RTE: Rapid and Reliable Trust Evaluation for Collaborator Selection and Time-Sensitive Task Handling in Internet of Vehicles

Jiazhi Chen, *Graduate Student Member, IEEE*, Xianbin Wang, *Fellow, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—By enabling connectivity and collaboration among moving vehicles, Internet of Vehicles (IoV) is expected to bring dramatically improved road safety and traffic efficiency. With limited onboard resources and real-time operational constraints, achieving these goals through handling time-sensitive IoV services and tasks inevitably relies on rapid and reliable collaboration among moving vehicles. Due to safety-related considerations, such collaboration always requires complex evaluation of potential collaborative vehicles, resulting in increased latency in time-sensitive IoV task handling. To achieve rapid and reliable IoV collaboration, a comprehensive concept of trust among neighboring vehicles is first conceptualized in this article to maximize Quality of Experience (QoE) by expediting the IoV collaborator selection as well as overall task handling. Specifically, we propose a new concept of indirect trust and the related Rapid and reliable Trust Evaluation (RTE) mechanism by enabling trust transfer from reliable third parties to reduce the trust evaluation latency of potential collaborative peers. Furthermore, capability trust and direct experiential trust are introduced as two additional evaluation factors in RTE to assess the capability and reliability of collaborators and to reduce task computation time. Finally, the different factors of the proposed trust, i.e., indirect trust, direct experiential trust, and capability trust, are integrated and adaptively utilized at different stages of IoV collaboration by a proposed adaptive trust factor aggregation scheme. Simulation results demonstrate that the proposed RTE mechanism achieves higher QoE with reduced task completion latency by swiftly selecting the optimal IoV collaborator compared to existing trust evaluation mechanisms.**

***Index Terms*—Collaboration, Internet of Vehicles (IoV), Quality of Experience (QoE), time-sensitive task handling, trust.**

I. Introduction

INTERNET of Vehicles (IoV) has emerged as a new paradigm which facilitates ubiquitous connectivity and dynamic collaboration among moving vehicles through Vehicle-to-Vehicle (V2V) communication [1], [2]. A plethora of time-sensitive IoV services and tasks, including collision avoidance and traffic monitoring for autonomous driving, are expected to significantly enhance road safety and traffic efficiency and further empower the development of intelligent transportation systems (ITS) [3], [4]. To achieve these objectives, rapid and reliable collaboration among moving vehicles plays a pivotal role in expediting IoV services and task completion within the constraints of limited onboard resources and real-time operational demands of individual vehicles.

Given the fast mobility and resource constraints of vehicles, the realization of rapid and reliable IoV collaboration in the dynamic IoV environment can be extremely challenging. This challenge primarily stems from the complex security, capability and reliability requirements during the selection of potential IoV collaborators.

From the safety and security perspective, insufficient knowledge of unknown vehicles under the dynamic IoV environment makes vehicle identity authentication very difficult. Without robust IoV security, malicious vehicles could sneak into critical IoV collaborations by providing misleading information, thereby further undermining both communication security and road safety. To meet safety-related requirements, traditional authentication techniques might be useful to identify potential malicious vehicles and select legitimate ones for reliable collaboration. However, such security techniques often incur prolonged authentication latency due to the reliance on remote security servers, which could not fulfill the rapid demand of V2V authentication and collaboration [5]. Despite the existence of artificial intelligence (AI)-driven authentication methods that are lightweight and capable of achieving significantly reduced authentication latency [6], [7], a selected legitimate collaborating vehicle through authentication may lack sufficient computational resources as well as the intention to provide rapid collaboration, leading to increased task completion time [8]. Therefore, IoV collaboration could suffer from choosing unsuitable collaborative vehicles due to incomplete information on the capability and intention of a vehicle during the collaborator selection process.

In general, a collaborative task could fail when the selected IoV collaborator is unable to accomplish it within time constraints due to limited resources or refuses to participate in the collaboration. To guarantee the successful handling of collaborative tasks, game theory-based collaborator selection

Manuscript received 10 October 2023; accepted 9 November 2023. Date of publication 17 November 2023; date of current version 26 March 2024. This work was supported in part by the New Frontiers in Research Fund of Government of Canada under Grant NFRFE-2022-00512; in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Program under Grant RGPIN2018-06254; and in part by the Canada Research Chair Program. *(Corresponding author: Xianbin Wang.)*

Jiazhi Chen and Xianbin Wang are with the Department of Electrical and Computer Engineering, Western University, London, ON N6A 5B9, Canada (e-mail: jche629@uwo.ca; xianbin.wang@uwo.ca).

Xuemin Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: sshen@uwaterloo.ca).

Digital Object Identifier 10.1109/JIOT.2023.3333679

approaches have been proposed by considering resource situations and intentions of IoV collaborators [9], [10]. For instance, Wang et al. [11] proposed a mobility-aware vehicular recruitment scheme based on a greedy algorithm to select suitable IoV collaborators for task handling. However, the lengthy collaborator evaluation process in such approaches dramatically increases the overall task completion time, which is unsuitable for handling time-sensitive IoV tasks.

To overcome the aforementioned challenges in rapid and reliable IoV collaboration, a comprehensive trust concept among moving vehicles, is first conceptualized in this study to expedite the selection of reliable IoV collaborators with sufficient capability and intention. Psychologically speaking, trust in the context of humanity is defined as the confident expectation that another person will act in a certain way or have specific characteristics, [12], [13]. To achieve the desired goals of rapid and reliable IoV collaboration, we first broaden the definition of trust in assisting collaborative vehicle selection and introduce a multidimensional assessment framework. Specifically, we define trust in the context of IoV collaboration as an aggregated confident indicator constituted of multiple factors related to whether a collaborative vehicle can complete collaborative tasks as expected, where the relevant factors include but are not limited to collaborative vehicles' identity, capability and willingness. This reenvisioned trust concept offers a fresh perspective on V2V collaboration, distinguishing itself from existing IoV trust concepts by incorporating multifaceted evaluation criteria as well as expediting the selection of reliable IoV collaborators and task handling, ultimately facilitating rapid and reliable IoV collaboration.

Considering the changing needs at different stages of the IoV collaboration, the different factors in the newly proposed trust concept are further adaptively harnessed. By integrating and utilizing different trust factors adaptively, the trustworthiness of a potential IoV collaborator can be evaluated precisely to accommodate the needs at different stages of IoV collaboration. Specifically, a rapid and reliable trust evaluation (RTE) mechanism based on the transfer of indirect trust from reliable third parties is designed to expedite IoV collaborator selection in the initial collaboration stage with incomplete and unavailable information about IoV collaborators. Furthermore, the weighting of trust-related factors is dynamically adjusted to align with the distinct requirements of subsequent IoV collaboration stages.

By avoiding the needless and repeated authentication process and subsequently selecting more suitable IoV collaborators, our proposed trust concept and adaptive trust factor aggregation scheme could foster rapid and reliable collaboration among moving vehicles in the dynamic IoV environment.

A. Related Work

Existing trust concepts in the context of vehicle collaboration are not directly aligned with the specific and comprehensive needs of such collaboration [14], [15]. Such misalignment between trust and collaboration forms the basis for our proposed trust concept, which seeks to provide a more comprehensive trust concept. Most of the existing trust concepts in IoV are primarily concentrated on security aspects, particularly in identifying malicious vehicles and mitigating the potential risks [16], [17], [18]. While the focus on security is paramount, it may not fully encompass the multifaceted requirements of collaborative IoV tasks. Thus, a few recent studies broadened the trust concept by incorporating additional factors, such as effective communication distance [19], or assessing collaborators' capabilities using metrics like packet transmission rate and energy consumption rate [20]. However, these augmentations have not comprehensively covered the full spectrum of factors essential for IoV tasks. For instance, an important deficiency in existing IoV trust concepts is the inadequate consideration given to the willingness of IoV collaborators to engage in collaboration. This shortcoming inevitably results in increased task completion time and even task failure, highlighting a critical aspect that our proposed trust concept seeks to rectify. In a nutshell, our work seeks to align collaboration needs and trust factors by introducing a more comprehensive trust concept that not only encompasses security concerns but also integrates other essential factors to achieve rapid and reliable collaboration.

Additionally, fast mobility and dynamic resource conditions of vehicles pose significant challenges to existing static trust evaluation mechanisms in achieving changing objectives at every stage of IoV collaboration [21], [22]. Specifically, when complete information about collaborators is not available in the initial IoV collaboration stage, although trusted central authorities can be employed to collect feedback from third parties for precise trust evaluation, the poor connectivity between centralized authorities and vehicles in remote areas significantly diminishes IoV collaboration efficiency [23], [24]. Furthermore, relying on the static adjustment of various trust factors, such as direct collaboration experiences and received recommendations, at subsequent IoV collaboration stages often leads to inaccuracies in collaborator selection and a prolonged task-handling process [25], [26]. Consequently, this study recognizes the urgent need for adaptive trust evaluation mechanisms to effectively tackle the constraints associated with static approaches, where a situation-aware adaptation of the different trust factors in trust evaluation becomes critical to fulfilling the needs at different stages of IoV collaboration.

B. Contributions and Organization

To concurrently meet the needs of rapid and reliable IoV collaboration, this article proposes a comprehensive trust concept as well as the corresponding adaptive trust factor aggregation scheme tailored to various IoV collaboration stages, ultimately expediting the selection of suitable IoV collaborators and the handling of time-sensitive IoV tasks. The main contributions of this article are summarized below.

1) A comprehensive concept of trust among moving vehicles in IoV is first conceptualized, which includes three different trust evaluation factors, i.e., indirect trust, direct experiential trust, and capability trust, to achieve rapid and reliable IoV collaboration by accelerating the selection of reliable collaborative vehicles

with sufficient capability and intention. Specifically, by enabling indirect trust transfer from reliable third parties, the trust evaluation latency of potential IoV collaborators is reduced. Moreover, to reduce task computation time, reliable IoV collaborators with sufficient resources and positive intentions are selected based on capability trust and direct experiential trust.

