Multidimensional Trust Evidence Fusion and Path-Backtracking Mechanism for Trust Management in VANETs

Cheong Chak Lam, Yujie Song, Yue Cao, *Senior Member, IEEE,* Yu'ang Zhang, Bo Cai, Qiang Ni *Senior Member, IEEE*

***Abstract*—With the development of Vehicular Ad-hoc Networks (VANETs), several data security challenges are revealed, such as data hijacking and interception. Although vehicles are authorized, malicious behaviors still be carried out. Security lapses may lead to potential accidents, which emphasizes the importance of laying a solid security foundation for VANETs. Thanks to the base security layer provided by cryptography technologies, security problems can be solved in VANETs to avoid accidents. However, trust management focuses on the analysis and identification of misbehavior, to ensure secure interactions among vehicles, and preserve data integrity against security issues. This paper explores trust assessments that consider the transmission path of message as a novel indicator, to provide a comprehensive and accurate trust assessment. We propose a Multidimensional trust Evidence Fusion and Path-Backtracking mechanism for trust management scheme (MEFPB) in VANETs. MEFPB integrates the multidimensional trust evidence fusion and path-backtracking mechanism. Specifically, MEFPB utilizes the Dempster-Shafer theory to fuse multi-dimensional indicators (direct trust, indirect trust, and transmission path of message) for evaluating the trustworthiness of vehicles. The direct and indirect trust are supplied by the message-sending vehicle and its neighbors (i.e., other vehicles). The transmission path of message is provided by roadside units. Furthermore, the path-backtracking mechanism identifies and traces malicious behaviors based on the transmission path of message. Moreover, extensive experiments demonstrate that our scheme significantly outperforms other baseline schemes, exhibiting a high malicious behavior detection rate within VANETs.**

***Index Terms*—VANETs, Trust Management, Path-Backtracking, Dempster-Shafer Theory.**

I. Introduction

IN the field of intelligent transportation systems, Vehicular Ad-hoc Networks (VANETs) are becoming increasingly significant such as enhancing traffic safety [1]. VANETs are crucial for infotainment, road safety, and optimizing driving assistance systems [2], [3]. Characterized by the high dynamics and exceptional scalabilities of VANETs [4], these networks exhibit pronounced features. However, these pronounced features present unprecedented challenges to the security of VANETs [5], [6]. Due to the dynamic and mobile nature of VANETs, many conventional network protocols struggle to meet the high standards required for real-time data transmission [7]. More importantly, the open structure of VANETs renders them vulnerable to potential adversaries, exposing to various internaland external attacks[1] [8], [9].

To ensure the security of VANETs, various schemes utilize traditional cryptographic techniques, leveraging key pairs (private and public key) and digital signatures for each vehicles. Although these methods are effective against external attacks, they are incapable of countering internal attacks [10]. To address the above problem, research endeavors have shifted to security schemes based on trust management [11], [12]. Receivers in these schemes receive broadcast messages only from senders with high reputations within VANETs [13]. As a result, vehicle filters potential malicious communications from senders with low reputations, ensuring the trust mechanism effectively counters internal attacks.

Previous trust management schemes primarily focus on direct and indirect trust assessments [14]–[16]. These schemes assess the direct trust of receivers by analyzing its historical records. Other than direct trust, the indirect trust is advanced in the trust evaluation, utilizing feedback from neighbors (vehicle) to enhance the accuracy of trust assessment. Numerous data concerning both the receiver and its neighbors is essential for accurate trust assessments. In instances of data absence, neighbors might find it challenging to provide indirect trust, thus rendering the trust assessment incomplete. Particularly, in scenarios where there was no prior interaction between the sender and receiver, the assessment results could be inaccurate. Moreover, these schemes frequently lacked a quick mechanism for detecting malicious behavior. Since of this delay, malicious vehicles could persistently disrupt the VANETs environment.

In addition, some trust management models emphasize the accuracy and validity of information shared among vehicles. Vehicles transmit two primary types of messages: event-based messages and emergency warnings. These trust models [17], [18] emphasize evaluating the authenticity of each event. However, during high network traffic scenarios, these models may lead to high data latency and data loss. Furthermore, when evidence is insufficient, the above trust models typically exhibit suboptimal performance in scenarios characterized by information scarcity.

Cheong C. L., Y. Song, Y. Cao (corresponding author), Y. Zhang and Bo Cai 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, caib@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 attacks in VANETs involve malicious vehicles transmitting misleading information, while external attacks typically consist of denial of service attempts by flooding vehicles with excessive data packets, disrupting regular communication.

Motivated by above, we propse a Multidimensional trust Evidence Fusion and Path-Backtracking mechanism for trust management scheme (MEFPB) in VANETs, aiming to enhance the security of message exchange within VANETs. Furthermore, MEFPB measures the credibility of vehicles based on three dimensions: direct trust, indirect trust, and transmission path of message. To address the uncertainty in VANETs due to information scarcity, the Dempster-Shafer Theory (DST) [19] is utilized. DST fusions the above three dimension indicators. Moreover, RoadSide Units (RSUs) utilize the path-backtracking mechanism to further ascertain the malicious behavior of vehicles, ensuring the integrity and security of VANETs. In summary, the major contributions of MEFPB are as follows:

- MEFPB considers the transmission path of message as a novel indicator for trust assessments. Most existing literature, such as the studies presented in [14]–[16], primarily focuses on assessments based on the message-sending vehicles and their neighbors. However, rather than solely relying on evaluations from these sources, MEFPB incorporates trust evidence provided by RSUs. It ensures a comprehensive trust assessment of vehicles, especially in scenarios with data insufficiency. Concurrently, MEFPB utilizes a novel path-backtracking mechanism, aiding in the rapid and accurate identification of malicious behavior within VANETs. Through the path-backtracking mechanism, MEFPB further incorporates multi-path analysis (Section III-E3) and path similarity (Section III-E4) , thereby markedly enhancing the accuracy in identifying malicious vehicles.
- In addition, MEFPB utilizes DST to address the uncertainty issues triggered by information scarcity scenarios. Utilizing the DST, MEFPB is able to effectively distinguish between malicious and regular vehicles. Additionally, it ensures an efficient fusion of trust evidence across three dimensions. MEFPB further classifies a trust evidence of vehicle into four trust levels to refine the trust assessment. After the trust evidence from the three dimensions is fused, different weights are assigned to four trust levels (Section III-A2), enhancing the accuracy in evaluating the trustworthiness of a vehicle.

The remainder of this paper is organized as follows. Related works are presented in Section II. In Section III, we describe the details of proposed MEFPB scheme and path-backtracking mechanism. Section IV details the analysis of security. Simulation experiments and result analysis are then introduced in Section V. Finally, Section VI concludes of this paper.

II. Related Works

A. Traditional Trust Management Models

Traditional trust management models are perceived as widely accepted frameworks. These models mainly focus on enhancing resistance to simple attacks without relying on complex data processing or statistical inference techniques [20]–[23]. Ahmad *et al.* [20] proposed a man-in-the-middle attack resistant trust model named MARINE to identifying malicious vehicles executing man-in-the-middle attacks. Chuprov *et al.* [21] proposed a scheme that identifies vehicles disseminating illicit information for optimizing traffic management at intersections. Three key parameters are considered: authenticity, reputation, and trust. The work [22] established an efficient trust inference mechanism for VANETs, especially in addressing black/grey hole attacks. Suo *et al.* [23] proposed a hybrid distributed-centralized system. In this system, the Trusted Authority (TA) collaborates with vehicles to counteract dishonest behaviors among them. The system assumes malicious vehicles can forge information and is equipped to handle such attacks. However, traditional trust models exhibit certain limitations. These models do not effectively counter various types of attacks, particularly demonstrating significant inadequacy when faced with more complex attacks.

B. Blockchain-based Trust Management Models

Due to the capabilities of blockchain technology in ensuring data integrity and decentralization, it has garnered increasing interest for trust management in VANETs [24]–[26]. Many believe that blockchain technology can address centralization, security, and privacy issues while managing the storage, tracking, and exchange of data. Hbaieb *et al.* [24] developed a two-layer blockchain architecture where vehicles can evaluate the trustworthiness of one another. Trust is formed through reputation and location metrics. In a different scheme, Yang *et al.* [25] proposed a blockchain-based decentralized trust management model, wherein vehicles evaluate messages received from other vehicles and notify the RSU of their assessment results. Subsequently, the RSU calculates entity-based trust values for vehicles and creates trust blocks. The work [26] introduced a trust management scheme reliant on blockchain technology, evaluating each vehicle based on the opinions of neighboring vehicles and the legitimacy of the information disseminated by them. Records of all messages are preserved within the blockchain and are utilized as evidence in computing the reputation score for each vehicle. However, due to the high cost of blockchain, this technology was not utilized in our scheme.

C. Bayesian Inference-Based Trust Models

Bayesian inference utilizes probability and statistics to articulate uncertainty in data modeling and inference [27]. Trust models are constructed utilizing Bayesian inference [18], [28], [29]. The work [28] amalgamated Bayesian methods with the PageRank algorithm to construct an implicit network. It differentiates malicious and regular vehicles by merging local trust evaluations into a global trust value. Alternatively, Fang *et al.* [29] presented a trust management framework utilizing Bayesian networks. Trust computation is predicated on weighted direct and indirect trust. Direct trust emanates from the trust scores generated through current and past direct interactions between two vehicles. Furthermore, indirect trust is predicated on the highest direct trust values allocated to the message-receiving vehicle by all neighboring vehicles. The work [18] focuses on trust node management in VANETs, proposing a composite trust for each node that includes direct trust and recommendation trust. The former is dynamically

computed through historical interaction records and Bayesian inference. The latter defines the trust and reputation of neighbor nodes. However, these models struggle to cope with on-off attacks that are challenging to detect in a short timeframe.

D. DST-Based Trust Models

DST is capable of merging data from various sources to address the uncertainty caused by data scarcity in VANETs [30]–[32]. The work [30] shows that DST is utilized for trust calculation to facilitate location search. Li and Song [31] introduced an anti-attack trust management scheme to evaluate the credibility of nodes and messages. Initially, the scheme gathers message data from multiple nodes, utilizes DST to merge multiple messages, and assesses their credibility. Subsequently, the scheme utilizes a collaborative filtering algorithm to calculate node credibility. However, the accuracy of this scheme declines when the number of nodes is low. In a different scheme, Bhargava and Verma [32] propose a trust model based on uncertainty utilizing DST to handle information scarcity in VANETs. This model aims to establish fresh trust opinions by integrating direct and indirect trust values of message-sending vehicles. Nonetheless, the performance metrics of this scheme are only applicable to specific scenarios and do not adapt well to all situations, especially in contexts facing black hole attack.

E. Motivation

Based on the above concerns, we adopted the path-backtracking mechanism and employed backtracking verification to identify malicious behaviors of vehicles. Additionally, we utilized the DST to fuse multi-dimensional indicators, ensuring accurate trust evaluation outcomes. During the trust assessment process, a direct trust assessment is initially conducted to ascertain the cooperativeness of vehicles within VANETs. In the phase of indirect trust assessment, only regular vehicles are allowed to provide indirect trust evidence, ensuring the authenticity of the trust evidence. Moreover, for vehicles failing the backtracking verification process, we designed different scenarios based on the number of verification failures. Malicious vehicles repeatedly launching attacks received severe penalties. Through the above assessment process, the MEFPB is capable of effectively countering multiple types of attacks, such as on-off and black hole attacks.

