

Research on Trust Mechanism of C-V2X (Cellular Vehicle-to-Everything)

Yifan Xi^{1,2}, Jinling Hu^{1,2*}, Li Zhao^{1,2}, Jiayi Fang^{1,2}, Rui Zhao^{1,2}, Hui Deng^{1,2} and Shilei Zheng^{1,2}

¹ CICT Connected and Intelligent Technologies Co., Ltd., 100029, China

² National Engineering Research Center of Mobile Communications and Vehicular Networks, 100191, China

Received: xx xxxxxxxx 2021 / Revised: xx xxxxxx 2022 / Accepted: xx xxxxxxxx 2022 / Published online: xx xxxxx 2023

Abstract C-V2X (Cellular Vehicle-to-Everything) has emerged as a transformative and innovative technology in automotive and communication industries. C-V2X communication enables nearby traffic participants to exchange real-time information, such as status, positioning and location, thereby facilitating environmental perception, information sharing, and collaborative control capabilities. However, due to the dynamic nature of traffic topology and high vehicle mobility, improving safety and efficiency in the distributed C-V2X system is complex and context-dependent. The information shared among the participants requires a systematic technical solution to solve the untrustworthy issues. In order to address the challenges, this paper focuses on the trust mechanism in the C-V2X system. It analyzes the latest research progress on trust mechanisms for C-V2X from both academia and industry. A trustworthiness evaluation framework focused on lifecycle management of trust models is proposed, including trust information management and analysis, trust models management, trustworthiness evaluation, and trust decision. Taking two typical C-V2X scenarios as examples, this paper illustrates the detailed trust assessment process with different modules in the system. Finally, the open and important research issues are proposed for the future trust mechanism of C-V2X.

Keywords C-V2X, Trust framework, Trustworthiness evaluation

Citation Yifan Xi, Jinling Hu and Li Zhao, et al. Research on Trust Mechanism of C-V2X (Cellular Vehicle-to-Everything). *Security and Safety* 2024; x: xxxxxxxx.
<https://doi.org/10.1051/sands/xxxxxxx>

1 Introduction

V2X (Vehicle-to-Everything), as a new generation of information and communication technology spanning communication, automotive, and transportation industries, has become a prominent and profound reform and innovative technology in transportation and automotive industries [1]. As shown in Figure 1, V2X empowers all-round communication among vehicles and the surrounding environments, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Network (V2N). Through the efficient and accurate communication, it can provide environmental perception, information exchange and collaborative control capabilities for Intelligent and Connected Vehicle (ICV) and Intelligent Transportation System (ITS) applications [2].

V2X applications are evolving from basic functions such as road safety, traffic efficiency and infotainment services to the advanced applications like automated driving with diverse communication performance requirements. With the rapid changes in traffic topology and high mobility of vehicles, road safety applications have the stringent requirements of communication performance, mainly demanding high frequency, low latency and high reliability. Typical advanced V2X applications support scenarios like platooning, semi-/fully-automated driving, remote driving and extended sensors. Therefore, more exacting

* Corresponding author (email: hujinling@cictci.com)

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

© The Author(s), published by EDP Sciences and China Science Publishing & Media Ltd., 2023

communication requirements have emerged, including extremely low latency, extremely high reliability, higher transmission rate, larger communication range and support for higher moving speeds [3]. C-V2X (Cellular V2X), based on cellular communication technology, introduces technological innovation with its direct communication capabilities. Its short-range communication mode supports direct links, addressing low-latency and high-reliability communication challenges. Meanwhile, it leverages the existing mobile network infrastructure to facilitate long-range communication with high transmission rates.

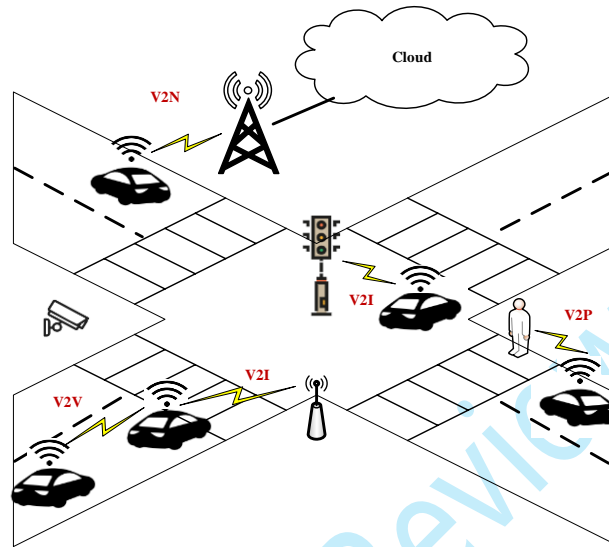


Figure 1. V2X communication types

With the development of ICV and ITS, the data exchange frequency between On-Board Units (OBUs) and Roadside Units (RSUs) has been increasing. Moreover, influenced by the dynamic changes of traffic flow, the scenarios of information exchange and environmental perception have become more complex [4]. As indicated in the global Status Report on Road Safety 2013, without immediate and decisive intervention, road traffic injuries will ascend to become the fifth leading cause of mortality by 2030 [5]. The capacity of connected vehicles to share data can facilitate safer driving practices, enhance traffic flow and improve management. Connected vehicles utilize their onboard communication capabilities to transmit real-time traffic data, predict changing road conditions, and identify the road signs and warnings.

However, if an OBU transmits false data due to hardware failure or malicious attacks, it may cause traffic disruptions, accidents, or collisions, resulting in property damage and even loss of life [6]. Therefore, the trust mechanisms for nodes and data transmission are of crucial importance, and the trust requirements in C-V2X have emerged. Distributed C-V2X systems present severe challenges to trust management mechanism due to the lack of a centralized communication infrastructure. For example, OBUs may receive heterogeneous, multi-source data with potential conflicts from sensors or other C-V2X traffic participants. Furthermore, as not all data sources are equally reliable, some may be damaged or malfunctioning, leading to incomplete or ambiguous information [7]. Therefore, establishing a unified trust mechanism for C-V2X is a highly challenging systematic project.