2) An adaptive trust factor aggregation scheme is designed to aggregate different trust factors in the proposed trust concept adaptively based on collaboration requestors' subjective experiences, which further meets changing needs of IoV collaboration at different stages. Specifically, in the initial collaboration stage, indirect trust is utilized as an objective trustworthiness rating to accelerate reliable IoV collaboration selection by fulfilling the gap of the insufficient direct interactions between collaboration requestors and IoV collaborators. Furthermore, to subsequently select more suitable IoV collaborators at other IoV collaboration stages, the role of indirect trust will be diminished when collaboration requestors gradually gain sufficient direct collaboration experiences with collaborators over time.
3) Comprehensive simulation results and performance evaluation demonstrate that the proposed RTE mechanism can select the optimal IoV collaborator under dynamic environments to align with the specific demands of collaborative tasks, while outperforming baseline trust evaluation mechanisms on significant indicators, including task completion time, Quality of Experience (QoE), trust evaluation accuracy, and convergence efficiency as well as defense performance against security threats.

The remainder of this article is organized as follows. Section II introduces the system model and problem formulation. Section III overviews the details of our proposed RTE mechanism. The performance of the proposed RTE is evaluated and compared to the other existing works in Section IV. Ultimately, Section V concludes this article.

II. System Model and Problem Formulation

This section first introduces the IoV system that comprises both network and threat models, where trust among moving vehicles is conceptualized to accelerate collaborator selection and task handling under potential security threats. Subsequently, the research problem under such an IoV system is formulated as a QoE maximization problem based on task completion time minimization.

A. IoV Network Model

An edge-enabled IoV network is considered to elaborate and analyze the proposed trust-based IoV collaborator selection approach, i.e., RTE mechanism, as shown in Fig. 1. The involved vehicles supported by V2V and Vehicle-to-Infrastructure (V2I) communication within the coverage of roadside units (RSUs) are divided into two categories:

1) A set of trustors (collaboration requestors) $\mathcal{M} = \{v_i | i \in \{1, 2, \ldots, M\}\}$ with collaborative tasks, where each $v_i \in \mathcal{M}$ only carries a single task that needs to be offloaded for execution, and a set of trustees (collaborators) $\mathcal{N} = \{v_j | j \in \{1, 2, \ldots, N\}\}$ that are evaluated by trustors for potential collaboration in handling the offloaded task.
2) An RSU equipped with an integrated edge server plays a pivotal role in initiating and expediting IoV collaboration by disseminating a trust evaluation factor, i.e., indirect trust, to trustors via V2I communication.

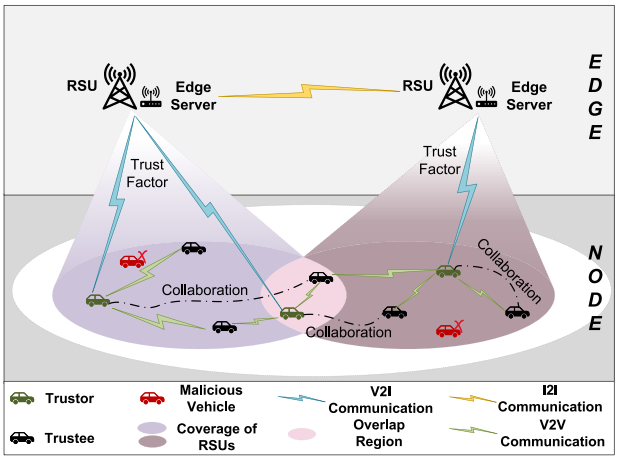


Fig. 1. Edge-enabled IoV system for trust-based IoV collaborator selection, where an edge server integrated with RSU sends a trust factor (i.e., indirect trust) to the trustor for initializing and accelerating IoV collaborator selection. The dashed-doted line denotes the trustor selects the trustee with optimal trust value from the trust ranking as the final IoV collaborator.

In this article, the collaborative IoV tasks considered are only focused on time-sensitive tasks that are critical to road safety and traffic efficiency, which is similar to several existing works [27], [28]. Besides, only one collaborator is selected by the trustor v_i to handle an offloaded time-sensitive IoV task based on a situation-aware adaptation of different factors in the proposed comprehensive trust concept.[1] The main symbols used are summarized in Table I.

B. IoV Threat Model

The inherent openness and decentralized nature of IoV lead to the potential infiltration of malicious vehicles, which initiate various threats in both communication security and road safety. By assigning low trust to different types of malicious vehicles, various security threats can be detected and eliminated. Specifically, to validate the defense performance against threats of the proposed trust evaluation mechanism, two IoV threats that have significant negative impacts on trust evaluation accuracy are considered in this study, which randomly undermine the trust information shared between trustees and trustors as well as deceiving trustors to trust malicious trustees by sharing misleading trust ratings [29], [30].

1) *On-and-Off Threats:* Malicious vehicles behave in a random pattern alternating between legitimate and malicious actions to launch routing attacks in IoV, i.e., Blackhole and Greyhole attacks that drop all or some of

[1]Multiple collaborators could be selected based on trust ranking but suffer from the increased complexity of task offloading and collaborator selection, which is more suitable for nontime-sensitive IoV tasks.

TABLE I
MAJOR NOTATIONS AND DEFINITIONS

Notation	Definition
$T_{i,j}$	Overall collaborative task completion time
$t^E_{i,j}$	Trust evaluation time between trustor v_i and trustee v_j
t^C_j	Task computation time of selected collaborator v_j
$t^T_{j,i}$	Task transmission time from v_j to v_i
$t^c_{i,j}$	Computation time of estimating trustee v_j's collaboration capability
$t^h_{i,j}$	Computation time of quantifying historical collaboration experience between v_i and v_j
$t^{in}_{i,j}$	Computation time of quantifying recommendations from third parties
T_e	Time constraint of trust evaluation
T_m	Time constraint of overall task completion
$\mathcal{H}_{p,j}$	A set of experiential collaboration records between recommender v_p and trustee v_j
$\mathcal{H}_{i,j}$	A set of direct experiential collaboration records between trustor v_i and trustee v_j
$\mathcal{U}^g_{i\to\mathcal{N}}$	Global trust value list between trustor i and all trustees $\mathcal{N}$
$\mathcal{U}^g_{i,j}$	Global trust value between v_i and v_j
$\mathcal{U}^c_{i,j}$	Capability trust value between v_i and v_j
$\mathcal{U}^h_{i,j}$	Direct experiential trust value between v_i and v_j

the received packets. Therefore, such vehicles could gain high trust by performing legitimate behavior following malicious behavior, which diminishes the ability of the trust evaluation mechanism to distinguish between trustworthy and untrustworthy collaborators, thereby significantly reducing trust evaluation accuracy.

2) *Recommendation Attacks:* These attacks are also known as bad-mouthing attacks and good-mouthing attacks, where malicious recommenders send deceptive recommendations to edge servers, thereby influencing trust evaluation accuracy with misleading data. When the trustor relies on manipulated trust ratings, it results in misguided trust decisions and potentially facilitates collaboration with untrustworthy parties.

C. Task Completion Time Minimization for QoE Maximization

Our specific goal is to minimize the overall collaborative task completion time through trust-based optimal IoV collaborator selection. Therefore, the trust-enabled collaborative task completion time $T_{i,j}$ among trustor v_i and trustee v_j becomes the primary evaluation indicator, which includes trust evaluation time $t^E_{i,j}$, task computation time t^C_j and transmission time $t^T_{i,j}$, can be given by

$$T_{i,j} = t^E_{i,j} + t^C_j + t^T_{i,j}. \tag{1}$$

Specifically, trust evaluation time $t^E_{i,j}$ is the time to determine the trustworthiness of potential IoV collaborators. In achieving rapid and reliable collaboration, different factors in trust evaluation will be adapted to minimize $t^E_{i,j}$ based on changing situations at different IoV collaboration stages. Depending on whether v_i can obtain recommendations about v_j's trustworthiness from RSU (indirect trust) and whether v_i has direct historical collaborations (direct experiential trust) with v_j, four situations are considered in the determination of $t^E_{i,j}$, formulated as

$$t^E_{i,j} = \begin{cases} t^c_{i,j}, & \mathcal{H}_{\mathcal{P}\to j} = 0 \ \& \ \mathcal{H}_{i,j} = 0 \\ t^h_{i,j}, & \mathcal{H}_{\mathcal{P}\to j} = 0 \ \& \ \mathcal{H}_{i,j} \neq 0 \\ t^c_{i,j} + t^{\text{in}}_{i,j}, & \mathcal{H}_{\mathcal{P}\to j} \neq 0 \ \& \ \mathcal{H}_{i,j} = 0 \\ t^c_{i,j} + t^h_{i,j} + t^{\text{in}}_{i,j}, & \mathcal{H}_{\mathcal{P}\to j} \neq 0 \ \& \ \mathcal{H}_{i,j} \neq 0 \end{cases}$$
$$\text{s.t.} \quad \mathbb{C}_1 : t^E_{i,j} \le T_e \le T_m \quad \forall v_i \in \mathcal{M} \quad \forall v_j \in \mathcal{N} \tag{2}$$

where $\mathcal{H}_{\mathcal{P}\to j} = 0$ denotes there are no recommendations about v_j's trustworthiness from reliable third parties $\mathcal{P} = \{v_p | p \in \{1, 2, \ldots, P\}\}$ and $\mathcal{H}_{i,j} = 0$ represents there are no direct collaboration experiences between v_i and v_j. Three factors are aggregated adaptively in overall trust evaluation time $t^E_{i,j}$, i.e., the computation time of estimating v_j's collaboration capability (capability trust) $t^c_{i,j}$, direct experiential trust computation time $t^h_{i,j}$, and indirect trust computation time $t^{\text{in}}_{i,j}$. $\mathbb{C}_1$ describes time constraints for trust evaluation, where T_e and T_m indicate the maximum trust evaluation time and maximum overall task completion time.

Assume the trustee v_j is selected as a collaborator, the task computation time t^C_j required by selected v_j is formulated by (3), where a_j indicates allocated CPU resources from v_j to accomplish v_i's requested collaborative task, f_j is the CPU frequency per unit CPU resource at v_j and h_i represents the number of CPU cycles required for processing v_i's tasks [31]

$$t^C_j = \frac{h_i}{a_j f_j}. \tag{3}$$

The transmission time $t^T_{i,j}$ is the overall time it takes for the data exchange related to task sharing and results returning between the selected collaborator v_j and collaboration requestor v_i, which is formulated in (4) as a ratio of the data size of collaborative task Υ_i to the available data transmission rate $\phi_{i,j}$ [32]

$$t^T_{i,j} = \frac{\Upsilon_i}{\phi_{i,j}} = \frac{\Upsilon_i}{B_{i,j}\log_2\left(1 + \frac{b_{i,j}F_{i,j}h^2}{N_0}\right)} \tag{4}$$

where $B_{i,j}$ is the channel bandwidth, $b_{i,j}$ is the instantaneous transmit power between v_j and v_i, $F_{i,j}$ is the path fading, and N_0 is the variance of Gaussian white noise.