III. Trust Evaluation and Update of MEFPB

A. Preliminaries

1) System Architecture: As depicted in Fig. 1, the system primarily comprises vehicles, RSUs, and a TA. Vehicles can communicate with other vehicles and RSUs through wireless links. RSUs possess superior computational and storage capacities, also communicate amongst themselves. Meanwhile, the TA represents the entity with the highest administrative authority within the network. It can interact and communicate with RSUs through a secure channel.

2) Trust Mechanism: The trust evaluation is conducted in a distributed manner, with each vehicle evaluating the trustworthiness of its surrounding vehicles. The vehicle that sends a message is termed as trustor V_i. Its primary role is to evaluate another vehicle. The vehicle that receives the message is termed trustee V_j, becoming the entity under evaluation. In MEFPB, the trustworthiness of a vehicle is gauged using trust evidence. Trust evidence is divided into four discrete levels: High Trust (HT), Trust (T), Distrust (D), and High Distrust (HD). Each trust level corresponds to a subjective probability range [0, 1], referred to as mass value $m(A)$, where $A = \{HT, T, D, HD\}$. When a vehicle consistently exhibits positive behaviors, it is deemed trustworthy and given a high trust rating. Conversely, if vehicle exhibits malicious behaviors, it gets marked as distrusted. Especially after several negative behaviors, vehicle should be treated as highly distrusted. Through these four levels in MEFPB, aiding the system in more accurately identifying and determining the trustworthiness of V_j.

3) Bilinear Group Key and Signature Verification: In the bilinear group setting, let $(\mathbb{G}_1, \mathbb{G}_2)$ represent two groups. Both groups have a size $|\mathbb{G}_1| = |\mathbb{G}_2| = p$, where p is a specific prime number. Typically, g_1 is the generator of $\mathbb{G}_1$ while g_2 is the generator of $\mathbb{G}_2$. This setting incorporates a collision-resistant hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$.

A digital signature method for a message Msg_i is a set of algorithms $(KGen, Sign, Verify)$ with the following syntax:

1. **Key Generation:** Randomly select two numbers x and y from $\mathbb{Z}_p^*$. Calculate $u = g_2^x$ and $v = g_2^y$, where g_2 is an element of $\mathbb{G}_2$. The public key (g_1, g_2, u, v), and the private key (x, y) are generated.

2. **Signature:** Given the private key $(x, y) \in \mathbb{Z}_p^*$ and $Msg_i \in \mathbb{Z}_p^*$, choose a random number $r \in \mathbb{Z}_p^*$ and compute $\sigma = g_1^{1/(x+Msg_i+yr)} \in \mathbb{G}_1$. If $x + Msg_i + yr = 0$, then a different random number r needs to be selected for recalculation. The final signature is (σ, r).

3. **Verification:** Given the public key (g_1, g_2, u, v), message $Msg_i \in \mathbb{Z}_p^*$, and signature (σ, r) , verify if the following equation holds:

$$e(\sigma, u, g_2^{Msg_i}, v^r) = e(g_1, g_2).$$

If the equation is satisfied, the signature is deemed valid. Otherwise, it's considered invalid [33].

B. System Overview

RSUs are regarded as entities with absolute trustworthiness. Only the trustworthiness of vehicles remains ambiguous. The primary process of MEFPB can be divided into the following five stages:

1. **Digital Signature Initialization Stage:** The system employs $KGen(1^\tau)$, where τ represents a security parameter, to initialize the basic settings for the digital signature method. This ensures a reliable foundation for subsequent interactions and path-backtracking.

2. **Key Distribution Stage:** Each vehicle obtains a pair of public and private keys (pk_i, sk_i) from the system. The private key sk_i, is primarily used in vehicle-to-vehicle interactions. As

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3363755

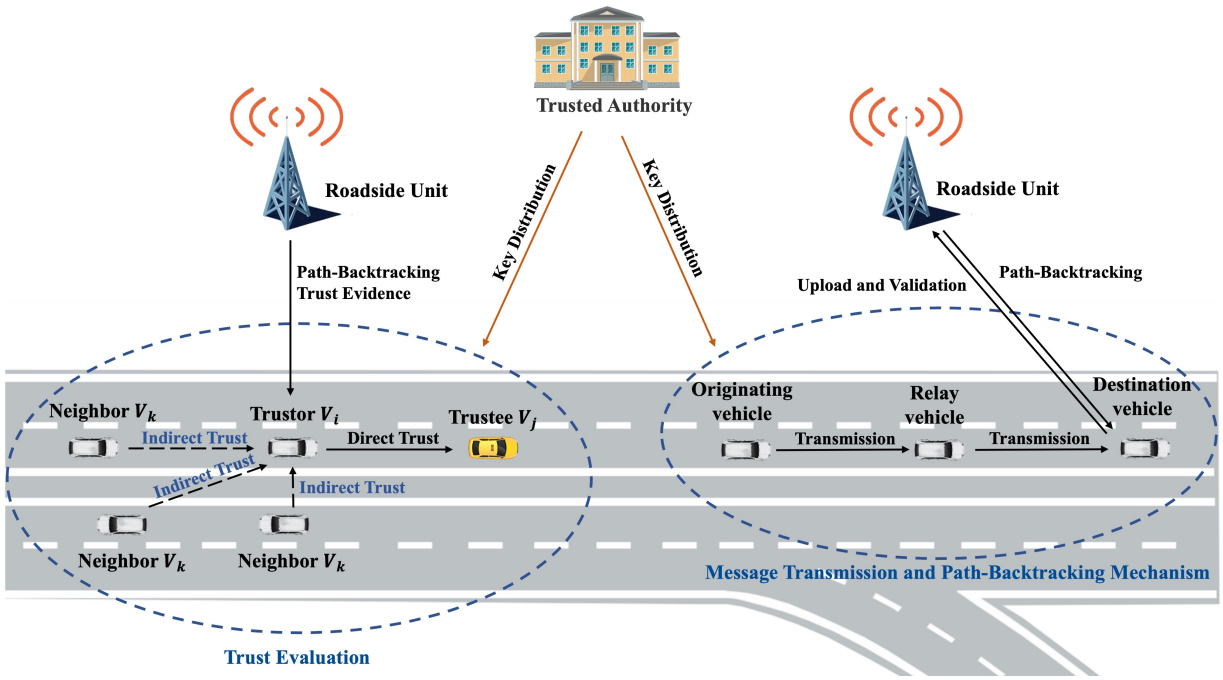


Fig. 1. The System Architecture of MEFPB.

for the public key pk_i, apart from being used in subsequent path-backtracking mechanisms for verification, it also verifies message signatures during the message registration stage.

3. **Message Registration and Verification:** When a vehicle generates a message, it first registers with the RSU, providing basic details of the message, e.g., source vehicle, destination vehicle, message content, and message ID. After generating the signature σ for Msg_i by utilizing $Sign(sk_i)$, σ and Msg_i is transmitted to the RSU for verification. The RSU then validates the signature by utilizing $Verify(pk_i)$. If the verification succeeds, the TA issues a certificate for that vehicle, serving as a trust root for future path-backtracking. Otherwise, no certificate is issued.

4. **Generation and Request of Trust Evidence:** When V_i sends a message to V_j, a direct trust assessment occurs, resulting in direct trust evidence $DT^t_{V_i,V_j}$. Simultaneously, for each neighbor V_k of V_i belonging to the neighbor set $Rec^t_{V_i}$, V_i collects indirect trust evidence $IT^t_{V_k,V_j}$ from V_k. To more comprehensively evaluate the trustworthiness of V_j, V_i also requests the path-backtracking trust evidence $PT^t_{V_j}$ from a nearby RSU.

5. **Trust Fusion:** V_i utilizes DST to merge the three types of evidences: $DT^t_{V_i,V_j}$, $IT^t_{V_k,V_j}$, and $PT^t_{V_j}$, forming an overall trust assessment for V_j. The consolidated trust evidence $CT^t_{V_i,V_j}$ becomes the benchmark for assessing the trustworthiness of V_j. Fig. 2 illustrates the relationships and computation process among all types of trust evidences.

TABLE I
NOTATIONS LIST.

Terms	Description
$A = \{HT, T, D, HD\}$	Trust levels
$\Theta = \{HT, T, D, HD\}$	Trust evidence
$m(A)$	Mass value of trust levels
$Rec^t_{V_i}$	Neighbor set of V_i
Msg_i	The ith message
t	The current time
$DT^t_{V_i,V_j}$	The direct trust evidence of V_j computed by V_i
$IT^t_{V_k,V_j}$	The indirect trust evidence of V_j gathered by V_k
$PT^t_{V_i}$	The path-backtracking evidence of i-th vehicle
$CT^t_{V_i,V_j}$	The consolidated trust evidence of V_j formed by V_i
$\lambda^t_{V_i,V_j}$	The forgetting factor from the view of V_i to V_j
$TS^{V_i}_{act}$	The interation threshold of V_i
N_{V_i,V_j}	The interation count between V_i and V_j
TS_{Coop}	The cooperation index threshold
C_{V_j}	The cooperation index of V_j
ver^i_s	The successful verification counter of i-th vehicle
ver^i_f	The malicious activity detection counter of i-th vehicle
φ_{V_i}	The growth factor of i-th vehicle
$S^{multi}_{V_i}$	The trust score of i-th vehicle based on multi-path analysis
TS_{multi}	The multi-path analysis trust score threshold
SIM	The average Jaccard similarity
$\Psi^t_{V_j}$	The trustworthiness of V_j

C. Direct Trust Evidence

The direct trust evidence for vehicles is based on three core elements: a forgetting function, the familiarity between vehicles, and the cooperativeness of vehicles. In essence, the forgetting function ensures that past behavioral records don't excessively influence the current trust evaluation of a vehicle. The familiarity between vehicles can impact the stability of trust. The cooperativeness assesses whether a vehicle is willing

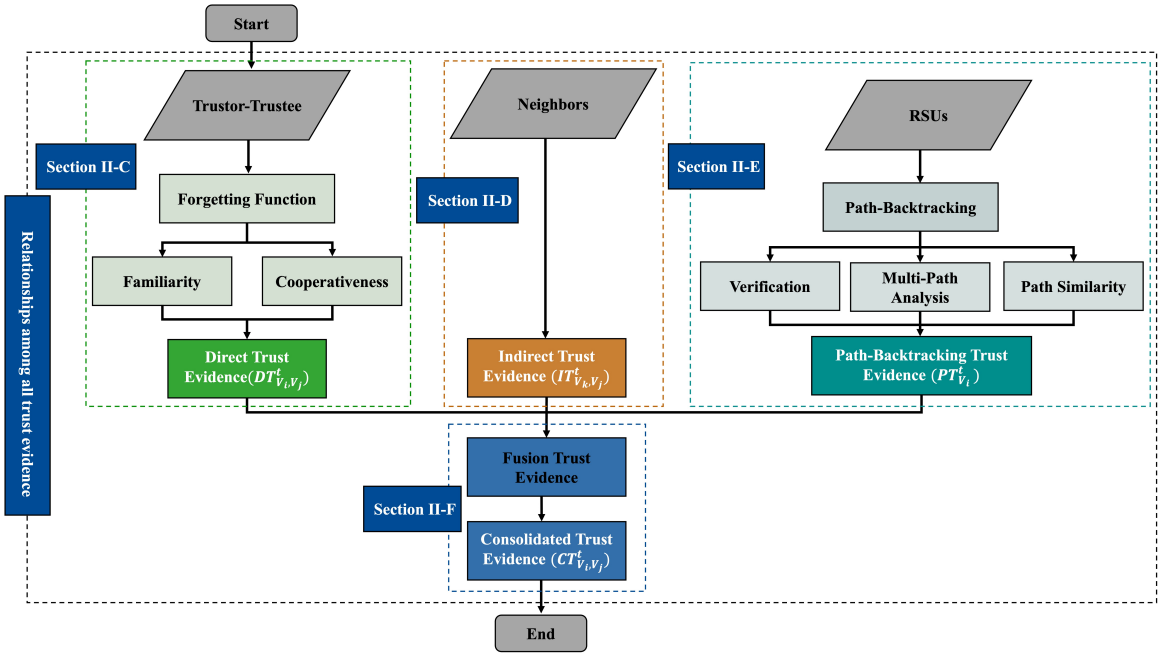


Fig. 2. The Relationships and Computaion Process Among All Types of Trust Evidences.

to share valuable information with other vehicles.

