Faculty of Engineering

Towards Resilient IoV Networks A Trust Management Perspective

Wang Yingxun

Doctor of Philosophy
2026

Towards Resilient IoV Networks — A Trust Management Perspective

Wang Yingxun

A thesis submitted

in fulfillment of the requirements for the degree of Doctor of Philosophy

(Electronic Engineering)

Faculty of Engineering

UNIVERSITI MALAYSIA SARAWAK

2026

DECLARATION

I declare that the work in this PhD dissertation was carried out in accordance with the regulations of Universiti Malaysia Sarawak. Except where due acknowledgments have been made, the work is that of the author alone. The PhD dissertation has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Wang Yingxun

.....

Signature

Name: Wang Yingxun

Matric No.: 21010376

Faculty of Engineering

Universiti Malaysia Sarawak

Date: March 27, 2026

ACKNOWLEDGEMENT

I would like to take this opportunity to extend my sincerest gratitude to my Academic Supervisors, i.e., Ts. Dr. Mohamad Faizrizwan Bin Mohd Sabri, Dr. Adnan Mahmood, and Dr. Hushairi Zen, for their meticulous guidance, patient instruction, and unwavering support throughout the duration of my PhD Studies. I am deeply grateful to them and, in particular, to Dr. Adnan Mahmood for extending supervision on a regular basis to shape this research and address all issues pertinent to the same. Their supervision style has allowed me to continuously surpass myself to gain an in-depth understanding of the significance and rigor of the notion of trust in the context of the emerging and promising paradigm of the Internet of Vehicles. This PhD dissertation would have never reached its completion without them.

I am also grateful to my immediate family for their kind and continuous support. Their encouragement has been the ultimate driving force behind my pursuit of academic excellence. Throughout this long yet rewarding academic journey, their love and companionship have been a true source of blessing. I also take this opportunity to extend my sincere appreciation to Universiti Malaysia Sarawak for providing me with all the necessary resources during the course of my PhD studies.

ABSTRACT

The emerging and promising paradigm of the Internet of Vehicles (IoV), also referred to as *Internet of Things–on–Wheels*, has evolved from the notion of Vehicular Ad hoc Networks and is an indispensable constituent of the modern Intelligent Transportation Systems (ITS). Accordingly, over the past decade or so, researchers from academia and industry have investigated and carefully developed architectures, salient characteristics, and applications pertinent to IoV, however, its security, particularly internal security, remains a considerable concern. This PhD dissertation is, therefore, an effort to tackle the internal security of such a highly dynamic and distributed network from the eyes of *trust*. In light of same, a state-of-the-art machine learning-based trust management mechanism which aggregates direct trust, indirect trust, and context to ascertain the trustworthiness of vehicles has been envisaged for segregating between trustworthy and untrustworthy vehicles via an optimal decision boundary. Extensive evaluations demonstrate that the said mechanism outperforms the other state-of-the-art trust management mechanisms. Moreover, a time-aware IoV-based trust management mechanism has been proposed to investigate the behavior of vehicles for ascertaining various trust-based attacks, i.e., zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks. Experimental results suggest that the proposed mechanism can ascertain the impact of multiple trust-based attacks instigated by the malicious vehicles across the entire time span of an IoV network in an intelligent manner. Furthermore, a first-of-its-kind dedicated IoV-based trust dataset has been introduced which encompasses 96,707 interactions from 79 vehicles across different time instances. The said IoV dataset comprises nine salient trust parameters which play an indispensable role for quantifying the trust of vehicles. Together, these contributions enhance the resilience and trustworthiness of IoV networks for next-generation ITS.

Keywords: Internet of Vehicles, network security, trust management, trust parameters, trust quantification, trust-based attacks

KE ARAH RANGKAIAN IOV YANG BERDAYA TAHAN – PERSPEKTIF PENGURUSAN KEBOLEHPERCAYAAN

ABSTRAK

Perkembangan pesat dan anjakan paradigma di dalam bidang Internet Pelbagai bagi Kenderaan (IPK) atau juga dikenali sebagai Internet Pelbagai Benda (IPB) beroda, telah berevolusi dari tanggapan umum sebagai rankaian ad hoc kenderaan kepada menjadi babak penting dalam sistem pengangkutan pintar moden. Dalam tempoh sedekad kebelakangan ini, penyelidik-penyelidik dari kalangan akademia mahupun industri telah meneliti dan secara rapi telah membangunkan arkitektur , ciri-ciri dominan dan pengaplikasian unik berhubung kait dengan IPK, namun, dari segi keselamatan, secara khususnya, keselamatan dalaman, ia kekal menjadi kebimbangan yang besar. Bersempena dengan itu, Thesis PhD ini berharap menjadi tunjang usaha ke arah menangani isu berkaitan keselamatan dalaman bagi rangkaian yang dinamik serta teredar sepertinya dari sudut pandang kebolehpercayaan. Dengan usaha mencapai maksud yang sama, satu mekanisma pengurusan kebolehpercayaan berpandukan pembelajaran mesin terkini yang mampu mengagregat kebolehpercayaan langsung, tidak langsung dan konteks bagi menentukan tahap kebolehpercayaan sesuatu kenderaan di dalam rangkaian IPK telah dirangka bagi membolehkan pengasingan di antara kenderaan-kenderaan yang boleh dipercayai dan tidak boleh dipercayai secara persempadanan pemilihan yang optimum. Penilaian yang meluas menunjukkan bahawa mekanisma tersebut mengatasi prestasi mekanisma-mekanisma pengurusan kebolehpercayaan terkini yang lain. Selain itu, mekanisma pengurusan kebolehpercayaan peka masa berpandukan IPK juga telah diusulkan sebagai salah satu cara menyiasat tingkah laku kenderaan-kenderaan di dalam rangkaian IPK bagi mengenalpasti pelbagai jenis serangan berasaskan kebolehpercayaan seperti serangan zig-zag, promosi kendiri, hidup-padam dan oportunistik. Hasil eksperimentasi menunjukkan model yang diusulkan berupaya mengenalpasti impak beber-

apa jenis serangan yang dilancarkan oleh kenderaan-kenderaan berniat jahat merangkumi keseluruhan jangka masa rangkaian IPK secara pintar. Tambahan lagi, set data khusus kebolehpercayaan berdasarkan IPK yang merangkumi 96,707 interaksi di antara 79 kenderaan dalam contoh masa berbeza dan yang pertama seumpamanya telah diperkenalkan. Set data IPK tersebut mengandungi sembilan parameter tunjang bagi kebolehpercayaan memainkan peranan yang sangat penting dalam usaha pengkuantifikasian kebolehpercayaan kenderaan. Bersama, sumbangan-sumbangan ini akan memperkukuh daya tahan dan tahap kebolehpercayaan bagi rangkainan-rangkaian IPK generasi akan datang.

Kata kunci: *Internet Pelbagai bagi Kenderaan, keselamatan jaringan, pengurusan kebolehpercayaan, parameter kebolehpercayaan, kuantifikasi kebolehpercayaan, serangan berasaskan kebolehpercayaan*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
DSRC	Dedicated Short-Range Communication
FL	Federated Learning
IoT	Internet of Things
IoV	Internet of Vehicles
ITS	Intelligent Transportation Systems
LTE	Long-Term Evolution
MANETs	Mobile Ad hoc Networks
OBUs	On-Board Units
QoS	Quality of Service
RSUs	Roadside Units
SIoT	Social Internet of Things
SOR	Social Object Relationships
SIoV	Social Internet of Vehicles
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VANETs	Vehicular Ad hoc Networks
WANETs	Wireless Ad hoc Networks
5G	Fifth Generation

CHAPTER 1

INTRODUCTION

With the realization of the Fifth Generation (5G) wireless communication, the Internet of Things (IoT), Artificial Intelligence (AI), and other similar related promising yet emerging technologies over the past decade or so, the notion of Vehicular Ad hoc Networks (VANETs) has evolved into the Internet of Vehicles (IoV) (Liu et al., 2025b)(Cao et al., 2024) which is an indispensable constituent of the modern intelligent transportation system and is, therefore, in a phase of rapid development (Aldhanhani et al., 2024). As of today, the application scenarios of the IoV encompasses autonomous driving, intelligent traffic management, intelligent logistics, in-vehicle infotainment services, amongst many others (Abdel-Hakim et al., 2024). In the realm of autonomous driving, IoV enhances driving safety, reduces the likelihood of traffic accidents, and optimizes driving routes through real-time data exchange between vehicles and other network entities via Vehicle-to-Everything (V2X) communication (Sivanantham and Sethuraman, 2026) (Muhammad and Safdar, 2025)(Yang et al., 2023a)(Taslimasa et al., 2023). In case of intelligent traffic management, IoV enables real-time monitoring of traffic conditions, dynamic adjustment of traffic signals and flow, and effective alleviation of traffic congestion (Rani and Sharma, 2023)(Elsagheer and AlShalfan, 2021). In the context of intelligent logistics, IoV facilitates real-time tracking of logistics-related vehicles' locations and their respective dynamic scheduling, thereby enhancing efficacy and safety (Leng and Li, 2022). Lastly, the in-vehicle infotainment services leverage internet connectivity and big data analytics to offer both drivers and passengers with real-time traffic information, satellite-based navigation, personalized music streaming (Sharma et al., 2024) and that too with voice assistance, thereby enhancing the driving experience and convenience.

As per the statistics of the International Organization of Motor Vehicle Manufacturers, the global vehicle ownership is anticipated to surpass 1.5 billion by 2025 (Miao et al.,

2024). As autonomous vehicles primarily rely on cameras, radar, sonar, GPS, LIDAR, and hundreds of other intelligent sensors for realizing their respective operations, each of them generates approximately 4,000 GB $\approx$ 4 TB of data a day (Shang and Deng, 2025)(Khezri et al., 2024)(Dai et al., 2024)(Partovi et al., 2023). This considerable volume of data traffic raises numerous critical questions: (a) how to intelligently process this vast amount of data to extract, analyze, and utilize meaningful information for safety-critical vehicular applications; (b) which particular wireless communication technologies would be able to support the transmission of such meaningful information with low end-to-end delay and extremely high data rates; (c) how to efficiently calculate and store this massive amount of data to minimize network management overhead; and most importantly; and (d) how to ensure the resilience of the network so that meaningful information is transmitted securely to its intended destination.

Nevertheless, the security of an IoV network is of paramount importance and is, therefore, the focus of this particular PhD dissertation. If an IoV network is not secure, it would have fatal consequences for both the vehicular passengers and the vulnerable pedestrians. According to one of the estimates of the World Health Organization, 1.35 million individuals die annually as a consequence of the road traffic accidents, thereby making this as one of the top ten global causes of mortality (Wei, 2024)(Xie et al., 2024). Although considerable advancements have already been made in the recent years in the development and deployment of the IoV-related technologies, connected vehicles still confront significant security challenges and any security breach could jeopardize the entire IoV network (Chen et al., 2026) (Taslimasa et al., 2023).

1.1 State-of-the-Art in the Internet of Vehicles

IoV manifests a highly dynamic communication network that facilitates interactions between vehicles via Vehicle-to-Vehicle (V2V) communication, vehicles and roadside infrastructure via Vehicle-to-Infrastructure (V2I) communication, vehicles and vulnerable pedestrians via Vehicle-to-Pedestrian (V2P) communication, and vehicles and backbone network via

Vehicle-to-Network (V2N) communication, thereby realizing V2X communication (Rishiwal et al., 2024)(Han et al., 2023)(Noor-A-Rahim et al., 2022). A typical architecture of an IoV network is depicted in Figure 1.1. It can be observed that the data source layer employs sensors to obtain data from not only the vehicles itself but also from their respective surrounding environment. The edge layer performs initial processing on the said data to minimize latency and alleviate bandwidth pressure. The fog layer leverages intermediate network infrastructure to further process vast amounts of data, thereby reducing reliance on the cloud resources for data analysis. Finally, the cloud layer focuses on large-scale data storage and in-depth analysis, thereby supporting global optimization and strategic decision-making (Xu et al., 2023)(Aman et al., 2021).

The components of an IoV encompass On-Board Units (OBUs), communication networks, cloud platforms, big data centers, and application services (Gupta et al., 2023)(Qureshi et al., 2021). Amongst them, OBUs are wireless communication devices installed in vehicles and are primarily responsible for facilitating the exchange of data between vehicles, and vehicles and supporting infrastructure, e.g., traffic signals, toll systems, and roadside units. OBUs, in fact, serve as an information collection and processing center of an IoV

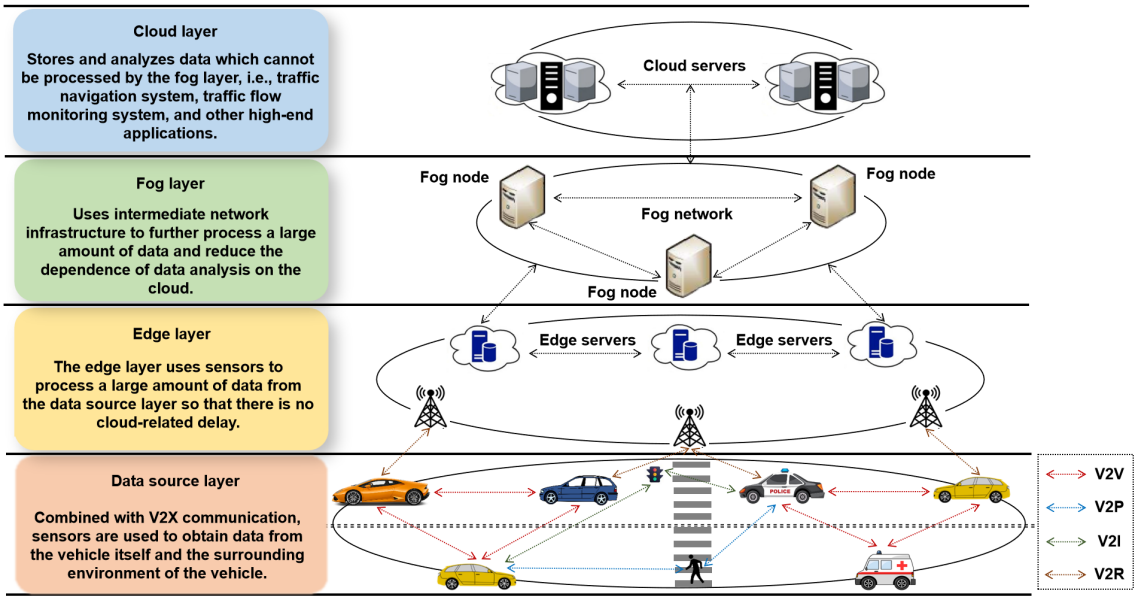

Figure 1.1 A System Architecture of the IoV.

network, and encompasses in-vehicle sensors, communication modules, in-vehicle computing platforms, navigation systems, and in-vehicle infotainment systems (Ji et al., 2020). It is pertinent to mention that a core function of the IoV is the rapid transmission of information via various wireless communication technologies, including but not limited to, Terahertz communication, Dedicated Short-Range Communication (DSRC), 5G, Wi-Fi, and Bluetooth (Zhu et al., 2024)(Li et al., 2020).

The IoV network necessitates robust data storage and processing capabilities for storing and analyzing massive amount of data. A cloud platform, therefore, serves as an indispensable infrastructure for supporting IoV network services, including but not limited to, real-time road information and condition, and intelligent cooperation amongst the network entities to ensure intelligent navigation for realizing safe driving patterns through advanced big data analytics (Ding et al., 2024)(Chen et al., 2023a)(Zeng et al., 2022)(Xu et al., 2022). Also, this facilitates drivers to remotely monitor and control their respective vehicles, e.g., for initiating remote start, shutdown, and climate control adjustments (Chen et al., 2023b).

A brief glimpse of the state-of-the-art reveals IoV research to have transpired in a number of distinct directions (Marwein et al., 2024). Ahmad et al. (2024) and Humayun et al. (2022) explored cutting-edge vehicle positioning technologies with a particular emphasis on sensor-based methods for precise vehicle location determination within a specific coordinate system. Guo et al. (2024) and Kaffash et al. (2021) examined the interplay between big data and IoV focusing on how IoV facilitates big data acquisition, storage, processing, and analysis. Lin et al. (2024), Qin et al. (2024), and Xing et al. (2023) investigated the applications of advanced intelligent techniques, including but not limited to, deep learning, federated learning, and blockchain, in an IoV network. Rani and Sharma (2023) and Feng et al. (2023) analyzed the extensive applications of AI in IoV networks, i.e., intelligent traffic management, autonomous driving, vehicle condition prediction, driving behavior analysis, and optimized route planning. Madani et al. (2022) studied the architecture, communication protocols, and data transmission methods of an IoV network. Wang et al. (2024a) and Osorio

et al. (2022) delineated the necessity of integrating an anonymous authentication scheme with a privacy protection mechanism to counter the threats posed by attacks. Alalwany and Mahgoub (2024) and Mahmood et al. (2023) analyzed how vehicles establish trust with the other vehicles and the respective messages they exchange. Du et al. (2024) and Ullah et al. (2023a) presented the latest solutions for security and privacy in V2X communications, i.e., cryptographic approaches (data encryption, identity verification, and intrusion detection) and trust management strategies.

Particularly, when it comes to the security of an IoV network, the aforementioned research lacks in-depth investigation. Consequently, the security of an IoV network still remains considerable challenge (Haider et al., 2026). Furthermore, conventional cryptography-based schemes are inadequate for addressing internal attacks in a highly dynamic IoV network (Marwein et al., 2024). Therefore, this PhD dissertation explicitly focus on addressing *internal security* issues in an IoV network from the perspective of *trust management*.

1.2 Problem Statements cum Research Questions

The broader research question of this PhD dissertation is as follows:

How can trust be intelligently quantified in a highly dynamic IoV network to classify between trustworthy (honest) and untrustworthy (dishonest) vehicles?

In light of the same, the specific research questions addressed in this particular PhD dissertation are:

i. **Problem Statements 1** – How to formulate an intelligent and resilient state-of-the-art context-driven IoV-based trust computational mechanism that can employ various salient trust parameters via machine learning techniques to ascertain an optimal trustworthiness boundary so as to segregate honest and dishonest vehicles in a highly dynamic IoV network?

ii. **Problem Statements 2** – How to intelligently investigate the time-varying patterns of trust values pertinent to the vehicles in a bid to ascertain trust-based attacks in a highly dynamic IoV network?

iii. **Problem Statements 3** – How to generate a first-of-its-kind, dedicated, and publicly available trust-based IoV dataset for facilitating researchers in both academia and industry to utilize and subsequently expand upon the same in order to address the open research directions pertinent to this emerging yet promising domain?

1.3 Research Objectives

In accordance with the research questions delineated above, the salient research objectives of this PhD dissertation are as follows:

i. ***Research Objective 1*** – To design an intelligent, context-aware trust management mechanism that employs learning-based techniques to dynamically aggregate several disparate trust parameters, thereby overcoming the limitations of conventional weighting-based mechanisms to ascertain optimal trustworthiness boundaries in an IoV network. This research objective is primarily addressed in Chapter 3, which introduces the MESMERIC model and details its methodology for achieving an optimal trust decision boundary.

ii. ***Research Objective 2*** – To intelligently study the behavior of the vehicles vis-à-vis time in a bid to accurately ascertain trust-based attacks, i.e., zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks, and their respective impact in an IoV network. The fulfilment of this research objective is the central focus of Chapter 4.

iii. ***Research Objective 3*** – To construct a first-of-its-kind publicly accessible, multifaceted trust-based IoV dataset that primarily captures vehicles' behaviors vis-à-vis dynamic contexts so that researchers and developers can leverage the same to test, optimize, and validate trust management models, thereby advancing research and practical applications in the domain of connected vehicle trust management. The TM – IoV dataset resulting

from this research objective is presented and analyzed in Chapter 5.

1.4 Research Hypotheses

To address the core challenges outlined in the research question, particularly the need for robust internal security mechanisms in IoV networks, the research hypotheses of this PhD dissertation are as follows:

i. ***Research Hypotheses 1*** – It is hypothesized that a machine learning-based trust model can achieve a more accurate and resilient segregation between trustworthy and untrustworthy vehicles in a dynamic IoV network in contrast to conventional models.

ii. ***Research Hypotheses 2*** – It is hypothesized that a time-aware trust evaluation mechanism can effectively identify dynamic trust-based attacks by analysing the temporal behavioural patterns of vehicles.

iii. ***Research Hypotheses 3*** – It is hypothesized that the introduction of a dedicated, multi-faceted trust parameter dataset significantly facilitates reproducible research and benchmarking in trust-based IoV network.

1.5 Research Scope

This PhD dissertation focuses exclusively on internal security attacks from a trust management perspective in contrast to the external attacks which are typically mitigated through conventional cryptographic schemes. To quantify trust, nine salient parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward / punishment, and context, have been employed. The said parameters collectively enable a comprehensive and multidimensional assessment of a vehicle's behavior and interaction patterns. In addition, four representative trust-based attacks, i.e., on-off attacks, zig-zag attacks, self-promoting attacks, and opportunistic attacks, have been investigated to better understand their respective attack patterns and behavioral dynam-

ics. Moreover, a dedicated TM-IoV dataset encompassing 96,707 interactions among 79 vehicles was constructed too.

However, it is important to note that this PhD dissertation does not address trust-related challenges arising from human-machine interaction, e.g., a driver's behavior, a user's intent, or socio-technical factors, that may influence trust formation and decision-making processes. Also, it does not consider highly dynamic attack vectors vis-à-vis dynamic contexts. These both remain avenues for future investigation.

1.6 Research Contributions

This PhD dissertation proposes novel contributions pertinent to IoV-based trust management and which are delineated as follows:

i. ***Research Contribution 1 – MESMERIC: Machine Learning-based Trust Management Mechanism for the Internet of Vehicles***

   To ensure that the safety-critical messages and the vehicles that disseminate them are highly reliable, this PhD dissertation envisages a state-of-the-art machine learning-based trust management mechanism, MESMERIC, that takes into account key components of direct trust (encompassing the trust attributes of interaction success rate, similarity, familiarity, and reward and punishment), indirect trust (involving confidence of a particular trustor on the neighboring nodes of a trustee, and the direct trust between the said neighboring nodes and the trustee), and context (comprising vehicle types and operating scenarios) factors in order to not only ascertain the trust of vehicles in an IoV network but to segregate the trustworthy vehicles from the untrustworthy ones by means of an optimal decision boundary. A comprehensive evaluation of the envisaged trust management mechanism has been carried out which demonstrates that it outperforms other state-of-the-art trust management mechanisms in terms of precision, recall, and F1 score.

ii. ***Research Contribution 2 – Towards Distinguishing Trust-based Attacks in an IoV***

Network

The security of an IoV network is paramount with internal attacks, in particular, being of considerable concern. Accordingly, this PhD dissertation investigates the behavior of the vehicles vis-à-vis time in a bid to ascertain various trust-based attacks, i.e., zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks. The experimental findings further demonstrate that the envisaged trust management heuristic exhibits prompt and accurate detection of the impact caused by the multiple trust-based attacks throughout the entire temporal span of an IoV network.

iii. ***Research Contribution 3 – TM – IoV: A First-of-its-Kind Multilabeled Trust Parameter Dataset for Evaluating Trust in the Internet of Vehicles***

To date, there is no dataset pertinent to trust management in the context of IoV networks and the same has proven to be a bottleneck for conducting an in-depth research in this particular domain. Accordingly, this PhD dissertation presents a first-of-its-kind trust-based IoV dataset encompassing 96,707 interactions amongst 79 vehicles at different time instances. The dataset involves nine salient trust parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward/punishment, and context, which play a considerable role in ascertaining the trust of a vehicle within an IoV network.

1.7 Outline of the Dissertation

The remainder of this PhD dissertation is structured as follows. Specifically, literature directly addressing the research questions defined in Section 1.2 is discussed in detail within their respective solution chapters (Chapters 3, 4, and 5) to provide a focused foundation and better explain the rationale behind the proposed methodologies. Chapter 2 provides a comprehensive overview of the trust management in an IoV network. It commences with an examination of the limitations inherent in VANETs that necessitate the evolution towards

IoV. Subsequently, a detailed in-depth analysis is conducted pertinent to the notion of trust, trust characteristics, trust constituents, trust attributes, trust evaluation parameters, and trust-related attacks. The trust management process is categorized into five key stages, i.e., trust formation, trust propagation, trust aggregation, trust update, and trust decision, thereby allowing for a comparative analysis of the existing literature. Furthermore, the-state-of-art trust management models are classified into two categories, i.e., conventional-based trust management models and AI-based trust management models. The strengths and limitations of the referred trust management models are critically evaluated vis-à-vis the specific trust components they employ and the contextual factors they consider. Additionally, this chapter explores the simulation tools and datasets frequently utilized in the trust-based IoV models.

Chapter 3 proposes a machine learning-based trust management mechanism, i.e., MES-MERIC, which integrates the concepts of direct trust, indirect trust, and context to assess the trustworthiness of vehicles in an IoV network and to segregate trusted vehicles from untrusted ones using optimal decision boundaries. Chapter 4 studies the behavior of the vehicles vis-à-vis time in a bid to accurately ascertain trust-based attacks, i.e., zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks, and their respective impact in an IoV network. Chapter 5 presents a first-of-its-kind trust-based IoV dataset encompassing 96,707 interactions from 79 vehicles across various time instances. This dataset encompasses nine critical trust parameters crucial for assessing the trustworthiness of vehicles in an IoV network.