In general, the task completion requirements in IoV, including overall task completion time, could vary dramatically. Meeting such requirements differently leads to varying task-specific satisfaction levels of trustors. Maximization of such satisfaction level is evaluated by a critical indicator, QoE [33], [34]. For time-sensitive tasks, reducing task completion time will lead to higher QoE. Therefore, the QoE of trustor v_i for a time-sensitive collaborative task is formulated as a logistic function based on collaborative task completion time $T_{i,j}$ [31], given by

$$\text{QoE}_i = \frac{1}{1 + e^{\gamma_1(T_{i,j} - \gamma_2)}} \tag{5}$$

where γ_1 indicates the growing trend of QoE and γ_2 indicates the mid-point of the logistic QoE function.

In a nutshell, this article aims to optimize QoE through task completion time minimization by selecting optimal collaborators. Hence, the objective of the research problem is formulated as

$$\begin{aligned} \max_{j} \quad & (\mathrm{QoE}_i) \\ \text{s.t.} \quad & \mathrm{C}_1 : j^* = \operatorname{argmax} \mathcal{U}^g_{i\to\mathcal{N}} \quad \forall v_i \in \mathcal{M} \quad \forall v_j^* \in \mathcal{N} \\ & \mathrm{C}_2 : T_{i,j} \le T_m \quad \forall v_i \in \mathcal{M} \quad \forall v_j \in \mathcal{N} \\ & \mathrm{C}_3 : \mathcal{U}^g_{i,j} \ge \delta \quad \forall v_i \in \mathcal{M} \quad \forall v_j \in \mathcal{N} \end{aligned} \tag{6}$$

where C_1 denotes the decision making of IoV collaborator selection that trustor v_i aims to select the trustee v_{j^*} with highest trust value for handling collaborative task. $\mathcal{U}^g_{i\to\mathcal{N}}$ represents a set of global trust value between trustor i and all trustees $\mathcal{N}$. C_2 indicates the overall task completion time $T_{i,j}$ in (1) should be less than a latency constraint T_m decided by trustor v_i. C_3 describes only legitimate vehicles can participate in the collaboration thus their global trust value $\mathcal{U}^g_{i,j}$ should be greater than a trustworthy threshold δ.

Remark 1: To solve the problem of (6), the decision-making process for IoV collaborator selection should be faster and more accurate. QoE will be decreased when collaboration requestors cannot timely select suitable IoV collaborators to complete the task. Hence, we propose a Rapid and RTE mechanism for IoV collaborator selection, including precise trust factor collection as well as an adaptive trust factor aggregation scheme.

III. Rapid and Reliable Trust Evaluation for IoV Collaborator Selection

The Rapid and RTE mechanism is proposed to establish trust-enabled collaboration among vehicles which achieves rapid and reliable IoV collaborator selection. To improve collaboration efficiency, the trust evaluation of potential collaborators should incorporate several critical factors that are required for rapid and reliable collaboration, where two perspectives are considered, i.e., subjective and objective, from different collaboration parties involved.

1) *From the Subjective Perspective of the Trustor v_i:* Whether the trustee v_j has the capability and willingness to complete the specific collaborative task. Specifically, capability trust $\mathcal{U}^c_{i,j}$ is introduced as a trust factor to estimate the collaboration capability of potential collaborators for a dedicated task in real-time. Additionally, due to the fact that v_j is usually more willing to participate in collaborations with more positive records in historical collaborations, the willingness of v_j is quantified based on its performance in historical collaborative tasks, i.e., direct experiential trust $\mathcal{U}^h_{i,j}$.
2) *From the Objective Perspective of Recommenders:* Whether the trustee v_j obtains good ratings from a set of recommenders $\mathcal{P}$. When trustor v_i has insufficient knowledge about trustee v_j, the recommendations from reliable third parties $\mathcal{P}$ fulfil the gap. Besides, the probability of poor performance in collaboration will be increased when the v_j obtains poor ratings from $\mathcal{P}$. The recommendations from $\mathcal{P}$ regarding the trustworthiness of v_j are quantified as a value, called indirect trust value $\mathcal{U}^{\mathrm{in}}_{i,j}$, which served as one of the trust evaluation factors.

Therefore, the proposed RTE mechanism is executed in a distributed manner considering three trust factors: 1) capability trust $\mathcal{U}^c_{i,j}$; 2) direct experiential trust $\mathcal{U}^h_{i,j}$; and 3) indirect trust $\mathcal{U}^{\mathrm{in}}_{i,j}$. Then aggregate the above three factors adaptively based on the proposed adaptive trust factor aggregation scheme to meet the specific needs of different IoV collaboration stages, as shown in Fig. 2. When encountering an unknown IoV collaborator in the initial IoV collaboration stage, the trustor v_i predicts the trustworthiness of an unknown trustee v_j through indirect trust transfer from nearby RSU and real-time capability trust evaluation. In the unstable IoV collaboration stage, the aggregated evaluation of capability trust $\mathcal{U}^c_{i,j}$, direct experiential trust $\mathcal{U}^h_{i,j}$ and indirect trust $\mathcal{U}^{\mathrm{in}}_{i,j}$ expedites IoV collaborator selection. In the stable IoV collaboration stage, v_i has sufficient direct collaboration experiences with the v_j and thus decides whether to collaborate. It is worth noting that the proposed RTE mechanism, can be extended for scenarios involving multiple tasks in the large-scale IoV by matching the tasks of trustors with the resources of trustees, offering versatility and practicality in real-world scenarios. The details of the proposed RTE for a single task handling are described as follows, including trust factor collection, adaptive trust factor aggregation, as well as trust decision and update.

A. Trust Factor Collection

1) Capability Trust: Capability trust value $\mathcal{U}^c_{i,j}$ indicates the estimation of potential collaborative vehicle v_j's capability to complete a target collaborative task in the current environment, which incorporates multiple attributes to reflect the collaboration capability of selected IoV collaborators. Even in the absence of prior collaboration experiences between trustor v_i and trustee v_j, v_i is able to predict the trustworthiness of v_j harnessing evaluated capability trust value, given by

$$\mathcal{U}^c_{i,j} = \varepsilon_1 L_{i,j} + \varepsilon_2 O_j + \varepsilon_3 R_j \tag{7}$$

where $L_{i,j}$, O_j, and R_j are the selected attributes with dynamic weights ε_1, ε_2, and ε_3. Specifically, $L_{i,j}$ indicates the location proximity between v_i and v_j, while O_j and R_j denote the role-oriented trustworthiness as well as the real-time resource situation of v_j.

The attributes incorporated into capability trust estimation are meticulously selected to ensure capturing the crucial factors that influence the collaboration capability assessment of potential collaborators. One fundamental attribute is related to how far the v_j will leave the communication range of the v_i. The collaboration constraint associated with this attribute stipulates that although the IoV collaborator may have sufficient resources to complete the collaborative task, the task will terminate once it leaves the v_i's communication range. Furthermore, the identity of vehicles emerges as another pivotal attribute that influences task completion. For example, malicious IoV collaborators will send misleading information, which leads to increased task completion time and even task failure. Most importantly, as depicted in (1), the task completion time $T_{i,j}$ encompasses the task computational

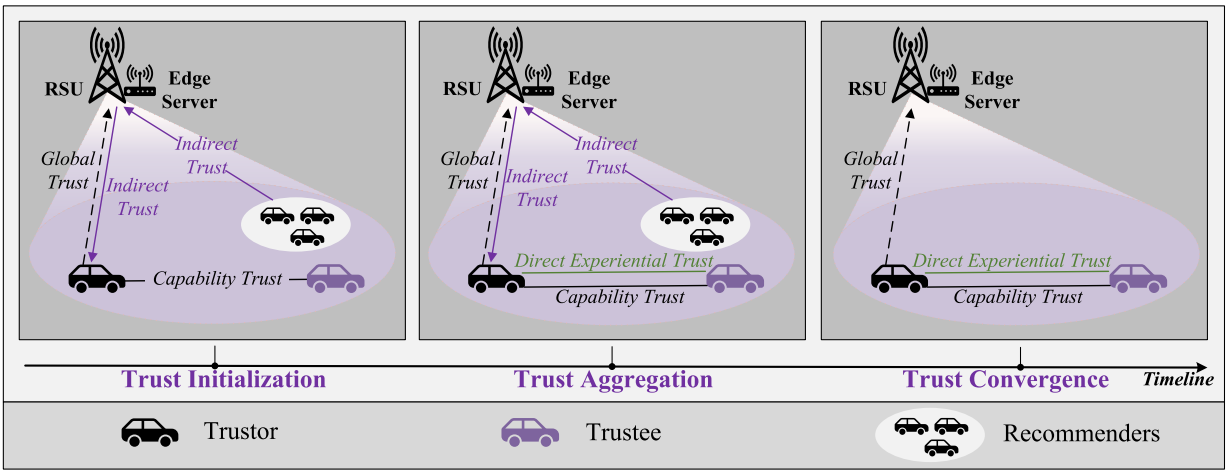


Fig. 2. Three stages of the proposed Rapid and RTE mechanism correspond to different stages of IoV collaboration. Specifically, the timeline of IoV collaboration between trustor and trustee is divided into three stages, i.e., trust initialization (initial collaboration stage), trust aggregation (unstable collaboration stage), and trust convergence (stable collaboration stage). Note that after the completion of a single collaborative task, the trustor will send the updated global trust value to RSU as feedback, which incorporated into historical records.

latency t_j^C and transmission delay $t_{i,j}^T$, which closely tied to real-time resource situations of potential collaborators, with attributes like CPU frequency and data transmission rate of the selected collaborator intricately affecting t_j^C and $t_{i,j}^T$.