At the outset of system initialization, each vehicle is assigned an initial set of direct trust evidence, represented as $DT^t_{V_i,V_j} = \{0.2, 0.4, 0.3, 0.1\}$. Such evidence anchors on four distinct trust levels: the HT mass value $DT^t_{V_i,V_j} \cdot HT = 0.2$, the T mass value $DT^t_{V_i,V_j} \cdot T = 0.4$, the D mass value $DT^t_{V_i,V_j} \cdot D = 0.3$, and the HD mass value $DT^t_{V_i,V_j} \cdot HD = 0.1$. The initial configuration assigns a foundational trust level to each vehicle at system start-up, promoting early interactions and collaborations. As interactions increase, the initial mass values undergo modifications based on the distinct behaviors of individual vehicles.

1) Forgetting Function: The forgetting function serves as a mechanism to process outdated trust evidence. To address the issue of outdated trust evidence, a forgetting factor $\lambda^t_{V_i,V_j}$ is utilized to adjust the direct trust evidence from prior interactions. Specifically, if V_j has not engaged in any interactions for a certain period, its trustworthiness may reduce. The calculation formula for $\lambda^t_{V_i,V_j}$ is as follows:

$$\lambda^t_{V_i,V_j} = \frac{t - t_f}{z}, \tag{1}$$

where t represents the current time and the last time V_j sent a message at time t_f. The constant z represents a fixed constant employed to standardize the time difference, ensuring the consistency of the forgetting factor. Here, z = 300.

To effectively account for the diminishing impact of older interactions on trust evaluation, V_i employs a method based on the Fibonacci sequence to adjust $DT^{t-1}_{V_i,V_j}$ from the previous period $t-1$. According to Eq. (1), the modification made by the forgetting function to the direct trust evidence is represented as follows:

$$\begin{aligned} DT^t_{V_i,V_j} \cdot T &= DT^{t-1}_{V_i,v_j} \cdot T - \rho fib(\lambda^t_{V_i,v_j}), \\ DT^t_{V_i,V_j} \cdot D &= DT^{t-1}_{V_i,v_j} \cdot D + \rho fib(\lambda^t_{V_i,v_j}), \\ \rho &\in [0.05, 0.15], \end{aligned} \tag{2}$$

where ρ is a parameter utilized to control the rate of trust decline, ensuring trust is not lost too rapidly. Here, ρ = 0.05 is taken from [32]. Furtermore, the value of $\lambda^t_{V_i,V_j}$ increases, it leads to a reduction in $DT^t_{V_i,V_j} \cdot T$ and an increment in $DT^t_{V_i,V_j} \cdot D$.

In Eq. (2), the employment of Fibonacci sequence is inherently logical. As the sequence progresses, the ratio between consecutive terms grows. This mirrors the accelerated decline of trust with increasing time differences, ensuring that older interactions progressively hold less sway in evaluations.

2) Familiarity: Familiarity reflects the interaction frequency between V_i and V_j. Frequent and sustained interactions often imply that both parties have accumulated positive experiences from previous exchanges, encouraging further interactions. Therefore, if the historical interaction count exceeds a certain interaction threshold $TS^{V_i}_{act}$, it not only indicates that V_i deems V_j as reliable, but also signifies that V_j has demonstrated its trustworthiness and stability throughout these interactions. $TS^{V_i}_{act}$ is calculated as:

$$TS^{V_i}_{act} = \frac{\sum_{c=1}^{n} N^c_{V_i}}{n}, \tag{3}$$

where n denotes the number of vehicles that have interacted with V_i, and $N^c_{V_i}$ represents the interaction count for each vehicle that has interacted with V_i.

When the interaction count between V_i and V_j (N_{V_i,V_j}, elaborated in Table I) surpasses $TS^{V_i}_{act}$, it can be inferred that V_j possesses a higher level of credibility. However, if N_{V_i,V_j} falls below $TS^{V_i}_{act}$, elevation should not be done hastily the

distrust level of V_j. A lower interaction frequency doesn't necessarily signify distrust. It might be due to a lack of interaction opportunities or other external factors. Based on the above discussion and according to Eq. (3), the variation in the current $DT^t_{V_i,V_j}$ is depicted in the subsequent equations:

$$\begin{aligned} DT^t_{V_i,V_j} \cdot D &= DT^t_{V_i,V_j} \cdot D(1 - \frac{N_{V_i,V_j} - TS^{V_i}_{act}}{TS^{V_i}_{act}}), \\ DT^t_{V_i,V_j} \cdot T &= DT^t_{V_i,V_j} \cdot T + (\frac{N_{V_i,V_j} - TS^{V_i}_{act}}{TS^{V_i}_{act}} * DT^t_{V_i,V_j} \cdot D), \\ &\text{if } N_{V_i,V_j} > TS^{V_i}_{act}, \end{aligned} \tag{4}$$

where the multiplier $\frac{N_{V_i,V_j} - TS^{V_i}_{act}}{TS^{V_i}_{act}}$ scales down the distrust level of V_j based on how much N_{V_i,V_j} exceeds $TS^{V_i}_{act}$. By subtracting this ratio from 1, a resultant value is obtained that proportionally reduces distrust as interactions increase.

3) Cooperativeness: Cooperativeness denotes the willingness of V_j to cooperate with other vehicles. Vehicles with a high degree of cooperativeness actively share information within the network. Conversely, those leaning towards selfish behavior prefer to minimize resource consumption, avoiding sharing. When vehicles demonstrate significant cooperativeness, message propagates more efficiently throughout the network. The cooperation index of V_j is defined as C_{V_j} and can be calculated by the following formula:

$$C_{V_j} = \frac{F_{V_i,V_j}}{|v| - 1}, \tag{5}$$

where F_{V_i,V_j} represents the number of vehicles in the network that have received forwarded messages from both V_i and V_j. The symbol $|v|$ represents the total number of vehicles in the network.

To precisely evaluate the cooperative behavior of vehicles, MEFPB utilizes a dynamic cooperation index threshold TS_{coop}. The threshold is considering as the average cooperation index of all vehicles within the network. Utilizing an average value as the threshold ensures that the assessment criteria align with the current network environment. According to Eq. (5), The calculation formula for TS_{coop} is as follows:

$$TS_{Coop} = \frac{\sum_{i=1}^{|v|} C_{V_i}}{|v|}, \tag{6}$$

In MEFPB, vehicles will upload their C_{V_i} to the nearby RSU. Then, RSUs broadcasts it, allowing vehicle to obtain C_{V_i} from other vehicles.

By comparing the cooperation index of an individual vehicle to the network average, MEFPB can effectively gauge the cooperative behavior of that vehicle. If $C_{V_j} \geq TS_{Coop}$, it indicates that the cooperation level of this vehicle surpasses the network average. Under this condition, $DT^t_{V_i,V_j} \cdot T$ increases, while $DT^t_{V_i,V_j} \cdot D$ decreases. According to Eq. (5) and Eq. (6), $DT^t_{V_i,V_j}$ is updated as follows:

$$\begin{aligned} DT^t_{V_i,V_j} \cdot D &= DT^t_{V_i,V_j} \cdot D - (C_{V_j} - TS_{Coop}), \\ DT^t_{V_i,V_j} \cdot T &= DT^t_{V_i,V_j} \cdot T + (C_{V_j} - TS_{Coop}), \\ &\text{if } C_{V_j} \geq TS_{Coop}. \end{aligned} \tag{7}$$

Algorithm 1: Direct Trust Evidence Calculation

Input: Trustor V_i, Trustee V_j
Output: Direct trust evidence $DT^t_{V_i,V_j}$

$DT^t_{V_i,V_j} = DT^{t-1}_{V_i,V_j}$;
Phase I: Forgetting Function, Section III-C1
Calculate $\lambda^t_{V_i,V_j} \leftarrow (t, t_f)$, Eq. (1);
Calculate $DT^t_{V_i,V_j} \leftarrow (\lambda^t_{V_i,V_j})$, Eq. (2);
Phase II: Familiarity, Section III-C2
Calculate $TS^{V_i}_{act} \leftarrow (N^i_{V_i}, n)$, Eq. (3);
if $N_{V_i,V_j} > TS^{V_i}_{act}$ **then**
  Calculate $DT^t_{V_i,V_j} \leftarrow (TS^{V_i}_{act}, N_{V_i,V_j})$, Eq. (4);
Phase III: Cooperativeness, Section III-C3
Calculate $C_{V_j} \leftarrow (F_{V_i,V_j}, |v|)$, Eq. (5);
Calculate $TS_{Coop} \leftarrow (C_{V_i}, |v|)$, Eq. (6);
if $C_{V_j} \geq TS_{Coop}$ **then**
  Calculate $DT^t_{V_i,V_j} \leftarrow (C_{V_j}, TS_{Coop})$, Eq. (7);
else
  Calculate $DT^t_{V_i,V_j} \leftarrow (C_{V_j}, TS_{Coop})$, Eq. (8);
return $DT^t_{V_i,V_j}$;

Conversely, if $C_{V_j} < TS_{Coop}$ this signifies cooperation level of V_j is below the network average. As a result, $DT^t_{V_i,V_j} \cdot T$ decreases, and $DT^t_{V_i,V_j} \cdot D$ increases. According to Eq. (5) and Eq. (6), $DT^t_{V_i,V_j}$ adjusts as follows:

$$\begin{aligned} DT^t_{V_i,V_j} \cdot D &= DT^t_{V_i,V_j} \cdot D + (TS_{Coop} - C_{V_j}), \\ DT^t_{V_i,V_j} \cdot T &= DT^t_{V_i,V_j} \cdot T - (TS_{Coop} - C_{V_j}), \\ &\text{if } C_{V_j} < TS_{Coop}, \end{aligned} \tag{8}$$

Algorithm 1 displays the direct trust evidence calculation for MEFPB. The symbol $\leftarrow (*)$, where $*$ represents the input of data.

D. Indirect Trust Evidence

At t, V_i evaluates V_j based on $DT^{t-1}_{V_i,V_j}$ from $t-1$. Additionally, V_i receives $IT^t_{V_k,V_j}$ from its neighbor $V_k \in Rec^t_{V_i}$. Vehicles that are deemed trustworthy are the only ones qualified to provide trust evidence (the method for evaluating trustworthy and untrustworthy vehicles will be explained in Section III-F). The reason for this choice is crucial: untrustworthy vehicles can provide inaccurate messages due to sensor errors, malware, or deception. Thus, trust evidence is only accepted from confirmed reliable vehicles.

