H^t_{V_j}, CR_{V_j})$, Eq. (21);
Case 2:
if $H^{t_n}_{V_j} > 1$ then
    $GT_{RSU_i,V_j} = 0$;
Case 3:
if $H^{t_n}_{V_j} > 1$ & $H^{t_n-1}_{V_j} > 1$ then
    Add $V_j$ to the blacklist;
    $T_{V_j} = 0$;
return $GT_{RSU_i,V_j}$
```

G. Multi-Trust Fusion

When trustor V_i interacts with trustee V_j, V_i calculates direct trust $DT^t_{V_i,V_j}$ and requests trust opinions about V_j from its neighbors V_k and RSUs (indirect trust IT_{V_i,V_j} and global trust GT_{RSU_i,V_j}). Due to malicious vehicles and RSUs may provide malicious trust opinions, V_i evaluates whether to adopt trust opinions based on the confidence level C_{E_i} of the entity E_i. If C_{E_i} is below a confidence threshold, V_i disregards its trust opinion, and utilizes a confidence-based weighted mechanism to integrate trust opinions from different sources (neighbors and RSUs).

Specifically, V_i assigns weights to $DT^t_{V_i,V_j}$, IT_{V_i,V_j}, and GT_{RSU_i,V_j} based on the confidence level of relevant entities to compute the trust value T_{V_j} of V_j. Its formula is as follows:

Case 1: If C_{RSU_i} exceeds or equal to C^{ts}_{RSU}, and there are trust opinions from neighbors (i.e., $C^{ts}_{RSU} \leq C_{RSU_i}$ & $IT_{V_i,V_j} \neq Null$), the formula of T_{V_j} is shown as follows:

$$T_{V_j} = \frac{C_{V_i} * DT^t_{V_i,V_j} + C^a_{V_k} * IT_{V_i,V_j} + C^a_{RSU_i} * GT_{V_i}}{C_{V_i} + C^a_{V_k} + C^a_{RSU_i}}, \tag{23}$$

Case 2: If C_{RSU_i} exceeds or equal to C^{ts}_{RSU}, and V_i does not have trust opinions from neighbors (i.e., $C^{ts}_{RSU} \leq C_{RSU_i}$ & $IT_{V_i,V_j} = Null$), the formula of T_{V_j} is shown as follows:

$$T_{V_j} = \frac{C_{V_i} * DT^t_{V_i,V_j} + C^a_{RSU_i} * GT_{V_i}}{C_{V_i} + C^a_{RSU_i}}, \tag{24}$$

Case 3: If C_{RSU_i} is below C^{ts}_{RSU}, and there are trust opinions from neighbors (i.e., $C^{ts}_{RSU} > C_{RSU_i}$ & $IT_{V_i,V_j} \neq Null$), the formula of T_{V_j} is shown as follows:

$$T_{V_j} = \frac{C_{V_i} * DT^t_{V_i,V_j} + C^a_{V_k} * IT_{V_i,V_j}}{C_{V_i} + C^a_{V_k}}, \tag{25}$$

Case 4: If C_{RSU_i} is below C^{ts}_{RSU}, and V_i does not have trust opinions from neighbors (i.e., $C^{ts}_{RSU} > C_{RSU_i}$ & $IT_{V_i,V_j} = Null$), the formula of T_{V_j} is shown as follows:

$$T_{V_j} = DT^t_{V_i,V_j}, \tag{26}$$

where $C^a_{V_k}$ refers to the average confidence level of V_k providing trust opinions. $C^a_{RSU_i}$ represents the average confidence level of RSUs providing trust opinions. These averages are applicable when the number of neighbors or RSUs providing opinions might be more than one (i.e., when the count of neighbors or RSUs within the communication range exceeds one). If $IT_{V_i,V_j} = Null$, it indicates V_i has no neighbors, or the confidence level of its neighbors is below the confidence threshold ($C_{V_k} < C^{ts}_V$), hence their trust opinions are not considered. $C^a_{V_k}$ and $C^a_{RSU_i}$ are calculated as follows:

$$C^a_{V_k} = \begin{cases} \frac{\sum_{k=1}^{len(Rec_{V_i})} C_{V_k}}{len(Rec_{V_i})}, & \text{if } len(Rec_{V_i}) \neq 0 \\ 0, & \text{if } len(Rec_{V_i}) = 0 \end{cases} \tag{27}$$

$$C^a_{RSU_i} = \begin{cases} \frac{\sum_{i=1}^{len(Rec_{RSU_i})} C_{RSU_i}}{len(Rec_{RSU_i})}, & \text{if } len(Rec_{RSU_i}) \neq 0 \\ 0, & \text{if } len(Rec_{RSU_i}) = 0 \end{cases} \tag{28}$$

where $len(Rec_{V_i})$ represents the number of neighbor set $RecV_i$ with $C_{V_k} > C^{ts}_{V}$. $len(Rec_{RSU_i})$ represent the number of RSUs with $C_{RSU_i} > C^{ts}_{RSU}$ providing trust opinions. After calculating trust value T_{V_j} of V_j, the specific trust decision as follows:

$$\begin{cases} Trustworthy, & \text{if } T_{V_j} \geq 0.5 \\ Untrustworthy, & \text{if } T_{V_j} < 0.5 \end{cases} \tag{29}$$

according to the literature [3], [30], the trust threshold of 0.5 is an established convention in the field of trust management, providing a balanced approach to classifying trustworthiness effectively. The aforementioned multi-trust fusion process in DCACA is illustrated in Algorithm 5.