Chapter 6 provides a thorough overview of the principal findings derived from this PhD dissertation. Open research directions are deliberated upon in the same too.

CHAPTER 2

LITERATURE REVIEW

This chapter presents a comprehensive review of trustworthiness management for an Internet of Vehicles (IoV) network. It initially explores the transition of Vehicular Ad hoc Networks (VANETs) to IoV followed by an examination of the notion of trust in various domains. Subsequently, the characteristics of trust, salient constituents of trust, key trust attributes, trust evaluation parameters, and trust-based attacks in the context of an IoV network have been delineated. Moreover, the five key processes involved in the trust management, i.e., trust formation, trust propagation, trust aggregation, trust update, and trust decision, have been investigated vis-à-vis the state-of-the-art. Furthermore, strengths and limitations of the state-of-the-art trust management models, i.e., conventional and Artificial Intelligence (AI) ones, have been carefully analyzed. Simulation tools and datasets employed in IoV-based trust models have been introduced. Figure 2.1 illustrates the taxonomy employed in this chapter.

2.1 Overview of the Chapter

2.1.1 Criteria for the Relevant Papers

To ensure the methodological rigor, relevance, and comprehensiveness of this literature review, a set of well-defined criteria was established for the selection of scholarly papers and other relevant materials. These criteria are delineated as follows:

i. ***Temporal Scope*** – To delineate a coherent and focused body of work, this review primarily incorporates scholarly publications from 2015 to 2025. This timeframe encompasses

Wang Yingxun, Hushairi Zen, Mohamad Faizrizwan Mohd Sabri, Wang Xiang, Kho Lee Chin (2022). *Towards Strengthening the Resilience of IoV Networks – A Trust Management Perspective*. Future Internet, 14 (7):202 (Q2, Impact Factor: 3.6).

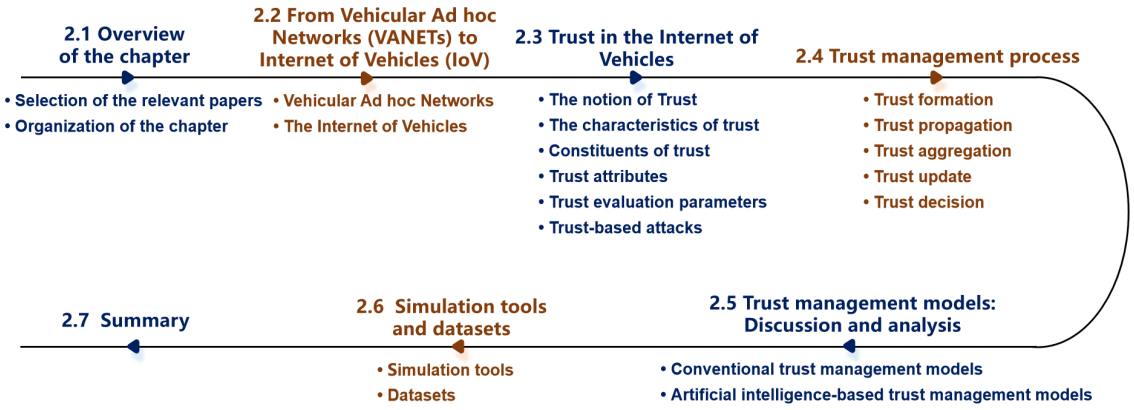

Figure 2.1 Taxonomy of the Chapter.

the period of most active development and consolidation of concepts related to trust management of IoV networks, allowing for an analysis of both foundational and state-of-the-art contributions.

ii. ***Source Type*** – The papers selected for this chapter are representative papers sourced from renowned scholarly journals, e.g., IEEE Transactions on Intelligent Transportation Systems (T – ITS), IEEE Transactions on Vehicular Technology (TVT), IEEE Transactions on Services Computing (TSC), IEEE Transactions on Network and Service Management (TNSM), IEEE Transactions on Computational Social Systems (TCSS), IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Human-Machine Systems (THMS) (given its significant focus on trust-related research in human-machine interaction contexts), ACM Transactions on Cyber-Physical Systems (TCPS), ACM Computing Surveys, IEEE Internet of Things Journal (IoT – J), Vehicular Communications, and IEEE Access, along with reputed conferences, e.g., IEEE International Conference on Computer Communications (INFOCOM), IEEE Global Communications Conference (GLOBECOM), and IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom).

iii. ***Topic Relevance*** – A comprehensive search pertinent to the keywords of 'trust', 'trustworthiness', and 'trustworthy' in conjunction with the 'Internet of Vehicles', 'IoV', 'Vehicular Ad hoc Networks', and 'VANETs' from various digital libraries has been conducted,

including but not limited to, IEEE Xplore (https://ieeexplore.ieee.org/), ACM Digital Library (https://dl.acm.org/), Elsevier's ScienceDirect (https://www.sciencedirect.com/), SpringerLink (https://springer.com/), and Google Scholar (https://scholar.google.com/). Subsequently, the selected papers were categorized based on their publication venue, i.e., journal or conference. Finally, papers that aligned with the scope of this research were selected by taking into consideration factors, i.e., novelty of the proposed methodology, employed trust attributes and trust aggregation mechanisms, trust evaluation parameters, trust-based attacks, simulation tools and datasets.

iv. ***Methodological Diversity*** – Literature was selected to encompass a broad spectrum of methodological approaches, includes conventional models and state-of-the-art AI models that integrate multiple methodologies. This diversity ensures a comprehensive understanding of the field's development and current trends.

2.1.2 Organization of the Chapter

Section 2.2 outlines the transition from conventional VANETs to IoV, emphasizing the key challenges that need to be addressed to achieve the primary objectives of an IoV network. Section 2.3 focuses on the promising notion of trust, the underlying characteristics of trust, key constituents of trust, trust attributes, trust evaluation parameters, and trust-based attacks in the context of IoV networks. Section 2.4 describes the five key processes involved in the trust management, i.e., trust formation, trust propagation, trust aggregation, trust update, and trust decision. Section 2.5 offers a comparative analysis of the state-of-the-art trust managements models, i.e., conventional and artificial intelligent-based ones. Finally, Section 2.6 discusses the simulation tools and datasets employed in the IoV-based trust models, whereas, Section 2.7 concludes this chapter. In essence, this particular chapter offers a comprehensive overview of the domain to its readers and serves as an entry point for them so as to explore the same.

2.2 From Vehicular Ad hoc Networks to the Internet of Vehicles

Over the past decade or so, significant and rapid advancements in the promising paradigms of the Internet of Things (IoT) and AI have transformed conventional VANETs into IoV. This transformation has brought connected and autonomous driving much closer to its realization. IoV is a novel concept in the Intelligent Transportation System (ITS) with a wide variety of both safety-critical and non-safety applications. By integrating mobile ad hoc networks with the IoT, IoV results into a Vehicle-to-Everything (V2X) network. However, this evolution was necessitated by critical limitations inherent to the VANETs architecture, particularly in terms of scalability and dynamic context management. The sheer growth in the number of connected vehicles and the bursty data traffic generated by them exposed the inability of early VANETs to efficiently manage network load and ensure consistent quality of service under dense traffic scenarios. Additionally, the highly dynamic nature of the vehicular environment demands trust models capable of adapting in real-time to rapidly changing contextual factors, inculding but not limited to, vehicle density, road topology, and time-of-day variations, which were not sufficiently addressed in traditional VANETs. It is noteworthy to mention here that researchers from both academia and industry have lately been focusing to secure IoV networks from both external and internal attacks. Accordingly, the development of reliable trust models for accurate trust assessments is indispensable for enhancing the security of such networks (Huang et al., 2026)(Dang et al., 2025)(Cheong et al., 2024b).

2.2.1 Vehicular Ad hoc Networks

VANETs, as an integral constituent of ITS, integrate the Mobile Internet and IoT as portrayed in Figure 2.2. It represents a distinctive form of Mobile Ad hoc Networks (MANETs) duly characterized by openness, high mobility, and dynamic topological changes

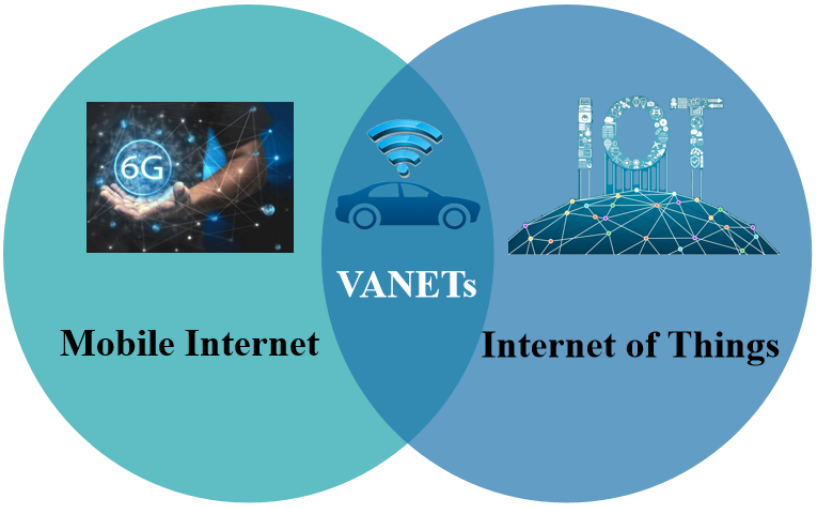

Figure 2.2 The Relationship Between the VANETs and the Internet.

in a network (Zhang and Li, 2025). It is pertinent to mention here that MANETs have themselves evolved from Wireless Ad hoc Networks (WANETs) (Di Pietro et al., 2014). Figure 2.3 depicts the evolutionary progression of VANETs.

In recent years, there has been a considerable development in wireless networking technologies (Vidhya et al., 2025). Accordingly, researchers from both academia and industry have expressed an increased interest in the development of VANETs, particularly, driven by the advancements in Long-Term Evolution (LTE) and Fifth Generation (5G) mobile communication technologies. Consequently, the concept of 5G–ITS is now being discussed in the

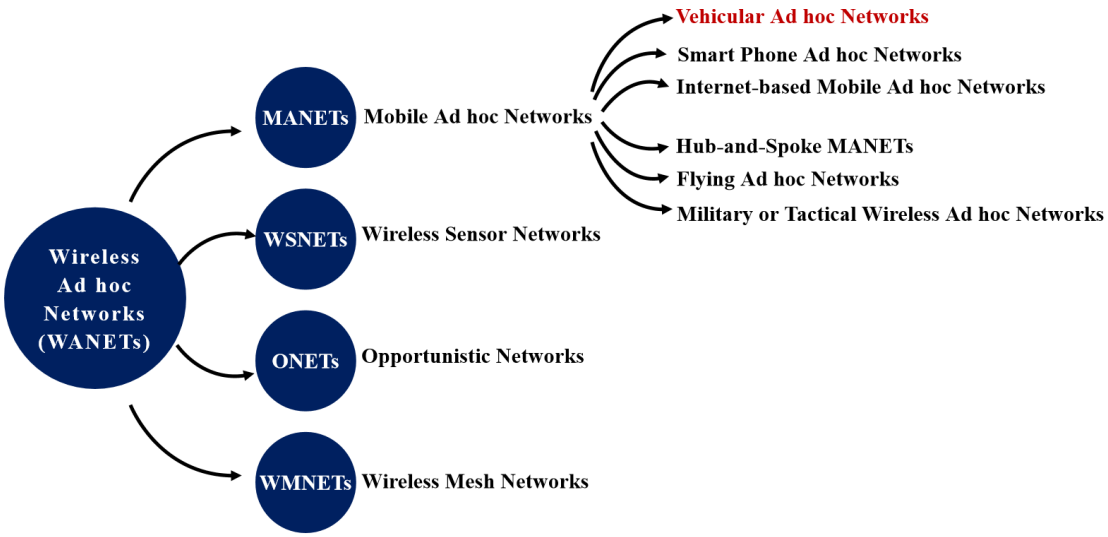

Figure 2.3 Evolution of the VANETs.

research literature since the deployment of 5G can significantly enhance IoV network capabilities by providing more robust and low-latency communication (Hossain et al., 2025)(Jamil et al., 2024)(Rathee et al., 2024).

2.2.2 The Internet of Vehicles

In an IoV network, vehicles exchange information with other vehicles, vulnerable pedestrians, supporting roadside infrastructure, and backbone networks to establish V2X communication. In order to realize the primary objectives of an IoV network, i.e., enhancing traffic safety (Yang and Tao, 2026)(Guo et al., 2024)(Taslimasa et al., 2023), optimizing traffic efficiency (Dutta et al., 2024)(Rani and Sharma, 2023), reducing energy consumption (Sun et al., 2024), and minimizing environmental pollution (Aldhanhani et al., 2024), it is indispensable to ensure (a) security and privacy in a bid to mitigate both external and internal attacks so that the malicious entities are unable to jeopardize such a network (Lu and Song, 2025)(Shang and Deng, 2025), (b) precise environmental perception for autonomous driving and traffic monitoring via in-vehicle sensors and sensing technologies (Rani and Sharma, 2024), (c) comprehensive data storage, analysis, and real-time processing capabilities by means of edge and cloud computing (Kang et al., 2025), (d) wireless communication technologies in a bid to facilitate efficient V2X communication (Wang et al., 2023b), (e) intelligent routing protocols to optimize the data transmission paths (Partani et al., 2025)(Anupama and Nagaraj, 2025), and (f) energy management and optimization schemes to enhance energy efficiency by optimizing routes and control systems (Mishra and Singh, 2023).

2.3 Trust in the Internet of Vehicles

As discussed earlier, the conventional cryptography-based schemes primarily cater for external attacks in an IoV network, however, they remain susceptible to internal attacks

(Khezri et al., 2024). Accordingly, trust has lately emerged as one of the promising solutions for handling internal attacks in highly dynamic and distributed networks (Philip et al., 2024).

Table 2.1, most existing surveys do not comprehensively cover all aspects of trust management in IoV networks. To address this gap, this chapter offers a detailed in-depth investigation pertinent to the notion of trust. It further taxonomizes the state-of-the-art IoV-based trust management approaches into conventional and AI-based ones, and critically evaluates the same vis-à-vis the specific salient trust attributes they employ and the trust-based attacks they consider.

2.3.1 The Notion of Trust

Trust, in essence, is subjective in nature and is, therefore, defined differently across diverse disciplines, i.e., sociology, psychology, economics, management science, medical science, and computer science (Siddiqui et al., 2023b). At its core, trust is a belief of an individual (trustor) in another individual's (trustee) ability to perform a certain task or tasks (Hbaieb et al., 2022). Figure 2.4 presents an overview of trust across diverse disciplines.

The notion of trust, as employed in this PhD dissertation, is as follows:

"Trust is a probability of a trustee, i.e., the one who is trusted, to provide a specific service (or services) pertinent to a particular application to a trustor, i.e., the one who trusts, at a given instance of time in a reasonable manner".

Similarly, the notion of trust value, as utilized in this PhD dissertation, is as follows:

"Trust value, also referred to as the degree of trust or credibility, is a quantitative measure used to assess trustworthiness of a trustee. It is generally represented in the range of [0, 1] with 0 signifying untrustworthiness and 1 manifesting trustworthiness".

Table 2.1 Comparison of Existing Surveys vis-à-vis This Survey.

Refs.	Main Focus	Trust Attributes	Trust Attacks	Trust Management Process	Trust Evaluation Parameters	Simulation Tools and Datasets
(Yang and Tao, 2026)	Systematically surveyed IoV-based trust management mechanisms via a multifaceted evolutionary analysis, i.e., by delineating how such approaches have evolved from conventional trust management mechanisms to ones leveraging privacy-aware designs and blockchain.	◐	◐	×	✓	◐
(Razafimanjato et al., 2025)	A literature review of blockchain-based trust management approaches for IoV across four aspects – trust computation, blockchain scalability, emerging technologies, and security and privacy.	✓	✓	◐	×	×
(Xu et al., 2025b)	Cataloged trust management approaches for Connected Autonomous Vehicles (CAVs) in the form of traditional and machine learning ones, and reviewed the later vis-à-vis CAVs-specific scenarios.	×	×	◐	×	×
(Alalwany and Mahgoub, 2024)	Classified the machine learning-driven IoV-based trust management approaches in terms of supervised learning, unsupervised learning, and reinforcement learning.	✓	×	◐	×	×

Table 2.1 continued

Refs.	Main Focus	Trust Attributes	Trust Attacks	Trust Management Process	Trust Evaluation Parameters	Simulation Tools and Datasets
(AlMarshoud et al., 2024)	Reviewed the state-of-the-art VANETs-based trust management approaches and discussed the impact of decentralization on integrity, security, and privacy.	×	✓	×	×	×
(Amari et al., 2023)	Taxonomized the VANETs-based trust management approaches in the form of emerging technologies and AI.	×	✓	◐	×	×
(Hbaieb et al., 2022)	Classification of IoV-based trust management approaches in terms of AI (clustering, reinforcement learning, fuzzy logic, game theory), and emerging technologies (cloud / fog / edge computing, blockchain, and SDN).	×	◐	◐	×	◐
(Che et al., 2022)	Taxonomized the VANETs-based trust management approaches in the form of conventional-, network-, data-, situation and location-, and AI-based ones.	×	✓	◐	×	◐
(Hussain et al., 2021)	Classified VANETs-based trust establishment and management approaches in terms of cryptography, recommendation, fuzzy logic, consensus, game theory, blockchain, infrastructure, and machine learning ones, and emerging technologies.	×	×	×	×	×

Table 2.1 continued

Refs.	Main Focus	Trust Attributes	Trust Attacks	Trust Management Process	Trust Evaluation Parameters	Simulation Tools and Datasets
(Siddiqui et al., 2021a)	Surveyed IoV-based trust management approaches with the key focus being weights quantification, threshold quantification, misbehavior detection, and attack resistance.	✓	✓	×	×	×
(Rehman et al., 2020)	A systematic literature review to investigate the state-of-the-art IoV-based trust management approaches, the effectiveness of the same, and the suitability of context awareness for trust establishment.	×	×	×	×	◐
This Survey	Conducted a detailed in-depth investigation pertinent to the notion of trust. Taxonomized the state-of-the-art IoV-based trust management approaches into conventional and AI-based ones and critically evaluated the same vis-à-vis the specific trust attributes they employ and the trust-based attacks they consider.	✓	✓	✓	✓	✓

✓: Addressed, ◐: Partially Addressed, ×: Not Addressed.

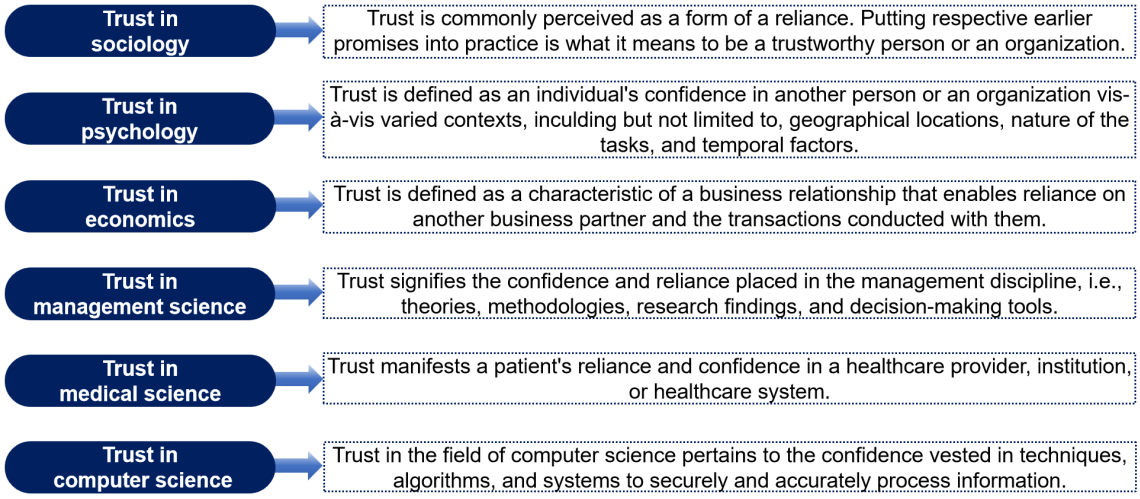

Figure 2.4 The Notion of Trust in Different Domains.

2.3.2 The Characteristics of Trust

In order to accurately ascertain the trust of vehicles in an IoV network, it is pertinent to take into account the following salient underlying characteristics of trust (Alalwany and Mahgoub, 2024)(Siddiqui et al., 2023b):

i. *Subjective* – Subjective trust is ascertained by taking into consideration the direct interaction with a trustee, i.e., it is, in essence, a direct observation made by a trustor pertinent to a trustee.

ii. *Objective* – In contrast to the subjective trust, the objective trust of a trustee is determined by leveraging the feedback, i.e., subjective trust, of its immediate neighbors (peers) in an IoV network.

iii. *Dynamic* – Trust is a dynamic construct and varies vis-à-vis the time primarily owing to a number of diverse contextual factors. This dynamic behavior of trust should be carefully observed in order to ascertain a wide variety of complex trust-based attacks instigated by the malicious vehicles.

iv. *Asymmetry* – Trust is intrinsically both asymmetric and unidirectional, i.e., the confidence vested by a trustor A in a rustee B does not automatically entail a reciprocated trust from

a trustee B towards a trustor A. These two forms of reliance are separate and autonomous.

v. *Local* – When the trust value is confined to a trustee and a trustee, it indicates a vehicle-vehicle relationship based on trust, wherein one vehicle evaluates the reliability of another vehicle via using local information, e.g., self-observation and past experiences. However, this value cannot be generalized across the IoV network (Hbaieb et al., 2022).

vi. *Global* – The concept of a global trust in an IoV network differs from the local trust since it involves assigning a unique and universally recognized trust value to each vehicle in an IoV network. This trust value is predominantly determined by aggregating all the local information pertinent to a vehicle in an IoV network.

vii. *Trust Decay* – The reliability of a trust value ascertain for a trustee in an IoV network is likely to decay over time, i.e., the older the estimate, the less credible and less accepted it would be within an IoV network.

viii. *Context Specific* – The level of trust amongst vehicles in an IoV network varies vis-à-vis the contextual factors, including but not limited to, network environment, vehicles' type, and operating scenarios.

ix. *History Dependent* – The trust of a trustee in an IoV network evolves vis-à-vis the time. The trust of a particular vehicle in an IoV network at any given time instance is, in fact, its accumulated trust, i.e., the historical trust is also taken into consideration albeit to a certain extent.

2.3.3 Constituents of Trust

There are two key constituents of trust, i.e., direct trust and indirect trust, as portrayed in Figure 2.5. The same are delineated as follows:

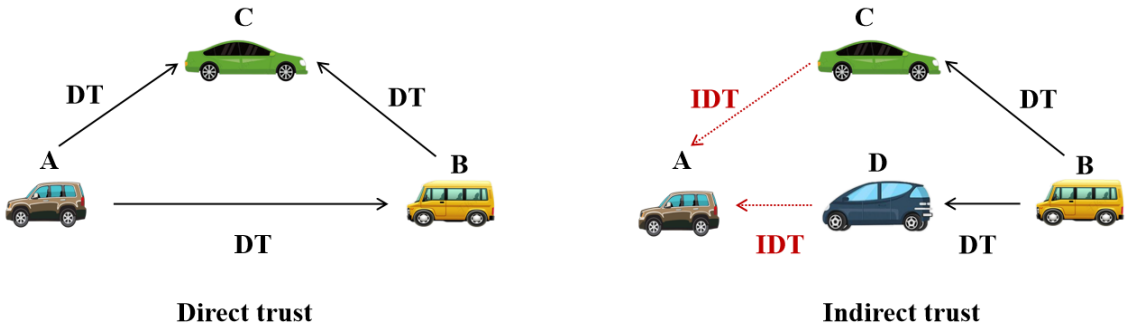

Figure 2.5 Direct Trust and Indirect Trust (Direct Trust – DT, Indirect Trust – IDT).

Table 2.2 Methodology for Direct Trust Calculation.

Reference	Method	Definition
(Sagar et al., 2024a), (Chen et al., 2024), (Su and Tong, 2023), (Li et al., 2023a), (Sun et al., 2023), (Sagar et al., 2023)	Positive and negative interactions	It takes into account both the positive and total interactions, with direct trust is determined by the ratio of positive interactions to total interactions.
(Qi et al., 2024), (Cao et al., 2024), (Wang et al., 2023c), (Huang et al., 2022)	Bayesian inference	The Bayesian inference method, based on the Beta distribution, is employed for the computation of direct trust.
(Shokrollahi and Dehghan, 2025)(Shokrollahi and Dehghan, 2023), (Siddiqui et al., 2023b), (Mahmood et al., 2023), (Mahmood et al., 2022), (Yin and Gong, 2022)	Trust parameters – weight summation	The proposed approach involves the aggregation of multiple trust parameters, each assigned with varying weights, to derive a measure of direct trust.

a. Direct Trust (DT)

The direct trust manifests a trustor's direct observation, i.e., knowledge, of a targeted vehicle (trustee) owing to the interaction amongst them (Yong-hao, 2020). Whilst direct trust is regarded as more significant than the indirect trust, a combination of both of them is usually taken into account for ascertaining the trustworthiness of a vehicle in an IoV network (Mahmood et al., 2019). To date, a number of methods have been employed in the research literature for quantifying the direct trust, the details of which are presented in Table 2.2.