In this paper, we focus on the core issues of trust mechanism in the C-V2X communication system. The following section analyzes the latest progress of the C-V2X related trust mechanism research from both academia and Standards Developing Organizations (SDOs). Then, an example of a trust framework that can be used for the trustworthiness evaluation in C-V2X is proposed, and the trust assessment process in typical C-V2X scenarios is presented. Subsequently, technical evolution towards the trust mechanism in C-V2X is discussed and the article is concluded.

2 Related Work

The trust mechanism has become a crucial element for the trustworthy operation of C-V2X system. Trust assessment is an essential component of trust mechanisms, prompting the research community to conduct

in-depth studies on the development and implementation of the trust mechanism.

For the trust mechanism, it is necessary to clarify the following two important concepts. “Trust” is typically defined as a measurable belief or confidence held by one entity (e.g., an OBU or a RSU) towards another entity. “Trustworthiness” is defined as the likelihood that a trusted entity will fulfil the trust expectations of the entity providing trust in a given context, where such expectations often pertain to the functionality of an entrusted task [8].

Trust assessment schemes play a vital role in trust mechanism within the context of C-V2X. The typical trust assessment schemes include entity-centric trust, data-centric trust, and integrated trust, as detailed below.

2.1 Entity-Centric Trust

In entity-centric trust scheme, the involved entities (e.g., OBUs, RSUs) are the core objects of trust assessment. To evaluate the trustworthiness among entities, the diverse attributes, behaviors, and associations of the entity are attached with great importance. These various characteristics of the vehicle itself are analyzed comprehensively, such as its historical performance in terms of reliability, its compliance with communication protocols, and its capacity to maintain the C-V2X connections with other entities [9]

For example, in the scenario of vehicle platooning, each vehicle needs to establish trust with other vehicles. The entity-centric trust assessment can assist the vehicles in the platoon to judge whether other vehicles are trustworthy. By evaluating the driving behaviors and communication capabilities of vehicles, those with a higher trustworthiness can be selected to form a platoon, ensuring the safety and efficiency of driving. Despite its advantages, entity-centric trust approaches struggle in highly dynamic environments, where frequent topology changes and high mobility make it difficult to maintain up-to-date behavioral records.

2.2 Data-Centric Trust

Data-centric trust, also called event-centric trust, is used to evaluate the trustworthiness of information associated with events such as accidents, collisions, traffic jams, etc., and to identify false information within it [10]. Here, the emphasis shifts to the data transmitted and received by the traffic participants. In the highly dynamic environments of C-V2X communication, the different aspects related to speed, distance, and environmental conditions, which can reflect the results of the trust assessment, should be considered. Key data metrics may include data quality, integrity, timeliness, consistency, discrepancies, and delays. By focusing on data-centric trust, potential issues related to false or misleading information can be identified and mitigated. Nevertheless, as C-V2X data includes sensor data, communication data, and environmental data, data-centric trust lacks a unified standard to evaluate the trustworthiness of different types of data.

2.3 Integrated Trust

Based on both entity-centric and data-centric trust schemes, the integrated trust scheme considers not only the trustworthiness of entities themselves, but also the quality and reliability of the data. It provides a comprehensive trust assessment for interactions with C-V2X. For example, when traffic information is transmitted among vehicles, the integrated trust will simultaneously consider the attributes such as the reputation of the transmitting vehicle as well as the quality of the transmitted traffic data.

Integrated trust schemes aim to mitigate the limitations of purely entity-centric or data-centric approaches. However, designing an effective integrated trust model remains challenging due to the need for efficient fusion of heterogeneous information and the adaptation of fusion rules to diverse and dynamic C-V2X scenarios. The computational complexity and the potential for increased communication overhead for exchanging both entity and data trust metrics are also significant concerns that need to be addressed.

In the automotive industry, some work related to trust modeling and assessment has already been done. In [11], the trustworthiness of data is calculated using the weighted method, leveraging OBUs, RSUs and sensors on the automated vehicle to measure the trustworthiness in V2I communication mode. Estimating the number of available sensors in automated vehicles and calculating their sensing capabilities, and then the credibility of automated vehicles is weighted and evaluated according to their ability to monitor the transmitted data. In [12], the decentralized trust management scheme uses a trustworthiness calculation method based on fuzzy logic to evaluate direct trust, that is, when the trustee node is within the transmission

range of the trustor node, the direct trust is evaluated using fuzzy logic. Meanwhile, a method based on reinforcement learning is also adopted to estimate indirect trust. When the behaviors of the trustee cannot be directly observed, the indirect trust is estimated through reinforcement learning. In [13], the subjective logic method is utilized where vehicles determine their subjective trust opinions of other vehicles based on direct and indirect trust assessments. In the direct trust assessment, vehicle i determines its view of another vehicle j according to the collected evidence and one-on-one interactions. To this end, vehicle i sends data packets to vehicle j and observes the forwarding behavior of vehicle j . Based on the enhanced on-demand ad-hoc distance vector protocol, trust opinions can be assigned to other vehicles, enabling them to calculate trust opinions based on the data. In [10], both entity-centric and data-centric trust schemes are used to calculate the trustworthiness of a node, and the decision is made on whether the corresponding node should be trusted. To this end, several decision-making logics such as weighted voting and Bayesian inference have been tried and compared.

In summary, within the research scope of C-V2X, the trustworthiness of vehicles is of great significance to the efficiency and security of transportation systems and has emerged as a pivotal area of investigation in this domain. Facing the new challenges, the trust mechanism needs to be continuously improved. The subsequent section will introduce existing trust standards to further elucidate the role of trust in C-V2X.