Due to the mobility nature of vehicles, v_j may leave the communication range of v_i during collaboration. However, only v_j within the trustor's communication range can be selected as a collaborator otherwise the communication path will break off. Therefore, the distance d that the v_j leaves from the beginning point of the diameter of the v_i's communication range circle should be considered as one of the collaboration constraints, given by

$$d = \sqrt{\left(v_{j_x} - (v_{i_x} - D)\right)^2 + \left(v_{j_y} - (v_{i_y} - D)\right)^2} \tag{8}$$

where D refers to the radius communication range of the trustor v_i, v_{i_x}, and v_{j_x} indicate the current location of v_i and v_j, respectively.

Then a factor called location proximity $L_{i,j}$ is involved in capability trust evaluation to satisfy the distance constraint, which is derived as

$$L_{i,j} = \begin{cases} e^{-\frac{d}{D}}, & d \le 2D \\ 0, & d > 2D. \end{cases} \tag{9}$$

The role-oriented trustworthiness O_j denotes the trustworthiness probability of various role-oriented vehicles, evaluating the capability of v_j from an identity perspective [19]. The role of vehicles can be divided into specific vehicles v_{spe}, i.e., ambulances, buses, and taxis, which are regarded as highly trusted vehicles, common vehicles v_{com}, and malicious vehicles v_{mal}. The calculation of O_j for different role-oriented vehicles is different based on the effective distance σ between two vehicles and confidence value η regarding the different roles of trustees v_j, which is formulated as

$$O_j = \sigma\eta \tag{10}$$

where

$$\sigma = \begin{cases} 1, & 0 < d \le D \\ 0.5, & D < d \le 2D \\ 0, & d > 2D \end{cases} \tag{11}$$

and

$$\eta = \begin{cases} \eta_0, & \text{if } v_j = v_{\text{spe}} \\ \eta_1, & \text{if } v_j = v_{\text{com}} \\ \eta_2, & \text{if } v_j = v_{\text{mal}}. \end{cases} \tag{12}$$

Due to the diversity of collaborative tasks, each collaborative task should have different requirements s_i^r and corresponding important weight λ_i decided by v_i that subject to $0 \le \lambda_i \le 1$. For example, some trustors may request tasks with stringent response time while others may prefer data protection and integrity. Therefore, R_j is estimated by aggregating differences between each requirement of the collaborative task from v_i and corresponding resources of v_j, given by

$$R_j = \sqrt{\sum_{l=1}^{n} \lambda_l \left(s_l^p - s_l^r\right)^2} \tag{13}$$

where the collection of different collaborative task requirements from v_i is defined as $\mathcal{S}_i^r = \{s_l^r | l \in \{1, 2, \ldots, n\}\}$, which should be fulfilled by v_j. Similarly, $\mathcal{S}_j^p = \{s_l^p | l \in \{1, 2, \ldots, n\}\}$ denotes the corresponding resources owned by v_j to satisfy the collaborative task requirements.

The capability trust $\mathcal{U}_{i,j}^c$ is formulated in (7). ε_1, ε_2 and ε_3 are, respectively, weight coefficients of location proximity $L_{i,j}$, the trustworthiness of role-oriented vehicles O_j and real-time resource situation of the trustee R_j, where $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 1$. These factors have different impacts on the capability trust evaluation thus it is critical to select an appropriate weight coefficient to calculate the capability trust. Gray relation analysis (GRA), a method of multifactor statistical analysis in [35], is harnessed for capability trust calculation to effectively isolate malicious vehicles with enhanced trust evaluation accuracy. The steps of GRA are stated as follows.

Step 1: Determine the referenced sequence and the comparative sequence. $x_0(z)$ is utilized to represent the referenced sequence given by the time sequence of global trust value, which is formulated as

$$x_0(Z) = \{\mathcal{U}_{i,j}^{g_z} | z \in \{1, 2, \ldots, Z\}\} \tag{14}$$

where $\mathcal{U}_{i,j}^{g_z}$ indicates the global trust value at time instant z and Z denotes current time instant.

$x_1(z)$, $x_2(z)$, and $x_3(z)$ represent the comparative sequences, which are the time sequences of above mentioned three capability trust attributes, given by

$$x_1(Z) = \left\{L_{i,j}^z | z \in \{1, 2, \ldots, Z\}\right\} \tag{15}$$

$$x_2(Z) = \left\{O_j^z | z \in \{1, 2, \ldots, Z\}\right\} \tag{16}$$

and

$$x_3(Z) = \left\{R_j^z | z \in \{1, 2, \ldots, Z\}\right\}. \tag{17}$$

Step 2: Compute the gray correlation coefficient $\zeta_r(z)$ between referenced sequence and comparative sequences based on (14)–(17), given by

$$\zeta_r(z) = \frac{\min_r \min_z |x_0(z) - x_r(z)| + \rho \max_r \max_z |x_0(z) - x_r(z)|}{|x_0(z) - x_r(z)| + \rho \max_r \max_z |x_0(z) - x_r(z)|} \tag{18}$$

where $r = 1, 2, 3$ is the index of the time sequence of different capability trust attributes. ρ is a constant ranging from 0 to 1 indicated as a resolution factor.

Step 3: Calculate the value of ε_1, ε_2, and ε_3 based on correlation degree ϱ_r. The mean value of the gray correlation coefficient $\zeta_r(m)$ forms the correlation degree, which is formulated as

$$\varrho_r = \frac{1}{Z} \sum_{z=1}^{Z} \zeta_r(z). \tag{19}$$

Based on (19), the weight coefficient of different capability trust attributes is given by

$$\varepsilon_r = \frac{\varrho_r}{\varrho_1 + \varrho_2 + \varrho_3}, \quad r = 1, 2, 3. \tag{20}$$

2) Direct Experiential Trust: Direct experiential trust evaluation is a prediction of trustee v_j's current behavior based on collaboration experiences, which also served as the estimation basis of v_j's collaboration willingness. This evaluation process will be ignored with no historical collaboration among moving vehicles. Experiential collaboration records $\mathcal{H}_{i,j}$ between v_i and v_j is formulated as

$$\mathcal{H}_{i,j} = \left\{\mathcal{U}_{i,j}^{g_z} \varphi_z | z \in \{1, 2, \ldots, Z\}\right\} \tag{21}$$

where

$$\varphi_z = e^{-(Z-z)} \tag{22}$$

is the time decay factor that diminishes the effectiveness of historical experiences before time instant z.

Based on (21), the summation of positive records α when $\mathcal{U}_{i,j}^{g_z} \varphi_z \geq 0.5$ and the summation of negative records β when $\mathcal{U}_{i,j}^{g_z} \varphi_z < 0.5$ are formulated as

$$\alpha = \sum \mathcal{H}_{i,j}^{+} \tag{23}$$

and

$$\beta = \sum \mathcal{H}_{i,j}^{-} \tag{24}$$

respectively.

The direct experiential trust value of v_i toward v_j obeys the beta distribution [36], and the statistical expectation of the direct experiential trust value is formulated as

$$\mathcal{U}_{i,j}^{h} = E(B(\alpha + 1, \beta + 1)) = \frac{\alpha + 1}{\alpha + \beta + 2}. \tag{25}$$

$\mathcal{U}_{i,j}^{h}$ is the direct experiential trust value calculated based on previous collaboration between v_i and v_j. However, the differences between the previous collaborative situations and the current situation should be considered in direct experiential trust calculations. Different from [36], the variety of collaborative situations for different IoV tasks is considered. Assume there used to be a set of collaborative situations $\mathcal{S}^Z = \{s^z | z \in \{1, 2, \ldots, Z\}\}$ between v_i and v_j, where latest situation is $s^Z = \{s_l^Z | l \in \{1, 2, \ldots, n\}\}$ including n task requirements. The weighted mean of different task requirements from a set of collaborative situations can be formulated as

$$\overline{s_l^r} = \frac{s_l^Z + \sum_{z=1}^{Z-1} \sum_{l=1}^{n} \varphi_z s_l^Z}{1 + \sum_{z=1}^{Z-1} \sum_{l=1}^{n} \varphi_z} \tag{26}$$

where $\varphi_z = e^{-(Z-z)}$ is also presented as the time decay factor that is used to decrease the effectiveness of experiential records of collaborative situations before time instant z.

Furthermore, the similarity Λ between the current collaborative situation and all previous situations is calculated as

$$\Lambda = 1 - \frac{\sum_{l=1}^{n} |s_l^r - \overline{s_l^r}|}{n} \tag{27}$$

which is used to update direct experiential trust value $\mathcal{U}_{i,j}^{h}$ in (25) as

$$\mathcal{U}_{i,j}^{h} = \Lambda \mathcal{U}_{i,j}^{h}. \tag{28}$$

3) Indirect Trust: Indirect trust refers to the aggregated global trust value from recommenders $\mathcal{P}$ regarding the trustworthiness of potential IoV collaborators $\mathcal{N}$. However, the time and resource overhead increase to meet the needs of analyzing the security and privacy implications of transferring recommendations, i.e., indirect trust, from third parties. To reduce the overall trust evaluation time and resource consumption, the whole process of indirect trust evaluation is executed in nearby edge servers offline. A set of recommenders $\mathcal{P} = \{v_p | p \in \{1, 2, \ldots, P\}\}$ will send their collaboration records to nearby edge servers, where the experiential collaboration records sent by a single recommender $v_p \in \mathcal{P}$ about the trustworthiness of $v_j \in \mathcal{N}$ is derived as

$$\mathcal{H}_{p,j} = \left\{\left(\mathcal{S}_p^{r_k}, \mathcal{U}_{p,j}^{g_k}\right) | k \in \{1, 2, \ldots, K\}\right\} \tag{29}$$