Sagar et al. (2024a) quantified the direct trust by taking into account positive and negative interactions pertinent to a trustor-trustee pair:

$$Trust^{t}_{DT}(i,j) = \frac{P^{t}(i,j)+1}{P^{t}(i,j)+N^{t}(i,j)+2} \quad \text{Equation 2.1}$$

where, $P^{t}(i,j)$ and $N^{t}(i,j)$ represent the positive and negative interactions, respectively between a trustor i and trustee j at any given time instance t.

Qi et al. (2024) employed the Bayesian approach based on beta distribution to quantify the direct trust:

$$DT_{i,j} = E(f(p_{i,j};\alpha+1,\beta+1)) = \frac{\alpha+1}{\alpha+\beta+2} \quad \text{Equation 2.2}$$

where, α and β represent the number of successful and unsuccessful communication between a trustor i (vehicle V_i) and a trustee j (vehicle V_j), respectively, and $p_{i,j}$ being the probability distribution follows the Beta distribution with parameters $(\alpha+1)$ and $(\beta+1)$.

Siddiqui et al. (2023b) determined direct trust of a trustor i towards a trustee j at a time instance k by considering both the Packet Delivery Ratio (PDR) at the said time instance and the weighted sum of the PDR from the earlier time instances:

$$DT_{i,j,k} = \frac{(1-\lambda_{i,j,k})PDR_{i,j,k} + \sum_{l=1}^{k-1}\Gamma_{i,j,l}PDR_{i,j,l}}{1+\sum_{l=1}^{k-1}\Gamma_{i,j,l}} \quad \text{Equation 2.3}$$

where, $\Gamma_{i,j,l}$ represents the weight of a particular historical interaction, i.e., the time decay factor, and $\lambda_{i,j,l}$ is a factor incorporated to ensure that the impact of the malicious behavior demonstrated by a trustee is not easily ignored.

b. Indirect Trust (IDT)

The indirect trust, also referred to as the recommendation trust, is ascertained by taking into consideration the recommendations pertinent to a trustee from the one-hop neighbors of a trustor (Chen et al., 2024). Cheong et al. (2024b) quantified indirect trust as:

$$IT_{V_i,V_j} = \frac{\sum_{k=1}^{len(Rec_{V_i})} DT_{V_k,V_j}^{tl}}{len(Rec_{V_i})} \quad \text{Equation 2.4}$$

where, DT_{V_k,V_j}^{tl} refers to the recommendation of a neighbor V_k pertinent to a trustee V_j. $len(Rec_{V_i})$ indicates the length of the neighbor set of a trustor V_i.

Similarly, Wang et al. (2023d) quantified indirect trust as:

$$IT_{i,j} = \frac{\sum_{k=1}^{V_i} DT_{i,k} \times DT_{k,j}}{|V_i|} \quad \text{Equation 2.5}$$

where, $DT_{i,k}$ implies the direct trust of a trustor i on its neighbor k. $DT_{k,j}$ represents the direct trust of a neighbor k on the trustee j. V_i is a set of neighbors pertinent to the trustor i.

In practice, the utilization of direct trust and indirect trust should be dynamically adapted in accordance to prevailing IoV network conditions. When a trustor can obtain valid indirect trust from neighboring nodes, a combined assessment that integrates both direct and indirect trust should be conducted. Such integration alleviates the limitations of relying on a particular single information source and enhances the robustness and reliability of the trust assessment. Conversely, in scenarios, wherein neighboring nodes are unavailable or indirect trust cannot be ascertained, trust evaluation must rely solely on direct trust with the resulting assessment being highly dependent on the quality, quantity, and recency of the historical interactions. Moreover, the assignment of weights to direct and indirect trust constitutes a critical aspect of trust aggregation and should be determined dynamically based on several factors, including but not limited to, information freshness, the credibility of recommenders, and contextual relevance, rather than using fixed proportions. For instance, when direct interaction records are abundant and recent, greater emphasis should be placed on direct trust. In contrast, when direct interactions are sparse or historical records are outdated or unreliable, increased reliance on indirect trust becomes necessary. This dynamic trust integration mechanism efficaciously accommodates the high-speed mobility and rapidly changing topological characteristic of IoV networks, thereby improving both accuracy and resilience of any envisaged trust model.

Figure 2.6 Trust Attributes in Trust Models.

2.3.4 Trust Attributes

The computation of the aforementioned trust constituents (direct trust and indirect trust) takes into account various trust attributes (parameters) as depicted in Figure 2.6.

i. *Packet Delivery Ratio* – The packet delivery ratio quantifies the degree of association between a trustor and a trustee, thereby reflecting the extent to which messages are successfully received and subsequently disseminated by a trustee (Jain et al., 2025)(Siddiqui et al., 2023b)(Akwirry et al., 2022)(Siddiqui et al., 2021b)(Li et al., 2021a)(Ahmad et al., 2020)(Wang et al., 2020)(Yu et al., 2017).

ii. *Similarity* – The similarity between a trustor and a trustee is usually quantified by taking into account either the degree of similar accessed content or similar services delivered by them over the course of their respective trajectory within an IoV network (Sagar et al., 2024a)(Cheong et al., 2024a)(Han et al., 2024)(Shamaeian and Pesch, 2024)(Li et al., 2023a)(Sun et al., 2023)(Yin and Gong, 2022)(Sagar et al., 2021)(Sagar et al., 2020b)(Sagar et al., 2020a).

iii. *Familiarity* – Familiarity demonstrates the level of acquaintance between a trustor and a trustee in an IoV network, i.e., a high degree of familiarity indicates a trustor to have a

considerable prior knowledge pertinent to a trustee (Cheong et al., 2024a)(Siddiqui et al., 2023a)(Siddiqui et al., 2023b)(Mahmood et al., 2023)(Siddiqui et al., 2021b)(Siddiqui et al., 2019).

iv. *Timeliness* – The timeliness of an interaction between a trustor and a trustee is ascertained by taking into account the time on which their respective interaction has transpired vis-à-vis the current time instance (Jain et al., 2025)(Mahmood et al., 2023)(Wang et al., 2023a)(Mao et al., 2023)(Chen and Wang, 2021)(Siddiqui et al., 2021b). Timeliness is of the utmost essence since an outdated information can result into obsolete decisions and which could have severe consequences for entities in an IoV network (Wang et al., 2020).

v. *Cooperativeness* – Cooperativeness reflects the extent to which a trustee interacts with the other vehicles in order to realize a particular service (or services) in a honest manner, i.e., vehicles that act cooperatively are relied upon by the other vehicles and, therefore, end up gaining higher privileges in an IoV network (Cheong et al., 2024a)(Cheong et al., 2024b)(Siddiqui et al., 2023b)(Sagar et al., 2021)(Sagar et al., 2020b).

vi. *Context* – Context plays an indispensable role in ascertaining the trust of a trustee in an IoV network. In essence, context facilitates to understand the underlying dynamics, wherein a trustee operates, including but not limited to, its respective geographical location, ambient traffic, and weather conditions hence resulting in a more accurate trust assessment (Alam et al., 2024).

vii. *Reward* – Reward, as an attribute, is employed to award or penalize a trustee based on its conduct in an IoV network. For instance, if a trustee continuously acts in a cooperative manner, it is awarded a certain factor that augments its respective trust. On the contrary, if a trustee acts selfishly or carry out any sort of a misconduct, its respective trust is decayed or penalized to a considerable degree (Wang et al., 2023c)(Sagar et al., 2020b).

2.3.5 Trust Evaluation Parameters

Trust evaluation plays a pivotal role in the trust management process and hence serves as a critical means to validate the reliability and efficacy of the proposed trust management models (Song et al., 2024). To date, the-state-of-art trust management models for IoV networks have primarily relied on particular trust parameters for evaluation purposes, including but not limited to, Precision (P), Recall (R), F1 score (F), Accuracy (A), True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate (FNR), Detection Rate (DR), Mean Absolute Error (MAE), and Mean Squared Error (MSE). The trust evaluation parameters discussed are elaborated in detail in Table 2.3.

The results of the statistical analysis (Figure 2.7) clearly demonstrate the prevalence of commonly employed trust evaluation parameters. Precision (26%), Recall (25%), FPR (13%), and Accuracy (11%) are widely adopted for evaluating trust models in existing literature. This finding underscores their relative efficacy in assessing general trust models.

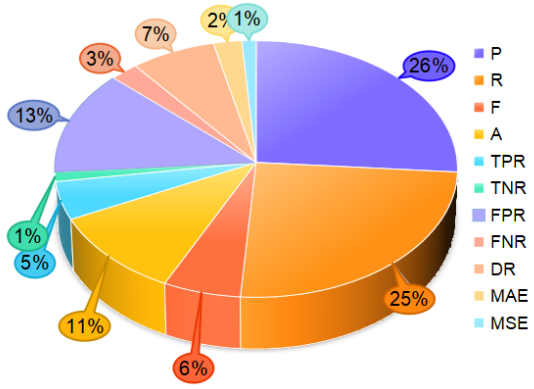

Figure 2.7 Frequency of the Trust Evaluation Parameters (Precision – P, Recall – R, F1 Score – F, Accuracy – A, True Positive Rate – TPR, True Negative Rate – TNR, False Positive Rate – FPR, False Negative Rate – FNR, Detection Rate – DR, Mean Absolute Error – MAE, and Mean Squared Error – MSE).

Table 2.3 Trust Evaluation Parameters in Trust Management Models (Precision – P, Recall – R, F1 Score – F, Accuracy – A, True Positive Rate – TPR, True Negative Rate – TNR, False Positive Rate – FPR, False Negative Rate – FNR, Detection Rate – DR, Mean Absolute Error – MAE, and Mean Squared Error – MSE).

Reference	Trust evaluation parameters	Definition
(Dang et al., 2025), (Cheong et al., 2024a), (Cheong et al., 2024b), (Cheong et al., 2024c), (Song et al., 2024), (Shamaeian and Pesch, 2024), (Li et al., 2023a), (Sun et al., 2023), (Wang et al., 2023c), (Wang et al., 2023d), (Junejo et al., 2023), (Qi et al., 2023a), (Siddiqui et al., 2023a), (Mao et al., 2023), (Zhang et al., 2023a), (El-Sayed et al., 2022), (Magdich et al., 2022), (Kaur and Kakkar, 2022)	P	Precision signifies the proportion of predicted positives that are actually positive.
(Cheong et al., 2024a), (Cheong et al., 2024b), (Cheong et al., 2024c), (Song et al., 2024), (Shamaeian and Pesch, 2024), (Li et al., 2023a), (Sun et al., 2023), (Wang et al., 2023c), (Wang et al., 2023d), (Qi et al., 2023a), (Junejo et al., 2023), (Siddiqui et al., 2023a), (Mao et al., 2023), (Zhang et al., 2023a), (El-Sayed et al., 2022), (Magdich et al., 2022), (Kaur and Kakkar, 2022), (Bhargava and Verma, 2022), (Fabi and Thampi, 2022b)	R	Recall, also known as TPR, denotes the proportion of actual positives that are correctly predicted.
(Dang et al., 2025), (Cheong et al., 2024a), (Cheong et al., 2024b), (Song et al., 2024), (Shamaeian and Pesch, 2024), (Cheong et al., 2024c), (Sagar et al., 2023), (Zhang et al., 2023a), (Qi et al., 2023a)	F	F1 score represents the weighted harmonic mean of precision and recall.
(Raza and Badidi, 2025), (Song et al., 2024), (Wan and Wang, 2024), (Chen et al., 2024), (Huang et al., 2022), (Haddaji et al., 2022), (Jing et al., 2022)	A	Accuracy depicts the proportion of all predictions that are correct.

Table 2.3 continued

Reference	Trust evaluation parameters	Definition
(Zhang et al., 2020)	TNR	TNR, also called specificity, implies the proportion of actual negatives that are correctly predicted.
(Dang et al., 2025), (Shamaeian and Pesch, 2024), (Jegatheesan and Arumugam, 2024), (Mao et al., 2023), (Sun et al., 2023), (Mahmood et al., 2022), (Zhang et al., 2022b), (Magdich et al., 2022)	FPR	FPR suggests the proportion of actual negatives that are incorrectly predicted as positives.
(Dang et al., 2025), (Shamaeian and Pesch, 2024), (Jegatheesan and Arumugam, 2024), (Mao et al., 2023), (Choukhairi et al., 2022)	FNR	FNR represents the proportion of actual positives that are incorrectly predicted as negatives.
(Sagar et al., 2024a), (Mahmood et al., 2023), (Choukhairi et al., 2022), (Kerrache et al., 2019), (Chen et al., 2019), (Ahmad et al., 2018)	DR	The detection rate reflects the probability of detecting malicious behaviors, thereby indicating their likelihood of being identified.
(Sagar et al., 2023), (Sun et al., 2023)	MAE	MAE calculates the average magnitude of errors between the actual and predicted values within a given dataset.
(Sagar et al., 2023)	MSE	MSE quantifies the average squared difference between the actual values and their corresponding predicted values in a given dataset.

2.3.6 Trust-based Attacks

In recent years, extensive research has been carried out on the notion of trust in the context of an IoV network. However, trust is also vulnerable to a number of attacks. Generally speaking, trust attacks are divided into two categories, i.e., self-interest-based trust attacks and reputation-based trust attacks. The self-interest-based trust attacks encompass opportunistic service attacks, self-promoting attacks, on-off attacks, zig-zag attacks, selective behavior attacks, and newcomer attacks (whitewashing attacks), whereas, the reputation-based trust attacks comprise ballot stuffing attacks (good-mouthing attacks), bad-mouthing attacks, collusion attacks, and time dependent attacks (Mahmood et al., 2023). It is pertinent to mention here that owing to the highly dynamic nature of an IoV network, a misbehaving vehicle primarily acts in a disguise in order to gain the trust of other vehicles, and once it finds itself in an advantageous position, it can initiate malign activities. In other words, a malicious vehicle disguises to provide superior services with the intention of establishing a higher reputation within an IoV network. However, once its reputation is established, it begins to deliver subpar services. More importantly, malicious vehicles may engage in trust-based attacks at specific time instances while functioning normally at other times (Naik and Dondeti, 2025)(Zhang et al., 2024)(Li et al., 2023b). Therefore, detecting such attacks poses a significant challenge.

a. Self-interest-based Trust Attacks

i. *Self-Promoting Attacks* – In a self-promoting attack, misbehaving vehicles consistently enhance their reputation to gain significant privileges, thereby jeopardizing the entire IoV network for their own malicious gains (Mahmood et al., 2023)(Magdich et al., 2022). Accordingly, a misbehaving vehicle can generate sophisticated Sybil identities, i.e., pseudonymous personas, to manipulate trust and deceive traditional reputation mech-

anisms (Chen et al., 2024)(Siddiqui et al., 2021b).

ii. *On-Off Attacks* – In an on-off attack, dishonest vehicles do not consistently exhibits malicious behavior, instead, intelligent attackers employ a strategic approach by alternating between honest and dishonest modes. These intermittent attacks allow perpetrators to cause damage without being detected and expelled from the IoV network. Therefore, by alternately presenting good and bad reputations, the possibility of misclassifying vehicles with poor reputation as malicious vehicles is ultimately reduced (Shokrollahi and Dehghan, 2025)(Cheong et al., 2024b)(Cheong et al., 2024c)(Azizi and Shokrollahi, 2024)(Shamaeian and Pesch, 2024)(Du et al., 2024)(Su et al., 2024)(Chen et al., 2024)(Siddiqui et al., 2023b)(Mao et al., 2023)(Magdich et al., 2022).

iii. *Zig-Zag Attacks* – Attackers may engage in intermittent malicious behavior to evade detection. For instance, they might choose to intermittently spoof incoming messages before switching to launch a bad-mouth attack, thereby resulting in a zig-zag attack. Whilst their exist similarities between zig-zag attacks and on-off attacks, nevertheless, the fluctuation pattern of zig-zag attacks lack regularity (Qi et al., 2023a).

iv. *Selective Behavior Attacks* – Analogous to gray hole attacks, in selective behavior attacks, misbehaving vehicles exhibit deceptive behavior towards certain nodes, while maintaining honest behavior towards others. Consequently, this may lead to conflicting trust scores assigned to a vehicle by its peers based on direct and/or indirect observations. Nevertheless, by this means, i.e., when a malicious vehicle does not intentionally prioritize computational intensive services, it can still uphold its legitimate reputation within an IoV network (Mo et al., 2022)(Mao et al., 2021)(Chen et al., 2019).

v. *Newcomer Attacks* – In a newcomer attack, a malicious vehicle registers a new identity to expunge its undesirable historical interactions. To mitigate this attack, newcomers are assigned a low initial trust value and an adaptive attenuation factor is incorporated to impede rapid escalation of the trust value, thereby necessitating consistent performance over an extended duration for trust accumulation (Shokrollahi and Dehghan, 2025)(Su

et al., 2024). The newcomer attack bears resemblance to the whitewashing attack.

b. Reputation-based Trust Attacks

i. *Bad-Mouthing Attacks* – In case of a bad-mouthing attack, attackers manipulate messages similarly to those in simple attacks, whereby false recommendations are sent by the attacker when a vehicle requests recommendations from a bad-mouthing attacks attacker, leading to inaccurate trust evaluation and misjudged decisions (Sagar et al., 2023)(Alnasser et al., 2020). The bad-mouthing attacks often manifest as coordinated groups, wherein multiple misbehaving vehicles collude to undermine the credibility of a specific honest vehicle (Ren et al., 2025)(Cheong et al., 2024b)(Song et al., 2024)(Shamaeian and Pesch, 2024)](Jegatheesan and Arumugam, 2024)(Sagar et al., 2024a)(Chen et al., 2024)(Wang et al., 2023c)(Mao et al., 2023)(Mahmood et al., 2023)(Magdich et al., 2022)(Zhang et al., 2022a)(Zhang et al., 2022b).

ii. *Ballot Stuffing Attacks* – In a ballot stuffing attack, a malicious vehicle can collaborate with other bad nodes to provide good recommendations about another bad vehicles, thereby enhancing its reputation. In this transaction, both the attacker and the target node exhibit characteristics of malicious social connections and unethical conduct. Furthermore, if these malicious vehicles are selected as cluster heads, it could have severe implications for the safety and dependability of the IoV network, posing a lethal threat to both occupants of the vehicles and vulnerable pedestrians (Shamaeian and Pesch, 2024)(Sagar et al., 2024a)(Chen et al., 2024)(Shokrollahi and Dehghan, 2023)(Mahmood et al., 2023)(Mao et al., 2023)(Sagar et al., 2023)(Magdich et al., 2022)(Zhang et al., 2020). Moreover, ballot stuffing attack is also known as good-mouthing attack.

iii. *Time Dependent Attacks* – In time dependent attacks, the attacker exhibits temporal variability in their behavior, demonstrating proficiency to gain trust from vehicles within the network for a certain duration while engaging in unfair rating practices at other times. Consequently, erroneous information and ratings are disseminated among neighboring

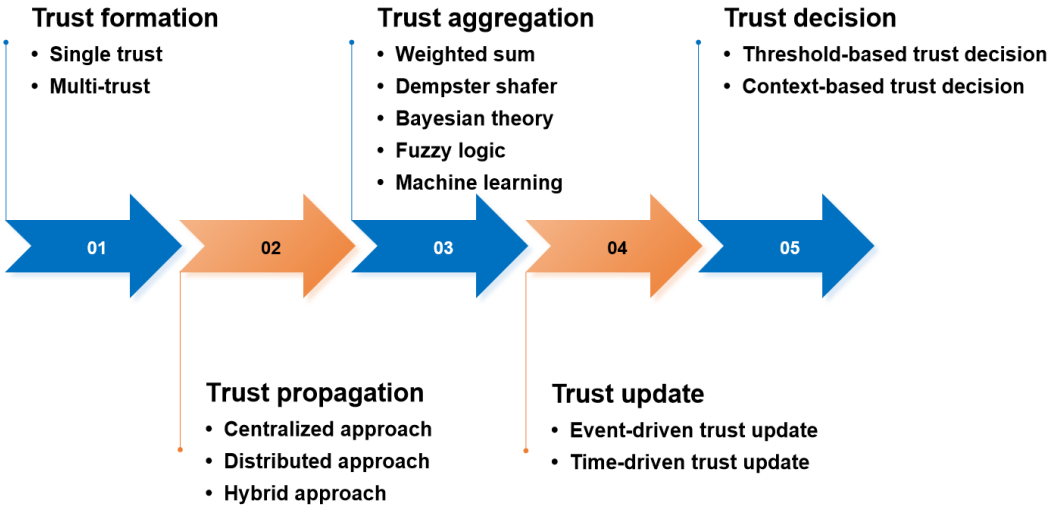

Figure 2.8 Trust Management Process.

vehicles during the course of the attack (Mao et al., 2021)(Chen et al., 2019).

2.4 Trust Management Process

This section outlines the five essential steps involved in the trust management process, i.e., trust formation, trust aggregation, trust propagation, trust update, and trust decision. A visual representation illustrating the inter-dependencies among these processes is presented in Figure 2.8.

2.4.1 Trust Formation

The process of trust formation typically involves the consideration of trust parameters which can be derived from either a single parameter (single trust) or multiple parameters (multi-trust):

i. *Single Trust* – The single trust takes into account only one specific attribute utilized in determining the total trust. In other words, when it comes to a single trust, evaluation predominantly relies on only one metric (Rai et al., 2020).

ii. *Multi-trust* – The multi-trust presents the notion of trust as a multidimensional concept,

wherein multiple factors (attributes) influencing trust are integrated to form a single trust value. Furthermore, the consideration of numerous attributes facilitates the acquisition of more precise and reliable trust (Yadav et al., 2025)(Honarmand and Keshavarz-Haddad, 2024)(Alam et al., 2024)(Shen et al., 2024)(Chen et al., 2024)(Mahmood et al., 2022)(Xia et al., 2019a)(Chen et al., 2016a).

2.4.2 Trust Propagation

Trust propagation refers to the process of disseminating trust of a trustee in an IoV network so that its trust can be collectively, and not individually, ascertained by all the vehicles interacting with it. This not only helps in reaching a more precise trust of a trustee but also facilitates in mitigating any trust-based attacks instigated by the same. Trust propagation typically falls within three primary categories:

i. *Centralized Approach* – The centralized approach relies on a central vehicle that not only collects trust-related information for trust computation purposes but also disseminates the said information. Consequently, this approach is susceptible to a single point of failure (Junejo et al., 2023)(Mahmood et al., 2022)(Kaur and Kakkar, 2022)(Suo and Sarma, 2019).

ii. *Distributed Approach* – In case there is no centralized authority, vehicles themself assume the responsibility for trust computation as well as trust propagation. While effectively addressing the issue of single point of failure inherent in the centralized approach, this methodology presents challenge pertinent to biased dissemination of trust within an IoV network (Cheong et al., 2024b)(Shen et al., 2024)(Rathee et al., 2024)(Chen et al., 2024)(Siddiqui et al., 2023b)(Zhang et al., 2023a)(Qi et al., 2023a)(Wang et al., 2023c)(El-Sayed et al., 2022)(Chen et al., 2016b)(Chen et al., 2016c).

iii. *Hybrid Approach* – The hybrid approach is commonly employed to mitigate the challenges posed by both centralized and distributed approaches. Furthermore, the hybrid approach

classifies propagation into two distinct types – locally distributed and globally centralized, as well as, locally centralized and globally distributed (Han et al., 2024)(Cao et al., 2024)(Mao et al., 2023)(Lu et al., 2023)(Shokrollahi and Dehghan, 2023)(Yin and Gong, 2022)(Akwirry et al., 2022).

However, while trust propagation is critical for establishing holistic IoV network awareness, its practical implementation in a highly dynamic IoV network introduces significant challenges. Foremost among these are the need for dynamic trust updates amid frequent node mobility and topological changes, and the requirement to address contextual sensitivity of trust relationships across diverse scenarios. These challenges, particularly maintaining accurate trust information flow under real-time variations in vehicle density, road conditions, and communication environments, directly align with the core problems addressed in subsequent chapters. Chapter 3 has proposed a machine learning-driven trust management mechanism that dynamically aggregates direct trust, indirect trust, and contextual factors through intelligent algorithms, explicitly mitigating the limitations of static weight assignment in traditional propagation models. Similarly, Chapter 4's analysis of temporal trust evolution patterns further unravel how contextual dynamics influence propagation mechanisms and their resilience against emerging trust-based attacks.