3 The Progress of Standardization

The SDOs and industrial alliances such as ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) and 5GAA (5G Automotive Association) have conducted the related research to advance the trust issues.

ITU-T released two recommendations for information and communication technology infrastructures and services. ITU-T Y.3052 [14] divides the world into physical, cyber and social worlds, analyzes the potential risks and necessity of trust, and presents the concept of trust with its characteristics and a relationship model. This recommendation introduces the trust assessment methods and trust-provisioning processes (data collection, management, analysis, dissemination, and lifecycle management). ITU-T Y.3057 [15] further provides a trust index model based on the research results of Y.3052; this model categorizes trust indicators into objective (like ability, integrity, benevolence) and subjective (such as experience, reputation, inclination) types. A trust index, a composite value combining multiple trust indicators, is used in the decision-making process. Stakeholders can utilize the model, but need to consider risks and limitations, and ensure transparency, explainability, and auditability.

5GAA launched work items related to trust of vehicles, including TPM4V2X (Trustable Position Metrics for V2X Applications), Trust4Auto (Creating Trust in Connected Automated Vehicles), and the ongoing Trust4CAV (Creating Trust in Connected and Automated Vehicles) research.

TPM4V2X focuses on the trustworthiness issues of positioning and location information exchange in the context of V2X communication [16]. It reviews existing ETSI (European Telecommunications Standards Institute) standards of GNSS (Global Navigation Satellite System), and analyzes gaps in current V2X standards regarding confidence information. It concludes that the confidence ellipse should be utilized in the V2X message, and the definition of confidence ellipse should be harmonized. OEMs' (Original Equipment Manufacturer) feedback indicates that the position confidence parameter is used in current and future use cases and is crucial for different applications.

Trust4Auto defines the dynamic trust assessment within the automotive domains, specifically for connected and automated vehicles (CAVs) [17]. It highlights the significance of trust mechanism in CAVs and defines fundamental concepts like trust objects, relationships, and networks. In conclusion, it underlines the importance of these defined concepts and the necessity for future exploration of concrete solutions in trust assessment while effectively dealing with the inherent uncertainty in the process. Based on Trust4Auto, Trust4CAV [18] aims to address challenges in assessing and quantifying trustworthiness in CAVs. The ongoing work item aims to achieve the consensus of the methodology for calculating the Actual Trustworthiness Level (ATL) and Required Trustworthiness Level (RTL) and addresses the challenges of establishing and quantifying trust in CAVs, ensuring safety and reliability in an increasingly automated driving environment.

4 Trustworthiness Evaluation Framework

In order to compare the differentiated trust among entities, a systematic method for measuring, quantifying

and evaluating trust is needed. The framework of trust mechanism of C-V2X is shown in Figure 2. This framework includes trust information management and analysis, trust model management, trustworthiness evaluation, and trust decision. The detailed information of the above modules is elaborated as follows.

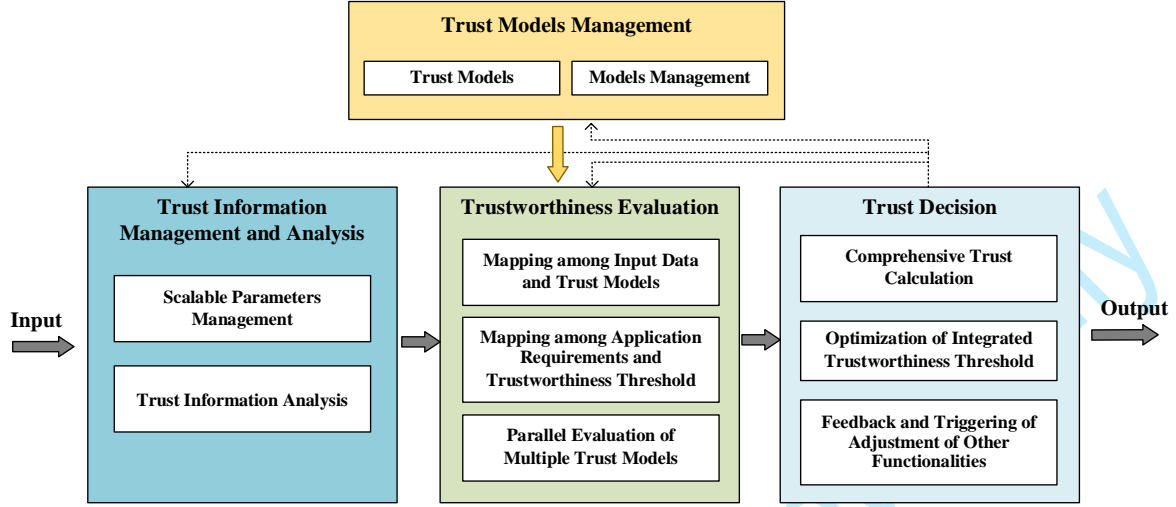


Figure 2. Trustworthiness Evaluation Framework

Algorithm 1 Trustworthiness Evaluation Framework Process

Input:

Entity set	$E = \{OBU, RSU, \dots\}$
Data source	D
Trust models	$M = \{M_1, M_2, \dots, M_n\}$
Application requirements	R (safety, efficiency, ...)
Trustworthiness threshold	T

Process:

```

// 1. Scalable parameter management and trust information analysis
P = ScalableParametersManagement(E, D)
// set I: trust sources, evidences, properties, relationships
I = TrustInformationAnalysis(P, E)
// 2. Parallel evaluation of multiple trust models
for each Mi ∈ M do in parallel
    ti = EvaluateTrustworthiness(I, Mi)           // single model trustworthiness
    Tmid = TmidUpdate(ti)
end for
// 3. Comprehensive trust calculation and optimization of integrated trustworthiness threshold
Tfinal = ComprehensiveTrustCalculation(Tmid) // weighted average, majority vote, etc.
Topt = OptimizationIntegratedThreshold(R, T) // safety and security constraints
// 4. Trust decision
if Tfinal ≥ Topt then
    decision = "Trustworthy"
    outMsg = TrustRecommendation(Tfinal)
else
    decision = "Untrustworthy"
    outMsg = Warning(Tfinal)
end if