Algorithm 1 Mini-Batch K-Means Based Indirect Trust Calculation Algorithm

Input: *P recommenders $\mathcal{P} = \{v_1, \ldots, v_p, \ldots, v_P\}$, current collaborative task requirement $\mathcal{S}_i^r$, experiential collaboration records $\mathcal{H}_{p,j}$ sent from each recommender v_p.*
for $v_p \in \mathbf{P}$ **do**
  RSUs receive $\mathcal{H}_{p,j}$ from v_p.
  Initialize two centroids: $\mathcal{S}_p^{r_k}$, $\mathcal{S}_i^r$.
  $d_1 = \sqrt{(s_{p_1}^r - s_{i_1}^r)^2 + .. + (s_{p_n}^r - s_{i_n}^r)^2}$
  $d_2 = \sqrt{(s_{p_1}^r - s_{p_1}^{r_k})^2 + .. + (s_{p_n}^r - s_{p_n}^{r_k})^2}$
  if $d_1 \leq d_2$ **then**
    $\Phi_1 = \Phi_1 \cup \mathcal{S}_p^{r_k}$
  else
    $\Phi_2 = \Phi_2 \cup \mathcal{S}_p^{r_k}$
  end if
  Calculate $\mathcal{U}_{p,j}^h$ using Eq. (28) based on Φ_2.
end for
Sort $\mathcal{U}_{\mathcal{P}\to j}^h$
Initialize two centroids: $Min(\mathcal{U}_{\mathcal{P}\to j}^h)$, $Max(\mathcal{U}_{\mathcal{P}\to j}^h)$
for $i \in \mathcal{U}_{\mathcal{P}\to j}^h$ **do**
  $d_3 = |\mathcal{U}_{p,j}^h - Min(\mathcal{U}_{\mathcal{P}\to j}^h)|$
  $d_4 = |\mathcal{U}_{p,j}^h - Max(\mathcal{U}_{\mathcal{P}\to j}^h)|$
  if $d_3 \leq d_4$ **then**
    $\Phi_3 = \Phi_3 \cup \mathcal{U}_{p,j}^h$
  else
    $\Phi_4 = \Phi_4 \cup \mathcal{U}_{p,j}^h$
  end if
  Return Φ_4
end for
Calculate $\mathcal{U}_{\mathcal{P}\to j}^{in} = Average(\Phi_4)$
Output: *$\mathcal{U}_{\mathcal{P}\to j}^{in}$*

where K denotes the total number of collaborations between v_p and v_j, and $\mathcal{U}_{p,j}^{g_k}$ and $\mathcal{S}_p^{r_k}$ indicate the corresponding global trust value and collaborative task requirements. With multiple recommenders $\mathcal{P}$, $\mathcal{H}_{\mathcal{P}\to j} \triangleq \cup_{v_p \in \mathcal{P}} \mathcal{H}_{p,j}$ is the union set of all recommendations that the edge server receives and analyzes.

Assume such collaboration records from recommenders will be shared among edge servers through Infrastructure-to-Infrastructure (I2I) communication, and these edge servers will collect and analyze collaboration records from recommenders, picking out the most appropriate collaboration record to calculate the indirect trust value of v_j. In consideration of the variety of environments and collaborative task types, the v_j with good objective ratings from third parties may not be appropriate for completing the target task. Therefore, mini-batch k-means clustering is utilized to detect and filter recommenders that are malicious and with low-collaboration situation similarity. Compared with the proposed k-means filtering algorithm that requires loading entire data into memory [37], [38], the mini-batch k-means reduces the computation time of indirect trust calculation with large data sets, which is more suitable for realistic situations. The formal description of the mini-batch k-means-based indirect trust calculation method is detailed in Algorithm 1 that is implemented in RSUs' nearby edge servers to speed up trust evaluation.

Changing collaborative situations (e.g., task type, channel conditions, and transmission bandwidth) impacts the trust establishment since a device may be trusted in one situation but not in another. Hence, only the recommendations based on similar tasks are utilized for the indirect trust evaluation. The data set of experiential collaboration records $\mathcal{H}_{p,j}$ as shown in (29) is constantly changing and growing over time, thus mini-batch of the data set is selected. Then similar to the k-means clustering algorithm, the current collaborative task requirement $\mathcal{S}_i^r$ from v_i and a random task requirement $\mathcal{S}_p^{r_k}$ from recommenders' experiential collaboration records $\mathcal{H}_{p,j}$ are assigned as centroids, respectively. The Euclidean distances d_1 and d_2 are then calculated between two centroids and other task requirements in $\mathcal{H}_{p,j}$. Finally, two clusters Φ_1 and Φ_2 are obtained based on the comparison between d_1 and d_2 where Φ_2 remains to calculate direct experiential trust value $\mathcal{U}_{p,j}^h$ between v_p and v_j based on (28). Thus, the union set of all direct experiential trust values from $\mathcal{P}$ is $\mathcal{U}_{\mathcal{P}\to j}^h \triangleq \cup_{v_p \in \mathcal{P}} \mathcal{U}_{p,j}^h$.

To eliminate the effects of recommendation attacks, the recommendations from malicious recommenders are discarded through second clustering. The filtered $\mathcal{U}_{\mathcal{P}\to j}^h$ is sorted to select two centroids based on the minimum and maximum values, respectively. Similar to the first clustering, each value in $\mathcal{U}_{\mathcal{P}\to j}^h$ is compared with two centroids based on Euclidean distance evaluation. The obtained d_3 and d_4 are utilized as evidence through a comparison for the cluster assignment. At the end of the for loop, two clusters Φ_3 and Φ_4 are obtained to indicate the group of low and high recommendations, respectively. Finally, Φ_4 is preserved as the primary recommendation and then averaged as the final indirect trust value $\mathcal{U}_{\mathcal{P}\to j}^{\text{in}}$.

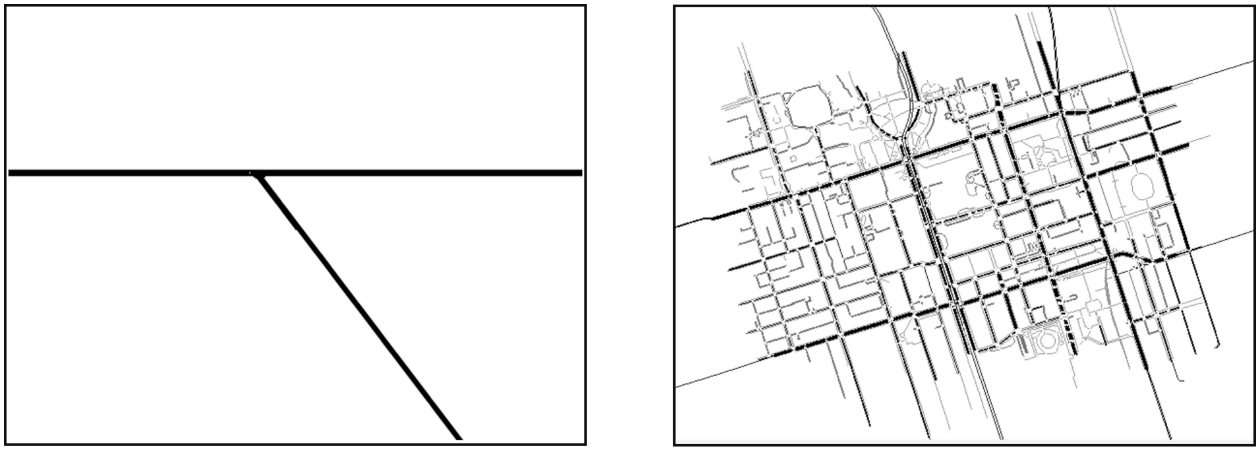
B. Adaptive Trust Factor Aggregation

Global trust represents the aggregated confident indicator from v_i to v_j for task completion by combining various trust factors. However, directly utilizing the weighted sum method to assign static weights for the above three trust evaluation factors without considering different situations brings about inaccurate trust evaluation. Therefore, an adaptive trust factor aggregation scheme is proposed, which is a dynamic aggregation of capability trust, direct experiential trust and indirect trust. Four possible situations in (2), namely, c_1, c_2, c_3, and c_4, are also considered to calculate global trust value $\mathcal{U}_{i,j}^g$ between v_i and v_j as follows:

1) c_1: $H_{\mathcal{P}\to j} = 0$ & $\mathcal{H}_{i,j} = 0$
2) c_2: $\mathcal{H}_{\mathcal{P}\to j} = 0$ & $\mathcal{H}_{i,j} \neq 0$
3) c_3: $\mathcal{H}_{\mathcal{P}\to j} \neq 0$ & $\mathcal{H}_{i,j} = 0$
4) c_4: $\mathcal{H}_{\mathcal{P}\to j} \neq 0$ & $\mathcal{H}_{i,j} \neq 0$.

Based on different situations, the global trust value is formulated as

$$\mathcal{U}_{i,j}^g = \begin{cases} \mathcal{U}_{i,j}^c, & c_1 \\ \min\left\{\mathcal{U}_{i,j}^c,\ \mathcal{U}_{i,j}^h\right\}, & c_2 \\ \min\left\{\mathcal{U}_{i,j}^{\text{in}},\ \mathcal{U}_{i,j}^c\right\}, & c_3 \\ \min\left\{\left(w\mathcal{U}_{i,j}^{\text{in}} + (1-w)\mathcal{U}_{i,j}^h\right),\ \mathcal{U}_{i,j}^c\right\}, & c_4 \end{cases} \tag{30}$$



(a) (b)

Fig. 3. Two simulated maps extracted from SUMO with varying densities of randomly moving vehicles: (a) Simple map with a single intersection and (b) complex map representing a portion of Toronto.

where

$$w = \max\left((1 - \frac{Z}{\Gamma} \times \varphi), 0\right) \tag{31}$$

is the adaptive weight for different cases, φ is a time decay factor that is used to decrease the effectiveness of the experiential record range from 0 to 1 and Z is the total number of collaborations between two vehicles. Once trustor v_i has sufficient direct collaboration with trustee v_j, it will ignore the recommendations from nearby RSUs and depend more on its own experience to avoid the recommendation attacks. Let Γ be the number of collaborations required to calculate global trust solely based on direct experiences while ignoring recommendations. Considering all potential IoV collaborators $\mathcal{N}$, the union set of all global trust values between v_i and $\mathcal{N}$ is $\mathcal{U}^g_{i\to\mathcal{N}} \triangleq \cup_{v_j\in\mathcal{N}}\mathcal{U}^g_{i,j}$.