2.4.3 Trust Aggregation

The purpose of trust aggregation is to aggregate trust parameters in order to derive a single trust value so that it can play a pivotal role within the framework of trust computing models and significantly influences the outcomes of trust evaluation. Over the years, numerous techniques for aggregating trust have been extensively deliberated in the research literature, including but limited to, weighted sum techniques (Shokrollahi and Dehghan, 2025), Dempster Shafer Theory (DST) (Cheong et al., 2024a), bayesian theory (Gao et al., 2022), fuzzy logic (Byeon et al., 2025), and machine learning (Liu et al., 2025a). The detailed

description of these aggregation techniques is delineated as follows:

i. *Weighted Sum Techniques* – This technique presents a straightforward approach to aggregate trust parameters by assigning each of them with either a static or a dynamic weight, thereby resulting in a single trust value (Ren et al., 2025)(Cheong et al., 2024b)(Wei et al., 2024)(Sagar et al., 2024a)(Qi et al., 2023a)(Wang et al., 2023d)(Lu et al., 2023)(Wang et al., 2023c)(Mahmood et al., 2022)(Ahmad et al., 2020)(Xia et al., 2019b).

ii. *Dempster Shafer Theory* – Dempster Shafer Theory, also refers to as belief theory or evidence theory, integrates multiple pieces of evidence so as to enable the combination of data from diverse independent sources to generate a belief level within the range of [0,1]. However, in the presence of malicious entities, conflicting uncertainties in DST can potentially confound the judgments made by legitimate entities, thereby compromising the reliability of decisions (Cheong et al., 2024a)(Shamaeian and Pesch, 2024)(Mirzadeh et al., 2023)(Mahmood et al., 2023)(Bhargava and Verma, 2022)(Chen et al., 2019).

iii. *Bayesian Theory* – Bayesian theory is a probabilistic framework that acquires empirical knowledge by employing historical statistical data instead of relying on expert knowledge. It quantifies uncertainty by treating probabilities as degrees of belief, where prior probability is combined with observed data (likelihood) to form a posterior probability. The trust in bayesian theory is represented as a beta-distributed random variable within the range of [0,1] (Gao et al., 2022)(Fang et al., 2020)(Xiao and Liu, 2019).

iv. *Fuzzy Logic* – Fuzzy logic is a mathematical framework that handles imprecision, uncertainty, and partial truth by extending the traditional binary logic. In contrast to boolean logic that takes precise inputs in the form of either 0 or 1, fuzzy logic provides a more realistic understanding similar to human reasoning. Therefore, fuzzy logic can solve uncertainty and fuzziness in the notion of trust (Honarmand and Keshavarz-Haddad, 2024)(Fabi and Thampi, 2022b)(Zhao et al., 2022)(Li et al., 2021a)(Xia et al., 2019a).

v. *Machine Learning* – This particular technique typically involves two steps, i.e., unsupervised learning (clustering) and multiclass supervised learning (classification), to

categorize nodes into distinct classes. ML approach is generally suitable for models with a relatively higher number of trust parameters, however, it can incur significant computational costs and delays (Liu et al., 2025a)(Wan and Wang, 2024)(Sagar et al., 2023) (Siddiqui et al., 2023a)(Wang et al., 2023a)(Rjoub et al., 2023)(Zhao et al., 2023).

2.4.4 Trust Update

The trust update process involves event-driven trust update and time-driven trust update as delineated below:

i. *Event-driven Trust Update* – In an event-driven approach, trust is updated vis-à-vis each transaction. However, this type of update leads to increased traffic overhead due to frequent transactions within an IoV network (Yadav et al., 2025)(Qi et al., 2024)(Shamaeian and Pesch, 2024)(Su and Tong, 2023)(Li et al., 2023a)(Siddiqui et al., 2023b).

ii. *Time-driven Trust Update* – In a time-driven approach, trust is accumulated and updated via trust aggregation schemes after a predefined duration of time. Nevertheless, the temporal synchronization in this context remains an ongoing challenge (Shokrollahi and Dehghan, 2025)(Wei et al., 2024)(Fabi and Thampi, 2022a)(Li et al., 2021a).

2.4.5 Trust Decision

The purpose of trust decision is to predict the trustworthiness of vehicles based on a trustee's trust value, thereby ascertaining whether a vehicle can be considered trustworthy or not.

i. *Threshold-based Trust Decision* – In a threshold-based trust decision approach, the trust value of a trustee is either compared with a static or a dynamically adaptive threshold to facilitate the trustworthy decision process in a highly dynamic IoV network (Jain et al., 2025)(Cao et al., 2024)(Shen et al., 2024)(Du et al., 2024)(Sagar et al., 2024a)(Cheong

et al., 2024a)(Qi et al., 2023a)(Lu et al., 2023).

ii. *Context-based Trust Decision* – This trust decision approach employs the contextual information, including but not limited to, location, temporal factor, and energy status so as to systematically formulate policies that can facilitate in determining whether a vehicle is classified as malicious or not (Wei et al., 2024)(Sagar, 2023)(García-Magariño et al., 2019)(Li et al., 2018).

Table 2.4 summarizes the trust management processes employed in the state-of-the-art trust management models.

2.5 Trust Management Models – Discussion and Analysis

Over the past decade or so, a large number of trust management models have been proposed in the context of IoV networks to address the increasingly intricate internal security challenges and diverse applications' requirements (Ren et al., 2025)(Cheong et al., 2024b)(Wan and Wang, 2024)(Siddiqui et al., 2023b)(Sun et al., 2023). This section, therefore, provides an in-depth analysis of the two salient categories in this regard, i.e., Conventional Trust Management Models (Con-TMM) and AI-based Trust Management Models (AI-TMM).

2.5.1 Conventional Trust Management Models (Con-TMM)

A distributed Hybrid Trust Management framework (HTMS-V) has been proposed in Byeon et al. (2025) to identify potential internal attacks in VANETs, i.e., false message injection attacks, on-off attacks, and collusion attacks. HTMS-V integrates both direct trust and indirect trust by leveraging direct interaction data and trust recommendations from one-hop neighbors. Moreover, the said framework enhances the subjective logic trust model with a distance-based weighted voting mechanism to improve trust accuracy. Furthermore,

the said framework incorporates inter-node distance and equips each vehicle with a trust evaluation and decision module to address certain challenges, i.e., incomplete trust variables, erroneous trust evaluations, and potential collusion attacks in distributed environments.

A Cross-Domain dynamic Trust inheritance mechanism (CDTE) for VANETs has been envisaged in Ren et al. (2025) in order to update the trust value of a vehicle in real time. The mechanism's architecture contains three layers, i.e., central management layer, edge node layer, and vehicle node layer. It first integrates direct trust and recommended trust to ascertain the single trust value of a vehicle, and then calculates its global trust value through a trust feedback strategy consisting of active trust feedback and passive trust feedback, thereby ensuring to punish malicious vehicles and reward reliable ones. Moreover, to address the trust discontinuity problem in cross-domain scenarios, the RSUs can rapidly retrieve and refresh a vehicle's historical trust records upon its first entry into a new domain.

A Dual-model Consensus-based Anti-risk Confidence Allocation (DCACA) trust management scheme in an IoV network has been proposed in Cheong et al. (2024b) so as to analyze and identify internal inappropriate behaviors of vehicles. The dual-model consensus mechanism incorporates a real-time consensus collection mechanism and a matrix-based consensus mechanism, thereby significantly enhancing the detection capability of malicious behaviors by aggregating and analyzing trust opinions from various vehicles. Additionally, an anti-risk confidence allocation mechanism has been designed to filter out negative trust opinions provided by malicious vehicles. Moreover, to ensure evaluation accuracy, the trust management scheme employed a confidence-based weighting method for integrating direct trust, indirect trust, and global trust.

Table 2.4 Trust Management Processes in the IoV-based Trust Management Models (*Note: Dempster Shafer Theory – DST, Machine Learning – ML*).

References	Trust formation	Trust aggregation	Trust propagation	Trust update	Trust decision
(Shokrollahi and Dehghan, 2025)	Multi-trust	Weighted sum	Hybrid	Time-driven	Threshold-based
(Byeon et al., 2025)	Multi-trust	Subjective logic	Distributed	Time-driven	Threshold-based
(Liu et al., 2025a)	Multi-trust	ML	Distributed	Time-driven	Threshold-based
(Cao et al., 2024)	Multi-trust	Weighted sum	Hybrid	Event-driven	Threshold-based
(Wan and Wang, 2024)	Multi-trust	ML	Distributed	Event-driven	Threshold-based
(Shamaeian and Pesch, 2024)	Multi-trust	DST	Hybrid	Event-driven	Threshold-based
(Honarmand and Keshavarz-Haddad, 2024)	Multi-trust	Fuzzy logic	Distributed	Event-driven	Threshold-based

Table 2.4 continued

References	Trust formation	Trust aggregation	Trust propagation	Trust update	Trust decision
(Qi et al., 2024)	Multi-trust	Weighted sum	Distributed	Event-driven	Threshold-based
(Wei et al., 2024)	Multi-trust	Weighted sum	Distributed	Time-driven	Threshold-based
(Cheong et al., 2024a)	Multi-trust	DST	Distributed	Event-driven	Threshold-based
(Sagar et al., 2023)	Multi-trust	ML	Distributed	Event-driven	Threshold-based
(Wang et al., 2023c)	Multi-trust	Weighted sum	Distributed	Event-driven	Threshold-based
(Siddiqui et al., 2023a)	Multi-trust	ML	Distributed	Event-driven	Threshold-based
(Zhang et al., 2023a)	Multi-trust	Weighted sum	Distributed	Hybrid	Threshold-based
(Shokrollahi and Dehghan, 2023)	Multi-trust	Weighted sum	Distributed	Event-driven	Threshold-based

Table 2.4 continued

References	Trust formation	Trust aggregation	Trust propagation	Trust update	Trust decision
(Mao et al., 2023)	Multi-trust	Weighted sum	Hybird	Event-driven	Threshold-based
(Li et al., 2023a)	Multi-trust	Weighted sum	Distributed	Event-driven	Threshold-based
(Mahmood et al., 2022)	Multi-trust	Weighted sum	Distributed	Event-driven	Threshold-based
(Fabi and Thampi, 2022a)	Multi-trust	Honey-bee algorithm	Centralized	Time-driven	Threshold-based
(Aalibagi et al., 2022)	Multi-trust	ML	Centralized	Event-driven	Threshold-based
(Yin and Gong, 2022)	Multi-trust	Information entropy	Hybrid	Hybrid	Threshold-based
(Zhang et al., 2022b)	Multi-trust	Weighted sum	Centralized	Event-driven	Threshold-based
(Bhargava and Verma, 2022)	Multi-trust	DST	Distributed	Event-driven	Threshold-based

Table 2.4 continued

References	Trust formation	Trust aggregation	Trust propagation	Trust update	Trust decision
(Choukhairi et al., 2022)	Single-trust	Fuzzy logic	Distributed	Event-driven	Threshold-based
(Marche and Nitti, 2021)	Multi-trust	ML	Distributed	Event-driven	Threshold-based
(Li et al., 2021a)	Multi-trust	Fuzzy logic	Distributed	Time-driven	Threshold-based
(Zhang et al., 2020)	Multi-trust	Bayesian	Distributed	Time-driven	Threshold-based
(Xia et al., 2019a)	Single-trust	Fuzzy logic	Distributed	Time-driven	Threshold-based
(Chen et al., 2019)	Multi-trust	DST	Distributed	Event-driven	Threshold-based
(García-Magariño et al., 2019)	Multi-trust	Weighted sum	Hybird	Event-driven	Context-based
(Jayasinghe et al., 2019)	Multi-trust	ML	Distributed	Event-driven	Threshold-based

An incentive mechanism scheme to provide decentralized and trusted service management for information sharing in VANETs has been proposed in Han et al. (2024). This scheme evaluates message credibility based on the trust value of the sending vehicle and incorporates a negative feedback function to prevent malicious vehicles' attacks. Furthermore, a reward and punishment mechanism, rooted in repeated game theory, has been designed to incentivize vehicles for active information sharing. Additionally, to ensure consistent trust management storage and reduce reliance on centralized institutions, a blockchain-based distributed trust management scheme has been presented, wherein Roadside Units (RSUs) serve as blockchain nodes responsible for calculating vehicles' trust values and maintaining their respective trust value list.

A RSU-assisted Trust-based Routing protocol for VANETs (RTRV) has been presented in Azizi and Shokrollahi (2024) which incorporates trust criteria to ensure secure routing for establishing reliable and efficient communication paths. An enhanced monitoring procedure for trust management has been introduced for leveraging the common neighbor between the current node and the next hop node to select the monitoring node. Additionally, it employs a dual-observer (sender and monitor node) monitoring mechanism to observe the behavior of the next hop while utilizing RSU in trust management. This approach enhances resistance against good-mouthing attacks, bad-mouthing attacks, on-off attacks, gray hole (selective forwarding) attacks, collusion attacks, and newcomer attacks.

A reliable task offloading mechanism based on trusted RSU service for an IoV network has been established in Mao et al. (2023) to detect simple attacks, recommendation attacks, and on-off attacks for ensuring the security of an information service task in the context of an IoV network. This infrastructure trust management model includes the Quality of Service (QoS) trust and social trust, wherein QoS trust takes into account connectivity trust and timeliness trust, whereas, the social trust among RSUs is established through unselfish trust, neighbor recommendation, and cooperation trust. Moreover, a vehicle task unloading model considering delay optimization has been proposed to quantitatively analyze the delay caused

by task offloading. Furthermore, an algorithm based on trusted RSU service is designed to realize the offloading of networked vehicles' task.

A Multi-Dimensional Trust (MDT) model for VANETs has been put forward in Qi et al. (2023a) to effectively counter common malicious attacks, e.g., simple attacks, recommendation attacks, and zigzag attacks. The MDT model comprises four stages, i.e., (a) collection of local trust data, (b) trust aggregation, (c) abnormal data filtering, and (d) global trust updating. This model takes into consideration various trust attributes of vehicles, i.e., behavior trust, data trust, and recommendation trust, and employs the entropy weighting method to dynamically adjust the weights of the said attributes and ultimately achieves a comprehensive trust evaluation. Furthermore, the model utilizes the Median Absolute Deviation (MAD) to filter out abnormal evaluation results more effectively against both complex and dynamic intelligent attacks.

A trust model for VANETs aimed at mitigating attacks originating from legitimate network participants has been envisaged in Zhang et al. (2022b). Trust evaluation encompasses both local trust and social evaluation and RSUs-based trust aggregation. The local trust and social evaluation involve estimating the social relationships between vehicles through their respective trajectories and interaction history, in conjunction with social recommendations from neighboring vehicles. To achieve an accurate and comprehensive assessment of trust, the model utilizes RSUs to aggregate weights derived from eigenvector centrality and social indicators within the local trust network.

A content distribution model based on Entity Trust (ET) and Social Trust (ST) has been proposed in Zhao et al. (2022) in a bid to enhance the quality of service in a Social Internet of Vehicles (SIoV) network. The model segregates the trust evaluation into ET and ST. ET describes the communication capability of vehicle equipment, e.g., OBUs, antennas, the processing units, and the receiving and sending units, which is assessed based on historical communication (direct and indirect trustworthy ratio) between vehicles. On the contrary, the evaluation of ST stems from the process of establishing new social connections and

receiving feedback from acquaintances. Subsequently, fuzzy comprehensive evaluation has been employed for assessing ET and ST, thereby establishing an overall trust framework that effectively regulates the driving application functions and social behavior within SIoV network. Additionally, this model improves blocking rules of content distribution too.

The analysis of Table 2.5 reveals that the state-of-the-art conventional trust management models have a relatively small number of trust parameters due to the ongoing challenge in implementing a dynamic weighting mechanism. However, this reduced set of trust parameters presents drawbacks in evaluating the efficacy of the trust model.

2.5.2 Artificial Intelligence-based Trust Management Models (AI-TMM)

Due to the limitations inherent in conventional trust management models, i.e., limited number of trust parameters and challenges pertinent to dynamic weights, a number of AI-TMM have been proposed in the research literature (Liu et al., 2025a)(Wan and Wang, 2024)(Alshahrani, 2024)(Sun et al., 2023)(Sagar et al., 2023)(Siddiqui et al., 2023a).

A Q-Learning based Adaptive Trust Threshold control strategy (QART) has been proposed for VANETs in Liu et al. (2025a) to enhance the accuracy and efficiency of malicious vehicle detection. Firstly, an error degree has been defined to quantify the likelihood of false alarms and which serves as a foundation for determining an adaptive trust threshold. Subsequently, QART leverages reinforcement learning's reward and punishment mechanisms to balance detection efficiency and false alarm rates. Finally, a dynamic update control method has been developed to incorporate the latest trust evaluation results for timely and adaptive decision-making.

A trust-based client selection framework for federated learning has been developed in Raza and Badidi (2025) in a bid to address the issue pertinent to malicious or unreliable clients' updates in the context of an IoV network. By incorporating contextual information, reputation scores, and resource availability, the said framework adaptively aggregates clients

trust levels to prioritize reliable contributions and suppress adversarial influence. This framework encompasses several key components, i.e., central server, clients, communication network, trust evaluation module, and client selection module to ensure that only the most reliable clients participate in the FL training process. The central server sends the global model to all the clients who train and evaluate local models, and return updates and trust metrics. The trust evaluation module calculates and updates trust scores of each client, whereas, the client selection module opts for the most trustworthy ones. The central server aggregates updates from the selected clients to update the global model and repeats the process until it converges.

A hierarchical trust evaluation method based on data transmission success rate, network reliability and real time performance, and nodes' historical behaviors to determine the total trustworthiness of nodes has been proposed in Wan and Wang (2024). The proposed training model considers the issue of non Independent and Identically Distributed (non-IID) data affecting Federated Learning (FL) model convergence speed and, accordingly, introduced a Federated Adaptive (FedAdp) weighting algorithm encompassing initialization, local update, and global update processes to enhance or attenuate the positive or negative contributions from the participating nodes.

A Verifiable Discrete Trust Model (VDTM) for the Social Internet of Vehicles has been proposed in Alshahrani (2024) in a bid to address the risks associated with data leakage and trustworthiness when sharing social information, thereby ensuring secure information sharing. Consistent FL has been employed to verify both forward and reverse trust for enhancing authentication across different shared sessions. Moreover, key-based authentication has been implemented to ensure session integrity during information sharing.

Table 2.5 Conventional Trust Management Models (Con-TMM).

References	Trust attributes	Trust attacks	Context	Strengths	Limitations
(Ren et al., 2025)	Identity trust, Historical trust, Distance trust	On-off attack, Bad-mouthing attack, Data tampering attack, Collusion attack	Yes	A cross-domain dynamic Trust inheritance mechanism has been proposed, which integrates direct and recommended trust through a trust feedback strategy. It also addresses the trust discontinuity problem in cross-domain scenarios.	A vehicle initiates multiple attacks was not considered.
(Cheong et al., 2024b)	Transmission reliability of vehicles, Cooperativeness	Simple attack, Black hole attack, Colluding bad-mouthing attack, On-off attack, RSUs bad-mouthing attack	Yes	An anti-risk confidence allocation trust management scheme based on dual model consensus has been proposed. Dual-model consensus mechanism includes real-time collection consensus mechanism and matrix-based consensus mechanism.	Dynamic weighting mechanism hasn't been employed in the computation of global trust.
(Azizi and Shokrollahi, 2024)	Packet delivery ratio, Cooperativeness, Penalty, Transmission range	Bad-mouthing attack, Good-mouthing attack, On-off attack, Gray hole attack, Collusion attack, Newcomer attack	Yes	A motion metric-based enhanced vehicle position prediction mechanism has been proposed to achieve higher accuracy, while an improved greedy routing protocol has been suggested to enhance the speed and reliability of successful packet delivery.	The evaluation phase does not take into account the impact of the attack.

Table 2.5 continued

References	Trust attributes	Trust attacks	Context	Strengths	Limitations
(Han et al., 2024)	Distance, Reputation value, Information similarity	Message deception attack, Defamation attack	No	A trust-based message evaluation system combining reputation assessment and negative feedback functions has been proposed to evaluate the credibility of information. A reward and punishment mechanism based on repeated games to encourage vehicles to actively share information has been introduced.	The operational scenario of a vehicle has not been taken into consideration.
(Siddiqui et al., 2023b)	Packet delivery ratio, Time decay, Confidence, Frequency of interaction, Propagation delay, Cooperativeness, Familiarity	On-off attack, Selective node attack	Yes	Enhance the trust management framework by integrating contextual information and diverse contribution attributes of inter-vehicle communication. Employ appropriate influence parameters as weights to address issues related to weight quantization.	The operational scenario of a vehicle has not been taken into consideration.

Table 2.5 continued

References	Trust attributes	Trust attacks	Context	Strengths	Limitations
(Mao et al., 2023)	Connectivity, Timeliness, Blacklist similarity, Interaction frequency, Cooperation	Simple attack, Recommendation attack, On-off attack	Yes	A trust management model for RSU has been proposed to effectively detect and mitigate malicious attacks. A delay optimization-based model for vehicle task unloading is presented.	Dynamic weighting mechanism hasn't been employed in the computation of global trust.
(Qi et al., 2023a)	Packet delivery ratio, Driving status	Black hole attack, Recommendation attack, Zia-zag attack	Yes	A multi-dimensional trust model has been proposed. To account for the variability in local trust data and the disparities among different trust indicators, an entropy weight method to dynamically adjust the weight coefficient of each trust attribute has been employed.	The evaluation parameters of the model are singular.
(Lu et al., 2023)	Link-based trust evidence, Node-based trust evidence, Data based trust evidence, Experienced-based trust evidence	–	Yes	An Intermediate Vehicle Assisted Task Unloading enhanced scheme has been proposed to ensure quick and stable convergence results through the utilization of the Proximal Policy Optimization algorithm.	The consideration of defense mechanisms against various attacks has been overlooked.

Table 2.5 continued

References	Trust attributes	Trust attacks	Context	Strengths	Limitations
(Zhang et al., 2022b)	Interaction-based social metric, Trajectory-based social metric	Message manipulation attack, Bad-mouthing attack	Yes	The social relationship between vehicles has been estimated by integrating vehicle trajectories, interaction history, and social recommendations from neighboring vehicles.	The update component of the trust value is not addressed.
(Fabi and Thampi, 2022b)	Attitude toward behavior, Subjective norms, Perceived behavioral control	–	Yes	A pioneering integration of the Theory of Planned Behavior (TPB) from human psychology with parameters for evaluating trust in IoV network has been proposed. Fuzzy logic theory has been employed to assess the degree of trust by mapping TPB attributes.	The consideration of defense mechanisms against various attacks has been overlooked.
(Zhao et al., 2022)	Social activity, Feedback of the acquaintances	–	Yes	A model for entity and social trust perception has been proposed, categorizing trust assessment in SIoV into entity trust and social trust.	The consideration of defense mechanisms against various attacks has been overlooked.

Table 2.5 continued

References	Trust attributes	Trust attacks	Context	Strengths	Limitations
(Fabi and Thampi, 2022a)	Number of connections, Velocity of nodes	–	Yes	The forest fire model concept has been proposed for the selection of a minimal number of competent nodes to efficiently broadcast emergency messages.	The consideration of defense mechanisms against various attacks has been overlooked.
(Ahmad et al., 2021)	Role-oriented trust, Information quality, Effective distance	Man-in-the-Middle attack, Zig-zag attack	Yes	A hybrid trust framework based on the IoV protocol stack has been proposed, which is efficient and lightweight, capable of evaluating both node trustworthiness and data trustworthiness.	The mechanism for trust fusion lacks clarity in its explanation.

To address the inability of the current trust models to select appropriate recommendation nodes and dynamically adjust the weight of the recommendation trust, a trust model based on IoV topological structure has been put forward in Sun et al. (2023). The model contains three layers, i.e., local trust management, cluster trust management, and global trust management. Prior to calculating of recommendation trust, a fuzzy C-means algorithm has been employed to filter out malicious recommendation values, followed by assessing the reliability of recommendation trust values through degrees of similarity and dissimilarity.

A trust framework based on artificial neural networks has been envisaged in Sagar et al. (2023) to establish a robust foundation for trust assessment in the context of Social Internet of Things (SIoT). A number of key trust metrics, i.e., direct trust, reliability and benevolence, credible recommendations, and context-based degree of relationships, have been taken into account. Furthermore, a knowledge graph embedding model to estimate the social similarity among IoT objects has been employed.

The utilization of machine learning technique to address the challenges associated with intelligent weight assignment and optimal misconduct detection threshold in an IoV network has been proposed in Siddiqui et al. (2023a). Firstly, a feature matrix that incorporates four key trust parameters (packet delivery ratio, familiarity, timeliness, and interaction frequency) has been established. Subsequently, two different approaches have been employed to calculate the aforementioned feature matrix, i.e., (a) treating all four trust parameters calculated by each trustor for the trustee as a single feature, and (b) considering the collective average of the said four parameters calculated by all trustors for the trustee. Moreover, various machine learning algorithms, i.e., k-means clustering, fuzzy c-means clustering, hierarchical clustering, and gaussian mixture clustering, have been utilized to label each generated feature matrix. Finally, support vector machine, k-nearest neighbor, set subspace k-nearest neighbor, and subspace classification methods have been employed for the classification of vehicles into honest and dishonest ones.

A hybrid optimization-based Deep Maxout Network (DMN) for classifying attacks in

VANETs has been suggested in Kaur and Kakkar (2022). The selection of cluster head and routing process are performed using fractional aquila optimizer algorithm which combines fractional calculus and aquila optimization techniques (Abualigah et al., 2021). Moreover, the selection process takes into account the impact of distance, trust factors, energy levels, and entropy weighted models. The trust factors incorporate direct trust (forwarded packets, overall energy depletion, and energy depletion per packet), indirect trust, and recent and historical trust. Attack detection is segregated into two stages – feature selection and classification. The feature selection uses congruence coefficients to select key attributes. Finally, according to whether the nodes are malicious or normal, DMN is used to classify the nodes.

A time-aware machine learning-driven trust evaluation model to determine and predict the behavior of an object in a SIoT network has been envisaged in Sagar et al. (2021). The trust model encompasses four trust parameters, i.e., friendship similarity, community-of-interest, co-work similarity, and cooperativeness. Machine learning has been employed to aggregate the said trust parameters and to classify objects as trustworthy or untrustworthy. Moreover, change in the trust values vis-à-vis time has been analyzed so as to determine the influence of each trust parameter on an object's aggregated trust. A somewhat similar SIoT-based trust model encompassing direct trust and indirect trust has been presented in Sagar et al. (2020b), wherein objects have been classified as trusted, neutral, or untrusted.