```

Output:

Comprehensive trust value	T_{final}
Decision label	decision
Human-readable message	outMsg

Figure 3. Trustworthiness Evaluation Framework Process Algorithm

4.1 Trust Information Management and Analysis

4.1.1 Scalable Parameters Management

In the trustworthiness evaluation framework, input parameters are primarily derived from trust-related

information collected from diverse entities and data sources. In the distributed C-V2X environment, entities can include OBUs, RSUs, and on-board sensors. Data may be gathered from heterogeneous and multiple sources; for example, driving behaviors such as sudden braking and sharp turning maneuvers can be collected from neighboring nodes. The collected information also includes security-related data, such as node authentication status (success/failure), cryptographic signature validity to avoid suspected Sybil attempts (e.g., duplicate device IDs detected within the same communication range). These numerous parameters form the fundamental input information for conducting trustworthiness evaluation.

4.1.2 Trust Information Analysis

The collected parameter information is filtered to extract parameters relevant to trust assessment from the entities type and data type information. Meaningful trust information is extracted from the parameters by considering Trust Sources, Trust Evidences, Trust Properties, and Trust Relationships.

For the Trust Sources, the appropriate trust sources should be selected to evaluate trustworthiness. In [17], trust sources are initially classified into six categories, including trust sources related to communication, trust sources related to system integrity, trust sources related to applications, trust sources related to entity behavior, sources of trust from safety point of view, and trust sources related to sensor data integrity. Regarding Trust Evidences, the process of trust assessment is based on evidences derived from a range of sources, providing verifiable information about the specific trust attributes. For example, the historical behaviors through trust relationship can be utilized for the formulation of trust evidences. The Trust Properties define the characteristics of entities and can reflect the dynamic characteristics of trust. The trustworthiness may be evaluated to assess whether the trusted party has the right relevant attributes to meet the trustor's expectations in a given trust relationship. Typical trust properties include reliability, robustness, accuracy, etc. The Trust Relationships are between two trust objects and is defined according to specific attributes. Even for the same evaluating party, if different trust properties are evaluated, the trust relationship may be different. Typical trust relationships include direct trust and indirect trust. In direct trust relationships, nodes evaluate not only communication reliability but also the authenticity of identities.

4.2 Trust Model Management

The trustworthiness evaluation model can be deployed by various entities. Due to the diverse requirements, entities may utilize different trust metrics. Each entity is able to manage the trust models flexibly and scalably, helping it determine whether to accept the trust results provided by the specific trustworthiness evaluation model.

4.2.1 Trust Model

In the context of uncertainty and unpredictability in C-V2X, the typical statistical models can be used for trustworthiness evaluation as follows.

Probabilistic Logic [19] utilizes probability theory to deal with uncertainty and evaluate the possibility of trust. For example, the trustworthiness is determined by calculating the probability that a node's behavior conforms to expectations. For example, the trustworthiness T of a node can be expressed as $T = P(B|E)$, where B denotes the behavior conforming to expectations, and E represents the observed evidence.

Bayesian Probability [20] is a probabilistic graphical model used to represent the probabilistic relationships between variables. The trustworthiness update can be formulated as

$$P(H|E) = \frac{P(E|H) \cdot P(H)}{P(E)}$$

where H is the hypothesis (e.g., the node is trustworthy), and E represents the new evidence. Based on Bayes' theorem, trustworthiness is updated by combining prior knowledge and new evidences. Bayesian probability allows for the continuous adjustment of the trustworthiness evaluation in response to the updated information and over time. In C-V2X, the Bayesian probability can take the trust-related factors as variables, such as the historical behavior of vehicles, communication quality, environmental factors. These variables are then used to calculate and update the trustworthiness through Bayes' theorem.

Fuzzy Logic [21] addresses fuzziness and uncertainty by allowing trustworthiness evaluation in C-V2X to take values within a certain range. For example, "stable driving behavior" is a fuzzy concept that can be categorized into "very stable," "relatively stable," "less stable," or "very unstable" using fuzzy sets. The

trustworthiness is then assessed by establishing fuzzy rules, such as "If the rate of change of vehicle speed is small and the following distance is appropriate, then the driving behavior is very stable". Finally, a specific trustworthiness value is obtained through fuzzy reasoning and defuzzification operations.

Subjective Logic [22] represents a formal method used to handle uncertainty and subjective trust, enabling different users to evaluate trust according to their own needs and judgments. Besides trust and distrust, it also separately considers the level of uncertainty. This is very important for C-V2X, where a vehicle may be unable to calculate the trustworthiness in another entity due to insufficient information or other reasons.

Reputation-based Trust Model [23] evaluates the reputation of an entity by collecting and analyzing its historical behavior records, and then determines trustworthiness value. For C-V2X, the reputation of a vehicle can be established based on factors, including the accuracy of the information it has previously provided, its compliance with traffic rules, and its communication behavior.

4.2.2 Model Management

Model management includes the lifecycle management processes such as model configuration, update, deletion and combination. According to the characteristics of different scenarios and entities in C-V2X, it reasonably sets the parameters and structures of trust models to ensure their applicability. In the dynamic environment, models need to be continuously updated as new data keeps emerging or threat intelligence feeds, such as the driving data of vehicles and known Sybil attack patterns or emerging data spoofing techniques. The model management will take these data into consideration and update the models in a timely manner to reflect the latest trust status. When the related entities no longer participate in the C-V2X system, deletion operations can avoid the interference of the obsolete data on the evaluation. Meanwhile, the model management can combine different trust models to fully utilize the advantages of each model.