C. Trust Decision and Update

Based on the calculated global trust value of all potential collaborative vehicles, the vehicle that obtains the highest global trust in $\mathcal{U}^g_{i\to\mathcal{N}}$ is selected for collaboration. After the collaboration, as shown in (32), the global trust value of the selected collaborator will be updated based on the comparison between the calculated QoE and satisfaction threshold of trustor τ, where a reward factor R and a punish factor P are harnessed for increasing or decreasing global trust value, respectively. Then the updated global trust value is uploaded to edge servers as recommendation evidence

$$\mathcal{U}^g_{i,j} = \begin{cases} \mathcal{U}^g_{i,j} + R, \text{ if QoE} \geq \tau \\ \mathcal{U}^g_{i,j} - P, \text{ if QoE} < \tau. \end{cases} \tag{32}$$

Remark 2: The primary goal of this article that maximizes QoE with minimized task completion time is achieved based on the proposed RTE mechanism. Specifically, to reduce the task completion time $T_{i,j}$ as shown in (1), the most suitable collaborator is selected based on RTE with high-trust evaluation accuracy, meanwhile, the time used for trust evaluation $t^E_{i,j}$ is reduced based on the prior assessment of indirect trust in edge servers. Furthermore, due to the integration of estimating location proximity $L_{i,j}$ and real-time resource situations of collaborators R_j in capability trust evaluation, the selected collaborators will have high-data transmission rate and CPU frequency while guaranteeing uninterrupted communication, thus reducing the task computational delay $t^C_{i,j}$ and transmission delay $t^T_{i,j}$.

IV. Performance Evaluation

In this section, a series of simulations are conducted to evaluate the performance of our proposed RTE mechanism. The simulation goal is to validate the effectiveness of RTE in achieving rapid and reliable IoV collaboration with fast and accurate trust evaluation by harnessing several evaluation metrics, including task completion time, QoE, trust evaluation accuracy, and convergence rate.

A. Simulation Setup

To validate the proposed RTE mechanism, we exploit SUMO, a mobility traffic simulator, to design a simple map with only one intersection and a complex map of part Toronto as shown in Fig. 3, respectively, which generated a synthetic data set, including real mobility traces of different densities of vehicles [39]. Based on the data set, an edge-enabled IoV system with a wide variety of moving vehicles and RSUs is simulated in Python.

In our simulation, we consider a large-scale IoV environment consisting of multiple vehicles moving randomly, each equipped with a dedicated short-range communications (DSRCs) device offering an approximate communication range of 300 m (980 ft) [40]. Within this environment, the numerous moving vehicles are categorized into 100 trustors, each carrying a single task to be offloaded, while the number of trustees varies from 100 to 1000, encompassing different collaboration capabilities and willingness levels. To assess the security of the trust-based IoV collaborator selection process, we conducted experiments with varying proportions of malicious trustees, combining On-and-Off threats and recommendation attacks as hybrid attacks, each initiated

TABLE II
CONFIDENCE VALUE ASSIGNMENT BASED ON VEHICLE CATEGORIES

Vehicle Categories	Confidence Value η
Malicious Vehicles	$0 \leq \eta_0 < 0.5$
Common Vehicles	$0.5 \leq \eta_1 < 0.8$
Specific Vehicles	$0.8 \leq \eta_2 < 1$

TABLE III
MAJOR SIMULATION PARAMETERS

Parameters	Value
Total Trustors	100
Total Trustees	[100, 1000]
Total Malicious Trustees (%)	[10, 70]
Specific Trustees (%)	5
Collaboration Satisfaction Threshold (τ)	0.5
Vehicle Communication Range Radius D (m)	300
Reward Factor R	0.01
Punish Factor P	0.1
Computation size of task h_i (10^9 cycles)	[0.2, 3.2]
Vehicle computational capacity $a_j f_j$ (GHz)	[5, 10]
Data size of task Υ_i (KB)	[50, 500]
V2V bandwidth $B_{i,j}$ (MHz)	10
Vehicle signal transmission power $b_{i,j}$ (dBm)	32
White Gaussian noise N_0 (dBm)	-124

by an equal proportion of malicious vehicles. Specifically, recommendation attackers continually provide misleading recommendations to nearby edge servers, while On-and-Off attackers alternate between normal and malicious behaviors within specific time intervals. The simulation parameters are summarized in Tables II and III.

B. Evaluation Metrics and Comparison Methods

Several evaluation metrics are considered which are divided into three distinct classes for the performance evaluation of the proposed RTE.

1) *Robustness:* Due to the involvement of a large number of trustees with different types and complicated road conditions in IoV, it is necessary to evaluate the robustness performance of RTE under varying trustee densities (ranging from 100 to 1000) and random percentages of malicious trustees (spanning from 10% to 70%) in complicated traffic environments. Collaborative task completion time in (1) and the defined QoE function in (5) are considered as two main metrics for robustness performance evaluation.
2) *Accuracy:* Accurate trust evaluation serves as the basis to support rapid and reliable IoV collaborator selection, which further affects the overall IoV task completion time. We assume the trustworthiness ground truth g_j of legitimate and malicious trustees are 1 and 0, respectively. The accuracy of trust evaluation $\mathcal{A}$ is derived based on the comparison between predicted global trust value $\mathcal{U}_{i,j}^g$ and ground truth g_j of trustee v_j, given by

$$\mathcal{A} = 1 - |\mathcal{U}_{i,j}^g - g_j|. \tag{33}$$

3) *Convergence Rate of Trust Ground Truth:* To validate that the proposed RTE can achieve rapid evaluation, the rate of converging to trust ground truth is compared with other trust models. The convergence value in our simulation is the maximum number of IoV collaborations (iterations) that are required for converging to trust ground truth.

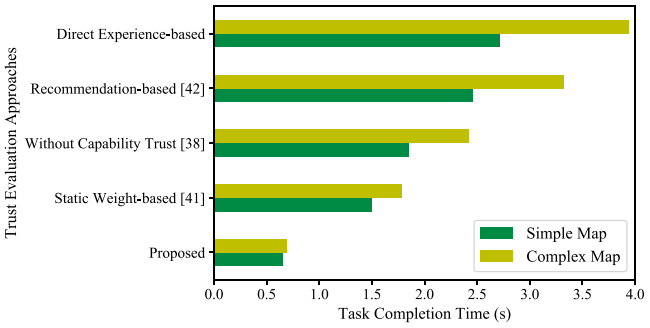


Fig. 4. Task completion time comparison based on different trust evaluation mechanisms in a simple map and a complex map.

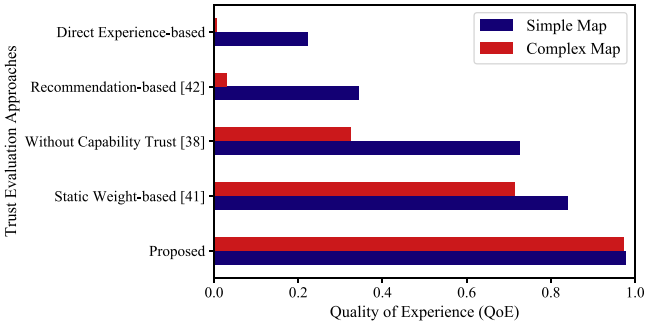


Fig. 5. QoE comparison based on different trust evaluation mechanisms in a simple map and a complex map.

To make the experimental results more convincing, four different trust evaluation mechanisms are considered and compared with the proposed RTE.

1) *Static Weight-Based Trust Model* assigns fixed weights for different trust evaluation factors in global trust evaluation [41].
2) *Trust Model Without Capability Trust Evaluation* that assigns the initial trust values for all unknown vehicles as a fixed constant, i.e., 0.5 [38].
3) *Recommendation-Based Trust Model* solely relies on the trustors themselves to compute both direct evidence from past experiences and recommendations from third parties, independent of assistance from edge servers [42].
4) *Direct Experience-Based Trust Model* that only considers previous experiences between two parties where the evaluated trust value of trustee is derived based on (28).

C. Robustness Performance

In this section, several existing trust models and the proposed RTE will be compared based on task completion time and QoE, aiming at demonstrating the better robustness performance of the proposed RTE.

1) Impact of Traffic Environments: The simulation involved 1000 trustees, and hybrid attackers with proportions ranging from 10% to 70%. Figs. 4 and 5 present the average

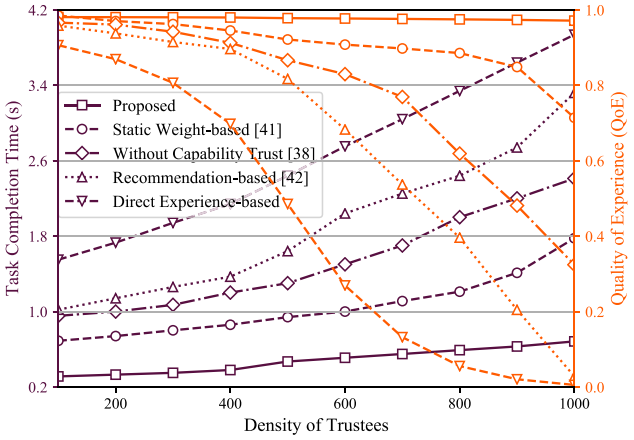


Fig. 6. Task completion time and QoE comparison based on different trust evaluation mechanisms under various trustee densities.

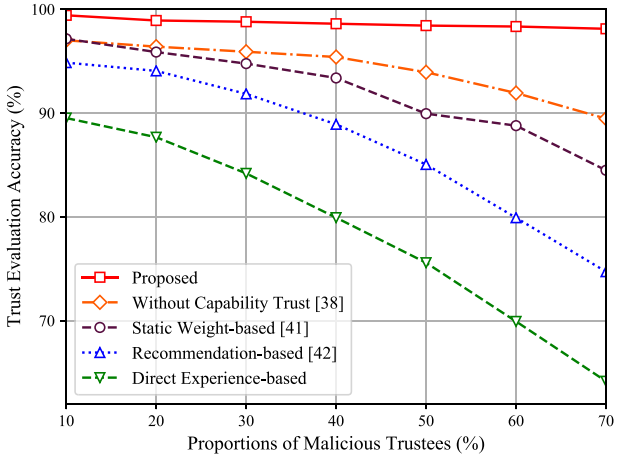


Fig. 7. Comparison of accuracy among different trust evaluation mechanisms across varying percentages of malicious trustees employing hybrid attacks.

outcomes of 100 collaborations, comparing task completion time and QoE performance across different trust models in both simple and complex maps. In summary, as traffic complexity increases, task completion time rises, and QoE diminishes. This effect is particularly pronounced for direct experience-based, recommendation-based, and trust models without capability evaluation since they struggle to accurately assess trust values for unknown collaborative trustees, elevating the risk of selecting malicious ones. Furthermore, the static weight-based trust model experiences increased task completion times and deteriorated QoE due to growing pending data for trust evaluation. However, our proposed RTE, by incorporating precalculations in edge servers and assessing collaborator capabilities and willingness, consistently maintains the shortest task completion time and the highest QoE performance, even in complex traffic scenarios.