Algorithm 5: Multi-Trust Fusion

```
Input: Direct trust $DT^t_{V_i,V_j}$, Indirect trust $IT_{V_i,V_j}$,
       Global trust $GT_{RSU_i,V_j}$ Trustee $V_j$
Output: Trust value $T_{V_j}$
if $len(Rec_{V_i}) \neq 0$ then
    Calculate $C^a_{V_k} \leftarrow (len(Rec_{V_i}))$, Eq. (27);
else
    $C^a_{V_k} = 0$;
if $len(Rec_{RSU_i}) \neq 0$ then
    Calculate $C^a_{RSU_i} \leftarrow (len(Rec_{RSU_i}))$, Eq. (28);
else
    $C^a_{RSU_i} = 0$;
Case 1:
if $C^{ts}_{RSU} \leq C_{RSU_i}$ & $IT_{V_i,V_j} \neq Null$ then
    $T_{V_j} = \frac{C_{V_i}*DT^t_{V_i,V_j}+C^a_{V_k}*IT_{V_i,V_j}+C^a_{RSU_i}*GT_{V_i}}{C_{V_i}+C^a_{V_k}+C^a_{RSU_i}}$,
    Eq. (23);
Case 2:
if $C^{ts}_{RSU} \leq C_{RSU_i}$ & $IT_{V_i,V_j} = Null$ then
    $T_{V_j} = \frac{C_{V_i}*DT^t_{V_i,V_j}+C^a_{RSU_i}*GT_{V_i}}{C_{V_i}+C^a_{RSU_i}}$, Eq. (24);
Case 3:
if $C^{ts}_{RSU} > C_{RSU_i}$ & $IT_{V_i,V_j} \neq Null$ then
    $T_{V_j} = \frac{C_{V_i}*DT^t_{V_i,V_j}+C^a_{V_k}*IT_{V_i,V_j}}{C_{V_i}+C^a_{V_k}}$, Eq. (25);
Case 4:
if $C^{ts}_{RSU} > C_{RSU_i}$ & $IT_{V_i,V_j} = Null$ then
    $T_{V_j} = DT^t_{V_i,V_j}$, Eq. (26);
Trust decision:
if $T_{V_j} \geq 0.5$ then
    $V_j$ is Trustworthy;
else
    $V_j$ is Untrustworthy;
return $T_{V_j}$
```

IV. Security and Complexity Analysis

A. Attack Model

Five main attack models are addressed by DCACA, where malicious vehicles typically have knowledge about each other. They are Simple Attack (SA), Black Hole Attack (BHA), Colluding Bad-Mouth Attack (C-BMA), On-Off Attack (OFA), and RSU Bad-Mouth Attack (R-BMA).

SA: Malicious vehicles compromise network communication by tampering with the content of messages in transmission.

BHA: Malicious vehicles deliberately drop all received messages, thereby sabotaging the message delivery process.

C-BMA: C-BMA is a combination of collusion and bad-mouth attacks [31], [32]. Malicious vehicles collaborate by providing favorable trust opinions for each other and unfavorable ones for normal vehicles.

OFA: Vehicles alternate between normal and malicious behaviors to avoid anomaly detection. Vehicles involved in OFAs alternate between conducting C-BMA and SA at different intervals, rendering their behavior patterns more unpredictable and challenging to discern.

R-BMA: Malicious RSUs give unfavorable trust opinions to vehicles with higher trust values and favorable trust opinions to those with lower trust values, distorting the overall trust evaluation process.

B. Security Analysis

1) Network Integrity: The combination of ACAM and dual-model consensus mechanisms enhances network integrity. It ensures trust decisions are based on data that is both verified and risk-assessed. ACAM uses historical behavior and interaction patterns to filter trust opinions, which are then processed through RCCM or MCM for consensus.

2) Dynamic Adaptability and Scalability: Trust evaluations change with the environment, as neighbors provide trust opinions while the trustor performs the calculations. The flexibility of neighbor sets, which can consist of different vehicles, ensures adaptability and scalability across different network sizes and densities.

3) Countermeasures of Attack Models: Through the anti-risk confidence allocation and dual-model consensus mechanisms, DCACA can effectively counter these attack models defined in Section IV-A.

SA Countermeasures: Three trust dimensions—direct, indirect, and global trust are employed to mitigate SA. Direct trust decreases for an SA vehicle as it transmits more altered messages, negatively influencing its transmission reliability (Eq.(15)). This reduced direct trust impacts indirect trust, which is derived from the trust evaluations of neighboring vehicles. Additionally, global trust is compromised when altered messages fail verification and do not reach their intended destinations, reducing the cooperative reliability (Eq.(22)) of vehicles. Consequently, the overall trust level of an SA vehicle decreases across all dimensions.

BHA Countermeasures: BHAs are identified by examining the cooperativeness of vehicles in the calculation of direct trust. BHA vehicles, exhibit significantly low cooperativeness (Eq.(16)), leading to a reduction in direct trust. Their prolonged non-interactive behavior increases their forgetting factors (Eq.(14)), further diminishing their trust levels. Additionally, since BHA vehicles do not contribute to successful message deliveries, their global trust levels are also adversely impacted, reflecting their non-cooperative behavior in the network.

C-BMA Countermeasures: To mitigate the effects of C-BHAs, which involve malicious vehicles providing disproportionately high trust ratings to collaborators and unfairly low ratings to others, DCACA employs the MCM and RCCM. These mechanisms scrutinize trust opinions by comparing them across the network. Vehicles exhibiting outlier trust opinions or biased evaluations are promptly identified and appealed. Repeated appeals lead to a significant decrease in their global trust values.

OFA Countermeasures: DCACA addresses OFAs by utilizing MCM and RCCM to detect inconsistent behavior patterns (alternate between normal and malicious behaviors). MCM and RCCM effectively identify vehicles that tamper with message contents and unjustly alter trust opinions to favor other malicious entities. Though transmission reliability initially flags these deviations, it alone cannot fully mitigate OFA risks. As OFA vehicles persist in their malicious behavior, their global trust values are decreased, ultimately leading to their blacklisting and trust value reset to 0.

R-BMA Countermeasures: To combat R-BMAs, where malicious RSUs provide skewed trust opinions to manipulate overall trust evaluations, DCACA deploys the MCM. It scrutinizes and compares trust opinions across multiple RSUs to detect anomalies. MCM effectively pinpoints RSUs issuing biased trust opinions and initiates appeals to the TA. As these malicious RSUs are repeatedly identified and appealed, their confidence levels diminish. When their confidence levels fall below the predefined threshold, their trust opinions are excluded from consideration in further trust evaluations.

C. *Complexity Analysis*

To analyze the time complexity of DCACA, we considered the computational workload required by its three core mechanisms: RCCM, MCM, and ACAM.