Through these functionalities, trust model management provides the model basis for trustworthiness calculation, ensuring that the trustworthiness can be reasonably evaluated and guaranteeing the trustworthy operation of the C-V2X system.

4.3 Trustworthiness Evaluation

4.3.1 Mapping among Input Data and Trust Models

Based on the results of Trust Information and Analysis and the configured Trust Models, the input information, including entity-centric and data-centric types, can respectively correspond to the applicable trust models to calculate a trust metrics. For example, entity types can utilize fuzzy logic through centralized or distributed processing, while data types can make use of Bayesian probability. The subjective logic trust models can be utilized for both entity-centric and data-centric types of input information.

4.3.2 Mapping among Application Requirements and Trustworthiness Thresholds

The trustworthiness thresholds for different scenarios are determined according to specific application requirements. For example, in automated driving and safety-related scenarios, the trustworthiness threshold may be set relatively high because a wrong warning could lead to serious consequences. In this way, the mapping of the application requirements to the trustworthiness thresholds ensures that the system can make decisions based on appropriate trust criteria in different scenarios.

4.3.3 Parallel Evaluation of Multiple Trust Models

For one or more trust models configured in the trust model management module, the input information of entity types, data types or a mixture of entity types and data types can be utilized. It is necessary to weigh the pros and cons and choose the most appropriate way of parallel computation according to factors such as data scale, model complexity, the amount of entity interaction information processing, and limitations of computing resources.

4.4 Trust Decision

4.4.1 Comprehensive Trust Calculation

Based on the real-time outputs of multiple parallel trustworthiness computations in the Trustworthiness

Evaluation module, the ATL is dynamically calculated using the configured trust models. For example, the Bayesian probability model may focus on updating the trust probability based on real-time evidence, while the reputation-based model emphasizes evaluating reputation and trust through the accumulation of long-term behaviors. These models evaluate trustworthiness from different perspectives, and the results need to be integrated. Methods such as weighted averaging and voting mechanisms can be adopted to fuse the results of different trust models.

4.4.2 Optimization of Integrated Trustworthiness Threshold

Based on the mapping of application requirements and trustworthiness thresholds, optional calculation methods for trustworthiness thresholds from other sources may be considered, such as functional safety (FuSa), safety of the intended functionality (SOTIF), information and data security, and capability limitations of the system and components. The above related information is integrated to achieve the optimized integrated trustworthiness threshold for the subsequent trust decision.

4.4.3 Feedback and Triggering of Adjustment of Other Functionalities

To mitigate the impact of imbalanced input information on trustworthiness evaluation, a closed-loop trustworthiness feedback adjustment mechanism is constructed through the interaction processing between the Trust Decision module and other modules. For example, the scalable parameter management sub-module in Figure 2 can adjust the types of input parameters, while the trust information analysis sub-module can modify the processing methods for multi-dimensional information analysis.

After the completion of the trustworthiness calculation, it is necessary to finally make decisions with required output trustworthiness value, such as the output of trust level classification, the output of numerical trustworthiness, or the output of trust suggestions and decision support can be carried out.

Through this refined trustworthiness evaluation framework of C-V2X, trustworthiness can be evaluated more comprehensively and accurately for various scenarios.

4.5 Standardization Research

The trust framework may align with existing C-V2X protocols to facilitate interoperability. For example, the extension of Basic Safety Message (BSM) could reference CSAE 183-2021[24], which provides extensible fields for custom data. By leveraging the "Application Specific Extension" field, trust-related metadata (e.g., trust level score, evaluation timestamp) might be encoded in a structured manner.

For security layer integration, the framework may reference the YD/T 6013-2024[25] for security layer authentication and authorization. This standard specifies the architecture, security requirements, and authentication processes for C-V2X device authentication and authorization systems, applying to identity verification and access control of vehicle communication devices. During the initial trust establishment phase, a vehicle might obtain an initial trust baseline through the authentication procedures. For example, in this trust framework, a vehicle passing authentication could be assigned a baseline trust level, with subsequent dynamic adjustments based on real-time behavior monitoring.

Notably, this trust framework aims to leverage existing security mechanisms within a unified trust system, enabling rapid deployment across different C-V2X scenarios. By integrating security protocols and this trustworthiness evaluation framework, this approach may enhance system reliability while addressing challenges like data tampering or node impersonation. Future work could explore deeper fusion of security standards and trust models to create a more robust, unified trustworthiness management system for C-V2X.

4.6 Comparative Analysis of Existing Trust Models

To systematically position the proposed trust framework within the broader research landscape, this section presents a comparative analysis of key existing trust models in the literature. Table 1 summarizes their core characteristics, limitations, and application scenarios.

Table 1. Comparative Analysis of Trust Models

Trust Model	Core Characteristics	Limitations	Application Scenarios
-------------	----------------------	-------------	-----------------------

PKI-Based Trust Model	- Relies on Certificate Authorities (CAs) for identity verification - Uses digital certificates to authenticate nodes/messages	- Single-point failure (CA compromise collapses trust system) - High dependency on hierarchical CA infrastructure	- Structured networks (e.g., internal communications security certification for financial institutions)
Reputation-Based Trust Model	- Calculates trust via historical behavior (e.g., node cooperation, message reliability)	- Vulnerable to collusion attacks (malicious nodes inflate reputation) - Slow convergence in dynamic environments	- Static or low-mobility networks (e.g., online marketplaces, IoT device clusters)
Context-Aware Trust Model	- Incorporates environmental factors (time, location, network status) for trustworthiness evaluation	- Complex context modeling (high computational overhead) - Sensitivity to incomplete context data	- MANETs, edge computing environments with stable context patterns
The proposed framework	- Supports dynamic trust updates via real-time sidelink communication metrics - Distributed trust anchor management	- Higher computational complexity due to multi-model integration	- Urban and highway C-V2X scenarios, automated driving, and dynamic traffic topologies

The above comparison shows that the trust model proposed in this paper can be widely used in complex network scenarios of C-V2X, and can quickly adjust the trust value according to the node's dynamic behavior and environmental changes, thereby providing enhanced support for secure communication and reliable interaction of C-V2X.