An entity centric trust framework based on decision tree and artificial neural networks has been proposed in El-Sayed et al. (2020) so as to enhance the security of an IoV network. The said framework took into consideration direct trust, recommended trust, multifaceted entities-based role, and distance-based (euclidean) measures for calculating and evaluating trust amongst the vehicles. Moreover, a decision tree classification model has been employed to derive rules for trust calculation and artificial neural networks have been utilized to self-train vehicular nodes in order to ensure reliable message propagation.

Table 2.6 depicts a comparative analysis of the state-of-the-art AI-based trust management models.

Table 2.6 Artificial Intelligence-based Trust Management Models (AI-TMM).

References	Trust parameters	Trust attacks	Context	Strengths	Limitations
(Liu et al., 2025a)	Types of interactive information, Satisfaction, Distance	Intelligent attack, False message attack, Imbalance attack, Collusion attack	Yes	A Q-Learning-based adaptive trust threshold control strategy has been designed for VANETs to enhance malicious vehicle detection by dynamically balancing detection efficiency and false alarm rates.	The trust attack is not considered, and there are few trust parameters.
(Wan and Wang, 2024)	Data packet reception, Data transmission success rate, Network reliability and real-time, Node historical behavior	Gaussian noise attack, Sign-flipping attack	Yes	A federated adaptive weighted aggregation algorithm has been introduced to modulate the positive or negative contribution of participating vehicles.	The evaluation of experimental results is relatively simple.
(Alshahrani, 2024)	Packet delivery ratio	-	Yes	A verifiable discrete trust model to ensure secure information sharing in SIoV has been proposed, and it leveraged federated learning to validate both forward and reverse trust. A key-based authentication has been employed to guarantee session integrity during the process of information sharing.	Relevant countermeasures against various attacks have not been taken into account.

Table 2.6 continued

References	Trust parameters	Trust attacks	Context	Strengths	Limitations
(Sun et al., 2023)	Positive feedback, Negative feedback, Similarity, Difference	Switch attack	Yes	A trust model based on the topology of IoV network has been proposed, wherein adaptive weights are employed to comprehensively evaluate the vehicles.	The evaluation of the switch attack is examined.
(Sagar et al., 2023)	Positive interaction, Negative interaction, Recommendation, Reliability, Benevolence, Context-aware degree of relationship	Good-mouthing attack, Bad-mouthing attack	Yes	A trust framework based on artificial neural networks has been proposed to establish a robust foundation for trust assessment in the context of Social Internet of Things. The Knowledge Graph Embedding model has been employed to estimate the social similarity among objects.	The impacts of good mouthing attack and bad mouthing attack were not thoroughly examined.
(Siddiqui et al., 2023a)	Packet delivery ratio, Familiarity, Timeliness, Interaction frequency	–	No	A machine learning driven trust management model has been proposed to address the challenges associated with effective weight assignment and optimal misconduct detection threshold in an IoV network.	Computational inefficiency and significant latency.

Table 2.6 continued

References	Trust parameters	Trust attacks	Context	Strengths	Limitations
(Wang et al., 2023a)	Timeliness, Perceived trust degree, State formulas, Energy trust, Reliability, Success rate, Information transfer, Number of packets	Flooding attack	No	A hierarchical trust evaluation model that takes into account data transmission has been proposed. A personalized federated learning in heterogeneous networks as a means of reducing the cost associated with trust evaluation has been introduced.	The influence of context on trust has not been taken into account.
(Kaur and Kakkar, 2022)	Forwarded packets, Overall energy depletion, Energy depletion, Distance, Delay, Energy consumption	Various types of attacks	No	A hybrid optimized Deep Maxout Network (DMN) for classifying VANETs attacks in an efficient manner has been introduced. The selection of cluster head and routing process have been performed using the suggested Fractional Aquila Optimizer.	This research lacks specificity in classifying the types of attacks that can be categorized using DMN.
(Sagar et al., 2021)	Friendship similarity, Community-of-interest, Co-work similarity, Cooperativeness	–	No	A trust evaluation model to determine and predict the behavior of an object in the SIoT network over a period of time has been proposed. The model examined the temporal dynamics of trust value fluctuations and elucidates the impact of individual trust parameters on each vehicle's trustworthiness.	Insufficient analysis of the contextual influence on node interactions.

Table 2.6 continued

References	Trust parameters	Trust attacks	Context	Strengths	Limitations
(Sagar et al., 2020b)	Friendship similarity, Community-of-interest, Reward, Cooperativeness	Ballot-stuffing attack	No	A trust computing model for extracting individual trust features in the context of SIoT has been proposed. A heuristic algorithm based on machine learning is employed to aggregate all trust features and determine the total trust value to get a single of each vehicle.	Insufficient analysis of the contextual influence on node interactions.
(El-Sayed et al., 2020)	Message receiving time, Message delivering time, Similarity	–	No	An entity-centric trust framework based on decision tree classification and artificial neural network has been proposed. A decision tree classification model to derive rules for trust calculation, along with utilizing artificial neural networks to train onboard nodes has been designed.	Relevant countermeasures against various attacks have not been taken into account.
(Siddiqui et al., 2019)	Similarity, Infrastructure trust, Packet delivery ratio	–	No	Two distinct methodologies have been employed to compute the eigenmatrix of three parameters. A diverse machine learning algorithm has been utilized for the classification of vehicles into trustworthy and untrustworthy.	The consideration of defense mechanisms against various attacks has been overlooked.

2.6 Simulation Tools and Datasets

This section delineates simulation tools and datasets for assessing the performance of trust-based models in an IoV network.

2.6.1 Simulation Tools

The simulation method is predominantly employed for evaluating the trust models in an IoV network. The state-of-the-art simulation tools in this context include, but are not limited to, Veins (Dang et al., 2025)(Qi et al., 2024), Network Simulator 3 (NS-3) (Li et al., 2023a), Opportunistic Network Environment (ONE) (Song et al., 2024), NetLogo simulator (Xia et al., 2019a), MATLAB (Liu et al., 2025a), and Python (Nagaraju and Saini, 2025).

i. *Veins* – Veins (https://veins.car2x.org/) is a traffic simulation framework which integrates Simulation of Urban Mobility (SUMO) and OMNeT++ with a primary focus on simulating urban traffic flows and vehicular communications. Accordingly, researchers can manipulate several parameters, e.g., traffic signals, vehicles' behaviors, and communication protocols, to evaluate traffic management strategies, optimize flow dynamics, analyze congestion causes, and assess the impact of the same in an IoV network. The results can be visually presented using intuitive tools to facilitate decision-making processes and enhance traffic planning capabilities. Existing literature suggests that numerous studies on trust management have utilized Veins to validate their proposed trust management models (Azizi and Shokrollahi, 2024)(Su et al., 2024)(Shen et al., 2024)(Zhang et al., 2023a)(Qi et al., 2023a)(El-Sayed et al., 2022).

ii. *Network Simulator 3 (NS-3)* – NS-3 (https://www.nsnam.org/) is an open-source network simulation tool which utilizes the discrete event simulation method and provides support for various network protocols, e.g., transmission control protocol and user datagram protocol. Researchers can define the network topology and simulation parameters using Tool Command Language scripts that offer a high degree of flexibility (Riley and

Henderson, 2010). NS-3 thus enables the creation of realistic simulation scenarios and is, therefore, widely employed to validate trust management models (Honarmand and Keshavarz-Haddad, 2024)(Su and Tong, 2023)(Mahmood et al., 2022)(Fabi and Thampi, 2022a)(Fabi and Thampi, 2022b)(Najafi et al., 2022).

iii. *Opportunistic Network Environment (ONE)* – ONE (http://akeranen.github.io/the-one/) is a simulation environment which enables creating dynamic networking scenarios and facilitates the testing of numerous routing protocols. Also, it offers visualization tools that portrays a comprehensive depiction of nodes movement and data transmission processes. The flexibility and scalability inherent in ONE has encouraged researchers over the years to validate their respective trust management models in dynamic IoV scenarios (Cheong et al., 2024a)(Wang et al., 2023c)(Zhang et al., 2022b).

iv. *NetLogo Simulator* – NetLogo simulator (https://ccl.northwestern.edu/netlogo/) is an integrated development environment for multi-agent simulation well-suited for modeling complex systems (Wilensky, 1999). It enables the simultaneous movement of thousands of agents, thereby facilitating the exploration of individual microscopic entities and their interactions that give rise to macroscopic phenomena. NetLogo simulator has been instrumental in studying trust management within IoV networks by enabling the simulation of agent-based trust dynamics and communication protocols (Yin and Gong, 2022).

v. *Others* – In addition to the above, MATLAB and Python have also been extensively utilized to simulate and validate IoV-based trust management models. MATLAB offers capabilities in numerical analysis, numerical and symbolic computation, engineering and scientific plotting, and digital image processing. It is, therefore, widely employed by researchers for purposes of model creation, algorithm development, and data analysis. Moreover, MATLAB provides a dedicated Simulink platform for designing and deploying IoV applications. Accordingly, it has gained significant popularity within trust management community. Similarly, Python serves as a commonly used tool for simulating dynamic networks. To summarize, both MATLAB and Python have emerged

as preferred choices in the research literature for validating the performance of various IoV-based trust management models (Han et al., 2024)(Mao et al., 2023)(Wang et al., 2023a)(Siddiqui et al., 2023a)(Siddiqui et al., 2023b)(Mahmood et al., 2023)(Lu et al., 2023)(Sagar et al., 2023)(Huang et al., 2022)(Mahmood et al., 2022).

2.6.2 Datasets

Datasets are indispensable for validating IoV-based trust management models. Whilst there are no dedicated IoV-based trust datasets, i.e., with exception of the one envisaged in Chapter 5, a detailed analysis of the state-of-the-art reveals that both Epinions dataset and CRAWDAD dataset have been extensively employed for the said purpose (Sagar et al., 2024b)(Farahbakhsh et al., 2021).

i. *Epinions Dataset* – Epinions (https://cse.msu.edu/tangjili/datasetcode/truststudy.htm) is a publicly available trust dataset that encompasses six parameters, i.e., userid, productid, categoryid, rating, usefulness, and timestamp. A data trace, $[1, 2, 3, 4, 5, 6]$, in the Epinions dataset indicates that user 1 has given a rating of 4 to product 2 belonging to category 3 at timestamp 6 with helpfulness of the said rating as 5. The Epinions dataset, while not originally designed as an IoV dataset, has been appropriately transformed into one by certain researchers for evaluating the performance of IoV-based trust management models (Kerrache et al., 2019).

ii. *Epinions Dataset* – Community Resource for Archiving Wireless Data at Dartmouth (CRAWDAD) Dataset – CRAWDAD (https://crawdad.org/thlab/sigcomm2009/20120715/) is a dataset for the research community interested in wireless networks and mobile computing. This particular dataset was originally conceived as part of the SIGCOMM conference and hence encompasses traces of participants' devices, including but not limited to, their respective proximity, opportunistic message creation and dissemination (with interaction logs in terms of successful and unsuccessful interactions), and the social profiles (list of

friends and interest groups). Over the past few years, the CRAWDAD dataset has been widely employed in the research literature for the performance evaluation of IoV-based trust management models (Alalwany and Mahgoub, 2024)(Sagar et al., 2024a)(Siddiqui et al., 2023a)(Siddiqui et al., 2021b)(Sagar et al., 2021).

A dedicated IoV-based trust dataset, TM–IoV (Wang et al., 2024b), has been introduced as part of the research-at-hand and is discussed in detail in Chapter 5.

2.7 Summary

This chapter provides a thorough review of trust management in the context of an IoV network. It begins with a discussion of the evolution of VANETs into IoV followed by an exploration of the notion of trust across several different domains. The chapter then examines the key aspects of trust in an IoV network, i.e., its salient characteristics, constituents, attributes, evaluation parameters, and trust-based attacks. It also delves into the various processes involved in trust management, i.e., trust formation, trust propagation, trust aggregation, trust update, and trust decision. Moreover, the chapter highlights the strengths and limitations of existing IoV-based trust management models, i.e., conventional and AI ones. Furthermore, it introduces the simulation tools and datasets employed for the performance evaluation of IoV-based trust models, thereby providing a comprehensive overview of the current landscape of trust management in IoV networks.

CHAPTER 3

MESMERIC: MACHINE LEARNING-BASED TRUST MANAGEMENT MECHANISM FOR THE INTERNET OF VEHICLES

The emerging yet promising paradigm of the Internet of Vehicles (IoV) has recently gained considerable attention of researchers from both academia and industry. As an indispensable constituent of the futuristic smart cities, the underlying essence of the IoV is to facilitate vehicles to exchange safety-critical information with the other vehicles in their neighborhood, vulnerable pedestrians, supporting infrastructure, and the backbone network via vehicle-to-everything communication in a bid to enhance the road safety by mitigating the unwarranted road accidents via ensuring safer navigation together with guaranteeing the intelligent traffic flows. This requires that the safety-critical messages exchanged within an IoV network and the vehicles that disseminate the same are highly reliable (i.e., trustworthy); otherwise, the entire IoV network could be jeopardized. A state-of-the-art trust-based mechanism is, therefore, highly imperative for identifying and removing malicious vehicles from an IoV network. Accordingly, in this chapter, a machine learning-based trust management mechanism, MESMERIC, has been proposed that takes into account the notions of direct trust (encompassing the trust attributes of interaction success rate, similarity, familiarity, and reward and punishment), indirect trust (involving confidence of a particular trustor on the neighboring nodes of a trustee, and the direct trust between the said neighboring nodes and the trustee), and context (comprising vehicle types and operating scenarios) in order to not only ascertain the trust of vehicles in an IoV network but to segregate the trustworthy vehicles from the untrustworthy ones by means of an optimal decision boundary. A comprehensive evaluation of the envisaged trust management mechanism has been carried out which demonstrates that

Wang Yingxun, Adnan Mahmood, Mohamad Faizrizwan Mohd Sabri, Hushairi Zen, Kho Lee Chin (2024). *MESMERIC: Machine Learning-based Trust Management Mechanism for the Internet of Vehicles*. Sensors, 24 (3):863 (Q2, Impact Factor: 3.5).

it outperforms other state-of-the-art trust management mechanisms.

3.1 Overview

The rapid acceleration in urbanization and growth of the population has substantially increased the ownership of vehicles. A conservative estimate by the World Health Organisation suggests that traffic accidents kill approximately 1.35 million people every year and approximately 50 million people suffer from non-fatal injuries (Sun et al., 2025)(Miao et al., 2024)(Mirzadeh et al., 2023). Furthermore, the congestion of traffic is a global issue which also results in increased noise pollution and vehicular emissions (Akwirry et al., 2022)(Afrin and Yodo, 2020). Accordingly, numerous researchers from academia and industry over the years have focused on resolving such issues. Ensuring both passenger road safety and traffic congestion mitigation, therefore, requires an intelligent system of vehicular communication.

Vehicles today are an indispensable constituent of the Internet of Things (IoT) network and are accordingly equipped with hundreds of sensors onboard (Mo et al., 2022). As per an estimate, modern vehicles are equipped with approximately 100 sensors onboard with each vehicle capable of producing nearly 380 TB to 4.9 PB data annually (Fabi and Thampi, 2022b). Therefore, vehicle-mounted sensors (position, velocity, acceleration, pressure, and temperature sensors) and IoT devices would be able to construct a safe and efficient intelligent network of transportation (Arthurs et al., 2022).

The IoV is an application of IoT in the context of intelligent transportation systems. The IoV has a similar architecture to the IoT and features a hierarchical structure that includes data source, edge, fog, and the cloud layers (Siddiqui et al., 2023a). Vehicles share information with other vehicles, pedestrians, intelligent infrastructure, and backbone networks to establish vehicle-to-vehicle, vehicle-to-pedestrian, vehicle-to-infrastructure, and vehicle-to-network communication, thereby formulating vehicle-to-everything communication. The main IoV communication node is a vehicle with an on-board unit which can communicate with the

RSUs and other vehicles in its proximity. Due to the unique characteristics of IoV, i.e., openness, dynamic topology, and high mobility, it is susceptible to attacks; dishonest entities can modify legitimate security messages, spread forged information, or delay forwarding messages, thereby endangering human lives (Ding et al., 2024).

Accordingly, researchers have proposed several solutions for handling the issues pertinent to IoV security. Nevertheless, a number of these solutions rely on conventional cryptographic-related schemes and, therefore, rely on the notions of digital signatures, certificates, and public key infrastructure (Ahmad et al., 2024)(Hussain et al., 2021)(Singh et al., 2019). Moreover, conventional cryptographic-related schemes are only capable of mitigating external attacks and are ineffective against internal network attacks (Li et al., 2023b). It is due to this reason that the paradigm of trust has been recently introduced in the research literature.

The notion of trust originated in sociology as a means to understand how people are interdependent within a social organization (Drobot et al., 2023). Trust, over the years, has also been employed in various other disciplines, including but not limited to, philosophy, economics, engineering, and computer science. Trust is generally referred to as the confidence of a trustor in a trustee. Here, trustor refers to a node that is in a position to ascertain the trust of the other node (trustee) in the network, whereas, the trustee refers to a node whose trust is being ascertained (Tripathi et al., 2023). In the context of this chapter, trust refers to the likelihood that a trustee can perform a particular operation (contribute to realizing a particular application or service) within a specific situation at a specific time. It is also important to mention that trust computation primarily involves a weighted aggregation of both the direct trust and the indirect trust (Yuan et al., 2023). Direct trust is ascertained as a result of direct interactions between a trustor and a trustee and is generally referred to as a trustor's direct observation of a trustee (Siddiqui et al., 2023b)(Yong-hao, 2020). On the contrary, indirect trust is computed by taking into account the direct trust ascertained by the one-hop neighbors of a trustor pertinent to a trustee. The literature argues that direct trust is more significant in contrast to indirect trust (Mirzadeh et al., 2023).

To date, a number of trust management models have been proposed in the research literature which have been broadly classified into three types: entity-oriented trust models, data-oriented trust models, and hybrid trust models (Iqbal et al., 2025)(Qi et al., 2023a). Entity-oriented trust models aim to eradicate malicious entities (vehicles) from an IoV network by evaluating the reliability of the vehicles disseminating messages. Data-oriented trust models, on the other hand, eradicate the malicious messages instead of the entities from an IoV network (Raya et al., 2008). Finally, hybrid trust models take into account the salient characteristics of both the entity-oriented and data-oriented trust models and, therefore, regard the reliability of the entities and the respective messages disseminated by them in a bid to make a decision.

The trust parameters, also referred to as the trust attributes, are integral constituents of any trust model. The existing literature suggests that a number of research studies determined the global trust value of a particular vehicle in an IoV network by taking into account the weighted sum of a number of such trust parameters and which, in fact, is also subject to limitations (Siddiqui et al., 2023b)(Sagar et al., 2021). For instance, weights' settings are based on human subjectivity and, therefore, different researchers often set different weights for the same trust parameter which results in an inconsistent trust score. Keeping this in mind, the envisaged research employs the notion of machine learning to ascertain trustworthy and untrustworthy vehicles via an optimal trust boundary. In order to achieve the optimal trust evaluation results, the trust model needs more trust parameters, however, it will lead to an increase in the amount of calculation. Accordingly, a learning-based method has been used to train the trust model. In this way, the global trust value of each vehicle was established by combining all of its respective trust parameters such that the optimal influence of each trust parameter on the global trust value is prevalent.

Also, a number of trust models do not take into account the effect of context while ascertaining the trust of a particular vehicle. For instance, an urban scenario involves more vehicles and, therefore, the inter-vehicular interactions are much more as opposed to a highway

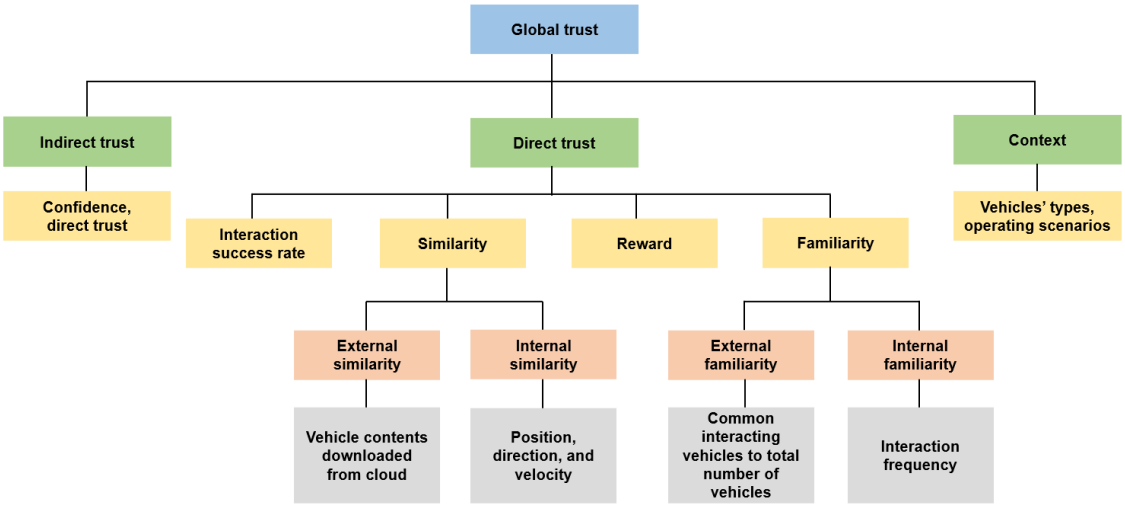

Figure 3.1 The Composition of the Global Trust.

scenario, wherein it is extremely challenging to establish trust among the vehicles. Similarly, public vehicles, including but not limited to, police cars, ambulances, and fire brigades have higher trust values in contrast to private vehicles. Moreover, drivers with many years of driving experience generally have higher trust values than novice drivers. This research, therefore, regards two contextual factors, i.e., vehicle types and operating scenarios, in order to obtain a more optimal trust value. Therefore, not only the direct trust and the indirect trust were included in the global trust of the envisaged trust model but the context was also incorporated (see Figure 3.1).

The salient contributions of the research-at-hand are as follows:

i. A novel trust management mechanism that regards direct trust (encompassing the trust attributes of interaction success rate, similarity, familiarity, and reward and punishment), indirect trust (involving recommendations via the one-hop neighboring nodes of a trustor pertinent to a trustee and the confidence of a trustor on the recommendations ascertained by the one-hop neighboring vehicles), and context (comprising vehicle types and operating scenarios) has been proposed to ascertain the trust of vehicles in an IoV network;

ii. In contrast to the conventional trust management heuristics, a machine learning-based trust aggregation scheme has been envisaged in a bid to ascertain the optimal trust score

of each vehicle in an IoV network so that they can be classified as either being trustworthy or untrustworthy;

iii. A comprehensive evaluation of the envisaged trust management mechanism has been carried out which demonstrated that it outperforms other state-of-the-art trust management mechanisms.

The rest of the section is systematically organized as follows. Section 3.2 delineates the state-of-the-art of trust management in IoV networks. Section 3.3 presents the envisaged trust management mechanism. Section 3.4 presents the experimental results and discussions pertinent to the same, and Section 3.5 concludes the chapter.

3.2 Related Works

In recent years, there has been an increase in research on trust management in the IoV (Li et al., 2023b)(Akwirry et al., 2022)(Fabi and Thampi, 2022a)(Fabi and Thampi, 2022b)(Bhargava and Verma, 2022)(Atwa et al., 2021a)(Rehman et al., 2021)(Sagar et al., 2021)(Jayasinghe et al., 2019). The existing trust management models have been divided into conventional- and learning-based ones.

3.2.1 Trust Parameters and Evaluation Parameters

A holistic overview of the existing trust management mechanisms reveals that a number of trust-based parameters have been applied in different settings in order to measure and evaluate trust. The trust-based parameters, including but not limited to, resource availability (Arthurs et al., 2022), similarity (Sagar et al., 2021)(Mao et al., 2021)(Siddiqui et al., 2019), familiarity (Mahmood et al., 2023)(Siddiqui et al., 2023a)(Arthurs et al., 2022)(Rehman et al., 2021), timeliness (Siddiqui et al., 2023a)(Wang et al., 2023a), context (Sagar et al., 2021)(Atwa et al., 2021b)(Sagar et al., 2020b)(Jayasinghe et al., 2019), cooperativeness (Sagar et al., 2021), community-of-interest (CoI) (Sagar et al., 2021), confidence (Alnasser

et al., 2020)(Ahmad et al., 2018), reward (Wang et al., 2023c)(Qiong et al., 2023)(Atwa et al., 2021b), attitude, subjective norms, and perceptual behavioral control (Fabi and Thampi, 2022b), freshness of data (Oubabas et al., 2018), and packet delivery ratio (Siddiqui et al., 2023a)(Siddiqui et al., 2019)(Ahmad et al., 2018). Also, the selection of a trust-based threshold for determining trustworthy and untrustworthy behavior is crucial. If the threshold is set too high by the system designers, the trustworthy nodes may be even removed from a network. Alternatively, if the threshold is set too low, the untrustworthy nodes would slowly jeopardize the entire network. A comparative summary of the trust parameters employed in the representative literature is depicted in Table 3.1.

It is interesting to note that context is the most frequently used trust parameter followed by cooperativeness, similarity and reward. Context is an extremely important trust parameter and a number of other trust parameters depend on the same, and are, therefore, dissimilar in different contexts. For instance, the number of interactions between vehicles is different in urban and highway scenarios. Also, different types of vehicles, i.e., high-priority vehicles, public transport vehicles, professional vehicles, and novice vehicles, have different trust values. Accordingly, this chapter proposes a context-based trust management model. Table 3.1 further depicts that there are not many trust parameters employed in the state-of-the-art trust management models. If there are few trust parameters, the accuracy of the global trust value calculated will also decrease. To mitigate this problem, a trust management model that includes six trust parameters, i.e., interaction success rate, similarity, familiarity, reward and punishment, confidence, and context, has been proposed.