1) RCCM: The RCCM employs a streamlined process, utilizing specific computations for efficient consensus. The primary operations include collection and analysis of trust opinions, each involving basic arithmetic calculations, which are inherently $O(n)$ operations, where n is the number of responding vehicles. Thereby, the time complexity of RCCM is $O(n)$.

2) MCM: The time complexity analysis of the MCM involves examining the computational effort of each component within the Algorithm 1. Specifically, Eq.(5), (6), (7) calculate trust opinion change rates and communication density with a complexity of $O(1)$ each, due to their reliance on basic arithmetic operations on scalar values. Furthermore, Eq.(3) and (4) which compute consensus thresholds, also operate in $O(1)$ time. The algorithm itself processes each row of the trust opinion matrix, iterating through each opinion to count trust and distrust instances and to identify diverging opinions. With n rows and m columns in the matrix, the complexity for these operations totals $O(nm)$. Therefore, the overall time complexity of MCM is $O(nm)$.

3) ACAM: The time complexity of the ACAM (Algorithm 2) can be determined by analyzing the computational demands of each equation involved. Specifically, Eq.(9) calculates the likelihood of malicious behavior, which scales linearly with the number of time windows t_n thus having a complexity of $O(t_n)$. The impact assessment in Eq.(10) is a constant-time operation $O(1)$, whether for vehicles or RSUs. The confidence level computation in Eq.(11) is also a direct arithmetic operation, contributing $O(1)$ to the complexity.

The critical computational step involves sorting the confidence levels of vehicles and RSUs to compute the confidence thresholds utilzing Eq. (12) and (13). This sorting process typically has a complexity of $O(nlogn)$, where n is the number of entities (vehicles and RSUs). Since sorting is required to calculate the median and interquartile range, it becomes the dominant factor in the overall algorithm complexity. Therefore, the total time complexity of the ACAM is $O(nlogn)$.

V. Simulation Experiment and Results Analysis

A. *Simulation Setup*

The performance of DCACA is evaluated through simulation experiments in the opportunity network environment simulator [33]. The experimental scenario is modeled after the actual physical layout of Helsinki, as shown in Fig. 4. Due to the high cost associated with RSU deployment and the limited coverage range, the simulation scenario reflects a more developed urban center where RSUs are densely clustered and provide a broader coverage area. In contrast, in more remote areas, RSUs are distributed more sparsely and cover smaller areas [34]. Vehicles are set to navigate towards predetermined destinations along the shortest paths calculated using the Dijkstra algorithm [35]. Detailed parameters for the simulation experiments are listed in Table III [36], [37].

In relevant experiments, the performance of DCACA was compared with two other schemes: IWOT-V [14] and MEFPB [16]. IWOT-V employs a Bayesian approach to construct implicit networks and integrates local trust evaluations to derive global trust values, thereby distinguishing between malicious and benign carriers. MEFPB utilizes the D-S evidence theory to merge multi-dimensional indicators, such as direct trust, indirect trust, and message transmission paths to assess vehicle credibility. Additionally, MEFPB employs a path-backtracking mechanism, utilizing the transmission path of message to identify and track malicious behaviors.

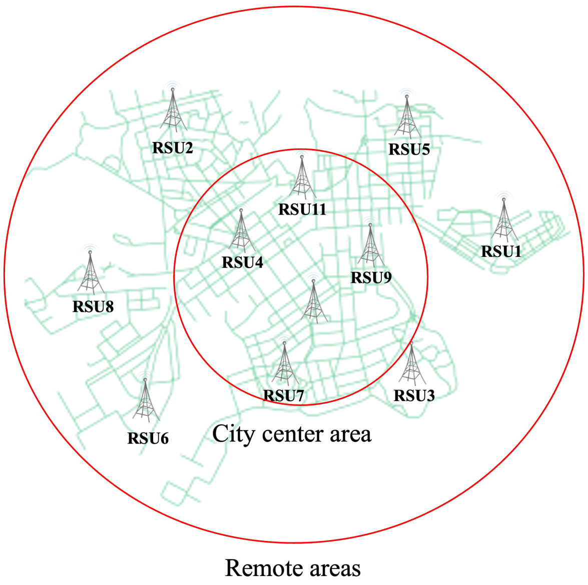


Fig. 4. Simulation scenario of Helsinki City.

Notably, all three schemes rely on the Spray and Wait routing protocol[6] [38].

TABLE III
SIMULATION PARAMENTERS.

Parameter	**Values**
Number of vehicles	100
Number of RSUs	11
Simulation time	4800s
Warm-up time	1200s
Simulation area	4500m × 3400m
Transmission range	300m
Transmission rate	900$kBps$
Buffer size	10MB

B. Evaluation Metric

The performance of DCACA relies on three main evaluation metrics: precision, recall, and F-measure [15].

Precision: Precision assesses the correctness of classification. It is defined as the ratio of samples correctly identified as positive to the total number of samples labeled as positive.

Recall: Recall concerns how many actual positive samples are correctly identified. It is defined as the ratio of samples correctly identified as positive to the total number of actual positive samples.