5 Trustworthiness Evaluation in Typical C-V2X Driving Scenarios

To illustrate the trustworthiness evaluation process of the proposed trust mechanism in the C-V2X, we exemplify the following two typical C-V2X scenarios by applying the trustworthiness evaluation framework to demonstrate the effectiveness [26].

5.1 Typical C-V2X Scenarios

Scenario 1: Abnormal Vehicles with Obstructions Ahead

When low visibility is caused by weather conditions or obstructions are present, abnormal vehicles in the same lane ahead may only be noticed when approaching, or the vehicle ahead may suddenly stop. In such situations, the vehicle behind usually makes an emergency lane change. If there are other vehicles closely following behind, the possibility of a rear-end collision is significantly increased. In Figure 4, when a Host Vehicle (HV) and a Remote Vehicle (RV) are driving at a steady speed with C-V2X information interaction. When the RV detects an abnormal vehicle RV1 ahead and is about to change lanes, the HV can receive the BSM transmitted by RV1. Subsequently, HV will trigger a warning of "Abnormal Vehicle Ahead".

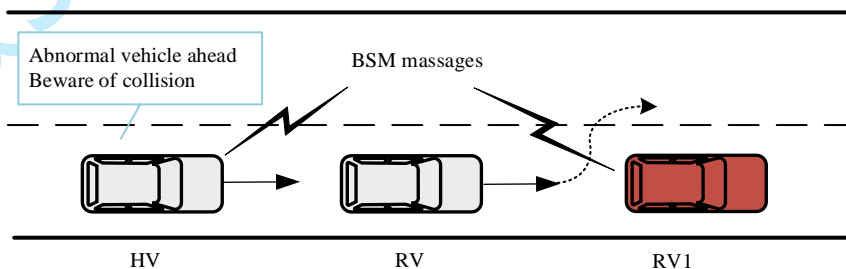


Figure 4. Scenario 1: Abnormal Vehicles with Obstructions Ahead

Scenario 2: Connected Autonomous Emergency Braking (C-AEB)

When obstacles (e.g. vehicles or pedestrians appearing suddenly from blind spots) are present on the

road, human drivers often cannot timely identify dangerous targets (e.g. vehicles, pedestrians) using only their vision, rear-view cameras, or single-vehicle sensors. For example, when the HV is driving through an intersection, vehicles on the side lanes may block the driver’s view of the HV, resulting in the inability to detect vehicles crossing from the left side. With the assistance of RSU or other vehicles, vehicles can obtain the position and attitude information of the obstructed objects in advance. The on-board C-V2X collaborative application system fuses the single-vehicle sensing data from cameras and radars with the C-V2X data to estimate the collision risk. When the collision risk is detected between the host vehicle and the object, the system will alert the driver through Human Machine Interface (HMI) with vehicle control signals (such as braking or reducing the vehicle speed) to avoid collisions or mitigate the severity of collisions.

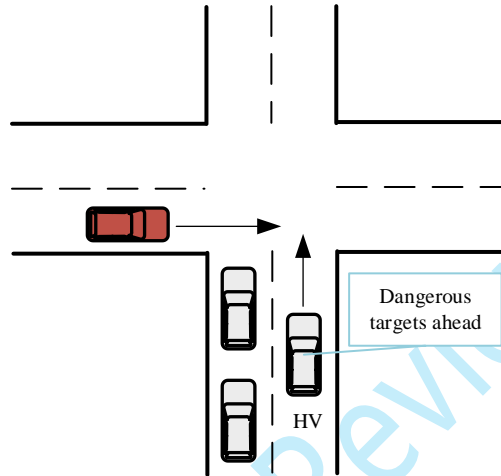


Figure 5. Scenario 2: C-AEB

Considering the high safety impact of these two scenarios, it is important to evaluate the trustworthiness of the received information. Table 2 presents an example of trustworthiness evaluation process based on the framework described in Section 4 for these two typical scenarios.

Table 2. Examples of Trustworthiness Evaluation of Two Typical Scenarios

Scenarios	Scenario 1: Abnormal Vehicles with Obstructions Ahead	Scenario 2: C-AEB
Scalable Parameters Management	<ul style="list-style-type: none"> Entity types: HV, RVs, RSU Data types: BSM messages, event messages, position information, attitude information, high-precision map information 	<ul style="list-style-type: none"> Entity types: HV, RVs, pedestrian, RSU Data types: camera signal data, radar signal data, BSM messages, event messages, position information, attitude information, high-precision map information
Trust Information Analysis	<p>Trust Sources:</p> <ul style="list-style-type: none"> Related to communication: transmission quality of BSM messages Related to entity behaviors: whether RV driving behaviors is standardized <p>Trust Properties:</p> <ul style="list-style-type: none"> Accuracy and reliability of HV’s and RVs’ position information <p>Trust Relationships:</p> <ul style="list-style-type: none"> Direct trust: vehicles that have been following the vehicle steadily for a long period of time Indirect trust: indirectly obtaining information through other vehicles 	<p>Trust Sources:</p> <ul style="list-style-type: none"> Related to communication: transmission quality of BSM messages Related to entity behaviors: whether RV driving behavior is standardized Related to the integrity of the sensing data: camera signal data, radar signal data <p>Trust Properties:</p> <ul style="list-style-type: none"> Accuracy and reliability of HV’s, pedestrian’s and RVs’ position information <p>Trust Relationships:</p> <ul style="list-style-type: none"> Direct trust: vehicles that have been following the vehicle steadily for a long period of time Indirect trust: indirectly obtaining information