Table 3.1 Trust Parameters in Trust Management Model (*Note: Community-of-Interest – CoI*).

References	Similarity	Familiarity	Timeliness	Context	Cooperativeness	CoI	Confidence	Reward
(Cheong et al., 2024a)	✓	✓	-	-	✓	-	-	-
(Cheong et al., 2024b)	-	-	-	-	✓	-	-	-
(Qiong et al., 2023)	-	-	-	✓	✓	-	✓	-
(Mao et al., 2023)	-	-	✓	-	-	-	-	-
(Siddiqui et al., 2023a)	-	✓	-	✓	✓	-	✓	-
(Siddiqui et al., 2023b)	-	✓	✓	✓	✓	-	✓	-
(Akwirry et al., 2022)	-	-	-	-	✓	-	-	-
(Fabi and Thampi, 2022a)	-	-	-	✓	-	-	-	-
(Bhargava and Verma, 2022)	-	-	✓	✓	-	-	-	-
(Yin and Gong, 2022)	✓	-	-	-	-	-	-	-
(Gao et al., 2022)	-	-	-	-	-	-	✓	-
(Jing et al., 2022)	-	-	-	-	-	-	-	✓
(Sagar et al., 2021)	✓	-	-	-	✓	✓	-	-
(Mao et al., 2021)	✓	-	-	-	-	-	-	-

Table 3.1 continued

References	Similarity	Familiarity	Timeliness	Context	Cooperativeness	CoI	Confidence	Reward
(Atwa et al., 2021b)	-	-	-	-	-	-	-	✓
(Sagar et al., 2020b)	-	-	-	-	-	-	-	✓
(Alnasser et al., 2020)	-	-	✓	✓	-	-	-	-
(Guo et al., 2020)	-	-	-	✓	-	-	-	✓
(Jayasinghe et al., 2019)	-	-	-	-	✓	✓	-	✓
(Siddiqui et al., 2019)	✓	✓	-	✓	-	-	-	-
(Xia et al., 2019a)	✓	✓	-	✓	-	-	-	-
(Oubabas et al., 2018)	-	✓	-	-	✓	-	-	-
(Ahmad et al., 2018)	-	-	-	✓	✓	-	-	-
This scheme	✓	✓	-	✓	✓	✓	✓	✓

There are two important steps in trust management, i.e., building a trust model and evaluating a trust model (Ahmad et al., 2018). The purpose of trust evaluation is to evaluate the accuracy, reliability, and practicality of an envisaged trust model. The literature suggests that typical evaluation parameters employed for the trust-based models, including but not limited to precision, recall, F1 score (Sagar et al., 2021)(Sagar et al., 2020b), false positive rate (Choukhairi et al., 2022), false negative rate (Choukhairi et al., 2022), true positive rate (Bhargava and Verma, 2022), true negative rate (Xia et al., 2019a), mean absolute error (Sun et al., 2023), mean squared error (Sagar et al., 2023), detection rate (Mahmood et al., 2023), and computational overhead (Feng et al., 2021).

3.2.2 Conventional Trust Management Models

A context-aware and attack-resistant trust model for the IoV networks has been suggested in Siddiqui et al. (2023b). This model considers (a) local trust encompassing the weighted sum of both direct trust (packet delivery ratio and time decay) and indirect trust (confidence factor) and (b) context-dependent trust (propagation delay, cooperativeness, and familiarity). Also, the notion of an adaptive misbehavior detection threshold has been proposed to segregate malicious vehicles from dishonest vehicles. Moreover, the resilience against on-off attacks and the selective node attacks has been demonstrated by employing optimal and rational influencing parameters as weights during the process of the weights' assignment.

A forest fire model has been proposed in Fabi and Thampi (2022a) to select the minimum number of competent nodes suitable for broadcasting emergency messages in an IoV network. At first, a social community is established by calculating the similarity of the social characteristics between the nodes. Subsequently, some key factors, including but not limited to, the number of connections, velocity of nodes, general activity of the nodes, and data forwarding capability of neighboring nodes, are used to select the core node and the complementary node

for the dissemination of emergency messages within the established social community. This establishes a trust estimation and management mechanism for nodes based on their behavior in an IoV network. Experimental results suggest that this particular model demonstrated high accuracy under a high density of malicious nodes.

A trust evaluation algorithm has been proposed in Fabi and Thampi (2022b) that exploited the attributes (attitude towards behavior, subjective norms, and perceived behavioral control) from the theory of planned behavior, i.e., a human psychological theory, to ascertain the trustworthiness of vehicles in a vehicular network within a given context and to decide whether to accept or not the traffic-related warning messages from a particular vehicle. Moreover, the notion of fuzzy logic has been employed in a bid to segregate the vehicles' trust levels as CompleteTrust, MediumTrust, and DisTrust. The effectiveness of the trust evaluation algorithm was verified via false positive rates, true positive rates, and F1 score vis-à-vis different proportions of malicious vehicles.

A novel hybrid trust management scheme for an IoV network has been proposed in Ahmad et al. (2021) to evaluate both node-centric and data-centric trust. Node-centric trust has been determined by employing the distance between the message sender and the message evaluator in tandem with the antenna height of the message sender and the message evaluator, whereas, data-centric trust has been ascertained by means of information quality and effective distance (via a tier-based approach) between the message sender and the message evaluator. A trust threshold has been further employed which facilitates rewarding (incrementing) and penalizing (decrementing) the trust score of the message sender. The performance of the trust management scheme has been evaluated via man-in-the-middle attacks and zigzag attacks.

3.2.3 Machine Learning-based Trust Management Models

A trust computational heuristic model has been envisaged in Sagar et al. (2021) to establish trustworthy relationships among the physical objects, i.e., devices, and for miti-

gating potential risks throughout the decision-making process in a Social Internet of Things (SIoT) environment. The direct trust of a particular object (trustee) is ascertained by taking into consideration the trust attributes of friendship similarity, community of interest, cooperativeness, and reward / punishment. The indirect trust, on the other hand, is computed by requesting the direct trust from the nodes that have interacted with the trustee. The authors exploited the notion of machine learning to (a) aggregate the trust attributes to determine an optimal trust score and (b) determine the best possible boundary to segregate between the trustworthy, untrustworthy, and neutral interactions. The neutral interactions are classified as trustworthy or untrustworthy via a percentage threshold mechanism.

A trustworthy object classification framework, Trust-SIoT, has been further proposed in Sagar et al. (2020b) to establish and maintain a trustworthy relationship between the IoT objects over time. The authors employed social characteristics of objects in the form of direct trust metrics, reliability and benevolence, credible recommendations, and the degree of relationships. A SIoT knowledge graph was further constructed in order to record five dynamic social relationships, i.e., co-location object relationships, parental object relationships, ownership object relationships, Social Object Relationships (SOR), and a variant of SOR (to connect public and private mobile devices) to ascertain the degree of relationships. An artificial neural network-based model was further employed for decision-making purposes, i.e., to identify the trustworthiness of a trustee. The performance of this framework is evaluated in terms of F1 score, Mean Absolute Error (MAE), and Mean Squared Error (MSE).

A quantifiable trust assessment model based on machine learning has been proposed in Jayasinghe et al. (2019) to make decisions autonomously, i.e., without human intervention, in an IoT network. This model encompasses trust features, i.e., co-location relationship, co-work relationship, cooperativeness-frequency-duration, reward system, mutuality and centrality, and community of interest, in order to assess the knowledge of a trustor towards a trustee. These trust parameters are aggregated via machine learning to obtain a single trust value for each pair of nodes (trustor and trustee) and which are then further segregated into trustworthy

and untrustworthy interactions via a decision boundary.

Similarly, a machine learning-based trust model (encompassing trust parameters of similarity, familiarity, and packet delivery ratio) has been put forward in Siddiqui et al. (2019) to identify and eliminate malicious vehicles within an IoV network. A context-aware trust management framework for a VANET network has been suggested in Guo et al. (2020) to ascertain the trustworthiness of messages received by vehicles to guarantee that no false information influences any driving decision-making process. This framework was composed of three modules, namely, information formalization, trust evaluation and strategy adjustment. The authors proposed a trust evaluation method based on evaluation strategy in different scenarios. In addition, information entropy theory was introduced into the trust calculation function to ensure more accurate evaluation results. Finally, a reinforcement learning model was proposed, and the evaluation strategy was dynamically adjusted according to the feedback of previous evaluation results.

To sum up, over the years, a number of conventional and machine learning-based trust management algorithms have been proposed in the research literature, and which have laid the foundations for the research envisaged in this chapter. Whilst these research papers have made some outstanding contributions, they still lack the potential of being a generic algorithm that can be suitably adapted to a particular research domain. In addition, they only take into consideration the traditional and limited trust parameters and a number of them even do not consider the influence of context on the trust values. Therefore, this research chapter envisages a machine learning-based trust management mechanism that considers key influential trust parameters and the context for ascertaining the trust of vehicles in an IoV network.

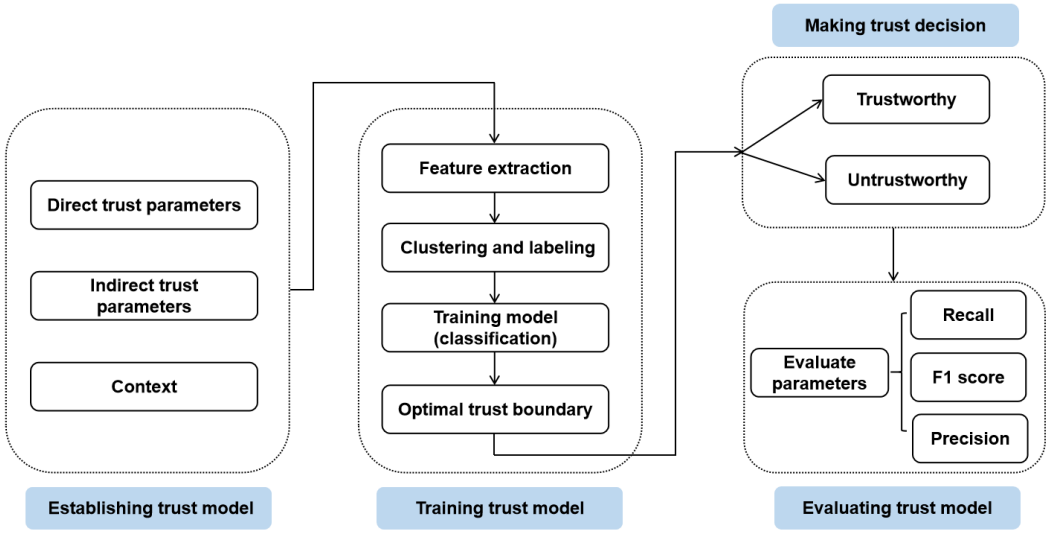

Figure 3.2 The Framework of the Proposed Trust Management Model.

3.3 Proposed Trust Evaluation Model

As depicted in Figure 3.2, a novel trust management framework has been designed in a bid to ascertain the trustworthiness of vehicles in an IoV network. The envisaged trust model primarily encompasses the following three salient steps:

i. *Step 1 — Establishing the Trust Model*

The trust of any particular vehicle (trustee) is ascertained via a trust model which takes into account direct trust, indirect trust, and context. The direct trust is a trustor's direct observation pertinent to a trustee and is composed up of four parameters, i.e., interaction success rate, similarity, familiarity, and reward and punishment. On the contrary, the indirect trust is computed via the respective trustor's one-hop neighbors' recommendations pertinent to a trustee and the degree of confidence of the respective trustor on the recommendations of its corresponding one-hop neighbors. It is also pertinent to mention that the model further takes into consideration the impact of context (vehicle types and operating scenarios) of both trustor and trustee.

ii. *Step 2 — Training the Trust Model*

Once the trust values have been computed via the trust model, unsupervised learning

algorithms, i.e., k-means, fuzzy c-means, and agglomerative (hierarchical) clustering, have been employed in order to ascertain two clusters, i.e., trustworthy and untrustworthy. Simply put, an unsupervised learning algorithm has been employed here to label the feature matrices ascertained in Step 1. Subsequently, supervised learning algorithms, i.e., k-nearest neighbors and random forest, have been used for training with 5-fold cross-validation so as to identify the optimal trust boundary for distinguishing between trusted and untrusted vehicles.

iii. *Step 3 — Evaluating the Trust Model*

The evaluation parameters, i.e., precision, recall, and F1 score are used for evaluating the performance of the envisaged IoV-based trust model.

A set of vehicles V_m, $m = 1, 2, ..., M$, i.e., comprising both trustworthy (honest) as well as untrustworthy (malicious) vehicles, has been defined. At every time instance $t^{'}$, $t^{'} = 1, 2, ..., t$, each vehicle interacts with vehicles in its immediate area to evaluate their trust based on the underlying interaction. This interaction takes place between a pair of a trustor i and a trustee j. The definitions of trust parameters employed in this section are delineated in Table 3.2.

3.3.1 Direct Trust ($T_{d(i,j,t)}$)

Direct trust refers to a trustor's direct observation of a trustee. However, it is pertinent to mention that the historical interactions between a trustor and a trustee should also be taken into consideration, i.e., in addition to the current interaction, for ascertaining the trust of a trustee since a malicious vehicle may behave intelligently by altering between a malicious and a non-malicious behavior. In the envisaged model, four key trust parameters, i.e., *interaction success rate*, *similarity*, *familiarity*, and *reward and punishment*, have been employed in order to ascertain the direct trust between a trustor i and a trustee j. The details of these parameters are as follows:

i. *Interaction Success Rate (ISR)* — The $ISR_{i,j,t}$ $(0 \leq ISR_{i,j,t} \leq 1)$ manifests the degree of

Table 3.2 Mathematical Symbols Employed in the Envisaged Trust Model.

Symbol	Definition
i	Trustor
j	Trustee
k	The neighbor of i
$t^{'}$	A time instance
t	The current time instance
Th_C	Confidence threshold (0.8)
Th_T	Trust value threshold (0.6)
ISR	Interaction success rate
Sim	Similarity
ES	External similarity
IS	Internal similarity
Fam	Familiarity
EF	External familiarity
IF	Internal familiarity
RP	Reward and punishment
VT	Vehicle types
OS	Operating scenarios
n	3,266 pairs of interactions

interaction between a trustor i and a trustee j in an IoV network, and is depicted as:

$$ISR_{i,j,t} = \frac{\sum_{t'=1}^{t} R_{i,j,t'}}{\sum_{t'=1}^{t} S_{i,t'}} \qquad \text{Equation 3.1}$$

where, $\sum_{t'=1}^{t} R_{i,j,t'}$ signifies total number of messages successfully received by a trustee j from a trustor i and $\sum_{t'=1}^{t} S_{i,t'}$ represents the total number of messages sent by the trustor i over the said time period.

ii. *Similarity (Sim)* — The similarity ($0 \leq Sim_{i,j,t} \leq 1$) itself is a weighted amalgamation of External Similarity (ES) and Internal Similarity (IS). The external similarity herein

implies the degree of similar content accessed by a trustor i and a trustee j over the time t (Equation (Equation 3.3)), whereas, the internal similarity represents the exchange of information, i.e., position, direction, and velocity between a trustor i and a trustee j (Equation (Equation 3.4)).

$$Sim_{i,j,t} = w_{ES} ES_{i,j,t} + w_{IS} IS_{i,j,t} \quad \text{Equation 3.2}$$

where, w_{ES} and w_{IS} refers to the weight of $ES_{i,j,t}$ and $IS_{i,j,t}$, respectively ($w_{ES} + w_{IS} = 1$). The $ES_{i,j,t}$ and $IS_{i,j,t}$ are ascertained as:

$$ES_{i,j,t} = \sum_{t'=1}^{t} w_{Es_{t'}} ES_{i,j,t'} \quad \text{Equation 3.3}$$

$$IS_{i,j,t} = \sum_{t'=1}^{t} w_{Is_{t'}} IS_{i,j,t'} \quad \text{Equation 3.4}$$

where, $w_{Es_{t'}}$ and $w_{Is_{t'}}$ manifests the weights of $ES_{i,j,t'}$ and $IS_{i,j,t'}$, respectively at a time t' ($w_{Es_{t'}} + w_{Is_{t'}} = 1$). The $ES_{i,j,t'}$ and $IS_{i,j,t'}$ are ascertained as:

$$ES_{i,j,t'} = \begin{cases} 1, & \text{if } C_{v_{i,t'}} = C_{v_{j,t'}} \\ 0, & \text{if } C_{v_{i,t'}} \neq C_{v_{j,t'}} \end{cases} \quad \text{Equation 3.5}$$

where, $C_{v_{i,t'}}$ and $C_{v_{j,t'}}$ implies the content accessed by a trustor i and a trustee j, respectively. Similarly, the $IS_{i,j,t'}$ is computed as:

$$IS_{i,j,t'} = \frac{Pos_{i,j,t'} + Dir_{i,j,t'} + Vel_{i,j,t'}}{3} \quad \text{Equation 3.6}$$

$$Pos_{i,j,t'} = \begin{cases} 1, & \text{if } Pos_{i,t'} = Pos_{j,t'} \\ 0, & \text{if } Pos_{i,t'} \neq Pos_{j,t'} \end{cases} \quad \text{Equation 3.7}$$

$$Dir_{i,j,t'} = \begin{cases} 1, & \text{if } Dir_{i,t'} = Dir_{j,t'} \\ 0, & \text{if } Dir_{i,t'} \neq Dir_{j,t'} \end{cases} \quad \text{Equation 3.8}$$

$$Vel_{i,j,t'} = \begin{cases} 1, & \text{if } Vel_{i,t'} = Vel_{j,t'} \\ 0, & \text{if } Vel_{i,t'} \neq Vel_{j,t'} \end{cases} \quad \text{Equation 3.9}$$

where, $Pos_{i,t'}$, $Pos_{j,t'}$, $Dir_{i,t'}$, $Dir_{j,t'}$, $Vel_{i,t'}$, and $Vel_{j,t'}$ represent the position, direction, and velocity, respectively of a trustor i and a trustee j at a time $t^{'}$.

iii. *Familiarity (Fam)* — The familiarity ($0 \leq Fam_{i,j,t} \leq 1$) is also segregated into External Familiarity (EF) and Internal Familiarity (IF). The external familiarity refers to the ratio of the number of common vehicles interacting with a trustor i and a trustee j to the total number of vehicles interacting with a trustor i over the time t, i.e., the more the number of common interacting vehicles, the higher the familiarity between a trustor i and a trustee j. On the contrary, the internal familiarity signifies the interaction frequency between a trustor i and a trustee j over the time t, i.e., the higher the interaction frequency, the higher is the familiarity between the two. The same is illustrated in Equations (Equation 3.10)–(Equation 3.12).

$$Fam_{i,j,t} = w_{EF} EF_{i,j,t} + w_{IF} IF_{i,j,t} \quad \text{Equation 3.10}$$

where, w_{EF} and w_{IF} refers to the weight of $EF_{i,j,t}$ and $IF_{i,j,t}$, respectively ($w_{EF} + w_{IF} = 1$). The $EF_{i,j,t}$ is ascertained as:

$$EF_{i,j,t} = \frac{\sum_{t'=1}^{t} F_{i,j,t'}}{\sum_{t'=1}^{t} F_{i,t'}} \quad \text{Equation 3.11}$$

where, $\sum_{t'=1}^{t} F_{i,j,t'}$ represents the number of common interacting vehicles of a trustor i and a trustee j, whereas, $\sum_{t'=1}^{t} F_{i,t'}$ is the total number of vehicles interacting with i.

Similarly, the $IF_{i,j,t}$ is computed as:

$$IF_{i,j,t} = \frac{\sum_{t'=1}^{t} I_{i,j,t'}}{t} \qquad \text{Equation 3.12}$$

where, $\sum_{t'=1}^{t} I_{i,j,t'}$ signifies the number of interactions between a trustor i and a trustee j.

iv. *Reward and Punishment (RP)* — The RP ($0 \leq RP_{i,j,t} \leq 1$) is employed to evaluate the rewards and punishments accorded to a trustee j by a trustor i depending on its behavior, i.e., a trustee j is rewarded by a trustor i for its cooperation, honesty, and reporting a critical event, and is punished for any misconduct. The RP is, therefore, calculated as:

$$RP_{i,j,t} = ISR_{i,j,t} e^{-\frac{N_p}{N_p+N_r}} \qquad \text{Equation 3.13}$$

where, $ISR_{i,j,t}$ is the interaction success rate between a trustor i and a trustee j. Also, N_p suggests the number of negative interactions, whereas, N_r exhibits the number of positive interactions.

3.3.2 Indirect Trust ($T_{ind(i,j,t)}$)

The indirect trust, also generally referred to as the recommendation trust, is ascertained by (a) soliciting the recommendations via the one-hop neighboring nodes of a trustor pertinent to a trustee and (b) by taking into account the confidence of a trustor on the recommendations ascertained by the one-hop neighboring vehicles (Alnasser et al., 2020)(Truong et al., 2017). The indirect trust is computed as:

$$T_{ind(i,j,t)} = \frac{\sum_{k=1}^{n} C_{i,k,t} T_{d(k,j,t)}}{n} \qquad \text{Equation 3.14}$$

where, $C_{i,k,t}$ implies the confidence score assigned by a trustor to the recommendations of its one-hop neighboring vehicles pertinent to a trustee, $T_{d(k,j,t)}$ refers to the recommendations ascertained by the said one-hop neighboring nodes, and n implies the total number of one-hop

neighboring nodes. The confidence score, $C_{i,k,t}$, is calculated as:

$$C_{i,k,t} = \begin{cases} 1, & \text{if } T_{d(i,k,t)} \geq Th_C \\ 0.5, & \text{if } Th_T \leq T_{d(i,k,t)} < Th_C \\ 0, & \text{if } T_{d(i,k,t)} < Th_T \end{cases} \quad \text{Equation 3.15}$$

where, Th_C and Th_T refer to the confidence threshold and the trust threshold, respectively and act as a weight for distinguishing between a good, an average, or a bad recommendation (Guo et al., 2020).

3.3.3 Context (T_c)

A number of existing trust models ignore the significance of context, thereby making them quite unrealistic for real-world settings. In this model, the notion of context has been primarily determined by two factors, i.e., the vehicle types and the operating scenarios, the details of which are as follows:

i. *Vehicle Types (VT)* — Five types of vehicles have been taken into consideration in the proposed model. Police cars, ambulances, and fire engines are regarded as High-Priority (HP) vehicles since the information disseminated by these particular vehicles possesses considerable confidence of a centralized trusted authority. The second type is Public Transport (PT) vehicles, i.e., buses, taxis, and subways, which are also considered reasonably trustworthy since they have been approved by specific authorized departments. Similarly, private vehicles are classified into Professional (P) vehicles and Novice (N) vehicles primarily depending on their respective driver's driving experience, i.e., professional drivers are regarded to have extensive driving expertise in contrast to beginners and are, therefore, considered to be more trustworthy. Finally, malicious vehicles have been considered to be untrustworthy in nature. Equation (Equation 3.16) illustrates the trust values vis-à-vis the suggested vehicle types:

$$T_{VT} = \begin{cases} 1, & \text{if } Vehicles = HP \\ 0.8, & \text{if } Vehicles = PT \\ 0.6, & \text{if } Vehicles = P \\ 0.4, & \text{if } Vehicles = N \\ 0, & \text{if } Vehicles = Malicious \end{cases} \quad \text{Equation 3.16}$$

ii. *Operating Scenarios (OS)* — In the envisaged model, two operating scenarios, i.e., an urban and a highway one, have been considered. In Section 3.4, the simulation results for these two scenarios have been delineated in detail. It is pertinent to highlight here that the high mobility and the random geographical distribution of vehicles in an IoV network results in several different contextual scenarios. Therefore, it is indispensable to consider such settings while ascertaining the trust of a trustee. For instance, owing to the limited mobility of vehicles and the high density of RSUs in an urban scenario, there is a considerable number of interactions, both trustworthy and untrustworthy, between the vehicles. However, in scenarios involving highways, the mobility of the vehicles is generally much higher than that in an urban scenario. Furthermore, vehicles in highway settings have a more sparse geographical distribution, thereby resulting in fewer interactions between them. Trust management often relies on a large number of RSUs, but there are fewer RSUs on highways, so trust management cannot be well implemented in this scenario.

3.4 Results and Discussion

3.4.1 Simulation Setup and Feature Extraction

Epinions dataset (https://cse.msu.edu/tangjili/datasetcode/truststudy.htm) has been used in order to map the data traces for the trust parameters of the envisaged IoV-based trust model. Epinions, in essence, is a publicly available trust dataset that encompasses six parameters:

userid, productid, categoryid, rating, helpfulness, and timestamps. For instance, a data trace of [1, 2, 3, 4, 5, 6] in the Epinions dataset implies that user 1 accords a rating of 4 to product 2 belonging to category 3 at timestamp 6. The helpfulness of the accorded rating is 5. For the sake of the research-at-hand, Epinions dataset has been appropriately transformed into an IoV dataset in light of the similar transformation envisaged in Kerrache et al. (2019).