F-Measure: F-measure represents the harmonic mean of precision and recall, aiming to reflect the importance of precision and recall in a single measure. The formula for the F-measure is as follows:

$$\text{F-measure} = \frac{2 * (Precision * Recall)}{Precision + Recall}.$$

C. Impact of Four Attack Types

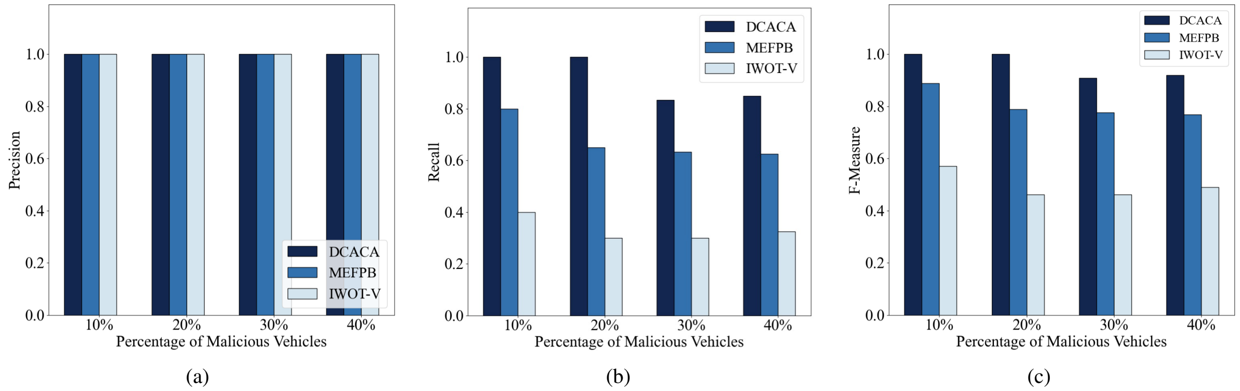
Firstly, Fig. 5(a) displays the precision performance. Under the four attack models, DCACA, MEFPB, and IWOT-V consistently achieve a 100% precision, indicating that none of these schemes generated any incorrect identifications of malicious activity. Secondly, Fig. 5(b) shows the recall performance. The recall of DCACA declined to 83.33% from 100% when the proportion of malicious vehicles reached 30%. Furthermore, the recall of MEFPB gradually decreased from 80% at 10% malicious vehicle proportion to 62.5%, while the performance of IWOT-V declined from 40% to 30% alongside the rise in malicious vehicle proportion from 10% to 30%. Thirdly, Fig. 5(c) reveals the overall performance of F-measure. DCACA maintained an F-measure above 90% within the range of 10% to 40% malicious vehicle proportion, especially reaching 91.89% at 40% malicious vehicle proportion. Moreover, the F-measure of MEFPB demonstrated a steady decline, dropping from 88.89% with a 10% malicious vehicle proportion to 76.92%. The F-measure of IWOT-V fluctuated slightly from 57.14% at 10% malicious vehicle proportion, falling to 49.06% at 40% malicious vehicle proportion.

The fundamental reason for the above differentiation is that both MEFPB and IWOT-V fall short in adequately addressing four types of attacks. Specifically, MEFPB demonstrates weaknesses in countering C-BMA, because its design did not account for this type of attack model. As a result, it fails to accurately identify vehicles involved in C-BMA, leading to a decrease in recall. Conversely, IWOT-V shows reduced effectiveness against C-BMA due to its lack of mechanisms for identifying and filtering malicious trust opinions. Moreover, its inability to counter OFA arises from the lack of a mechanism to track and penalize repeat attacks. It is noteworthy that the recall rate of IWOT-V experiences a slight increase when malicious vehicles constitute 40%. This occurrence is attributable to the presence of six BHA vehicles, six SA vehicles, seven C-BHA vehicles, and seven OFA vehicles at a 30% rate of malicious vehicles. When the proportion of malicious vehicles rises to 40%, the number of vehicles for each attack model reaches ten. The weaker performance of IWOT-V in addressing C-BHA and OFA leads to its recall rate being around 2.5% lower at a 30% malicious vehicle rate compared to 40%.

D. Impact of Vehicle counts

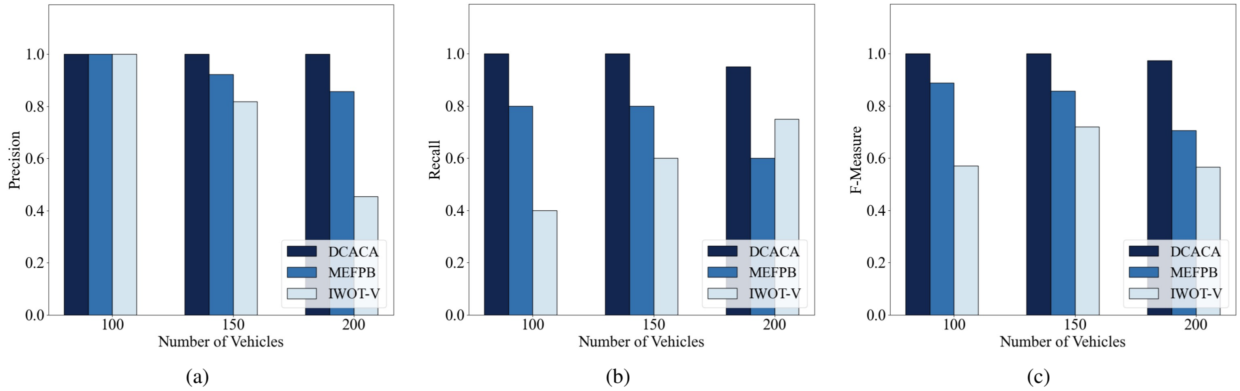
Firstly, Fig. 6(a) displays the precision performance at different vehicle counts. DCACA demonstrates excellent stability, maintaining 100% precision whether the vehicle count is 100, 150, or 200. In contrast, the precision of MEFPB drops from 100% to 85.71%, while IWOT-V significantly decreases from 100% to 45.45%, indicating a notable impact on the performance of MEFPB and IWOT-V. Secondly, Fig. 6(b)

[6] The ”Spray and Wait” routing protocol is a communication mechanism utilized in environments with frequent changes in network structure, particularly suited for the Internet of Vehicles. It enhances the reliability of transmission by creating multiple copies of a message in the network until one of the copies successfully reaches its destination.



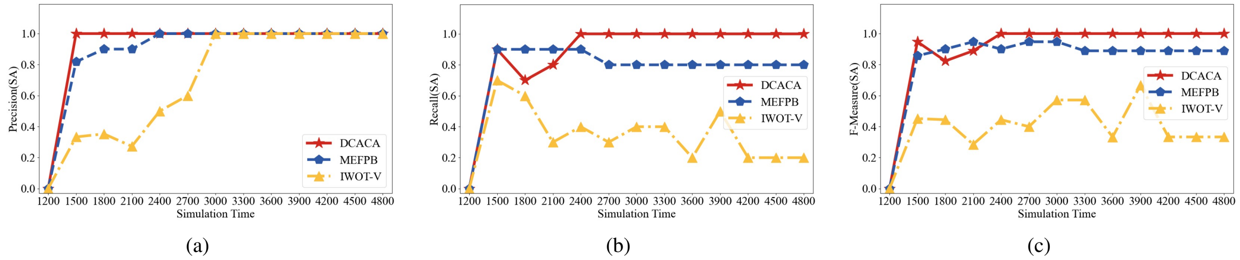
(a) (b) (c)

Fig. 5. DCACA, MEFPB, and IWOT-V impacted by four types of attacks (SA, BHA, C-BMA, and OFA). (a) Precision vs percentage of malicious vehicles. (b) Recall vs percentage of malicious vehicles. (c) F-measure vs percentage of malicious vehicles.