However, in realistic interaction environments, vehicles may have different interaction experiences with V_j, depending on factors like interaction time and nature. Although one vehicle might deem V_j as trustworthy based on their interactions, another vehicle might have a completely different experience and deem V_j as untrustworthy. This discrepancy complicates the process of assessing overall trustworthiness. Nonetheless, utilizing DST can effectively address these discrepancies. Specifically, the indirect trust $IT^t_{V_k,V_j}$ of V_j is based on $CT^{t-1}_{V_k,V_j}$ (Section III-F) of neighbor at $t-1$. Therefore, $IT^t_{V_k,V_j}$ can be expressed as follows:

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3363755

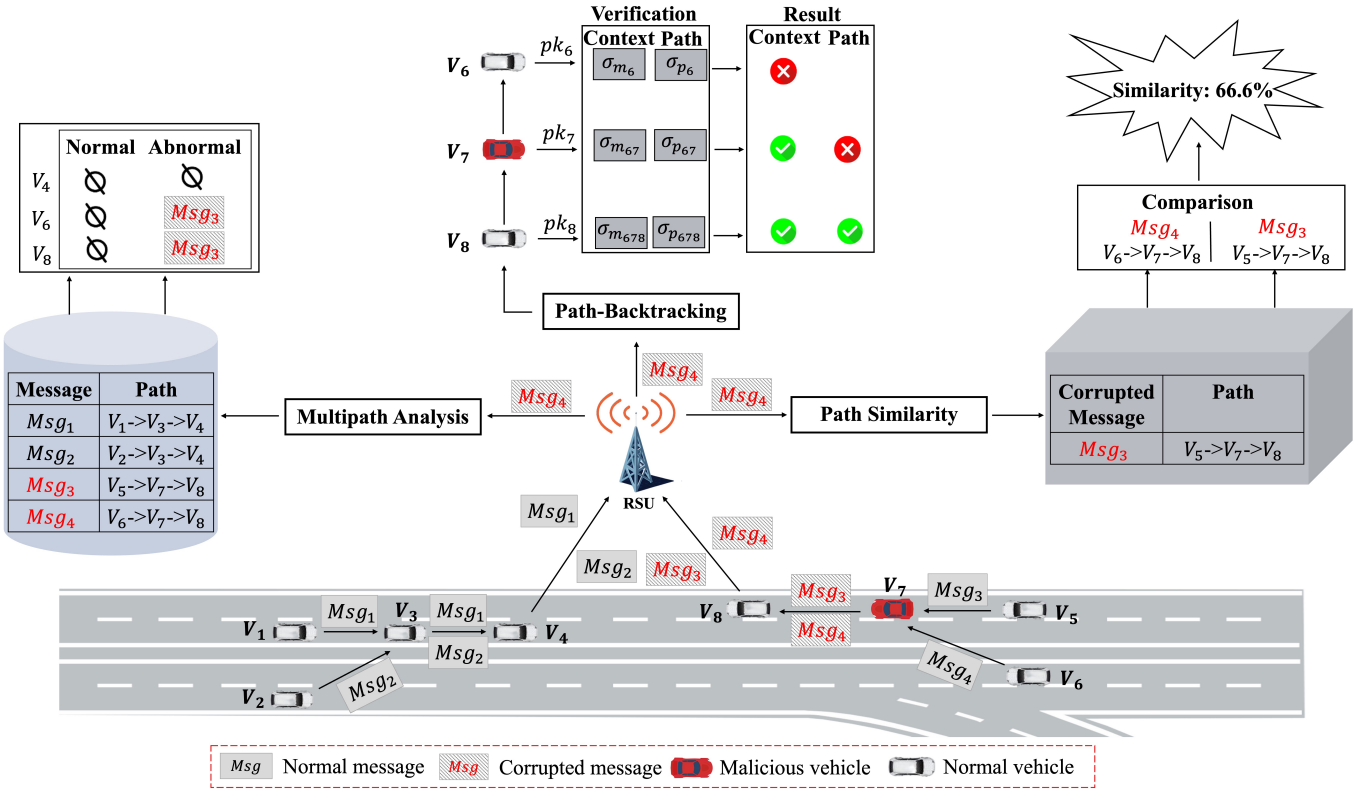


Fig. 3. The Path-Backtracking Evidence of MEFPB.

$$IT^{t}_{V_k,V_j} = CT^{t-1}_{V_k,V_j}. \tag{9}$$

E. Path-Backtracking Mechanism and Path-Backtracking Trust Evidence

RSUs play a pivotal role in the network by jointly maintaining and updating a path-backtracking trust evidence table. Within this table, $PT^{t}_{V_i}$ for all vehicles in the network are recorded. Consequently, whenever V_i seeks to assess the trustworthiness of V_j, RSUs provide V_j with the $PT^{t}_{V_j}$ related to V_j. By adopting this approach, RSUs offer the entire network a centralized trust reference, aiding vehicles in trust assessment from a routing path perspective.

1) Message Transmission and Path-Backtracking Mechanism: When the message is forwarded to the destination vehicle, the destination vehicle will upload the message to the RSU. The RSU will then initiate verification, identifying malicious vehicles through path backtracking and hop-by-hop validation.

Message Content Signature and Path-Backtracking Verification:

- **Message Content Signature:** As illustrated in Fig. 3, the vehicle V_6 utilizes $Sign(sk_6)$ to sign the message it sends, generating σ_{m_6}. After this signed message is initially relayed to the intermediary vehicle V_7, upon receipt, V_7 utilizes $Sign(sk_7)$ to sign again, producing $\sigma_{m_{67}}$. Then, this newly signed message, is delivered to the destination vehicle V_8. After receiving, V_8 utilizes $Sign(sk_8)$ to sign again, creating $\sigma_{m_{678}}$, and then forwards this final $\sigma_{m_{678}}$ to the nearly RSU.
- **Message Content Verification:** When the RSU receives $\sigma_{m_{678}}$ uploaded by V_8, it first utilizes $Verify(pk_8)$ for verification. If this verification is proven successful, the RSU then validates $\sigma_{m_{67}}$ from V_7, followed by σ_{m_6} from V_6. Since there be a mismatch between σ_{m_6} signature content from V_6 and the subsequent $\sigma_{m_{67}}$ signature content from V_7, it suggests unauthorized tampers were made to the message content by V_7. Then, the malicious activity detection counter ver^{i}_{f} for V_7, increase to $ver^{7}_{f} + 1$. Meanwhile, the successful verification counters ver^{i}_{s} for V_8 and V_6, increase respectively, becoming $ver^{8}_{s} + 1$ and $ver^{6}_{s} + 1$.

Message Path Signature and Path-Backtracking Verification:

- **Message Path Signature:** As illustrated in Fig. 3, V_6 functions as the source vehicle while V_8 acts as the destination vehicle. Upon transmitting a message, V_6 appends its ID into the transmission path of message. It then utilizes $Sign(sk_6)$ to sign this transmission path along with a certificate (granted by TA at the time of message registration), producing σ_{p_6} Following this, the message is relayed to V_7. Similarly, after receiving the message, both V_7 and V_8 incorporate their IDs into the transmission path of message. They generate $\sigma_{p_{67}}$ and $\sigma_{p_{678}}$ respectively, utilizing $Sign(sk_7)$ for the former and $Sign(sk_8)$ for the latter. Ultimately, V_8 uploads $\sigma_{p_{678}}$ to the nearly RSU.

- **Message Path Verification:** Initially, the RSU utilizes $Verify(pk_8)$ to verify σ_{p678}. If the verification be successful, the RSU subsequently verifies σ_{p67} and σ_{p6}, and finally examines the certificate given to V_6 by TA. All these measures are undertaken to ensure the authenticity and integrity of the message's transmission path. If during the verification, the RSU discovers that σ_{p_6} of V_6 cannot be verified, it implies that the transmission path of message signed by V_6 was tampered with by V_7. Consequently, V_7 is flagged for malicious behavior, and its malicious activity detection count ver_f^i activates and increases to $ver_7^i + 1$. In contrast, the successful verification counter ver_s^i for V_8, activates and increases to ver_s^8+1. Suppose it is eventually found that the certificate issued by the TA is absent. In that case, the transmission path of message is deemed as lacking a trusted root, indicating irregular actions by the source vehicle (such as deletion of a prior transmission path or transmission without registration). Consequently, its malicious behavior count increments by 1, and the successful verification counters for subsequent relay vehicles also increase by 1.

Forgiving Function: To ensure that vehicles are not subjected to prolonged and unfair penalties for minor, occasional missteps, the system incorporates a forgiveness function. Specifically, when a vehicle has not engaged in malicious behavior for a specified period, meaning its malicious behavior detection count ver_f^i remains unchanged, this count will automatically decrease. Such a mechanism can more fairly reflect the true behavioral status of a vehicle, preventing it from receiving excessive penalties for short-lived misbehaviors. Let t_{ver}^i represents the time when the vehicle's last malicious behavior was detected. If the difference between t_{ver}^i and t surpasses a fixed threshold μ, then ver_f^i will be decreased by 1 (i.e., $ver_f^i - 1$). Here, $\mu = 800$.

Considering our primary research focus is not on cryptography, the cryptographic techniques employed in the path-backtracking mechanism might not delve deeply into issues of signature anonymity and efficiency.

2) Path-Backtracking Verification: Considering the potential severe impact of tampering with messages, trust deduction for the tamperer should be more severe than discarding the message.

Case-1: For vehicles that tamper with messages but the number of malicious activity detection count does not exceed 1, the adjustment of the path-backtracking trust evidence is defined as:

$$\begin{gathered} PT_{V_i}^t \cdot HT = PT_{V_i}^{t-1} \cdot HT(1 - \frac{ver_f^i}{ver_s^i+ver_f^i}), \\ PT_{V_i}^t \cdot T = PT_{V_i}^{t-1} \cdot T(1 - \frac{ver_f^i}{ver_s^i+ver_f^i}), \\ PT_{V_i}^t \cdot HD = PT_{V_i}^{t-1} \cdot HD + \frac{ver_f^i}{ver_s^i+ver_f^i} \\ (PT_{V_i}^{t-1} \cdot HT + PT_{V_i}^{t-1} \cdot T), \\ \text{if } ver_f^i = 1 \ \& \ ver_s^i \geq 1. \end{gathered} \tag{10}$$

Case-2: For vehicles with frequent malicious behaviors, MEFPB employs a stricter penalty. Specifically, when their malicious activity detection count exceeds 1, the system reduces their path-backtracking trust evidence. The adjustment to the path-backtracking trust evidence is defined as:

$$\begin{gathered} PT_{V_i}^t \cdot D = PT_{V_i}^{t-1} \cdot D + PT_{V_i}^{t-1} \cdot T, \\ PT_{V_i}^t \cdot HD = PT_{V_i}^{t-1} \cdot HD + PT_{V_i}^{t-1} \cdot HT, \\ PT_{V_i}^t \cdot T = 0, \\ PT_{V_i}^t \cdot HT = 0, \\ \text{if } ver_f^i > 1. \end{gathered} \tag{11}$$