2) Impact of Trustee Density: The collaboration performance is degraded by the higher existence probability of hybrid attackers due to increased trustee densities. Similarly, in this simulation, 100 collaborations are conducted and the average is shown for each point (e.g., 200 trustees) in Fig. 6. As shown in Fig. 6, different densities of vehicles ranging from 100 to 1000 are considered during the simulation, where a larger density will lead to a higher task completion time and worse QoE performance. In contrast, our proposed RTE is less sensitive to changes in trustee densities, which can maintain around 0.5 s of task completion time and approximately 0.98 QoE value under a total of 1000 moving trustees, while the other baseline trust models require more than 1.8 s as well as much worse QoE performance.

D. Accuracy Performance

In this section, the accuracy of the proposed RTE is evaluated considering different impacts under various percentages of malicious vehicles, where hybrid attacks are launched.

1) Impact of Hybrid Attacks: In Fig. 7, we present a comparison of trust evaluation accuracy, considering all the baseline trust models outlined in the simulation setup. The proportions of malicious trustees are varied from 10% to 70%. Notably, a higher proportion of malicious vehicles consistently leads to decreased trust evaluation accuracy across all models. However, the proposed RTE consistently outperforms other models, especially when incorporating capability trust in the evaluation process. While the static weight-based trust model achieves higher accuracy than the recommendation-based and direct experience-based schemes, the lack of adaptive trust factor aggregation limits its performance. The inclusion of capability trust evaluation and adaptive trust factor aggregation significantly improves the evaluation accuracy of RTE. Importantly, the proposed RTE experiences only minimal impact from increased proportions of malicious vehicles, largely due to the exclusion of malicious recommendations from recommendation attackers and unrelated recommendations through the mini-batch k-means algorithm.

To further evaluate the impact of malicious vehicles in trust evaluation, the evaluated trust value under different trust models is compared for a legitimate trustee and a malicious trustee, respectively. As shown in Fig. 8(a) and (b), a legitimate and a malicious trustee are selected randomly, thus the evaluated trust value close to 1 and 0, respectively, should be expected even with increased proportions of malicious trustees. Specifically, compared with other models, it can be observed that the proposed RTE obtains minimal trust value bias while nearly maintaining the same value with increased proportions of malicious trustees.

2) Impact of Adaptive Trust Factor Aggregation: To evaluate the effectiveness of adaptive trust factor aggregation, a comparison is conducted between the adaptive and fixed global trust evaluation methods under varying proportions of malicious trustees, as illustrated in Fig. 9. As the proportion of malicious vehicles increases from 10% to 70%, the accuracy of fixed global trust evaluation decreases, whereas the adaptive scheme maintains stable accuracy levels. In (31), the w served as the proportion of recommendation trust affects the global trust evaluation. Especially, recommendation trust value becomes inaccurate with large proportions of malicious vehicles, thus assigning larger w will have a negative impact on trust evaluation accuracy. However, the proposed adaptive trust factor aggregation scheme mitigates the above issue, which improves the accuracy of trust calculation.

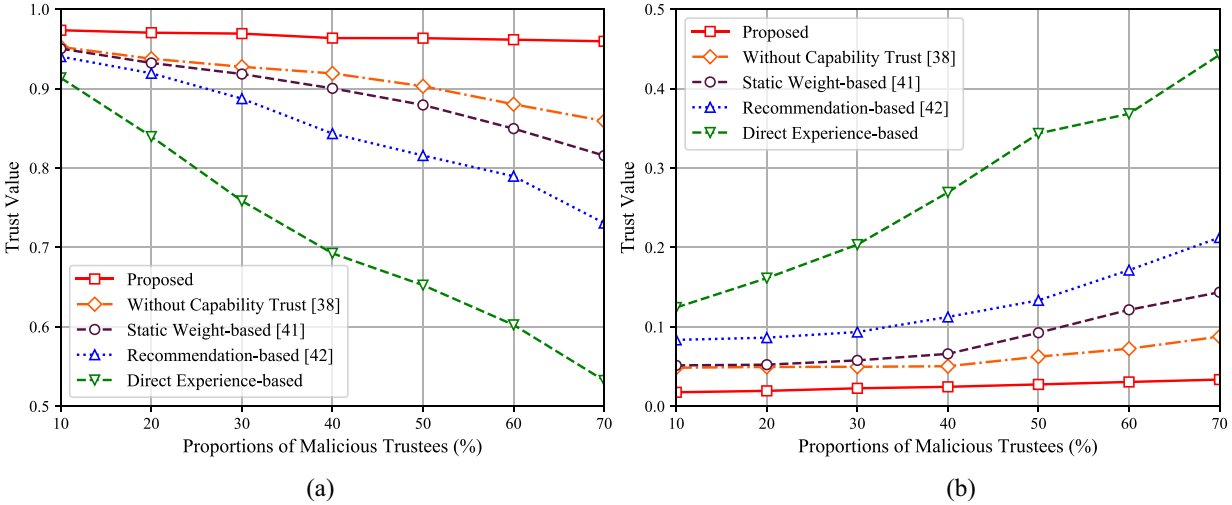


Fig. 8. Comparison of trust values under different trust evaluation mechanisms with varying proportions of trustees launching hybrid attacks. (a) Legitimate trustee. (b) Malicious trustee.

TABLE IV
COMPARISON AND SUMMARY OF SIMULATION RESULTS UNDER DIFFERENT EVALUATION METRICS

	Task Completion Time (s)	QoE	Accuracy (%)	Convergence Value
Static weight-based [41]	1.78	0.71	84.48	50
Without capability trust [38]	2.41	0.32	89.46	40
Recommendation-based [42]	3.32	0.02	74.71	60
Direct experience-based	3.94	0.006	64.15	70
Proposed	0.68	0.97	98.11	10

Notes: Task completion time, QoE, and accuracy are assessed in a complex map with 70% malicious trustees, while convergence value represents the maximum iterations needed for convergence to trust ground truth.

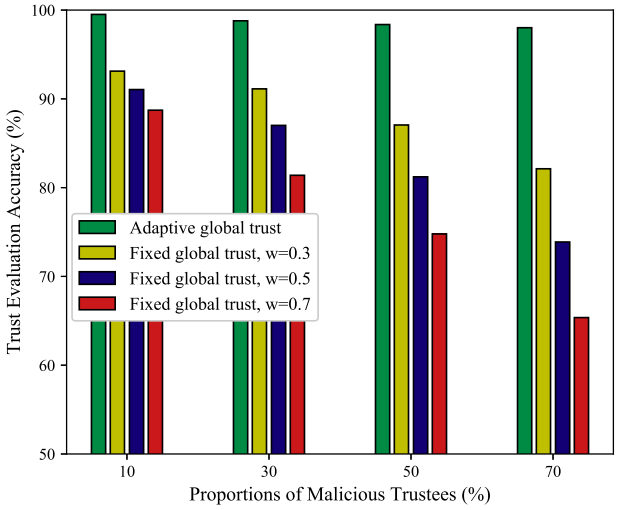


Fig. 9. Accuracy comparison between adaptive and fixed global trust evaluation, where the global trust evaluation is based on our proposed adaptive trust factor aggregation scheme while fixed global trust evaluation is achieved by assigning a static weight w for different trust evaluation factors.

E. Convergence Performance

As shown in Fig. 10(a), for a legitimate trustee, based on our proposed RTE, the trust value converges to the ground truth 1 faster and the trust value bias is minimal with more collaboration because precalculations in edge servers speed up the trust evaluation. Similarly, for a malicious trustee, Fig. 10(b) shows our proposed RTE also has a better convergence performance than other models. Moreover, for a vehicle that changes from legitimate status to malicious status in the 50th collaboration by launching routing attacks, Fig. 10(c) validates the new ground truth is also converged faster by RTE and it further validates our proposed RTE can prevent On-and-Off threats. To illustrate the effectiveness of the proposed RTE mechanism more intuitively, Table IV provides a comprehensive comparison and summary of simulation results across various evaluation metrics.

V. CONCLUSION

In this article, we first introduce a comprehensive trust concept tailored to the demands of rapid and reliable IoV collaboration. Different factors, i.e., indirect trust, direct experiential trust, and capability trust, are incorporated into this trust concept and further harnessed in the adaptive trust factor aggregation scheme to maximize QoE. Specifically, RSU-transferred indirect trust streamlines trust evaluation, while the introduction of capability trust and direct experiential trust expedites collaborator selection, thus reducing task completion time. Simulation results show that the proposed RTE outperforms existing models in task completion time, QoE, trust evaluation accuracy and attacker detection. In the future, we aim to explore the integration of machine learning-based techniques to further optimize trust evaluation efficiency and accuracy. Additionally, we plan to extend our

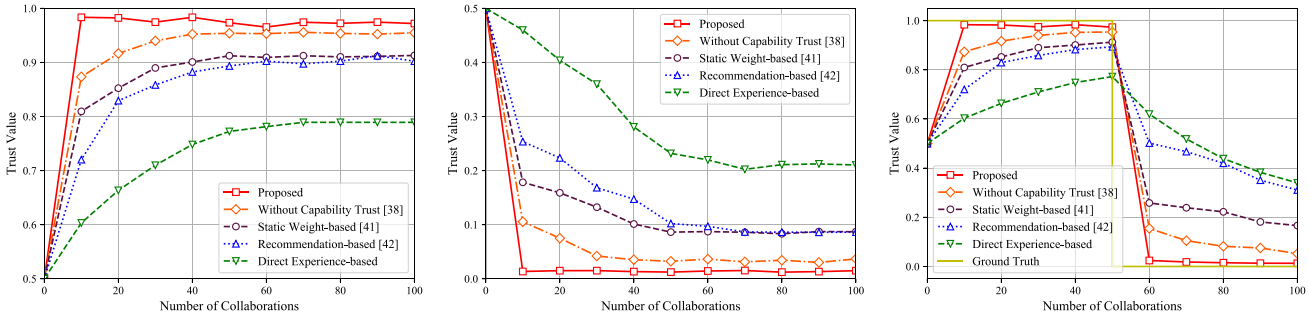


Fig. 10. Convergence performance comparison based on different trust evaluation mechanisms: (a) legitimate trustee, (b) malicious trustee, and (c) from legitimate trustee to malicious trustee.

research to encompass a broader range of task types, beyond time-sensitive tasks, to support diverse collaboration services and applications.