(a) (b) (c)

Fig. 6. DCACA, MEFPB, and IWOT-V impacted by vehicle counts (10% malicious vehicles). (a) Precision vs vehicles counts. (b) Recall vs vehicle counts. (c) F-measure vs vehicles counts.

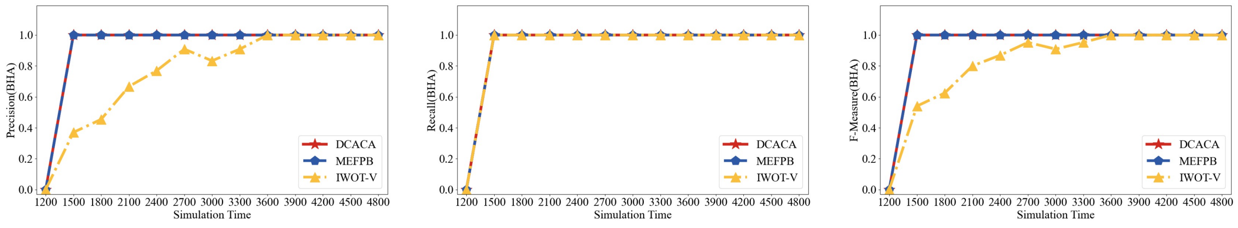


(a) (b) (c)

Fig. 7. DCACA, MEFPB, and IWOT-V impacted by SA (10% SA vehicles). (a) Precision vs time. (b) Recall vs time. (c) F-measure vs time.

shows the recall performance at different vehicle counts. The recall of DCACA slightly declines from 100% to 95%. In comparison, the recall of MEFPB stabilizes at 80% before ultimately falling to 60%, whereas the recall of IWOT-V rises from 40% to 75%. Thirdly, Fig. 6(c) presents the F-Measure performance at different vehicle counts. DCACA exhibits extremely high efficiency, maintaining a high level of 97.44% F-Measure even with 200 vehicles. In contrast, the F-Measure of MEFPB declines from 88.89% to 70.59%, and IWOT-V peaks at 72% with 150 vehicles but drops to 56.6% with 200 vehicles.

The fundamental reason for the above differentiation is that as the number of vehicles in the network increases, the volume of data that needs to be processed also increases, including both normal and malicious trust opinions. Consequently, the influence of BMA vehicles also grows, leading to a significant drop in the precision of both MEFPB and IWOT-V. Due to the increased influence of BMA vehicles, it becomes increasingly difficult to identify malicious behavior, resulting in a rise in the number of vehicles recalled (including normal vehicles). As the number of vehicles increases, the recall of IWOT-V improves because it identifies more actual malicious acts (true positives). However, this results in an increase in false positives, where normal vehicles are mistakenly marked as malicious. This leads to a decrease in precision as the proportion of true positives is diluted by a higher number of false positives.



(a)

(b)

(c)

Fig. 8. DCACA, MEFPB, and IWOT-V impacted by BHA (10% BHA vehicles). (a) Precision vs time. (b) Recall vs time. (c) F-measure vs time.

E. Impact of SA

Firstly, Fig. 7(a) illustrates the precision affected by SAs. DCACA rapidly achieves perfect precision of 100% at 1500*s*, maintaining 100% throughout all subsequent test points. Moreover, MEFPB reaches an precision of 81.82% at 1500*s*, stabilizing at 100% after 2100*s*, while the precision of IWOT-V reaches 50% at 2400*s* and maintains 100% from 2700*s*. Secondly, Fig. 7(b) demonstrates the recall influenced by SA. The recall of DCACA quickly escalates to 90% at the 1500*s*, reaching and sustaining 100% from 2400*s*. Furthermore, the recall of MEFPB remains relatively stable throughout the timeframe, maintaining 90% from 1500*s* but slightly decreasing to 80% from 2700*s*. The recall of IWOT-V exhibits more fluctuation, starting at 70% at 1500*s* and gradually declining, mostly stabilizing around 20% after 3600*s*. Thirdly, Fig. 7(c) depicts the F-measure under SA impact. DCACA swiftly climbs to 94.74% at 1500s and remains at 100% from 2400s. In addition, F-Measure of MEFPB is relatively stable throughout the period, peaking at 94.74% and later stabilizing around 88.89%. Furthermore, IWOT-V shows larger fluctuations with F-Measure peaking only at 66.67%, and most of the time ranging between 33.33% and 57.14%.

The fundamental reason is that DCACA starts trust evaluations only after completing the warm-up phase. Due to a lack of sufficient trust opinions from neighbors in the early stages, it initially fails to identify SA vehicles, leading to a slight decline in the recall. However, as vehicle interactions increase over time, more neighbors begin to provide trust opinions, allowing for gradually more accurate identification of SA vehicles. Consequently, the recall initially experiences a minor decrease, followed by an upward trend. Additionally, since IWOT-V is unable to verify the integrity of message contents, it struggles to identify SA vehicles, leading to a reduced recall. Moreover, the constant attempts by IWOT-V to recall SA vehicles, hindered by its incapacity to accurately classify them as malicious, lead to significant fluctuations in the recall.