Case-3: For vehicles that consistently exhibit good behavior without any malicious behaviors, the system will increase their $PT_{V_i}^t \cdot T$ and $PT_{V_i}^t \cdot HT$ based on the growth factor φ_{V_i}. It's worth noting that φ_{V_i} is inversely proportional to $PT_{V_i}^{t-1} \cdot D$, and φ_{V_i} can be expressed as follow:

$$\varphi_{V_i} = 1 - PT_{V_i}^{t-1} \cdot D, \tag{12}$$

According to Eq. (12), for vehicles that pass verification without exhibiting malicious behavior, the adjustment to the path trust evidence is shown as follows:

$$\begin{gathered} PT_{v_i}^t \cdot D = PT_{v_i}^{t-1} \cdot D * \varphi_{V_i}, \\ PT_{v_i}^t \cdot T = PT_{v_i}^{t-1} \cdot T + \alpha * \Delta x, \\ PT_{v_i}^t \cdot HT = PT_{v_i}^{t-1} \cdot HT + \beta * \Delta x, \\ \text{if } ver_f^i = 0 \ \& \ ver_s^i > 0, \end{gathered} \tag{13}$$

where α and β represents two increaseing factors for controlling the rate of trust levels rise. Here, $\alpha = 4$, $\beta = 1$. The increaseing value Δx can be expressed as follow:

$$\Delta x = PT_{v_i}^{t-1} \cdot D * (1 - \varphi_{V_i})/(\alpha + \beta). \tag{14}$$

3) Multi-Path Analysis: As illustrated in Fig. 3, based on the comparison between the content of registered messages and received messages, Msg_4 is determined to have been tampered with. Specifically, the analysis result of registered messages shows that V_6 did not transmit other tampered messages and V_7 had previously transmitted a tampered Msg_3. Based on this, V_7 transmitted tampered messages twice in succession, whereas V_6 only did once. This indicates that V_7 has a higher likelihood of being a potential malicious vehicle. To quantitatively evaluate the behavior of vehicles based on the above consideration, a multi-path analysis-based trust score $S_{multi}^{V_i}$ is constructed and is shown as follows:

$$S_{multi}^{V_i} = \begin{cases} \frac{T_s^{V_i} - T_f^{V_i}}{T_s^{V_i} + T_f^{V_i}}, & \text{if } T_s^{V_i} > T_f^{V_i}, \\ 0, & \text{otherwise}, \end{cases} \tag{15}$$

where $T_s^{V_i}$ represents the number of V_i relayed normal messages, while $T_f^{V_i}$ indicates the number of V_i relayed tampered messages.

To distinguish vehicular behaviors, a threshold for the multi-path analysis trust score TS_{multi} is introduced. TS_{multi} is the average trust score of all vehicles. The formula is derived from Eq.(6), and can be expressed as follows:

$$TS_{multi} = \frac{\sum_{i=1}^{|v|} S_{multi}^{V_i}}{|v|}. \tag{16}$$

For vehicles with $S^{V_i}_{multi} \geq TS_{multi}$, it indicates that the vehicle has fewer instances of tampered transmissions and is less likely to be malicious. The vehicle should be rewarded, and the adjustment for path-backtracking trust evidence is as follows:

$$\begin{aligned} PT^t_{V_i} \cdot D &= PT^t_{V_i} \cdot D - (S^{V_i}_{multi} - TS_{multi}), \\ PT^t_{V_i} \cdot T &= PT^t_{V_i} \cdot T + (S^{V_i}_{multi} - TS_{multi}), \\ &\text{if } S^{V_i}_{multi} \geq TS_{multi}, \end{aligned} \tag{17}$$

Conversely, when $S^{V_i}_{multi} < TS_{multi}$, the adjustment for path-backtracking trust evidence is as follows:

$$\begin{aligned} PT^t_{V_i} \cdot D &= PT^t_{V_i} \cdot D + (TS_{multi} - S^{V_i}_{multi}), \\ PT^t_{V_i} \cdot T &= PT^t_{V_i} \cdot T - (TS_{multi} - S^{V_i}_{multi}), \\ &\text{if } S^{V_i}_{multi} < TS_{multi}. \end{aligned} \tag{18}$$

4) Path Similarity: As illustrated in Fig. 3, during the path backtracking process, if there are vehicles that fail verification, the transmission path of that message will be considered untrustworthy. For instance, if the path $P_1 = (V_5 \rightarrow V_7 \rightarrow V_8)$ is deemed untrustworthy, it will influence the assessment of current assess path. When current assess path is similar to a untrustworthy one, vehicles on that path will be set relatively lower trust values. Specifically, if the path $P_2 = (V_6 \rightarrow V_7 \rightarrow V_8)$ shows high similarity to P_1, vehicles on P_2 have high probabilities of malicious behaviors.

To calculate the similarity between two paths, a metric based on Jaccard similarity is adopted. The average Jaccard similarity SIM of the currently evaluated vehicle path with all known untrustworthy paths is expressed as follows:

$$SIM = \frac{\sum_{i=1}^{m} \frac{|M_i \cap P|}{|M_i \cup P|}}{m}, \tag{19}$$

where m represents the number of known untrustworthy paths, M_i stands for the *i*-th untrustworthy path, and P is the path currently being assessed. Furthemore, according to Eq. (19), when $SIM \geq 0.5$, it indicates that 50% or more of the vehicles in P_2 used to be identified as malicious. To reduce their influence of message delivery, the path-backtracking trust evidence of them is adjusted as follows:

$$\begin{aligned} PT^t_{V_i} \cdot T &= PT^t_{V_i} \cdot T * (1 - SIM), \\ PT^t_{V_i} \cdot D &= PT^t_{V_i} \cdot D + SIM * PT^t_{V_i} \cdot T, \\ &\text{if } SIM \geq 0.5, \end{aligned} \tag{20}$$

Otherwise, when $SIM < 0.5$, the adjustment formula is shown as follows:

$$\begin{aligned} PT^t_{V_i} \cdot D &= PT^t_{V_i} \cdot D * [1 - (0.5 - SIM)], \\ PT^t_{V_i} \cdot T &= PT^t_{V_i} \cdot T + (0.5 - SIM) * PT^t_{V_i} \cdot D, \\ &\text{if } SIM < 0.5. \end{aligned} \tag{21}$$

Based on the above consideration, the process of path-backtracking trust evidence update in MEFPB is shown in Algorithm 2.

Algorithm 2: Path Trust Evidence Update

Input: Message Msg, Message path Msg_{path}, Message-receiving vehicle V_j

if V_j *is destination vehicle* **then**
  Trigger path-backtracking mechanism to identify malicious vehicle $\leftarrow (Msg, Msg_{path})$;
  for *each vehicle* V *in* Msg_{path} **do**
    $PT^t_V = PT^{t-1}_V$;
    Phase I: Path-Backtracking Verification, Section III-E2
    if $ver^V_f > 0$ ***and*** $ver^V_s \geq 1$ **then**
      Update $PT^t_V \leftarrow (ver^V_f, ver^V_s)$, Eq. (10);
    else if $ver^V_f > 1$ **then**
      Update PT^t_V, Eq. (11);
    else if $ver^V_f = 0$ ***and*** $ver^V_s > 0$ **then**
      Update $PT^t_V \leftarrow (\varphi_V, \Delta x)$, Eq. (13);
    Phase II: Multi-Path Analysis, Section III-E3
    Calculate $S^V_{multi} \leftarrow (TN^V_s, TN^V_f)$, Eq. (15);
    Update $TS_{multi} \leftarrow (S^{V_i}_{multi}, |v|)$, Eq. (16);
    if $S^V_{multi} \geq TS_{multi}$ **then**
      Update $PT^t_V \leftarrow (S^V_{multi}, TS_{multi})$, Eq. (17);
    else
      Update $PT^t_V \leftarrow (S^V_{multi}, TS_{multi})$, Eq. (18);
    Phase III: Path Similarity, Section III-E4
    Calculate $SIM \leftarrow (m, M_i, Msg_{path})$, Eq. (19);
    if $SIM \geq 0.5$ **then**
      Update $PT^t_V \leftarrow (SIM)$, Eq. (20);
    else
      Update $PT^t_V \leftarrow (SIM)$, Eq. (21);

F. Trust Evidence Fusion

When trustor V_i interacts with trustee V_j, V_i generates direct trust evidence ($DT^t_{V_i,V_j}$) towards V_j. Then, V_i receives indirect trust evidence ($IT^t_{V_k,V_j}$) and path-backtracking trust evidence ($PT^t_{V_i}$) from V_k and RSUs, respectively. To handle these three different types of trust evidence for V_j, and conduct an accurate and comprehensive trust evaluation, V_i utilizes DST to fuse trust evidence from all dimensions. In MEFPB, trust evidence is defined as $\Theta = \{HT, T, D, HD\}$, where HT, T, D, HD are four trust levels of Θ, each mass value of trust levels $m(A) \in [0, 1]$, $m(\varnothing) = 0$ and $\sum_{A_q \in \Theta} = 1$. Based on this, A_q denotes any subset of Θ. For a given trust level A in the framework, its belief function $bel(A)$ [19] is expressed as follow:

$$bel(A) = \sum_{A_q \subseteq A} m(A_q). \tag{22}$$

Let $bel_{V_1}(A) = DT^t_{V_i,V_j}$ and $bel_{V_2}(A) = IT^t_{V_k,V_j}$, the orthogonal combination of trust evidence is expressed as follow:

$$bel(A) = bel_{V_1}(A) \oplus bel_{V_2}(A) = \frac{\sum_{q,r,A_q \cap A_r = A} m_{V_1}(A_q) m_{V_2}(A_r)}{\sum_{q,r,A_q \cap A_r \neq \varnothing} m_{V_1}(A_q) m_{V_2}(A_r)}. \quad (23)$$

Resulting from the Eq. (23) is a four-dimensional tuple ($\{HT, T, D, HD\}$) made up of the described trust level mass values. Furthermore, after fusing direct, indirect, and path-backtracking, all trust evidences, are consolidated into a comprehensive trust evidence $CT^t_{V_i,V_j}$ to evaluate the trustworthiness $\Psi^t_{V_j}$ of V_j. The $\Psi^t_{V_j}$ is constructed as follows:

$$\Psi^t_{V_j} = w_1(m_{V_j}(HT) - m_{V_j}(HD)) + w_2(m_{V_j}(T) - m_{V_j}(D)), \quad (24)$$

where w_1 and w_2 represent two weights of trustworthiness proportion, and they follow two limitations, i.e., $w_1 > w_2$, and $w_1 + w_2 = 1$. The reason for $w_1 > w_2$ is that the influence of HT and HD on vehicle trustworthiness is greater than that of T and D. $m_{V_j}(HT)$, $m_{V_j}(T)$, $m_{V_j}(D)$, and $m_{V_j}(HD)$ represent the four trust levels in $CT^t_{V_i,V_j}$. Based on this, the condition $\Psi^t_{V_j} \geq 0$ indicates that V_j has prevailing trustworthiness. Since the positive trust mass values (such as HT) exceed negative ones (such as HD), signifying a prevailing trustworthiness, and thus, V_j is seen as trustworthy. Otherwise, V_j is considered as malicious vehicle.

IV. Security Analysis

A. Attack Model

Four attack models are utilized to evaluate the performance of MEFPB, including simple (SA), black hole (BHA), path tampering (PTA), and on-off (OFA) attacks.