REFERENCES

[1] M. Noor-A-Rahim et al., "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE.*, vol. 110, no. 6, pp. 712–734, Jun. 2022.

[2] M. B. Mollah et al., "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[3] L. Bréhon-Grataloup, R. Kacimi, and A.-L. Beylot, "Mobile edge computing for V2X architectures and applications: A survey," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108797.

[4] D. P. M. Osorio et al., "Towards 6G-enabled Internet of Vehicles: Security and privacy," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 82–105, 2022.

[5] J. Wang, L. Wu, H. Wang, K.-K. R. Choo, L. Wang, and D. He, "A secure and efficient multiserver authentication and key agreement protocol for Internet of Vehicles," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 24398–24416, Dec. 2022.

[6] H. Fang, Z. Xiao, X. Wang, and N. Al-Dhahir, "Lightweight flexible group authentication utilizing historical collaboration process information," *IEEE Trans. Commun.*, vol. 71, no. 4, pp. 2260–2273, Apr. 2023.

[7] B. D. Deebak et al., "A lightweight blockchain-based remote mutual authentication for AI-empowered IoT sustainable computing systems," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6652–6660, Apr. 2023.

[8] H. Tan, W. Zheng, P. Vijayakumar, K. Sakurai, and N. Kumar, "An efficient vehicle-assisted aggregate authentication scheme for infrastructure-less vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, May 30, 2022, doi: 10.1109/TITS.2022.3176406.

[9] H. Gao, Y. Xiao, H. Yan, Y. Tian, D. Wang, and W. Wang, "A learning-based credible participant recruitment strategy for mobile crowd sensing," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5302–5314, Jun. 2020.

[10] Y. Jiang et al., "Reliable distributed computing for metaverse: A hierarchical game-theoretic approach," *IEEE Trans. Veh. Technol.*, vol. 72, no. 1, pp. 1084–1100, Jan. 2023.

[11] X. Wang, W. Wu, and D. Qi, "Mobility-aware participant recruitment for vehicle-based mobile crowdsensing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4415–4426, May 2018.

[12] M. Ylianttila et al., "6G white paper: Research challenges for trust, security and privacy," 2020, *arXiv:2004.11665*.

[13] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jäntti, "A survey on blockchain-based trust management for Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 7, pp. 5898–5922, Apr. 2023.

[14] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the Internet of Vehicles," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108558.

[15] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A survey on trust models in heterogeneous networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2127–2162, 4th Quart., 2022.

[16] M. Poongodi, M. Hamdi, A. Sharma, M. Ma, and P. K. Singh, "DDoS detection mechanism using trust-based evaluation system in VANET," *IEEE Access*, vol. 7, pp. 183532–183544, 2019.

[17] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-based trust model for vehicle-to-everything (V2X)," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 440–450, Jan. 2020.

[18] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3157–3169, Mar. 2021.

[19] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu, "NOTRINO: A NOvel hybrid TRust management scheme for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9244–9257, Sep. 2021.

[20] T. Wang, H. Luo, X. Zeng, Z. Yu, A. Liu, and A. K. Sangaiah, "Mobility based trust evaluation for heterogeneous electric vehicles network in smart cities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1797–1806, Mar. 2021.

[21] X. Chen, J. Ding, and Z. Lu, "A decentralized trust management system for intelligent transportation environments," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 1, pp. 558–571, Jan. 2022.

[22] O. B. Abderrahim, M. H. Elhedhili, and L. Saidane, "CTMS-SIOT: A context-based trust management system for the social Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2017, pp. 1903–1908.

[23] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the Internet of Things (CTM-IoT)," in *Proc. 12th Int. Conf. Broad. Wireless Comput. Commun. Appl. (BWCCA)*, 2018, pp. 533–543.

[24] J. Chen, Z. Tian, X. Cui, L. Yin, and X. Wang, "Trust architecture and reputation evaluation for Internet of Things," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 8, pp. 3099–3107, 2019.

[25] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu, "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4757–4769, Jul. 2021.

[26] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang, "A semi-centralized trust management model based on blockchain for data exchange in IoT system," *IEEE Trans. Services Comput.*, vol. 16, no. 2, pp. 858–871, Mar./Apr. 2023.

[27] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, and A. Taherkordi, "Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2169–2182, Feb. 2023.

[28] Y. Sun et al., "Adaptive learning-based task offloading for vehicular edge computing systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3061–3074, Apr. 2019.

[29] J. Ni, K. Zhang, Q. Xia, X. Lin, and X. S. Shen, "Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 19, no. 6, pp. 1317–1331, Jun. 2020.

[30] M. Bin-Yahya, O. Alhussein, and X. Shen, "Securing software-defined WSNs communication via trust management," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22230–22245, Nov. 2022.

[31] S. Li, J. Huang, J. Hu, and B. Cheng, "QoE-DEER: A QoE-aware decentralized resource allocation scheme for edge computing," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 2, pp. 1059–1073, Jun. 2022.

[32] C. Chen, Y. Zeng, H. Li, Y. Liu, and S. Wan, "A multihop task offloading decision model in MEC-enabled Internet of Vehicles," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3215–3230, Feb. 2023.
[33] X. He, H. Lu, M. Du, Y. Mao, and K. Wang, "QoE-based task offloading with deep reinforcement learning in edge-enabled Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 4, pp. 2252–2261, Apr. 2021.
[34] C. Song, W. Xu, T. Wu, S. Yu, P. Zeng, and N. Zhang, "QoE-driven edge caching in vehicle networks based on deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5286–5295, Jun. 2021.
[35] W. Liang, J. Long, T.-H. Weng, X. Chen, K.-C. Li, and A. Y. Zomaya, "TBRS: A trust based recommendation scheme for vehicular CPS network," *Future Gener. Comput. Syst.*, vol. 92, pp. 383–398, Mar. 2019.
[36] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8857–8867, Jul. 2022.
[37] Z. Gao et al., "A credible and lightweight multidimensional trust evaluation mechanism for service-oriented IoT edge computing environment," in *Proc. IEEE Int. Cong. Internet Things. (ICIOT)*, 2019, pp. 156–164.
[38] G. Chen, F. Zeng, J. Zhang, T. Lu, J. Shen, and W. Shu, "An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems," *Comput. Netw.*, vol. 190, May 2021 Art. no. 107952.
[39] P. A. Lopez et al., "Microscopic traffic simulation using sumo," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, 2018, pp. 2575–2582.
[40] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.
[41] J. Chen and X. Wang, "TCNS: An efficient trusted cooperative node selection model for Internet of Vehicles," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, 2021, pp. 1–6.
[42] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social Internet of Things systems," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 684–696, Nov./Dec. 2016.

Jiazhi Chen (Graduate Student Member, IEEE) is currently pursuing the Ph.D. degree with Western University, London, ON, Canada.

She was a Research Assistant with the Department of Electrical and Computer Engineering, Western University. Her current research interests include communication and network security, trust modeling and management, mobile collaborative computing, task offloading, and machine learning.

Xianbin Wang (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from The National University of Singapore, Singapore, in 2001.

He is a Professor and a Tier-1 Canada Research Chair in 5G and Wireless IoT Communications with Western University, London, ON, Canada. Prior to joining Western University, he was a Research Scientist/Senior Research Scientist with the Communications Research Centre Canada, Ottawa, ON, Canada, from 2002 to 2007. From 2001 to 2002, he was a System Designer with STMicroelectronics, Mississauga, ON, Canada. He has over 500 highly cited journals and conference papers, in addition to over 30 granted and pending patents and several standard contributions. His current research interests include 5G/6G technologies, Internet of Things, communications security, machine learning, and intelligent communications.

Dr. Wang has received many prestigious awards and recognitions, including the IEEE Canada R. A. Fessenden Award, the Canada Research Chair, the Engineering Research Excellence Award at Western University, the Canadian Federal Government Public Service Award, the Ontario Early Researcher Award, and nine best paper awards. He was involved in many IEEE conferences, including GLOBECOM, ICC, VTC, PIMRC, WCNC, CCECE, and CWIT, in different roles, such as the General Chair, the TPC Chair, the Symposium Chair, the Tutorial Instructor, the Track Chair, the Session Chair, and a Keynote Speaker. He serves/has served as the Editor-in-Chief, an Associate Editor-in-Chief, and an editor/associate editor for over ten journals. He was the Chair of the IEEE ComSoc Signal Processing and Computing for Communications Technical Committee and is currently serving as the Central Area Chair for IEEE Canada. He is a Fellow of the Canadian Academy of Engineering and the Engineering Institute of Canada.

Xuemin (Sherman) Shen (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990.

He is a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on network resource management, wireless network security, Internet of Things, 5G and beyond, and vehicular ad hoc and sensor networks.

Dr. Shen received the Canadian Award for Telecommunications Research from the Canadian Society of Information Theory in 2021, the R.A. Fessenden Award in 2019 from IEEE, Canada, the Award of Merit from the Federation of Chinese Canadian Professionals (Ontario) in 2019, the James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society, the Joseph LoCicero Award in 2015 and the Education Award in 2017 from the IEEE Communications Society, and the Technical Recognition Award from Wireless Communications Technical Committee in 2019 and the AHSN Technical Committee in 2013. He has also received the Excellent Graduate Supervision Award in 2006 from the University of Waterloo and the Premier's Research Excellence Award in 2003 from the Province of Ontario, Canada. He served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom' 16, IEEE Infocom'14, IEEE VTC'10 Fall, IEEE Globecom'07, and the Chair for the IEEE Communications Society Technical Committee on Wireless Communications. He is the President of the IEEE Communications Society. He was the Vice President for Technical and Educational Activities, the Vice President for Publications, the Member-at-Large on the Board of Governors, the Chair of the Distinguished Lecturer Selection Committee, the Member of IEEE Fellow Selection Committee of the ComSoc. He served as the Editor-in-Chief of the IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, and *IET Communications*. He is a Registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, a Chinese Academy of Engineering Foreign Member, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society.