F. Impact of BHA

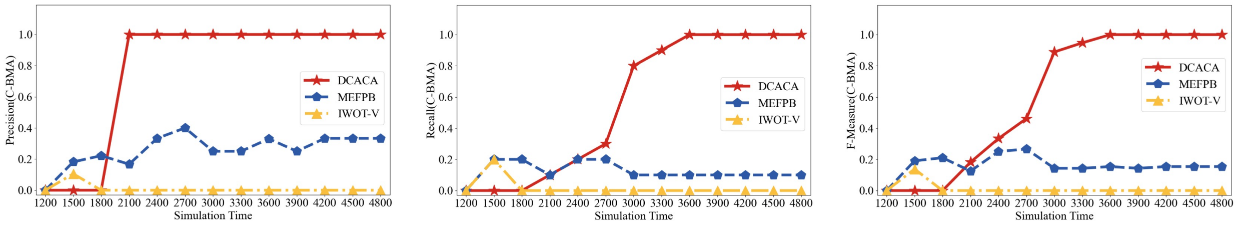
Firstly, Fig. 8(a) shows the precision performance impacted by BHA. Both DCACA and MEFPB achieve 100% precision starting from 1500*s*, consistently maintaining this standard throughout the entire time range. In contrast, the precision of IWOT-V gradually increases from 37.04% at 1500*s* and reaches and sustains 100% from 3900*s*. Secondly, Fig. 8(b) presents the recall performance under BHA impact. All three schemes reach 100% at 1500*s*, successfully identifying all BHA vehicles. Thirdly, Fig. 8(c) depicts the F-measure performance impacted by BHA. The DCACA and MEFPB schemes achieve a 100% F-measure from 1500*s*, continually maintaining this perfect performance, while the F-measure of IWOT-V gradually increases from 54.05% at 1500*s* and remains at 100% from 3600*s*.

The fundamental reason is that DCACA and MEFPB calculate direct trust based on vehicle cooperativeness, and utilize a forgetting factor to reduce the direct trust of BHA vehicles. This effectively counters BHA, maintaining all three metrics at 100% after the warm-up phase. Moreover, since IWOT-V updates trust values based on vehicle interactions, and BHA vehicles do not interact with others, the trust values of BHA cannot be updated, keeping the recall at 100% after the warm-up phase.

G. Impact of C-BMA

Firstly, Fig. 9(a) reveals the precision performance influenced by C-BMA. DCACA reaches 100% precision at 2100*s* and maintains this level at subsequent time points. In contrast, the precision of MEFPB shows considerable fluctuation, peaking at only 40%, while IWOT-V consistently demonstrates lower precision, persisting at 0% from 1800*s*. Secondly, Fig. 9(b) displays the recall performance under C-BMA. The recall of DCACA significantly increases from 2100*s*, rising from 10% to 90% at 3300*s*, and maintains 100% from 3600*s*. The recall of MEFPB is relatively stable but low throughout the period, staying between 10% and 20%. The recall of IWOT-V drops to 0% starting from 1500*s* and remains at this level for the entire duration. Thirdly, Fig. 9(c) depicts the F-measure performance impacted by C-BMA. The F-measure of DCACA substantially increases from 18.18% at 2100*s* to 94.74% at 3300*s* reaches and maintains 100% from 3600*s*. In comparison, the F-measure of MEFPB is consistently lower, staying around 14.29% to 25%, and the F-measure of IWOT-V remains low throughout, ranging from 0% to 13.79% starting from 1500*s*.

The fundamental reason is that DCACA begins trust evaluations only after completing the warm-up phase, meaning the trust opinion matrix remains unchanged during warm-up phase. This leads to an inability to reach consensus or make appeals at the beginning, resulting in a 0% recall. However, as time progresses and the trust matrix starts updating, consensus and appeals gradually occur, leading to an increase in recall.

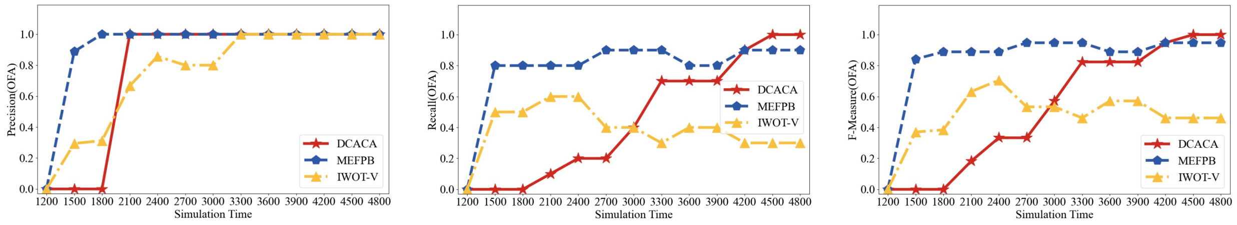


(a)

(b)

(c)

Fig. 9. DCACA, MEFPB, and IWOT-V impacted by C-BMA (10% C-BMA vehicles). (a) Precision vs time. (b) Recall vs time. (c) F-measure vs time.



(a)

(b)

(c)

Fig. 10. DCACA, MEFPB, and IWOT-V impacted by OFA (10% OFA vehicles). (a) Precision vs time. (b) Recall vs time. (c) F-measure vs time.

As a result, DCACA shows a trend of 0% recall between 1500-1800*s*, with an increase after 2100*s*. In contrast, due to MEFPB and IWOT-V do not possess mechanisms to counter C-BMA, normal vehicles are impacted, leading to reduced precision and recall. Consequently, MEFPB shows slight precision fluctuations, while the three metrics of IWOT-V are 0%.

H. Impact of OFA

Firstly, Fig. 10(a) shows the precision performance impacted by OFA. The precision of DCACA reaches and maintains a high level of 100% after 2100*s*, exhibiting significant improvement. In contrast, MEFPB consistently maintains 100% precision from 1500*s* onwards. Conversely, IWOT-V initially displays fluctuating performance, with precision gradually stabilizing between 66.67% to 85.71% from 2400*s* and eventually stabilizing at 100% after 3300*s*. Secondly, Fig. 10(b) displays the recall performance under OFA impact. The recall of DCACA significantly rises from 2100*s*, increasing from an initial 10% to 70% at 3300*s*, and ultimately reaching 100% at 4500*s*. In comparison, the recall of MEFPB is relatively stable throughout, fluctuating between 80% and 90%, while the recall of IWOT-V shows greater variability, gradually decreasing from 50% at 1500*s* to 30%. Thirdly, Fig. 10(c) depicts the F-measure performance affected by OFA. The F-measure of DCACA progressively increases from 18.18% at 2100*s* to 82.35% at 3300*s* ultimately reaches and maintains 100% at 4500*s*. The F-measure of MEFPB remains relatively stable throughout, mostly between 88.89% to 94.74%, while IWOT-V exhibits greater fluctuations, with its F-measure dropping to 46.15% in later stages.