- **SA:** Through intercepting and altering messages, the vehicle can control the flow of message.
- **BHA:** The compromised vehicle drops all messages received from other vehicles.
- **PTA:** By hijacking and altering the message routing path, the vehicle can control the direction of message transmission and mislead RSUs.
- **OFA:** Malicious vehicles with the on-off attack model alternate their behaviors, oscillating between benign and malicious behaviors to avoid being detected.

B. Analysis

1) SA: Interception and alteration messages by malicious vehicles pose a significant threat to the integrity of message flow. In MEFPB, the path-backtracking mechanism is utilized to counter SAs. Whenever a vehicle dispatches a message, it signs the message using its private key and producing a corresponding signature.

Upon receiving a signed message from a vehicle, RSUs undertake a series of validation steps (path-backtracking and hop-by-hop validation). Verification is conducted by the RSU utilizing the public key of the target vehicle. Futhermore, path-backtracking and hop-by-hop validation ensure the integrity of messages and authenticity during message transmission. If any unauthorized alterations be detected in this process, the RSU can pinpoint the malicious vehicle responsible for the tampers.

2) BHA: MEFPB integrates three core concepts: forgetting function, familiarity, and cooperativeness, to counter black hole attacks. If other vehicles interact with this black hole vehicle and the vehicle stops transmitting data after a certain period, the trustworthiness of the black hole vehicle should decline. The detail is shown as follows:

Fristly, the forgetting function offers a robust mechanism. By utilizing the Fibonacci sequence, the impact of older interactions with the black hole vehicle diminishes, to detect BHA model vehicles.

Secondly, familiarity describes the frequency of interactions between vehicles. Initially, black hole vehicles might behave normally to build trust. However, their consistent message discarding can make consecutive interactions abnormal. When interactions with such a vehicle stay below a set threshold, its trustworthiness decreases.

Thirdly, cooperativeness serves as an indicator of the efficacy with which a vehicle interacts with others. Since black hole attackers discard incoming messages, their cooperation is notably below the network average. If the cooperation index of a vehicle drops significantly below this average, its trustworthiness receives a downward adjustment.

3) PTA: Ensuring the authenticity of a message path is crucial. It becomes a significant threat, especially when attackers attempt to hijack and alter the message path, directing the flow of message and misleading RSUs. Message path signing and path-backtracking mechanism are utilized to counter this threat. Specifically, message path signing permits each vehicle to append its identifier during the transmission process, ensuring that each vehicle on the message path is known and verifiable. As a message transmits from one vehicle to another, the latter appends its ID to the message path and signs the message path utilizing its private key. Then, when a message reaches its destination, it bears a clear record of the entire transmission path, complete with digital signatures for each step.

In addition, message path-backtracking validation provides RSUs with a means to ascertain the authenticity and integrity of received messages. Initially, the RSU verifies the final signature and traces back the entire path, to ensure each signature remains valid. Such a layered validation process substantially raises the difficulty for attackers to successfully tamper with a message. If any signature fails validation during this procedure, it becomes evident that the message was altered by another vehicle prior to reaching the one with the failed signature. Path-backtracking mechanism not only alerts the RSU about the unreliability of message, but it also identifies the specific vehicle involved in the malicious activity.

4) OFA: To counter OFAs, a defense strategy is designed, and its core idea is to impose amplified penalties on vehicles that launch repeated attacks. Specifically, by monitoring the number of validation failures of a vehicle, an assessment can be made. If validation failures of a vehicle exceed once, it indicates persistent or frequent malicious behaviors, warranting more stringent penalties. Substantial adjustments imply that even if the vehicle exhibits commendable behavior at times, its malicious actions will have long-lasting repercussions.

C. Complementary Research Avenues: Trust Models and Privacy Concerns

Our research in the realm of trust management for vehicle networks complements studies focused on vehicle privacy. However, a deliberate decision was made to concentrate on trust models due to the relative maturity of privacy solutions in this domain. The field of privacy solutions in vehicular networks has reached a considerable level of development, with a wealth of established protocols and methodologies already in place. This maturity provides a stable foundation upon which we can build, allowing us to direct our efforts towards areas that present more novel challenges and opportunities for innovation, such as trust models.

By combining the proven strengths of privacy solutions, such as their robustness and reliability, with the adaptive and responsive capabilities of trust management systems, we aim to achieve a more secure and efficient vehicular network. This approach allows us to harness the advantages of each domain: the privacy solutions provide a stable and trusted backdrop, while the focus on trust management addresses the immediate and practical challenges of security and reliability in dynamic VANET environments. In doing so, we have built upon the foundational privacy methodologies established in works such as [34] and [35], leveraging their insights to ensure our trust model operates within a secure privacy framework.

Looking ahead, our future endeavors aim to explore lightweight and holistic methods that seamlessly integrate privacy concerns with trust models. This will involve devising strategies that not only maintain the robustness of trust management but also ensure the comprehensive protection of privacy within vehicular networks. Such an integrated approach is pivotal in advancing the field, aligning with the ongoing efforts to achieve a balanced and secure vehicular communication system.

V. Simulation Experiment and Results Analysis

A. Simulation Setup

The performance of MEFPB is evaluated by simulation experiments based on the Opportunity Network Environment simulator [36]. The experimental scenario is modeled after the physical layout of Helsinki city, as shown in Fig. 4. Furthermore, the vehicles navigate towards predetermined endpoints by following the shortest path computed by the Dijkstra algorithm [37]. Detailed parameters of the simulation are listed in Table II [38], [39].

In the conducted experiments, the MEFPB was compared with the IWOT-V [28], DUEL [32], and TECS [40] schemes. Specifically, IWOT-V utilizes the Bayesian approach to construct an implicit network. By consolidating local trust evaluations, it derives a global trust value to differentiate between malicious and benign vehicles. DUEL utilizes DST to integrate the direct and indirect trust values of message-sending vehicles. During this integration, DUEL incorporates punishment function, a forgetting function, rewarding factor, and importance factor based on uncertainty. In TECS, each RSU collects local data from nearby vehicles and derives aggregated weights from the centrality of feature vectors in the local trust network and social metrics. Vehicles are considered malicious if their trust values fall below a preset threshold. Notably, the four models rely on the spray and wait routing protocols[2] [41].

TABLE II
Simulation Paramenters.

Parameter	Values
Number of vehicles	100
Number of RSUs	12
Simulation time	1800s
Warm-up time	400s
Simulation area	4500m × 3400m
Transmission range	100m
Transmission rate	900$kBps$
Buffer size	10MB

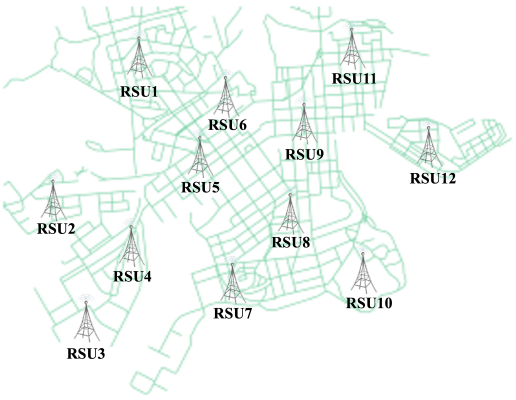


Fig. 4. Simulation scenario of Helsinki City.

B. Evaluation Metric

The performance of MEFPB relies on three primary evaluation metrics: precision, recall, and F-measure [42].

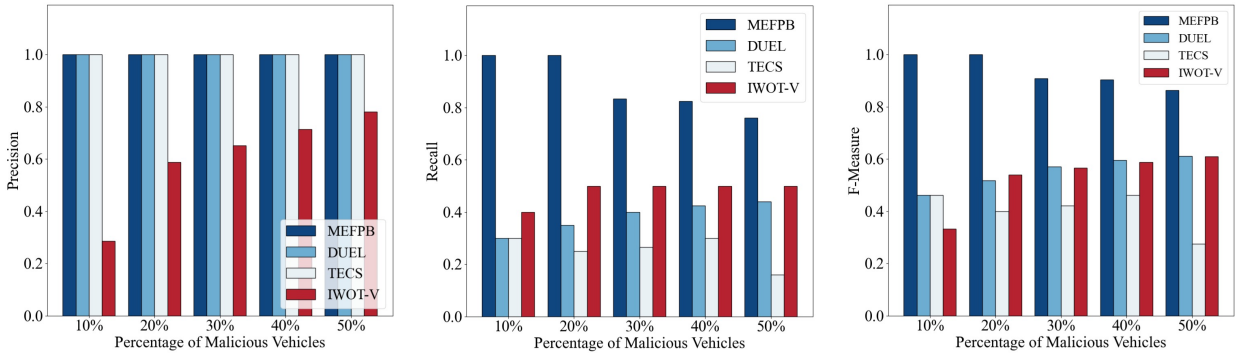
Precision: Precision evaluates the correctness of classification. It's defined as the ratio of samples correctly identified as positive to the total number of samples labeled as positive.

Recall: Recall addresses how many of the actual positive samples are correctly identified. It's defined as the ratio of samples correctly recognized as positive to the entire count of actual positive samples.

F-measure: F-measure represents the harmonic mean of precision and recall, aiming to reflect the significance of both metrics in a singular measure. The formula for F-measure is shown as follows:

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

[2]The Spray and Wait routing protocol is an efficient way to send messages in intermittently connected networks. It works by sending multiple copies of a message and opportunistically forwarding them through the network until the message is received by the destination node.



(a) (b) (c)

Fig. 5. MEFPB, DUEL, IWOT-V, and TECS impacted by four types of attacks. (a) Precision vs percentage of malicious vehicles. (b) Recall vs percentage of malicious vehicles. (c) F-measure vs percentage of malicious vehicles.

C. Impact of Four Attack Types

Fig. 5 illustrates the performance of precision, recall, and F-measure for the MEFPB, DUEL, IWOT-V, and TECS schemes, given varying percentages of malicious vehicles (with an equal distribution across the four attack models).

Firstly, Fig. 5(a) illustrates the precision performance. Both MEFPB, DUEL and TECS achieve a 100% precision rate, with the accuracy of MEFPB attributed to its path-backtracking mechanism. However, the precision of IWOT-V increases as the percentage of malicious vehicles rises but never hits 100%. Secondly, Fig. 5(b) depicts the recall performance. MEFPB started strong at 100% for lower malicious percentages but experienced a mild drop as the malicious percentages grew. Meanwhile, DUEL showed a steady rise, IWOT-V hovered around 40-50%, and TECS consistently maintains around 25%-30%, until there is a notable decline when malicious vehicles reach 50%. Thirdly, Fig. 5(c) shows the overall performance of F-measure. MEFPB consistently outshined, maintaining high scores even with increasing malicious rates. However, DUEL and IWOT-V exhibited growth but remained below the performance of MEFPB throughout. Meanwhile, TECS stays around 40% until there is a significant drop when malicious vehicles reach 50%.

The fundamental reason for the above differentiation is that both DUEL, IWOT-V, and TECS cannot fully counteract the four types of attacks. Specifically, DUEL encounters difficulties when confronting BHAs and PTAs. Similarly, IWOT-V is less effective against OFAs and PTAs. As for TECS, it struggles with effectively addressing BHAs and PTAs and shows limited capability in handling OFAs, leading to their reduced performance. The precision of IWOT-V rises with an increase in the percentage of malicious vehicles, due to its higher false positive rate, which leads to more vehicles being recalled. Consequently, the number of malicious vehicles among those recalled also increases, enhancing the precision of the scheme. Regarding the recall rate of IWOT-V, it is 40% at a malicious vehicle ratio of 10%, with a slight rise to 50% at higher percentages. This modest increase is because, out of 10 malicious vehicles, there are 3 PTA vehicles, 3 OFA vehicles, 2 SA vehicles, and 2 BHA vehicles. As IWOT-V is unable to effectively address the PTA and OFA issues, its recall rate is capped at 40%.