A total of 3,266 pairs of interactions between trustors and trustees, i.e., pertinent to 64 nodes (vehicles), have been taken into consideration. The same are arranged in the form of a feature matrix M as illustrated in Equation (Equation 3.17).

$$[M_{n\times 7}] = \begin{bmatrix} ISR_1 & Sim_1 & Fam_1 & RP_1 & confidence_1 & VT_1 & OS_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ ISR_n & Sim_n & Fam_n & RP_n & confidence_n & VT_n & OS_n \end{bmatrix}_{n\times 7} \quad \text{Equation 3.17}$$

The dimension of this feature matrix is $n \times 7$, wherein n = 3,266 and 7 implies the trust-based feature vectors via-à-vis each of the 3,266 trustor trustee pairs. It is pertinent to mention here that there is no need for the features' normalization since each trust feature value falls in the range of [0, 1]. The seven features are concatenated into three features, i.e., direct trust, indirect trust, and context, in a bid to form a new feature matrix N with a dimension of $n \times 3$, wherein the direct trust implies interaction success rate, similarity, familiarity, and reward and punishment, the indirect trust is ascertained via direct trust and confidence, and the context comprises vehicle types and operating scenarios. Since it is not feasible to display a three-dimensional vector, two out of three features are selected and displayed at a time for demonstration purposes.

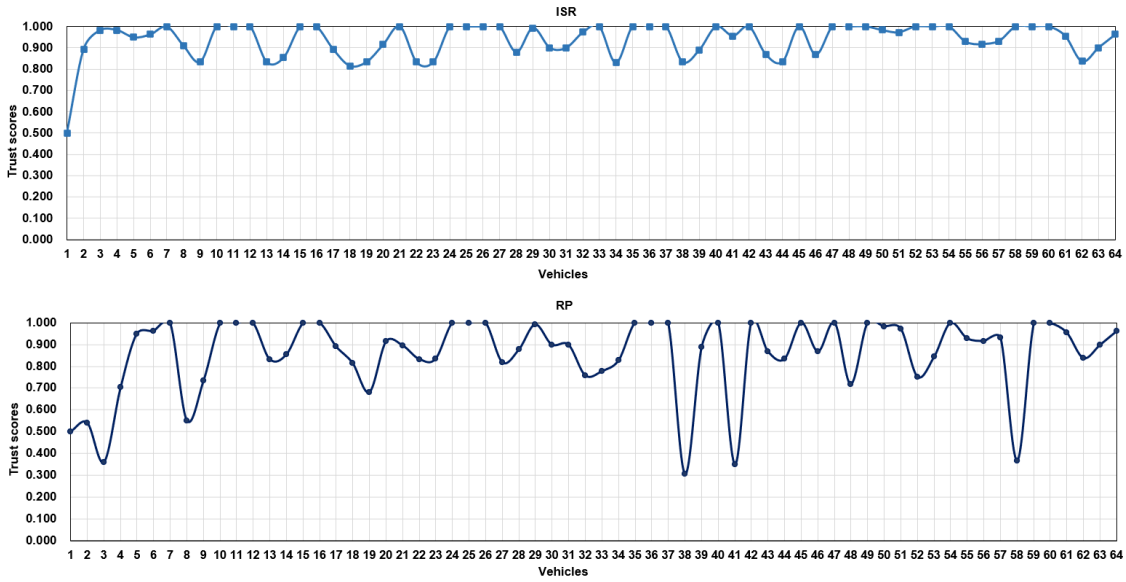

Figure 3.3 Trust Scores of Vehicles in an IoV Network vis-à-vis *ISR* and *RP* (ISR here implies interaction success rate, and RP refers to reward and punishment).

$$[N_{n\times 3}] = \begin{bmatrix} direct & trust_1 & indirect & trust_1 & context_1 \\ \vdots & & \vdots & & \vdots \\ direct & trust_n & indirect & trust_n & context_n \end{bmatrix}_{n\times 3} \quad \text{Equation 3.18}$$

Table 3.3 depicts the trust-based parametric values of 22 randomly selected vehicles in the IoV network. Figure 3.3 further portrays two of such parameters, i.e., ISR and RP, for all of the 64 vehicles in the IoV network. It is evident that the change in the parametric values of RP is proportional to the parametric values of ISR with the exception of a few. For instance, vehicles 3, 32, 48, 52, and 58 possess high ISR values but low RP values. This is owing to the fact that although the interactions carried out by these vehicles are considerable, most of them were accounted for as being negative.

Table 3.3 Trust Parameters' Values Pertinent to 22 Random Vehicles in an IoV Network (Interaction Success Rate – ISR, Reward and Punishment – RP, Similarity – Sim, Familiarity – Fam).

Vehicles	ISR	Sim	Fam	RP	Confidence	Context
1	0.500	0.614	0.167	0.500	0.000	0.333
2	0.894	0.593	0.120	0.542	0.000	0.711
3	0.982	0.665	0.119	0.361	1.000	0.800
4	0.982	0.770	0.111	0.704	1.000	0.567
5	0.950	0.453	0.104	0.950	0.500	0.850
6	0.964	0.484	0.107	0.964	0.000	0.857
7	1.000	0.515	0.125	1.000	1.000	0.650
8	0.911	0.541	0.226	0.552	1.000	0.771
9	0.833	0.476	0.262	0.735	1.000	0.686
10	1.000	0.524	0.217	1.000	1.000	0.720
11	1.000	0.600	0.292	1.000	1.000	0.933
12	1.000	0.763	0.200	1.000	0.500	0.840
13	0.833	0.750	0.222	0.833	1.000	0.600
14	0.855	0.750	0.375	0.855	1.000	0.550
15	1.000	0.540	0.229	1.000	1.000	0.500
16	1.000	0.529	0.319	1.000	1.000	0.600
17	0.893	0.638	0.351	0.893	0.500	0.729
18	0.815	0.700	0.100	0.815	1.000	0.618
19	0.834	0.585	0.323	0.683	1.000	0.775
20	0.915	0.700	0.333	0.915	1.000	0.600
21	0.750	0.374	0.438	0.750	0.625	0.550
22	0.833	0.530	0.292	0.603	0.550	0.560

3.4.2 Clustering and Labeling

Subsequent to the extraction of the desired trust features, three unsupervised learning algorithms, i.e., k-means, fuzzy c-means, and agglomerative clustering, have been employed

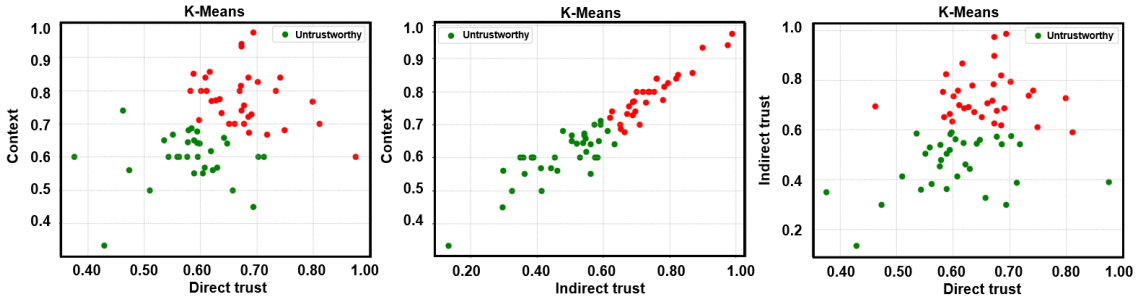

Figure 3.4 Labels via Unsupervised Learning (K-means Clustering) – Direct Trust vs. Context, Indirect Trust vs. Context, and Direct Trust vs. Indirect Trust.

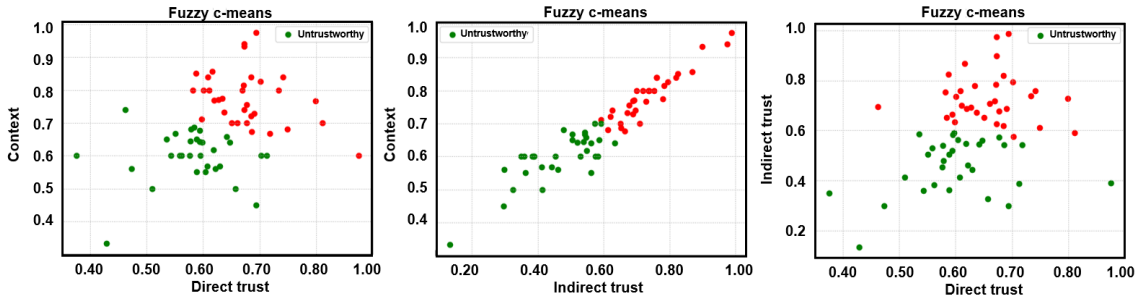

Figure 3.5 Labels via Unsupervised Learning (Fuzzy C-means Clustering) – Direct Trust vs. Context, Indirect Trust vs. Context, and Direct Trust vs. Indirect Trust.

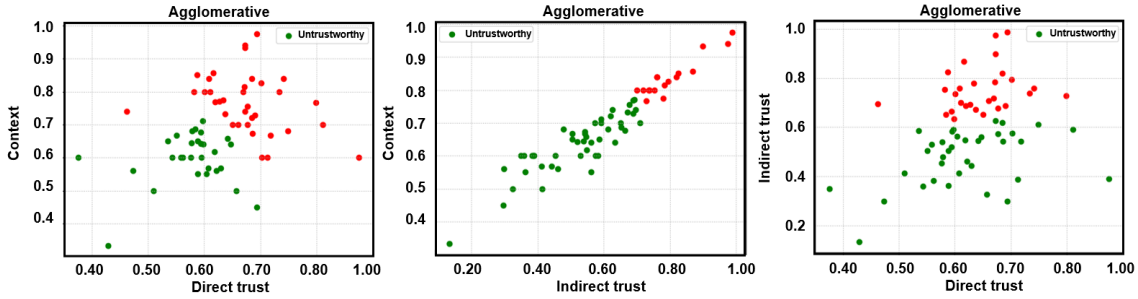

Figure 3.6 Labels via Unsupervised Learning (Agglomerative Clustering) – Direct Trust vs. Context, Indirect Trust vs. Context, and Direct Trust vs. Indirect Trust.

to label the feature matrices. It is noteworthy that unsupervised learning algorithms have been employed in a bid to ascertain a credible and reliable ground truth. Accordingly, two clusters, trustworthy and untrustworthy, have been obtained as a result of the same and are depicted in Figures 3.4–3.6.

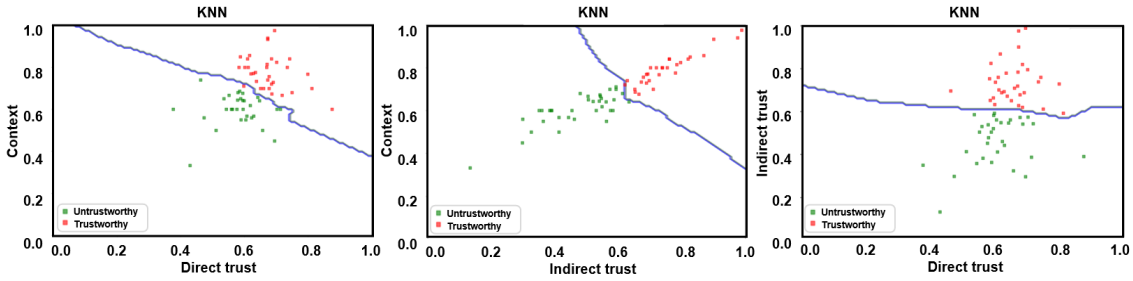

Figure 3.7 Trust Boundary Results for KNN Algorithm – Direct Trust vs. Context, Indirect Trust vs. Context, and Direct Trust vs. Indirect Trust.

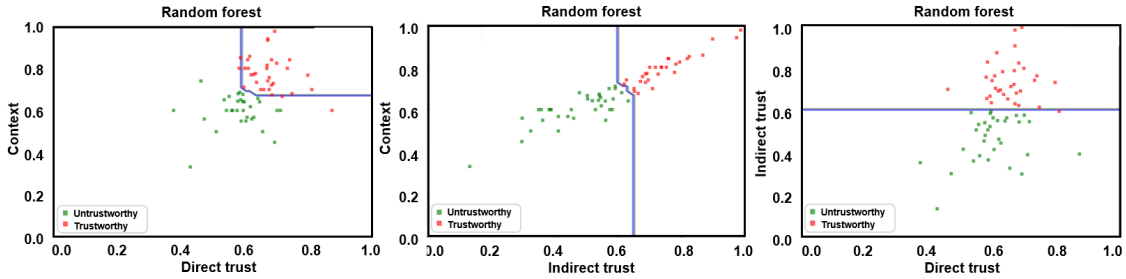

Figure 3.8 Trust Boundary Results for RF Algorithm – Direct Trust vs. Context, Indirect Trust vs. Context, and Direct Trust vs. Indirect Trust.

3.4.3 Classification and Model Evaluation

A number of supervised learning algorithms, including but not limited to, K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Random Forest (RF), and ensemble ones have been employed in the research literature for classification purposes (Siddiqui et al., 2023a). For the manuscript-at-hand, KNN and RF classifiers have been employed on the resulting feature matrix for training purposes via a 5-fold cross-validation approach in a bid to ascertain the malicious nodes via a decision boundary. The same is depicted in Figures 3.7 and 3.8 for KNN and RF classifiers, respectively, wherein the trusted and untrusted regions can be clearly observed. It is pertinent to mention that the rationale of opting for KNN and RF classifiers lies in their non-parametric nature, i.e., they make no assumption pertinent to the underlying data distribution, and are robust to noise and complex, non-linear relationships (Bozkurt et al., 2025)(Awotunde et al., 2023). The envisaged trust model's accuracy has been subsequently evaluated via the following three evaluation parameters:

Table 3.4 Evaluation Results via Supervised Learning Algorithms, i.e., KNN and RF (K-nearest Neighbor – KNN and Random Forest – RF).

Scenarios	Classifier	Precision	Recall	F1 score
Urban	KNN	1.0000	1.0000	1.000
	RF	1.0000	0.9400	0.9684
Highway	KNN	0.9804	0.9623	0.9713
	RF	0.9764	0.9338	0.9546

i. Precision: Precision depicts the ability of the envisaged trust model to correctly predict malicious vehicles as being malicious.

ii. Recall: Recall refers to the proportion of malicious vehicles that have been correctly ascertained by the envisaged trust model.

iii. F1 score: F1 score implies the weighted harmonic mean of the precision, and recall and ascertains the model's accuracy.

For this particular trust model, vehicles under two different operating scenarios, i.e., urban and highway, have been considered. Also, owing to the space constraint, only the figures pertinent to the urban scenario have been portrayed. Nevertheless, the precision, recall, and F1 score for both urban and highway scenarios have been depicted in Table 3.4. It is pertinent to mention here that the precision, recall, and F1 score of the envisaged trust model as demonstrated by the KNN classifier under both urban and highway settings is much higher in contrast to the precision, recall, and F1 score demonstrated by the RF classifier under the same settings. KNN is regarded as one of the simplest classification algorithms, i.e., with mature theory, low training time complexity, and insensitivity to outliers. This particular algorithm is quite suitable for an automatic classification of class domains with large sample size (Siddiqui et al., 2023a). It is also noteworthy to mention that the trust can be ascertained in a relatively more accurate manner in an urban setting in contrast to the highway setting since vehicles interact much more frequently in the former owing to their low speeds as opposed to the latter which is designed to enable them to traverse with high speeds.

Table 3.5 Comparison of the Precision of Trust Models (NC – 1: (El-Sayed et al., 2020), NC – 2: (Gyawali et al., 2020), Conv1: (Fabi and Thampi, 2022a), Conv2: (Xia et al., 2019a), Conv3: (Rai et al., 2020)).

Model	Proposed	NC – 1	NC – 2	Conv1	Conv2	Conv3
Precision	1.0000	0.9234	0.9005	0.9700	0.9700	0.9750

Table 3.5 depicts the comparison of the envisaged trust model vis-à-vis machine learning-based trust mechanisms, i.e., (El-Sayed et al., 2020)(Gyawali et al., 2020) – labeled as NC – 1 and NC – 2, respectively, that have not taken the notion of context into consideration. Whilst the said trust models demonstrate high precision, the envisaged trust model still outperforms them since it takes into account the context pertinent to the interactions on the premise that the interaction between a trustor and trustee is different in different contexts. Table 3.5 further outlines the comparison of the envisaged trust model vis-à-vis conventional (weighted sum) trust mechanisms, i.e., (Fabi and Thampi, 2022a)(Rai et al., 2020)(Xia et al., 2019a) – labeled as Conv1, Conv2, and Conv3, respectively. It can once again be seen clearly that the envisaged trust model performs considerably better in terms of precision in contrast to the conventional trust mechanisms. This reinforces the fact that the weighted sum mechanisms have strong subjectivity and are influenced by numerous underlying factors. Hence, when a number of trust parameters are in play, a machine learning-based mechanism is optimal for not only aggregating the same but ascertaining an intelligent trust boundary.

3.5 Summary

An intelligent transportation system is an intrinsic component of smart cities since it allows vehicles to employ vehicle-to-everything communication in a bid to exchange safety-critical messages with the other road entities and the supporting infrastructure to ensure highly secure and intelligent traffic flows. However, road entities within an IoV network are vulnerable to a number of attacks and malicious actors prevailing in the same are always on the lookout to manipulate the IoV network for their malicious gains. In this manuscript, a

machine learning-based trust management mechanism, MESMERIC, has been proposed that takes into account direct trust, indirect trust, and context (each with a number of qualifying attributes) to not only ascertain the trust of vehicles in an IoV network but to segregate the trustworthy vehicles from the untrustworthy ones by means of an optimal decision boundary. In the near future, designing and launching of a number of dynamic trust-related attacks via a state-of-the-art trust-based IoV testbed would be investigated in order to understand the underlying nitty gritty of such dynamic attacks so that more resilient IoV-based trust models could be formulated. Additionally, an intelligent weighting-based conventional mechanism would be proposed in a bid to mitigate any possible subjectivity that could arise during the trust aggregation process.

CHAPTER 4

TOWARDS DISTINGUISHING TRUST-BASED ATTACKS IN AN IoV NETWORK

The paradigm of the Internet of Vehicles (IoV) promises significant innovative advancements and is receiving an increased attention of the researchers from both academia and industry. The IoV creates an intelligent network between different road entities and their corresponding roadside infrastructure via state-of-the-art sensing and communication technologies and, therefore, facilitates in addressing a range of safety-critical and non-safety vehicular applications. Accordingly, the security of an IoV network is of importance with internal attacks being of considerable concern. Although the conventional cryptography-based schemes are extremely intelligent in tackling the external attacks, trust has been recently employed to handle the internal attacks. Nevertheless, trust-based attacks also present a formidable challenge. Therefore, in this chapter, an IoV-based trust management heuristic has been envisaged that takes into account both direct trust and indirect trust to ascertain the behaviors of the vehicles vis-à-vis time in a bid to detect various trust-based attacks, i.e., zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks, along with the attackers' multiple attacking strategies. The experimental findings further demonstrate that the envisaged IoV-based trust management heuristic exhibits prompt and accurate detection of the trust-based attacks in contrast to the state-of-the-art trust management mechanisms.

4.1 Overview

Over the past two decades or so, state-of-the-art advancements in information and communication technologies and artificial intelligence have led to an accelerated increase in the number of Internet of Things (IoT) enabled devices (Gu et al., 2024)(Tripathi et al.,

Yingxun Wang, Adnan Mahmood, Mohamad Faizrizwan Mohd Sabri, Hushairi Zen (2025). *Towards Distinguishing Trust Based Attacks in an IoV Network*. Journal of King Saud University – Computer and Information Sciences, 37:39 (Q1, Impact Factor: 6.1).

2023). According to the statistical data, the number of connected IoT devices were 16.6 billion towards the end of 2023. The same is anticipated to reach 21.5 billion by the end of 2025 and is forecasted to be approximately 40 billion by 2030 (Xu et al., 2025a)(Cui and Yi, 2024). The IoV is referred to as IoT-on-wheels and has emerged owing to the convergence of the traditional Vehicular Ad hoc Networks (VANETs) with the IoT.

In the realm of the IoV paradigm, each vehicle is regarded as an intelligent object duly equipped with a powerful multi-sensor platform, computing unit, communication technology (ies), and IP-based internet connectivity for sensing, processing, and communication purposes (Kerrache et al., 2019). Moreover, vehicle-to-everything communication facilitates seamless connectivity amongst the entities in an IoV network so as to realize numerous vehicular applications (Cao et al., 2024). It is pertinent to mention that vehicular applications are segregated into two categories, i.e., safety-critical vehicular applications and non-safety vehicular applications, and the same are depicted in Figure 4.1. Safety-critical vehicular applications comprise immediate and potential critical alerts pertinent to hazardous road events, including but not limited to, emergency vehicle alert, queue warning, cooperative adaptive cruise control and platooning, traffic signal priority and optimal speed advisory, blind intersection, and curve speed warning. On the contrary, non-safety vehicular applications primarily cater for infotainment-related services. Regardless of the type of vehicular application, if and when a specific vehicle is victim of a malicious attack, it poses a significant risk to the entire IoV network (Kerrache et al., 2019). Hence, numerous solutions, with the most noticeable being cryptography ones have been proposed by researchers in academia and industry in order to address such concerns in an effective manner (Du et al., 2024).

Nevertheless, conventional cryptography-based schemes are unable to address internal attacks in the context of a highly dynamic and decentralized IoV network (Hussain et al., 2021). Therefore, the notion of *trust* has lately emerged in the research literature with the underlying rationale being that vehicles primarily compute the trust of one another based on their respective interaction-related experience (observations) and decisions are subsequently

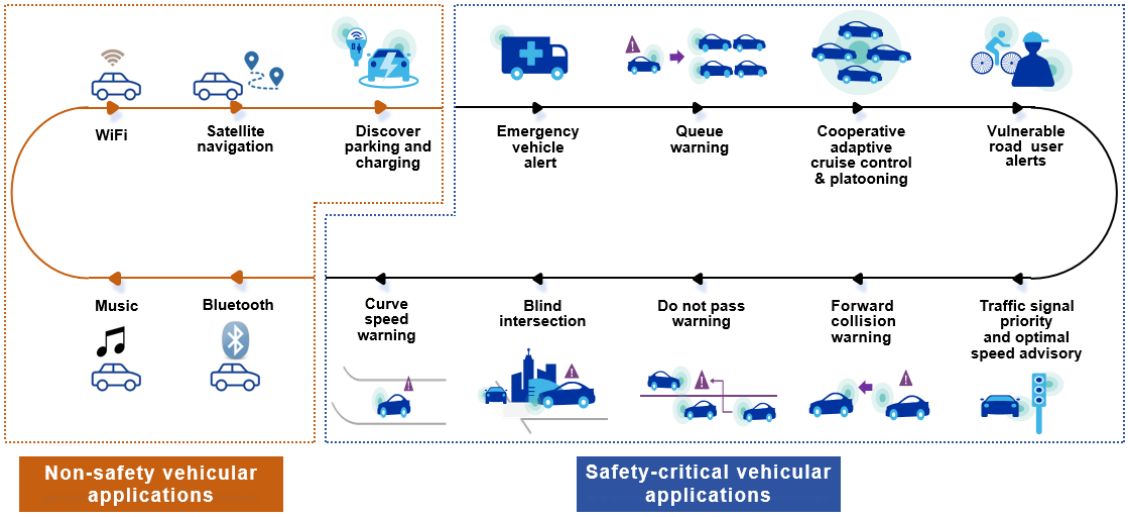

Figure 4.1 Vehicular Applications, i.e., Safety-critical and Non-Safety Ones.

made in light of the same (Cao et al., 2024)(Sagar et al., 2023)(Qi et al., 2023b)(Mirzadeh et al., 2023)(Sasikumar et al., 2023)(Kchaou et al., 2020). However, it is pertinent to mention that vehicles not only rely on their own direct observations (also referred to as the direct trust) but also take into account the observations reported by their immediate neighbors (indirect trust) (Qi et al., 2024). Whilst trust as a notion has already been defined in diverse fields, e.g., sociology, economics, political science, and psychology, in different ways (Ismail et al., 2025)(Rezvi Shahariar, 2023)(Hbaieb et al., 2022)(El-Sayed et al., 2022)(Rathore et al., 2022)(Sharma et al., 2020), it can be also defined as:

Trust suggests a trustor's confidence in a trustee within a specific context and at any given period of time for executing a certain task or a set of tasks.

Establishing trust amongst vehicles within an IoV network is of paramount importance. Usually, trust is established in three key ways – task-specific trust, time-based trust, and context-driven trust. Task-specific trust refers to the establishment of trust based on specific objectives. Also, given the inherent high mobility of vehicles, their respective behaviors evolve over the time. Therefore, time-based trust pertains to the evolving trust of a vehicle for the time it traverses in an IoV network. Moreover, a vehicle might exhibit trust towards

another vehicle in one particular context while withholding trust for the same in a distinct context (Mahmood et al., 2023).