The fundamental reason is that DCACA relies on a dual-model consensus mechanism to counter OFA, necessitating trust matrix updates post-warm-up phase to achieve consensus and appeals, leading to a 0% recall in the early simulation stages. However, as time progresses and the trust matrix begins updating, reaching consensus and filing appeals, the recall increases. In contrast, due to MEFPB employs path-backtracking and stringent penalty mechanisms, enabling it to detect and diminish trust value of malicious vehicles. Additionally, since MEFPB prohibits untrustworthy vehicles from providing trust opinions, resulting in increased precision and recall. Moreover, IWOT-V does not possess mechanisms to counter OFA, resulting in decreased recall.

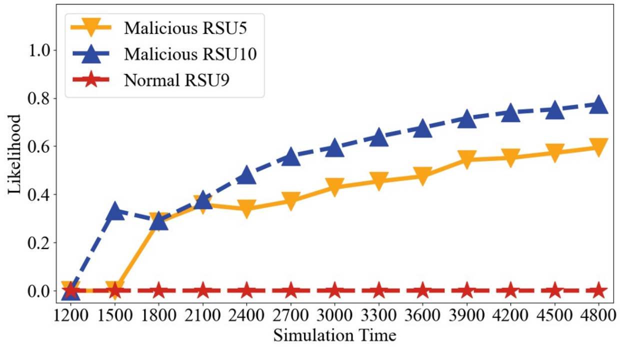


Fig. 11. Variation of $Likelihood_{RSU_i}$ under R-BMA impact.

I. Impact of R-BMA

Fig. 11 illustrates the changes in $Likelihood_{RSU_i}$ for RSU5, RSU9, and RSU10 when facing R-BMA, reflecting the frequency of their being appealed. In this scenario, RSU5 and RSU10 are set as malicious RSUs, while RSU9 is a normal RSU (specific locations shown in Fig. 4).

The $Likelihood_{RSU_5}$ of RSU5 gradually rises from 2100*s*, increasing from an initial 0.2857 to a final 0.5944. Concurrently, the $Likelihood_{RSU_{10}}$ of RSU10 grows more rapidly and substantially, starting from 0.3333 at 1500*s* and eventually reaching 0.775. In contrast, RSU9, as a normal RSU, maintains a $Likelihood_{RSU_9}$ of 0 throughout, indicating it was never appealed.

The fundamental reason for the above differentiation is that the varying traffic densities caused by the geographical locations of RSU5 and RSU10, affecting the efficiency of consensus and the frequency of appeals. RSU5, situated in a more remote location, only achieves consensus and is appealed by vehicles around $1800s$, leading to the increase in $Likelihood_{RSU_5}$. Meanwhile, RSU10, located in a denser traffic center, reaches consensus as early as $1500s$ and is ultimately appealed more frequently.

VI. Conclusion

This paper proposed an innovative dual-model consensus-based anti-risk confidence allocation trust management scheme in IoVs. Designed to effectively integrate trust opinions from RSUs, aiming to enhance the integrity of trust evaluations in IoVs. Particularly mindful of the potential presence of untrustworthy RSUs in IoVs, the DCACA implements an innovative dual-model consensus and anti-risk confidence allocation mechanism. The dual-model consensus mechanism identifies and appeals against entities providing malicious trust opinions. The anti-risk confidence allocation mechanism prioritizes filtering out trust opinions from malicious entities. In the final stage of trust fusion, utilizing the confidence level of entities as weighted factors, it effectively minimizes the undue influence of malicious entities on the results of trust evaluations. Moreover, the DCACA included a range of countermeasures, especially against vehicles frequently or continuously engaging in malicious behaviors, ensuring stringent punishment for such vehicles. Simulation experiment demonstrates that DCACA exhibits excellent efficacy and high security in ensuring network safety. In the future, incorporating dynamic adjustments based on real-time network conditions could further enhance its adaptability, allowing it to respond more effectively to evolving threats and changes in vehicle behavior.

References

[1] Z. Shen, Y. Wang, H. Wang, P. Liu, K. Liu, and J. Zhang, “Trust mechanism privacy protection scheme combining blockchain and multi-party evaluation,” *IEEE Transactions on Intelligent Vehicles*, pp. 1–10, 2024.

[2] C. Chen, W. Chenyu, C. Li, X. Ming, and P. Qingqi, “A v2v emergent message dissemination scheme for 6g-oriented vehicular networks,” *Chinese Journal of Electronics*, vol. 32, no. 6, pp. 1179–1191, 2023.

[3] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu, “Notrino: A novel hybrid trust management scheme for internet-of-vehicles,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9244–9257, 2021.

[4] Y. Cao, S. Li, C. Lv, D. Wang, H. Sun, J. Jiang, F. Meng, L. Xu, and X. Cheng, “Towards cyber security for low-carbon transportation: Overview, challenges and future directions,” *Renewable and Sustainable Energy Reviews*, vol. 183, p. 113401, 2023.

[5] L. Xujie, T. Jing, X. Yuan, and S. Ying, “Mobility-aware multi-task migration and offloading scheme for internet of vehicles,” *Chinese Journal of Electronics*, vol. 32, no. 6, pp. 1192–1202, 2023.

[6] W. Qiong, S. Shuai, W. Ziyang, F. Qiang, F. Pingyi, and Z. Cui, “Towards v2i age-aware fairness access: A dqn based intelligent vehicular node training and test method,” *Chinese Journal of Electronics*, vol. 32, no. 6, pp. 1230–1244, 2023.

[7] F. Azam, S. Kumar, K. Yadav, N. Priyadarshi, and S. Padmanaban, “An outline of the security challenges in vanet,” in *2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*. IEEE, 2020, pp. 1–6.

[8] S. Abbas, M. A. Talib, A. Ahmed, F. Khan, S. Ahmad, and D.-H. Kim, “Blockchain-based authentication in internet of vehicles: A survey,” *Sensors*, vol. 21, no. 23, p. 7927, 2021.

[9] S. Tangade, S. S. nvi, and P. Lorenz, “Decentralized and scalable privacy-preserving authentication scheme in vanets,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8647–8655, 2018.

[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, pp. 229–242, 2014.