Additionally, DUEL shows a slight increase in performance as the proportion of malicious vehicles rises. This is because DUEL operates on a vehicle-to-vehicle evaluation basis, where each vehicle has a distinct trust opinion of another. Therefore, as the percentage of malicious vehicles increases, more vehicles form negative trust opinions about these malicious vehicles, leading to a slight increase in the recall rate. In contrast, MEFPB with its path-backtracking mechanism, can effectively conter the SAs, OFAs, and PTAs, and it efficiently counters the BHAs in the direct trust dimension.

D. Impact of SA

Fig. 6 illustrates the trend over time for MEFPB, DUEL, IWOT-V, and TECS concerning precision, recall, and F-measure under a 20% SAs scenario.

Firstly, Fig. 6(a) shows the precision performance impacted by SAs. The precision of MEFPB rose sharply from 35% at 400s to a consistent 100% by 800s, outperforming the varying precision of IWOT-V. In contrast, DUEL and TECS maintained a steady 100% precision throughout. Secondly, Fig. 6(b) illustrates the recall performance impacted by SAs. The recall of MEFPB began at 35% and stabilized at 100% from 1400s, clearly surpassing DUEL, IWOT-V, and TECS. While DUEL plateaued at below 70%, IWOT-V peaked at 60%, and TECS maintained a level of 80% at 900 seconds. Thridly, Fig. 6(c) depicts the F-measure performance impacted by SAs. The F-Measure of MEFPB swiftly escalated, maintaining 100% from 1400s, whereas DUEL, IWOT-V, and TECS lagged behind, capping at 82.35%, 69.77%, and 88.89% respectively. Overall, MEFPB outperformed the two baseline schemes.

The fundamental reason for the above tendency is that MEFPB increases its interactions with regular vehicles. Additionally, there is an uptick in the number of path-backtracking verifications. Consequently, a gradual rise in precision can be observed. For DUEL, the initial strategy is to treat all vehicles as trustworthy by default. Trust values are then gradually reduced utilizing a penalty factor, distinguishing between malicious and regular vehicles. Ideally, this approach grants DUEL a relatively good performance in precision. For TECS, the scheme initially designates all vehicles as honest uses

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3363755

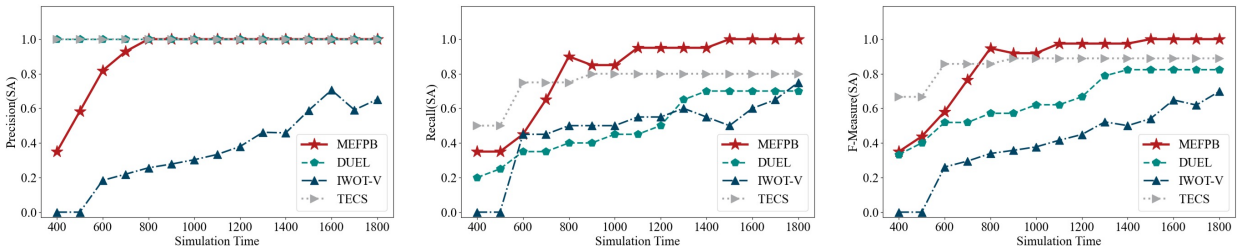


Fig. 6. MEFPB, DUEL, IWOT-V, and TECS impacted by SA. (a) Precision vs time. (b) Recall vs time. (c) F-measure vs time.

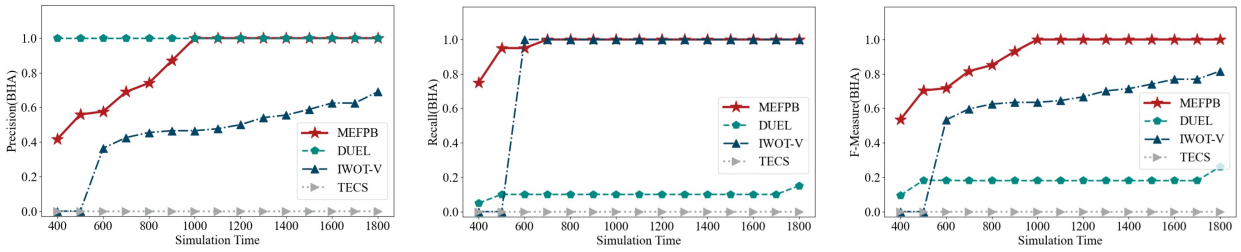


Fig. 7. MEFPB, DUEL, IWOT-V, and TECS impacted by BHA. (a) Precision vs time. (b) Recall vs time. (c) F-measure vs time.

verification and cryptographic techniques to identify malicious vehicles. As the scheme does not make false judgments, its precision consistently remains at 100%. Furthermore, MEFPB exhibits an increase in completed transmissions as interactions with malicious vehicles rise, indicating a continuous growth in the number of malicious vehicles identified by the path backtracking mechanism.

E. Impact of BHA

Fig. 7 illustrates the trend over time for MEFPB, DUEL, IWOT-V, and TECS concerning precision, recall, and F-measure under a 20% BHAs scenario.

Firstly, Fig. 7(a) shows the precision performance impacted by BHAs. During the simulation from 400*s* to 900*s*, the precision of MEFPB rose from 41.67% to 86.96% and stabilized at 100% from 1000*s* onwards. In contrast, DUEL consistently maintained a precision of 100%, while IWOT-V gradually increased from 36.36% at 600*s* to 68.97% by 1800*s*. In the case of TECS, it consistently recorded a 0% precision throughout the duration of the simulation. Secondly, Fig. 7(b) depicts the recall performance impacted by BHAs. The recall of MEFPB quickly rose from 75% at 400*s* and remained at 100% from 700*s*. In contrast, DUEL peaked at a recall of 15%, while IWOT-V swiftly reached and sustained 100% after 600*s*. Meanwhile, TECS consistently remained at 0% throughout the period. Thridly, Fig. 7(c) illustrates the F-measure performance impacted by BHAs. From the simulation time of 400*s* to 900*s*, the F-measure of MEFPB rose from 53.57% to 93.02% and stayed at 100% after 900*s*. In contrast, both DUEL and IWOT-V had lower performances, DUEL peaked at 26.09% by 1800*s*, while IWOT-V reached 81.63% at the same time. Alternatively, TECS maintained a consistent 0% throughout the simulation period. Overall, MEFPB outperformed the two baseline schemes.

The reason for the above tendency is MEFPB uniquely diminishes trustworthiness based on the behavior of vehicles executing BHAs. If such a vehicle remains isolated, its trust declines. Initially, some vehicles might have low trust due to limited interactions, causing misjudgments. Furtermore, IWOT-V utilizes a trust assessment scheme grounded in vehicle-to-vehicle interactions. As vehicles in the BHA model do not partake in interactions, their trust values consistently fall below the preset threshold, leading to their comprehensive identification. Conversely, DUEL assesses the trustworthiness of vehicles sending messages. Since BHA vehicles do not send messages, DUEL faces challenges in offering effective evaluations for BHAs. Similarly to DUEL, since BHA vehicles lack interaction, TECS is unable to calculate trust values and therefore cannot identify such vehicles.

F. Impact of OFA

Fig. 8 illustrates the trend over time for MEFPB, DUEL, IWOT-V, and TECS concerning precision, recall, and F-measure under a 20% OFAs scenario.

Firstly, Fig. 8(a) shows the precision performance impacted by OFAs. During the simulation from 400*s* to 800*s*, the precision of MEFPB rose from 31.58% to 100% and stabilized at 100% post-800*s*. In contrast, while DUEL and TECS consistently held at 100%, IWOT-V peaked at 31.82% by 1200*s* but declined to 12.5% by 1800*s*. Secondly, Fig. 8(b) depicts the recall performance impacted by OFAs. The recall of MEFPB dropped from 30% to 20% between 400*s* to 500*s* but later exhibited a rising trend, eventually reaching 100% by 1700*s*. In contrast, the recall of DUEL peaked at 65% by 1300*s* and then stabilized at 70%, while IWOT-V gradually

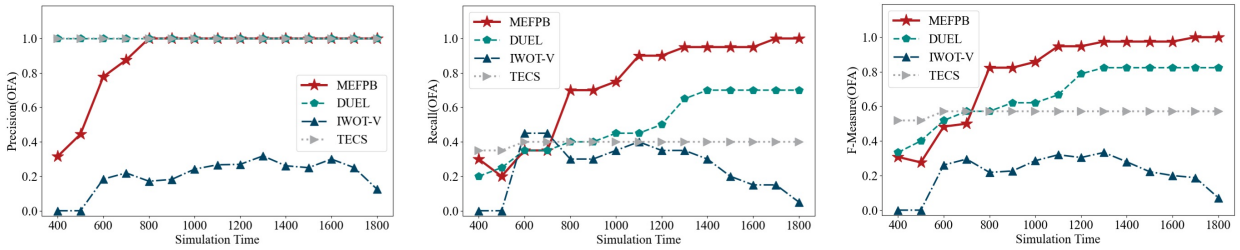


Fig. 8. MEFPB, DUEL, IWOT-V, and TECS impacted by OFA. (a) Precision vs time. (b) Recall vs time. (c) F-measure vs time.

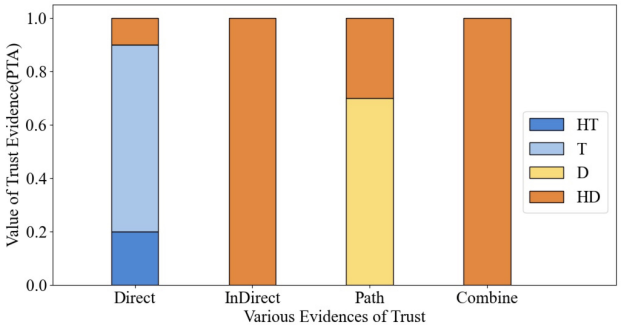


Fig. 9. Four trust evidence types of MEFPB under PTA.

declined post-600s. As for TECS, it maintained a steady 40% after 600s. Thridly, Fig. 8(c) illustrates the F-measure performance impacted by OFAs. The F-measure of MEFPB rose from 35% at 400s to 43.75% at 500s and continued its ascent, stabilizing at 100% by 1500s. In contrast, DUEL remained steady at 82.35% post-1300s, while IWOT-V peaked at 64.86% by 1600s before slightly declining. Regarding TECS, it maintained a steady 57.14% after 600s. Overall, MEFPB can rapidly identify OFA vehicles and outperforming the two baseline schemes.

The reason for the above tendency is that OFA vehicles attempt to evade the detection mechanism of MEFPB. Moreover, IWOT-V and TECS struggles against OFA due to its lack of mechanisms to counter complex attacks.

G. Four Trust Evidence Types of PTA

Fig. 9 illustrates a comprehensive evaluation of various trust levels within the four trust evidences for vehicles operating under the PTA model.