		through other vehicles
Trust Model Management	<ul style="list-style-type: none"> • Configuration: The tolerance parameter for error in location information in the probabilistic logic model • Update: Bayesian Probabilistic model is updated according to new BSM messages and new camera, radar data received by HV in real time 	
Trustworthiness Evaluation	<p>Mapping among Input Data and Trust Models:</p> <ul style="list-style-type: none"> • Probabilistic logic model can be used to evaluate trustworthiness by calculating the probability that information about the positional attitude of surrounding vehicles meets the expectation of normal driving. • Bayesian probabilistic model can be used to update trustworthiness by combining the historical behavior of vehicles and new BSM messages. • Fuzzy logic can deal with fuzzy concepts, such as “relatively stable driving attitude” and “Higher risk of collision.” • Subjective logic takes into account the subjective judgments of information trustworthiness by different vehicles' subjective judgments of information trustworthiness. • Reputation-based model can build reputation scores based on the accuracy of information provided by vehicle history and compliance with traffic rules. <p>Mapping among application requirements and trustworthiness thresholds:</p> <ul style="list-style-type: none"> • Trustworthiness threshold can be set relatively high for both scenarios, as false warnings can lead to unnecessary driver stress and operational errors. 	
Trust Decision	<p>Comprehensive Trust Calculation:</p> <ul style="list-style-type: none"> • Weighted consideration of the contribution of the vehicle's historical reputation and the accuracy of its current location information to the trustworthiness <p>Optimization of Integrated Trustworthiness Threshold:</p> <ul style="list-style-type: none"> • FuSa (the stability of the warning system itself), information and data security (whether BSM messages have been tampered with), and limitations on the capabilities of the system components (limitations on the accuracy of the positioning system, camera and radar sensing range and accuracy) • The final threshold is calculated by performing a weighted average based on above individual threshold 	
Output	The output of trust level classification can be carried out.	

5.2 Scalability: high-density urban deployment scenarios

In high-density urban traffic scenarios (e.g., commercial centers, transportation hubs), the C-V2X system needs to handle trustworthiness evaluation requirements for a large number of dynamic nodes, placing higher demands on the real-time performance and resource efficiency of the framework. The trustworthiness analysis framework adapts through the following mechanisms.

1. Congestion Control

The framework employs priority-based congestion control to manage trustworthiness evaluation. Trust messages can be categorized into emergency (e.g., collision warnings with higher priority level) and routine (e.g., status updates with lower priority level). During resource contention, emergency trustworthiness evaluations preempt non-critical tasks, with dedicated scheduling ensuring lower latency for safety-critical messages.

2. Multi-Hop Trust Propagation

Trustworthiness transmission for non-proximity vehicles can be achieved through trusted relay nodes. Vehicles can indirectly obtain trust information of remote vehicles via intermediate nodes. For example, vehicle A obtains historical behavior records of vehicle C through the forwarding of vehicle B, and evaluates vehicle C's trustworthiness based on the trustworthiness of vehicle B. Relay nodes with direct interaction (e.g., previously communicated vehicles) are preferentially selected. A trust chain verification mechanism is adopted, where each level of relay node must provide signature endorsement for the transmitted trust information to ensure information traceability and tamper resistance.

3. Adaptive Trust Tailoring

In complex scenarios where full trust metadata transmission is infeasible, the framework can support adaptive trust tailoring via trust-related information subset transmission. For example, dynamic parameter

tailoring transmits critical subsets (e.g., position, safety-critical event flags) instead of complete trust-related information, which can reduce data volume while maintaining evaluation accuracy.

6 Conclusion

This paper summarizes the current status of trust mechanism of C-V2X research in academia and industry. The trustworthiness evaluation framework applicable to C-V2X is proposed with key factors such as behaviors, reputations, and security of various entities. Through trustworthiness evaluation, all the traffic participants can achieve the trustworthiness evaluation results of other entities, thereby making corresponding trust decisions.

In the field of C-V2X, the construction of trust mechanism is currently facing a series of key issues and challenges for future research, which are highly significant for achieving efficient and secure communication. In [27], the security issues faced by the integrated vehicle-road-cloud system and their corresponding solutions were discussed. Besides, there are still some problems to be solved. The following open and important research issues are proposed for the future trust mechanism of C-V2X.

Firstly, because of the high mobility of vehicles, trust mechanism must possess sufficient flexibility and adaptability to maintain the accuracy and effectiveness of trustworthiness evaluation to avoid the situations such as the interruption or incorrect evaluation of trust relationships caused by frequent changes in the topology. Furthermore, the construction of trust mechanism for many-to-many C-V2X communications is a key aspect, involving how to establish and maintain trust relationships among numerous communication entities with the respective unique security requirements. In addition, adapting trust models to match specific scenarios and service requirements is also a challenge. C-V2X covers a wide range of application scenarios, and different scenarios and services have significant differences in their focus and requirements for trust models. For example, in automated driving scenarios, the trustworthiness of real-time data collected by vehicle sensors is strictly required, while in parking lot management scenarios, more emphasis is placed on the trustworthiness of vehicle identification information and location information. The focus of future research lies in designing trust models that can flexibly and intelligently adjust model parameters and evaluation strategies according to different scenarios and service requirements. Finally, the integration of communication, trust, and security is one of the core tasks in the development of the C-V2X system. Additionally, exploring the deep fusion of cryptographic technologies (e.g., elliptic curve encryption for data integrity) and blockchain-based trust anchoring, a unified trust-security framework will be formed to achieve decentralized trust management and real-time security verification. It will be necessary to organically integrate an efficient communication system, a reliable trust mechanism, and a solid security framework into a synergistic whole, enabling them to promote each other and jointly drive the robust development of C-V2X technology in complex traffic environment. At this initial research stage, the work primarily focuses on proposing the trustworthiness evaluation framework. In the future, we will collaborate with industry partners to advance technical research and standardization efforts, and further verify the rationality of the proposed scheme through simulations and field tests in real-world traffic environments.

Conflicts of interest

The author declares no conflict of interest.