[11] A. Alnasser, H. Sun, and J. Jiang, “Recommendation-based trust model for vehicle-to-everything (v2x),” *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 440–450, 2020.

[12] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, “Decentralized trust evaluation in vehicular internet of things,” *IEEE Access*, vol. 7, pp. 15 980–15 988, 2019.

[13] A. Bhargava and S. Verma, “Duel: Dempster uncertainty-based enhanced- trust level scheme for vanet,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 15 079–15 090, 2022.

[14] 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.

[15] 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.

[16] C. Cheong, Y. Song, Y. Cao, Y. Zhang, B. Cai, and Q. Ni, “Multidimensional trust evidence fusion and path-backtracking mechanism for trust management in vanets,” *IEEE Internet of Things Journal*, pp. 1–1, 2024.

[17] N. Ullah, X. Kong, Z. Ning, A. Tolba, M. Alrashoud, and F. Xia, “Emergency warning messages dissemination in vehicular social networks: A trust based scheme,” *Vehicular Communications*, vol. 22, p. 100199, 2020.

[18] 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.

[19] A. Lahbib, K. Toumi, A. Laouiti, A. Laube, and S. Martin, “Blockchain based trust management mechanism for iot,” in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1–8.

[20] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, “A scalable blockchain based trust management in vanet routing protocol,” *Journal of Parallel and Distributed Computing*, vol. 152, pp. 144–156, 2021.

[21] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, “Blockchain-based decentralized trust management in vehicular networks,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.

[22] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, “Blockchain-based adaptive trust management in internet of vehicles using smart contract,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3616–3630, 2021.

[23] Y. Wang, Z. Su, J. Li, N. Zhang, K. Zhang, K.-K. R. Choo, and Y. Liu, “Blockchain-based secure and cooperative private charging pile sharing services for vehicular networks,” *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 1857–1874, 2022.

[24] 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.

[25] L. Elgaroui, S. Pierre, and S. Chamberland, “New routing protocol for reliability to intelligent transportation communication,” *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 2281–2294, 2023.

[26] S. Zhang, R. He, Y. Xiao, and Y. Liu, “A three-factor based trust model for anonymous bacon message in vanets,” *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 11 304–11 317, 2023.

[27] M. Castro, B. Liskov *et al.*, “Practical byzantine fault tolerance,” in *OsDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[28] G. Stoneburner, A. Goguen, A. Feringa *et al.*, “Risk management guide for information technology systems,” *Nist special publication*, vol. 800, no. 30, pp. 800–30, 2002.

[29] C. Cheong, Y. Song, Y. Zhang, Y. Cao, C. Leow, and X. Wang, “A path-backtracking-based trust management scheme for vanets,” pp. 1–1, 2024.

[30] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "Trust in vehicles: Toward context-aware trust and attack resistance for the internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 9, pp. 9546–9560, 2023.

[31] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "Aatms: An anti-attack trust management scheme in vanet," *IEEE Access*, vol. 8, pp. 21 077–21 090, 2020.

[32] C. Zhang, W. Li, Y. Luo, and Y. Hu, "Ait: An ai-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3157–3169, 2021.

[33] 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.

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

[35] D. Cantone and S. Faro, "Two-levels-greedy: a generalization of dijkstra's shortest path algorithm," *Electronic Notes in Discrete Mathematics*, vol. 17, pp. 81–86, 2004.

[36] Y. Song, Y. Cao, K. Jiang, Y. Li, Y. Lai, and L. Wang, "Mp-vrcr: A multi-dimension and priority-based vehicle-road collaborative routing protocol," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10 797–10 812, 2023.

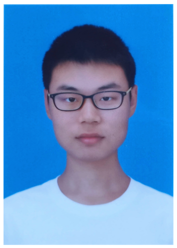
[37] Y. Wang, Y. Zhang, Y. Song, Y. Cao, L. Zhang, and X. Ren, "Appeal-based distributed trust management model in vanets concerning untrustworthy rsus," in *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, 2023, pp. 1–6.

[38] 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.

Chaklam Cheong holds a Bachelor's degree from Huazhong University of Science and Technology, China, in 2022. He is presently advancing his studies by working toward an M.S. degree in Cyberspace Security at Wuhan University, Wuhan, China. His main areas of research encompass Vehicular Networking, and Trust Management.

Yujie Song is pursuing his Ph.D. degree at the School of Cyber Science and Engineering, Wuhan University, China. He received his B. S. degree from Chengdu University of Information and Technology, in 2019, and M. S. degree from Wuhan University in 2023. His research interests include Internet of Vehicles, Networking Transmission, Space-ground Integrated Information Network, and Trust Management.

Yue Cao received the Ph.D. degree from the Institute for Communication Systems (ICS) formerly known as Centre for Communication Systems Research, University of Surrey, Guildford, U.K., in 2013. Further to his PhD study, he had conducted a Research Fellow with the University of Surrey, and academic faculty with Northumbria University, U.K., Lancaster University, U.K., and Beihang University, Beijing, China. He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His multidisciplinary research interest focuses on the theme of ITS, including cyber security, wireless network and service optimization. He has been also the Fellow of British Computer Society, Fellow of Royal Society of Arts and Fellow of Higher Education Academy.



Yuang Zhang was born in China in 2000. He is currently pursuing a M.Sc. degree at School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His research interests focus on the misbehavior detection in V2X applications.

Haoxiang Wang received the B.E. degree in information security from the Wuhan University, Wuhan, China, in 2023. He is currently pursuing the Ph.D. degree in computer engineering with the Wuhan University, with a focus on VANETs security and blockchain technology and its applications.

Qiang Ni is currently a Professor and the Head of the Communication Systems Group, School of Computing and Communications, Lancaster University, U.K. His research interests include the areas of future generation communications and networking, including green communications and networking, millimeter-wave wireless communications, cognitive radio network systems, non-orthogonal multiple access (NOMA), 5G and 6G, IoTs, cyber physical systems, AI and machine learning, and vehicular networks. He has authored or co-authored 300+ papers in these areas. He was an IEEE 802.11 Wireless Standard Working Group Voting Member and a contributor to various IEEE wireless standards.