The composition of the four trust evidences are as follows: direct trust evidence $\{HT = 0.2, T = 0.7, D = 0, HD = 0.1\}$, indirect trust evidence $\{HT = 0, T = 0, D = 0, HD = 1\}$, and path-backtracking trust evidence $\{HT = 0, T = 0, D = 0.7, HD = 0.3\}$. After fusion through DST, the comprehensive trust evidence is $\{HT = 0, T = 0, D = 0, HD = 1\}$.

The fundamental reason is that PTA vehicles exhibit behaviors similar to regular vehicles in the network. This similarity makes their interactions and message-forwarding appear trustworthy, rendering the task of identifying them as malicious based solely on direct interactions quite challenging. However, MEFPB has a path-backtracking mechanism, ensuring accurate identification of PTA vehicles. Consequently, based on the path trust evidence, these vehicles are deemed untrustworthy. Furthermore, indirect trust evidence provided by neighbors corroborates untrustworthy, emphasizing malicious behaviors of PTA vehicles. Since these various trust evidence, it's evident that MEFPB can accurately detect malicious behaviors of PTA vehicles and defend effectively against such attacks.

H. Impact of Forgetting Factor

Table III demonstrates the variation in direct trust evidence for a normal vehicle number 66 under different values of z (excluding familiarity and cooperativeness).

In this table, the quadruple consists of HT as the first element, T as the second, D as the third, and HD as the fourth (with values remaining constant post-1400s). Notably, at z=100, the trust level T of vehicle was reduced three times, specifically at 600s, 800s, and 1000s. Conversely, with z=200, there was a single reduction in trust level T at 600s. When the value was set to z=300, the outcomes mirrored those observed at z=400.

The observed data indicates that the forgetting function came into play at z=100 and z=200, likely due to vehicle's remote positioning and lesser frequency of interactions. However, at z=300, normal vehicle did not activate forgetting function, aligning with the results at z=400. This alignment supports the premise that normal vehicles are not expected to trigger the forgetting function, leading to the selection of z=300 as the optimal value for our experiments.

I. Time Required for Malicious Behaviour Detection

Table IV displays the time required by MEFPB, DUEL, IWOT-V, and TECS to detect malicious vehicles in a 20% SA scenario. The times listed in the table represent the duration to identify the first malicious vehicle (without any warm-up period). MEFPB demonstrates the fastest response in detecting malicious vehicles. Such efficiency is largely due to its advanced detection mechanism, which enables rapid tracing of vehicles involved in malicious activities as soon as a tampered message relays the target vehicle. This process facilitates a swift reduction in the trustworthiness of these vehicles. MEFPB's ability to quickly backtrack the path of a tampered message allows for immediate identification of the malicious vehicle. In comparison to other schemes, MEFPB stands out with its significantly superior performance.

TABLE III
DIRECT EVIDENCE IMPACTED BY FORGETTING FACTOR.

Simulation Time (s)	400	600	800	1000	1200	1400
z=100	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.2, 0.5, 0.1\}$	$\{0.2, 0.1, 0.6, 0.1\}$	$\{0.2, 0.0, 0.7, 0.1\}$	$\{0.2, 0.0, 0.7, 0.1\}$	$\{0.2, 0.0, 0.7, 0.1\}$
z=200	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.2, 0.5, 0.1\}$	$\{0.2, 0.2, 0.5, 0.1\}$	$\{0.2, 0.2, 0.5, 0.1\}$	$\{0.2, 0.2, 0.5, 0.1\}$	$\{0.2, 0.2, 0.5, 0.1\}$
z=300	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$
z=400	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$	$\{0.2, 0.4, 0.3, 0.1\}$

TABLE IV
MALICIOUS BEHAVIOUR DETECTION TIME.

Scheme	MEFPB	DUEL	IWOT-V	TECS
Malicious Behaviour Detection Time	26s	217s	83s	53s

VI. CONCLUSION

This paper proposes an innovative trust management scheme, focusing on incorporating the transmission path of message as a new dimension for trust assessment. To address the uncertainty arising from data sparsity in VANETs, we utilized the DST. Simultaneously, by introducing a Path-backtracking mechanism, malicious vehicle behaviors can be identified more accurately. Additionally, we integrated a forgetting function, and assessed the familiarity and cooperativeness of direct trust evidence to ensure a high level of cooperation among vehicles in the network. In terms of path evaluation, this study utilized verification counts based on path-backtracking, multi-path analysis, and path similarity as key metrics. Simulation experiment demonstrates that the MEFPB exhibits excellent effectiveness and stability in ensuring network security.

VII. ACKNOWLEDGEMENT

The funding is supported by EU HORIZON-TMA-MSCA-SE project TRACE-V2X under grant (101131204) and Hubei Province International Science and Technology Collaboration Program (2022EHB002) and Wuhan Industrial base Innovation Program (2023010402010783) and Fundamental Research Funds for the Central Universities, China (2042022rc0020).

REFERENCES

[1] F. Z. Bousbaa, C. A. Kerrache, N. Lagraa, R. Hussain, M. B. Yagoubi, and A. E. K. Tahari, "Group data communication in connected vehicles: A survey," *Vehicular Communications*, vol. 37, p. 100518, 2022.

[2] Z. Yang, R. Wang, D. Wu, B. Yang, and P. Zhang, "Blockchain-enabled trust management model for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12 044–12 054, 2023.

[3] C.-M. Chen, Z. Li, S. Kumari, G. Srivastava, K. Lakshmanna, and T. R. Gadekallu, "A provably secure key transfer protocol for the fog-enabled social internet of vehicles based on a confidential computing environment," *Vehicular Communications*, vol. 39, p. 100567, 2023.

[4] M. Annoni and B. Williams, "The history of vehicular networks," *Vehicular ad hoc Networks: Standards, Solutions, and Research*, pp. 3–21, 2015.

[5] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[6] C.-M. Chen, Y. Hao, and T.-Y. Wu, "Discussion of "ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps"," *IEEE Transactions on Industry Applications*, vol. 59, no. 2, pp. 2091–2092, 2023.

[7] M. Maad Hamdi, L. Audah, S. Abduljabbar Rashid, A. Hamid Mohammed, S. Alani, and A. Shamil Mustafa, "A review of applications, characteristics and challenges in vehicular ad hoc networks (vanets)," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020, pp. 1–7.

[8] 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)*, 2020, pp. 1–6.

[9] R. Krishnan P. and A. R. Kumar P., "Security and privacy in vanet : Concepts, solutions and challenges," in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 789–794.

[10] S. Tangade, S. S. Manvi, 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.

[11] 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.

[12] C. A. Kerrache, N. Lagraa, R. Hussain, S. H. Ahmed, A. Benslimane, C. T. Calafate, J.-C. Cano, and A. M. Vegni, "Tacashi: Trust-aware communication architecture for social internet of vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5870–5877, 2019.

[13] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei, and F. Yang, "A security authentication method based on trust evaluation in vanets," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, pp. 1–8, 2015.

[14] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (vanet)," *Wireless Networks*, vol. 24, no. 2, pp. 373–382, 2018.

[15] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "A security solution for v2v communication within vanets," in *2018 Wireless Days (WD)*. IEEE, 2018, pp. 181–183.

[16] H. Gao, C. Liu, Y. Yin, Y. Xu, and Y. Li, "A hybrid approach to trust node assessment and management for vanets cooperative data communication: Historical interaction perspective," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16 504–16 513, 2021.

[17] A. Mahmood, W. E. Zhang, Q. Z. Sheng, S. A. Siddiqui, and A. Aljubairy, "Trust management for software-defined heterogeneous vehicular ad hoc networks," *Security, privacy and trust in the IoT environment*, pp. 203–226, 2019.

[18] 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.

[19] G. Shafer, *A mathematical theory of evidence*. Princeton university press, 1976, vol. 42.

[20] 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.

[21] S. Chuprov, I. Viksnin, I. Kim, E. Marinenkov, M. Usova, E. Lazarev, T. Melnikov, and D. Zakoldaev, "Reputation and trust approach for security and safety assurance in intersection management system," *Energies*, vol. 12, no. 23, p. 4527, 2019.

[22] 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.

[23] D. Suo and S. E. Sarma, "Real-time trust-building schemes for mitigating malicious behaviors in connected and automated vehicles," in *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*. IEEE, 2019, pp. 1142–1149.

[24] A. Hbaieb, S. Ayed, and L. Chaari, "Blockchain-based trust management approach for iov," in *International Conference on Advanced Information Networking and Applications*. Springer, 2021, pp. 483–493.

[25] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE internet of things journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[26] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "Bars: A blockchain-based anonymous reputation system for trust management in vanets," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 98–103.

[27] Z. Fei, K. Liu, B. Huang, Y. Zheng, and X. Xiang, "Dirichlet process mixture model based nonparametric bayesian modeling and variational inference," in *2019 Chinese Automation Congress (CAC)*. IEEE, 2019, pp. 3048–3051.

[28] 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.

[29] W. Fang, W. Zhang, Y. Liu, W. Yang, and Z. Gao, "Btds: Bayesian-based trust decision scheme for intelligent connected vehicles in vanets," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. e3879, 2020.

[30] K. Sharma and B. K. Chaurasia, "Trust based location finding mechanism in vanet using dst," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 763–766.

[31] 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, 2016.

[32] 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.

[33] D. Boneh and X. Boyen, "Short signatures without random oracles," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2004, pp. 56–73.

[34] J. Li, Y. Ji, K.-K. R. Choo, and D. Hogrefe, "Cl-cppa: Certificate-less conditional privacy-preserving authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 332–10 343, 2019.

[35] X. Li, H. Zhang, Y. Ren, S. Ma, B. Luo, J. Weng, J. Ma, and X. Huang, "Papu: Pseudonym swap with provable unlinkability based on differential privacy in vanets," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 789–11 802, 2020.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] Y. Zhang, Y. Song, Y. Wang, Y. Cao, X. Ren, and F. Yan, "Tecs: A trust model for vanets using eigenvector centrality and social metrics," in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2022, pp. 36–43.

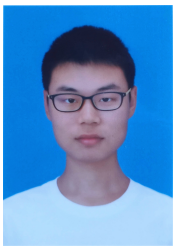
[41] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, 2005, pp. 252–259.

[42] 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.

Cheong Chak Lam holds a Bachelor's degree from Huazhong University of Science and Technology, China. 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.

Bo Cai received his Ph. D. in computer application from Computer School of Wuhan University. He is an associate professor in Computer School of Wuhan University. His research interests are in the areas of image processing, video information processing, virtual reality and satellite simulation. His research group develops novel analytical methods for video, such as the clustering and similarity algorithm of video shots, browse and retrieval method of video database and text region extraction in digital videos, vehicles and objects detection algorithm in digital videos. He has published more than 30 research papers in his research fields.

Qiang Ni received the Ph.D. degree in 1999 from HuaZhong University of Science and Technology (HUST), China. He subsequently spent two years as a Post-Doctoral Fellow at the Wireless Communication Research Laboratory, HUST. He is currently a Lecturer in the School of Engineering & Design, Brunel University, Uxbridge, U.K. Prior to that, he was a Senior Research Scientist at Hamilton Institute, National University of Ireland at Maynooth. He worked with INRIA France as a Researcher from 2001 to 2004. Since 2002, he has been active as an IEEE 802.11 Wireless Standard Working Group voting member and a contributor for the IEEE wireless standards. His research interests are wireless networking and mobile communications. He has published over 40 refereed papers in the above fields.