Data availability

No data are associated with this article.

Authors' contributions

Conceptualization, Yifan Xi, Jinling Hu, Li Zhao; investigation, Yifan Xi, Jinling Hu, Li Zhao, Jiayi Fang, Rui Zhao, Hui Deng and Shilei Zheng; writing-original draft preparation, Yifan Xi; writing-review and editing, Yifan Xi, Li Zhao.s

Acknowledgements

We greatly appreciate the comments and suggestions of all reviewers.

Funding

National Natural Science Foundation of China: Cooperative control and sensor fusion for self-organized vehicle-road-cloud systems using 5G and V2X technologies.

References

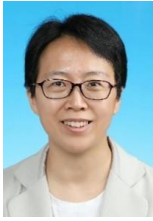
- [1] S. Z. Chen, J. L. Hu, Y. Shi, et al., "LTE-V: a TD-LTE-based V2X solution for future vehicular network," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 997-1005, 2016.
- [2] S. Z. Chen, Y. M. Ge, Y. Shi, et al., "Technology development, application and prospect of cellular vehicle-to-everything(C-V2X)," *Telecommunications Science*, vol. 38, no. 1, p. 12, 2022.
- [3] 3GPP, "Enhancement of 3GPP support for V2X scenarios: TS 22.186, v16.2.0," 2019.
- [4] ISO 21217:2014, "Intelligent transport systems - communications access for land mobiles (CALM) - architecture," 2014.
- [5] World Health Organization, "Global status report on road safety 2013: supporting a decade of action," 2013.
- [6] 3GPP TS 33.185, v14.1.0, "Security aspect for LTE support of vehicle-to-everything (V2X) services," 2017.
- [7] ETSI TS 102 941, v1.2.1, "Intelligent transport systems (ITS); security; trust and privacy management," 2018.
- [8] CONNECT Deliverable D3.1, "Architectural Specification of CONNECT Trust Assessment Framework, Operation and Interaction," 2024.
- [9] P. Angin, et al., "An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing," *IEEE*, pp. 177-183, 2010.
- [10] M. Raya, et al., "On data-centric trust establishment in ephemeral ad hoc networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008.
- [11] H. Wu, et al., "Spatial propagation of information in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, pp. 420-431, 2009.
- [12] S. Guleng, C. Wu, X. Chen, et al., "Decentralized Trust Evaluation in Vehicular Internet of Things," *IEEE Access*, 2019.
- [13] M. Sohail, L. Wang, S. Jiang, et al., "Multi-Hop Interpersonal Trust Assessment in Vehicular Ad Hoc Networks using Three-Valued Subjective Logic," *IET Information Security*, vol. 13, no. 3, pp. 223-230, 2018.
- [14] ITU-T Y.3052, "Overview of trust provisioning in information and communication technology infrastructures and services," 2017.
- [15] ITU-T Y.3057, "A trust index model for information and communication technology infrastructures and services," 2021.
- [16] 5GAA White Paper, "Trustable Position Metrics for V2X Applications," 2023.
- [17] 5GAA White Paper, "Creating Trust in Connected and Automated Vehicles," 2023.
- [18] 5GAA Work Item Description, "Creating Trust in Connected Automated Vehicles," 2024.
- [19] G. D. Wyss, H. K. Schriener, T. R. Gaylor, "Probabilistic logic modeling of network reliability for hybrid network architectures," in *IEEE Conference on Local Computer Networks*, IEEE, 1996.
- [20] P. Dempster, "A generalization of Bayesian inference," 1968.
- [21] L. A. Zadeh, "Fuzzy logic," *Computer*, 1988.
- [22] A. Josang, R. F. Hayward, S. Pope, "Trust Network Analysis with Subjective Logic," *IEEE*, 2008.
- [23] L. Mekouar, Y. Iraqi, R. Boutaba, "Reputation-Based Trust Management in Peer-to-Peer Systems: Taxonomy and Anatomy," Springer U.S., 2010.
- [24] China Society of Automotive Engineers (CSAE). Technical Specification for C-V2X Basic Safety Message (BSM) Format. CSAE 183-2021, 2021.
- [25] Ministry of Industry and Information Technology (MIIT). Technical Requirements for C-V2X Internet of Vehicles Authentication and Authorization System. YD/T 6013-2024, 2024.
- [26] White Paper, "Typical application scenarios and implementation references of C-V2X vehicle-vehicle/vehicle-road collaboration for Vehicle-Road-Cloud Integrated System," 2024.
- [27] J. S. WU, "Security & Safety Issues and Resilience Engineering for Vehicle-Road-Cloud integrated system," *Transportation and Vehicle Engineering Discipline Forum*, 2024.



Yifan Xi is currently a standardization research engineer at CICT Connected and Intelligent Technologies Co., Ltd. Her current research interests focus on C-V2X wireless communication technologies.



Jinling Hu is currently the chief expert at CICT Connected and Intelligent Technologies Co., Ltd. Her current research interests focus on C-V2X and key technologies in next generation mobile communication.



Li Zhao is currently a senior standardization expert at CICT Connected and Intelligent Technologies Co., Ltd. Her current research interests focus on C-V2X and key technologies in next generation mobile communication.



Jiayi Fang is currently a director of system and standardization department at CICT Connected and Intelligent Technologies Co., Ltd. His current research interests focus on C-V2X and key technologies in next generation mobile communication.



Rui Zhao is currently a senior standardization expert at CICT Connected and Intelligent Technologies Co., Ltd. His current research interests focus on C-V2X wireless communication technologies.



Hui Deng is currently a standardization research engineer at CICT Connected and Intelligent Technologies Co., Ltd. Her current research interests focus on C-V2X wireless communication technologies.



Shilei Zheng is currently a standardization research engineer at CICT Connected and Intelligent Technologies Co., Ltd. His current research interests focus on C-V2X wireless communication technologies.