In the recent years, a considerable amount of research has been conducted pertinent to the notion of trust within an IoV network. However, trust itself is also susceptible to attacks. Generally speaking, trust-related attacks can be segregated into two categories – self-interest ones and reputation-based ones. The self-interest ones encompass self-promoting attacks (Magdich et al., 2022)(Siddiqui et al., 2021b), on-off attacks (Chen et al., 2024)(Azizi and Shokrollahi, 2024)(Li et al., 2023b)(Magdich et al., 2022)(Mao et al., 2021)(Zhang et al., 2020), zig-zag attacks (Qi et al., 2023a)(Zhang et al., 2021)(Ahmad et al., 2021), selective behavior attacks (Mao et al., 2023)(Mo et al., 2022)(Chen et al., 2019), opportunistic service attacks (Magdich et al., 2022), and newcomer attacks (whitewashing attacks) (Magdich et al., 2022)(Zhang et al., 2020). Contrarily, the reputation-based ones comprise ballot stuffing attacks (good-mouthing attacks) (Chen et al., 2024)(Azizi and Shokrollahi, 2024)(Sagar et al., 2024a)(Shokrollahi and Dehghan, 2023)(Mahmood et al., 2023)(Magdich et al., 2022)(Mao et al., 2021), bad-mouthing attacks (Chen et al., 2024)(Azizi and Shokrollahi, 2024)(Sagar et al., 2024a)(Mao et al., 2023)(Wang et al., 2023d)(Wang et al., 2023c)(Sagar et al., 2023)(Mahmood et al., 2023), and simple attacks (Qi et al., 2023a)(Zhang et al., 2022b).

Moreover, since vehicles traverse at high speeds and interact with a number of other vehicles, i.e., along their respective trajectory, their corresponding trust is highly dynamic in nature and, therefore, needs to be intelligently studied vis-à-vis time. This is of essence since malicious vehicles may attempt to manipulate an IoV network by instigating trust-based attacks within specific time instances, i.e., as and when they find an opportunity so as to do so, but may operate completely normal during the other time instances. Therefore, in this chapter, a time-aware trust management heuristic has been proposed for ascertaining the total trust of each vehicle in an IoV network via employing direct trust and indirect trust. The salient contributions of this particular chapter are as follows:

i. An IoV-based trust management heuristic encompassing both direct trust and indirect

trust has been envisaged. The direct trust comprises interaction experience, interaction frequency, interaction timeliness, and received message quality, whereas, acquisition of the indirect trust is facilitated through the combination of the opinion (observation) of the one-hop neighbor of a trustor pertinent to a trustee and the direct trust of the trustor on the respective one-hop neighbor.

ii. The behavior of the vehicles has been studied vis-à-vis time for ascertaining various trust-based attacks, i.e., zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks, in an IoV network. The experimental findings further demonstrate that the envisaged trust management heuristic exhibits prompt and accurate detection of the impact caused by the multiple trust-based attacks throughout the entire temporal span of an IoV network.

The rest of this particular chapter is organized as follows. Section 4.2 presents an overview of the state-of-the-art trust management models. Section 4.3 delineates the envisaged trust management heuristic, and the simulation results and analysis pertinent to the same have been presented in Section 4.4. Finally, Section 4.5 summarizes this chapter and highlights future research directions.

4.2 State-of-the-Art

In this section, the state-of-the-art trust management models have been segregated into two categories, (a) trust-based identification models (the ones envisaged for identifying the trust-based attacks in the context of an IoV network) and (b) time-aware-based trust management models (the ones employed for analyzing the temporal behavior of vehicles for ascertain their respective dynamic trust patterns).

4.2.1 Trust-based Attacks Identification Models

As of date, numerous trust-based attacks identification models have been envisaged for tackling diverse attacks within an IoV network (see Table 4.1). A robust hybrid trust-based emergency message dissemination model has been envisaged in Qi et al. (2024) which integrated entity trust together with the data trust for mitigating interference of the malicious attacks on the trust decision making. In Siddiqui et al. (2023b), a context-driven trust management model has been proposed to cater for attack resistance in an IoV network, wherein local trust encompassing direct trust and indirect trust, and context-dependent trust has been employed for the purpose of trust quantification together with a flexible adaptive misbehavior detection threshold for primarily mitigating both on-off attacks and selective node attacks.

In order to address intelligent attacks in an IoV network, a multi-dimensional trust model has been suggested in Qi et al. (2023a) for a comprehensive evaluation of diverse trust parameters in an IoV network. The said trust model encompasses four stages – collection of the local trust-related data, trust aggregation, abnormal data filtering, and updating of the global trust. For trust aggregation purposes, the entropy weight method has been employed to dynamically adjust the corresponding weight coefficients based on the fluctuation of respective trust parameters. Moreover, the median absolute deviation algorithm has been employed for filtering abnormal evaluation results, thereby enabling effective mitigation of complex and dynamic intelligent attacks, e.g., bad-mouthing attacks, ballot stuffing attacks, and on-off attacks. In Wang et al. (2023d), a trust model based on eigenvector centrality and social metrics has been deliberated for handling trust-based attacks in an IoV network. The trust evaluation involves local trust evaluation of the vehicles and trust aggregation of the roadside units. Considering the highly dynamic nature of an IoV network, this model integrates vehicles' trajectories and their respective interaction histories to estimate social relationships. Roadside units employed eigenvector centrality and social metrics to

periodically aggregate stored data-based trust, subsequently, broadcasting the aggregated trust values to nearby vehicles for identification purposes against malicious entities. The experimental results demonstrate that this model exhibits a higher detection rate against bad-mouthing attacks.

In Cheong et al. (2024a), a multidimensional trust evidence fusion and path-backtracking mechanism has been envisaged to efficiently and accurately identify malicious behaviors in VANETs. The said trust model employed the Dempster Shafer Theory to aggregate (a) direct trust evidence (forgetting function, familiarity, and cooperativeness), (b) indirect trust evidence, and (c) path-backtracking trust evidence. Subsequent to trust aggregation, the trust evidences of vehicles are categorized into four discrete levels: High Trust (HT), Trust (T), Distrust (D), and High Distrust (HD). The experimental analysis demonstrated that the model exhibits exceptional accuracy in detecting several diverse attacks, i.e., simple attack, black hole attack, path tampering attack, and on-off attack. In Zhang et al. (2022a), a trust-based and privacy-preserving platoon recommendation scheme has been proposed for VANETs, wherein a filtering truth discovery algorithm has been deliberated for the optimal selection of head vehicles within a vehicular platoon. Moreover, pseudonyms and Paillier cryptosystem (Paillier, 1999) have been employed as to safeguard the privacy of the vehicles. Furthermore, novel authentication protocols have been devised so that only legitimate vehicles are able to pass authentication. The experimental results demonstrated that the proposed scheme effectively mitigates a couple of attacks, i.e., bad-mouth attack, on-off attack, collusion attack, and link attack in VANETs.

Table 4.1 Trust-based Attacks vis-à-vis State-of-the-Art Trust Management Models (Self-promoting Attacks – SPA, On-off Attacks – OOA, Zig-zag Attacks – ZZA, Selective Behavior Attacks – SBA, Opportunistic Service Attacks – OSA, NewComer (Whitewashing) Attacks – NCA, Ballot Stuffing Attacks – BSA, Bad-mouthing Attacks – BMA, Simple Attacks – SA).

Attacks	Definition	References
	Self-interest attacks	
SPA	Malicious vehicles continuously augment their respective reputation via generating complex pseudonyms identities to gain considerable authorizations in an IoV network in a bid to manipulate the same for malign motives.	(Magdich et al., 2022)(Siddiqui et al., 2021b) (Cheong et al., 2024a)(Shamaeian and Pesch, 2024)
OOA	Malicious vehicles alternate between honest and dishonest behaviors at regular intervals to sustain reasonable reputation in an IoV network so as to avoid being classified as malicious.	(Qi et al., 2024)(Magdich et al., 2022)(Zhang et al., 2020)(Azizi and Shokrollahi, 2024)(Chen et al., 2024)(Qi et al., 2023a)(Ahmad et al., 2021)(Mao et al., 2023)(Shokrollahi and Dehghan, 2023)(Cheong et al., 2024a)(Zhang et al., 2022a)(Siddiqui et al., 2023b)(Cheong et al., 2024b)(Shamaeian and Pesch, 2024)
ZZA	Similar to an on-off attack, malicious vehicles alternate between honest and dishonest behaviors, however, at irregular intervals to avert eviction from an IoV network.	(Qi et al., 2023a)(Zhang et al., 2021)(Song et al., 2024)
SBA	Malicious vehicles act good for a certain service (with low-computational requirements) and bad for the other (with high-computational requirements) to disrupt the efficacy of an IoV network.	(Azizi and Shokrollahi, 2024)(Mo et al., 2022)(Shokrollahi and Dehghan, 2023)(Siddiqui et al., 2023b)

Table 4.1 continued

Attacks	Definition	References
OSA	A malicious vehicle disguises itself by furnishing better services to gain high reputation in an IoV network, and once it has realized the same, it commences the adverse activities.	(Magdich et al., 2022)(Cheong et al., 2024a)
NCA	A malicious vehicle registers a new identity to expunge its undesirable historical interactions in an IoV network in a bid to launch attack(s) afresh.	(Magdich et al., 2022)(Zhang et al., 2020)(Azizi and Shokrollahi, 2024)(Shokrollahi and Dehghan, 2023)(Shamaeian and Pesch, 2024)
Reputation-based attacks		
BSA	Malicious vehicles, in tandem, enhance the trust of a vehicle with malign intentions to assign it with substantial authorizations in an IoV network.	(Tripathi et al., 2023)(Mahmood et al., 2023)(Magdich et al., 2022)(Azizi and Shokrollahi, 2024)(Chen et al., 2024)(Mao et al., 2023)(Sagar et al., 2024a)(Shokrollahi and Dehghan, 2023)
BMA	Malicious vehicles collude to provide bad recommendations to a honest vehicle to harm its reputation in an IoV network.	(Tripathi et al., 2023)(Sagar et al., 2023)(Mahmood et al., 2023)(Magdich et al., 2022)(Siddiqui et al., 2021b)(Zhang et al., 2020)(Chen et al., 2024)(Qi et al., 2023a)(Chen et al., 2019)(Mao et al., 2023)(Sagar et al., 2024a)(Shokrollahi and Dehghan, 2023)(Wang et al., 2023c)(Wang et al., 2023d)(Zhang et al., 2022b)(Alnasser et al., 2020)(Ayed et al., 2023)(Zhang et al., 2022a)(Cheong et al., 2024b)(Song et al., 2024)
SA	Malicious vehicles compromise network communication by either disseminating excessive traffic (messages) or by dropping or altering the same.	(Qi et al., 2023a)(Zhang et al., 2021)

4.2.2 Time-aware-based Trust Management Models

A time-aware trust management model for the IoV network has been proposed in Siddiqui et al. (2021b), wherein the trust score is quantified by taking into consideration four trust parameters (familiarity, packet delivery ratio, timeliness, and the interaction frequency). Amongst the said trust parameters, timeliness and interaction frequency have been employed to ascertain the corresponding dynamic weights for familiarity and packet delivery ratio. It additionally analyzed the time-varying patterns to investigate the behavior of vehicles for the safety-critical and non-safety vehicular applications. In Sagar et al. (2021), a time-aware trust evaluation mechanism has been envisaged by employing social relationships – friendship similarity, community-of-interest, co-work similarity, and cooperativeness – among the objects for ascertaining their respective trust in a Social Internet of Things (SIoT) network. Moreover, it incorporated a machine learning-driven aggregation scheme and an optimal decision boundary to calculate a single trust score of each object and for segregating the trusted objects from the untrustworthy ones, respectively. The authors further gave an insight into how the trustworthiness of an object in a SIoT network varied vis-à-vis the time. Similar to Sagar et al. (2021), Sagar et al. (2020a) considered direct trust (encompassing community-of-interest similarity, friendship similarity, and the co-work similarity) and indirect trust, and aggregated the same via a dynamic weighted sum scheme for ascertaining the trustworthiness of SIoT objects vis-à-vis the time via a particular threshold.

Whilst the existing state-of-the-art offers several diverse trust-based models, the said models have not taken into consideration the temporal changes in the trust values of the vehicles in a bid to ascertain the underlying dynamics of various trust-based attacks. In other words, a considerable proportion of the models have regarded trust-based attacks to be of static in nature, thereby ignoring the fact that they evolve over time. It is pertinent to mention here that the underlying rationale behind launching a zig-zag attack and an on-off attack stems from a malicious vehicle's intent to manipulate trustworthiness thresholds in a bid to prolong

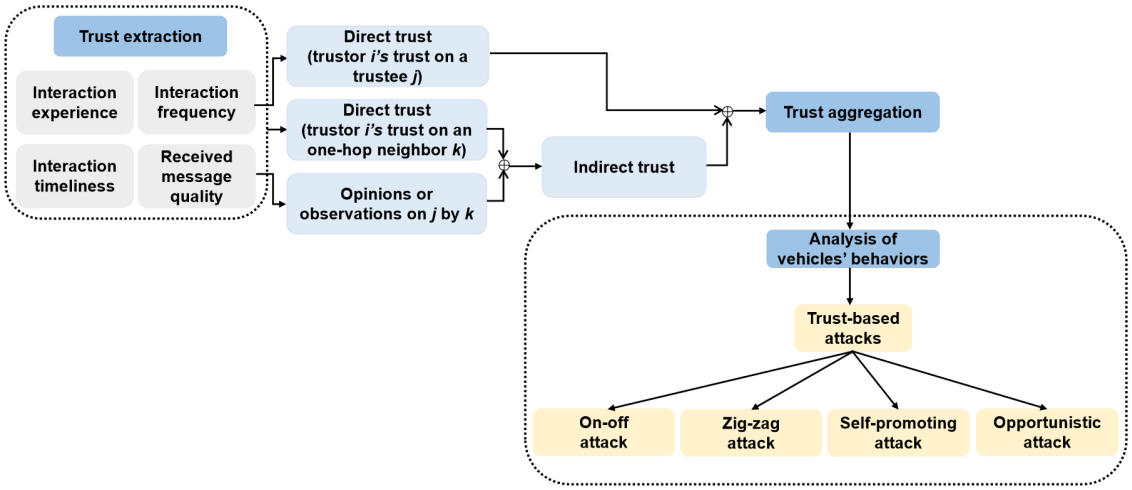

Figure 4.2 A Schematic Diagram of the Envisaged Time-aware Trust Computational Model.

its presence in an IoV network to achieve their respective malign objectives. Therefore, once a malicious vehicle comprehends the operational dynamics of an IoV network, it creates pseudonymous (Sybil) identities to boost its trustworthiness, thereby leading to a self-promoting attack. Moreover, only a handful of trust-based models have accounted for the opportunistic service attacks, nevertheless, none of them were able to determine a classical opportunistic service attack, i.e., wherein, a malicious vehicle (attacker) establishes a favorable reputation within an IoV network, and once it has established the same, it launches a sophisticated abrupt attack by deliberately providing unsatisfactory service. This thus mandates envisaging an IoV-based trust management heuristic to ascertain the behaviors of the vehicles vis-à-vis time in a bid to detect various trust-based attacks along with the attackers' multiple attacking strategies.

4.3 System Model

As depicted in Figure 4.2, distinguishing trust-based attacks within an IoV network encompasses the following steps:

i. *Step 1 : Trust Extraction*

A trust-based model that regards both direct trust and indirect trust has been designed,

wherein the direct trust comprises parameters, i.e., Interaction Experience ($IExp$), Interaction Frequency ($IFre$), Interaction Timeliness ($ITim$), and Received Message Quality (RMQ), whereas, acquisition of the indirect trust is facilitated through the combination of the opinion (observation) of a one-hop neighbor k of a trustor i pertinent to a trustee j and the direct trust of the trustor i on the respective one-hop neighbor k.

ii. *Step 2 : Trust Aggregation*

The trust values accorded to a particular vehicle, i.e., a trustee, via all of its one-hop neighboring vehicles, i.e., trustors, at a given time instance are aggregated via a weighted sum method in order to ascertain a *single* total trust value of the said trustee for that time.

iii. *Step 3 : Analysis of the Vehicles' Behaviors*

The trust-based attacks instigated by a malicious vehicle within an IoV network can be identified via analyzing the variation in its total trust value vis-à-vis the time, i.e., time series analysis. Moreover, the impact of the trust parameters vis-à-vis a respective attack has been studied in a bid to ascertain that which particular trust parameter(s) is (are) altered by a malicious vehicle to launch the said attack.

For the sake of envisaging a model, a set of vehicles has been taken into consideration $\{V\}$ which encompasses trustors $i = \{1, ..., I\}$, trustees $j = \{1, ..., J\}$, and the one-hop neighbors of the trustors $k = \{1, ..., K\}$ such that $i \neq j \neq k$. The trust-based interactions transpires in the form of pairs of trustors and trustees at time instances $t = \{1, ..., T\}$. The definitions of trust parameters employed in this section are delineated in Table 4.2.

4.3.1 Direct Trust ($T_{dir_{i,j,t}}$)

The direct trust implies the direct observation of a trustor i pertinent to a trustee j at a particular time instance t (Yong-hao, 2020) and encompasses four key trust parameters, i.e., Interaction Experience ($IExp_{i,j,t}$), Interaction Frequency ($IFre_{i,j,t}$), Interaction Timeliness ($ITim_{i,j,t}$), and Received Message Quality ($RMQ_{i,j,t}$). The trust parameters are delineated

Table 4.2 The Notations of the Model.

Symbol	Description
i	Trustor in an IoV network
j	Trustee in an IoV network
k	One-hop neighbors of trustor i
t	A particular time instance in an IoV network
T	The total time
I	Total number of trustors i
J	Total number of trustees j
K	Total number of the one-hop neighbors of trustor i
$T_{dir_{i,j,t}}$	Direct trust of i and j at time instance t
$T_{indir_{i,j,t}}$	Indirect trust of i and j at time instance t
$T_{total_{i,j,t}}$	Total trust of i and j at time instance t
$IExp_{i,j,t}$	Interaction Experience of i and j at time instance t
$IFre_{i,j,t}$	Interaction Frequency of i and j at time instance t
$ITim_{i,j,t}$	Interaction Timeliness of i and j at time instance t
$RMQ_{i,j,t}$	Received Message Quality of i and j at time instance t
T_{th}	Trust threshold
γ_1	The weight of $IExp_{i,j,t}$
γ_2	The weight of $IFre_{i,j,t}$
γ_3	The weight of $ITim_{i,j,t}$
γ_4	The weight of $RMQ_{i,j,t}$
w_1	The weight of the direct trust
w_2	The weight of the indirect trust

as follows:

i. *Interaction Experience* ($IExp_{i,j,t}$) – The interaction experience ($0 \leq IExp_{i,j,t} \leq 1$) manifests a direct interactive experience between a trustor i and a trustee j, and is thus ascertained by taking into consideration the ratio of positive interactions between i and j at a time instance t to their respective total interactions at the said time instance. This particular parameter primarily investigates the interplay between the vehicles, thereby contributing to the trustworthiness of vehicles through an analysis of their positive interactions.

$$IExp_{i,j,t} = \frac{\sum TF\{I_{s_{i,j,t}} = 1 \cap T_{v_{i,j,t}} >= T_{th}\}}{TI_{s_{i,j,t}}} \quad \text{Equation 4.1}$$

here, $I_{s_{i,j,t}}$ implies interaction segment between a trustor i and a trustee j at the time instance t, $T_{v_{i,j,t}}$ suggests the trust value assigned to a trustee j by a trustor i at the said time instance t, and T_{th} refers to the threshold for ascertaining positive and negative interactions. Moreover, $TF\{\cdot\}$ is the indicator function, i.e., $TF\{\cdot\} = 1$ indicates the inside condition to be true, whereas, $TF\{\cdot\} = 0$ stipulates it as false. Furthermore, $TI_{s_{i,j,t}}$ indicates the total number of interaction segments between i and j at the time instance t.

ii. *Interaction Frequency* ($IFre_{i,j,t}$) – The interaction frequency ($0 \leq IFre_{i,j,t} \leq 1$) implies the frequency with which a trustor i interacts with a trustee j at a time instance t, and is measured in terms of the ratio of the number of interactions between i and j at a time instance t to the total number of interactions between the trustor i and all vehicles with which it has interacted at the said time. The higher the frequency of interactions between a trustor and a trustee, the more conducive it becomes to establish an optimal trust. For instance, in urban settings, wherein vehicular mobility is generally low, the interaction frequency amongst the vehicles usually increases and which, in turn, facilitates in ascertaining the trust.

$$IFre_{i,j,t} = \frac{TI_{s_{i,j,t}}}{TI_{s_{i,j,t}} + \sum_{k=1}^{K} TI_{s_{i,k,t}}} \quad \text{Equation 4.2}$$

here, $\sum_{k=1}^{K} TI_{s_{i,k,t}}$ indicates the total number of interaction segments between i and k at time instance t.

iii. *Interaction Timeliness* ($ITim_{i,j,t}$) – The interaction timeliness ($0 \leq ITim_{i,j,t} \leq 1$) refers to the time at which a trustor i and a trustee j interacts vis-à-vis the current time. Owing to the high mobility of vehicles, it is indispensable to take into account the recent interactions in order to ascertain their respective trustworthiness since either (a) an honest vehicle may turn malicious over the time as a result of an attack or (b) a disguised vehicle may reveal

itself if and when it founds an opportunity to manipulate an IoV network.

$$ITim_{i,j,t} = \frac{t_{i,j}}{t_c} \qquad \text{Equation 4.3}$$

where, $t_{i,j}$ represents the time instance a trustor i and a trustee j interacts, and t_c implies the current time (Siddiqui et al., 2023a).

iv. *Received Message Quality* ($RMQ_{i,j,t}$) – The received message quality ($0 \leq RMQ_{i,j,t} \leq 1$) indicates the quality of the messages received by a trustee j from a trustor i at a time instance t. $RMQ_{i,j,t}$ directly relies on the Network Communication Quality (NetComQ) pertinent to an IoV network, i.e., a higher NetComQ suggests a considerable amount of information exchanged amongst the vehicles. However, the NetComQ is influenced by a number of factors, including but not limited to, the transmission medium, bandwidth, and weather conditions. For instance, lightning poses a significant threat to radio communication since it can cause electromagnetic interference, disrupt communication channels, and degrade signal quality (Lu et al., 2024). This not only impacts vehicular interactions but also makes an IoV network susceptible to a diverse range of attacks (Zhang et al., 2022b). Therefore, ensuring NetComQ is imperative for safeguarding the security of an IoV network. For the sake of the envisaged model, the NetComQ has been classified into five levels ($Q_5 < Q_4 < Q_3 < Q_2 < Q_1$) as delineated in Table 4.3, wherein P suggests a poor NetComQ (Q_5), $M - P$ indicates that the NetComQ is between medium and poor ($Q4$), M represents medium NetComQ (Q_3), $M - G$ refers that the NetComQ is between medium and good ($Q2$), and G implies good NetComQ (Q_1).

Table 4.3 The Levels of the NetComQ (Good – G, Between Medium and Good – $(M-G)$, Medium – M, Between Medium and Poor – $(M-P)$, Poor – P).

NetComQ	Level
G	Q_1
$M-G$	Q_2
M	Q_3
$M-P$	Q_4
P	Q_5

$$RMQ_{i,j,t} = \begin{cases} 1 & \text{if, } Q_2 < NetComQ_t \leq Q_1 \\ 0.75 & \text{if, } Q_3 < NetComQ_t \leq Q_2 \\ 0.50 & \text{if, } Q_4 < NetComQ_t \leq Q_3 \\ 0.25 & \text{if, } Q_5 < NetComQ_t \leq Q_4 \\ 0 & \text{if, } NetComQ_t \leq Q_5 \end{cases} \quad \text{Equation 4.4}$$

Finally, the four interaction-related parameters are aggregated to ascertain the direct trust:

$$T_{dir_{i,j,t}} = \gamma_1 IExp_{i,j,t} + \gamma_2 IFre_{i,j,t} + \gamma_3 ITim_{i,j,t} + \gamma_4 RMQ_{i,j,t} \quad \text{Equation 4.5}$$

here, γ_1, γ_2, γ_3, and γ_4 refers to the dynamic weight of $IExp_{i,j,t}$, $IFre_{i,j,t}$, $ITim_{i,j,t}$, and $RMQ_{i,j,t}$, respectively ($\gamma_1+\gamma_2+\gamma_3+\gamma_4 = 1$). It is pertinent to mention here that the selection of optimal weights is highly indispensable for ascertaining the direct trust in a bid to capture the realistic impact of the parameters employed for the same. Accordingly, the Grey Relation Analysis (GRA), i.e., a multi-factor statistical analysis method (Chen et al., 2024)(Liang et al., 2019), has been employed for aggregating the direct trust. The grey correlation coefficient ($\zeta_r(t)$) is computed as:

$$\zeta_r(t) = \frac{\min_r \min_t |x_0(t) - x_r(t)| + \rho \max_r \max_t |x_0(t) - x_r(t)|}{|x_0(t) - x_r(t)| + \rho \max_r \max_t |x_0(t) - x_r(t)|} \quad \text{Equation 4.6}$$

where, $x_0(t)$ implies the referenced time sequence and $x_r(t)$ suggests the comparative time sequences, i.e., which are the respective time sequences of the aforementioned four interaction-related direct trust parameters. ρ, herein, is a constant in the range of 0 to 1 and represents the resolution factor. The coorelation degree, i.e., mean value of the grey correlation coefficient ($\zeta_r(t)$), is formulated as:

$$\eta_r = \frac{1}{T}\sum_{t=1}^{T}\zeta_r(t) \qquad \text{Equation 4.7}$$

Finally, the dynamic weights for $IExp_{i,j,t}$, $IFre_{i,j,t}$, $ITim_{i,j,t}$, and $RMQ_{i,j,t}$ are calculated via the grey correlation coefficient:

$$\gamma_r = \frac{\eta_r}{\eta_1 + \eta_2 + \eta_3 + \eta_4}, r = 1, 2, 3, 4. \qquad \text{Equation 4.8}$$

4.3.2 Indirect Trust ($T_{indir_{i,j,t}}$)

The indirect trust ($0 \leq T_{indir_{i,j,t}} \leq 1$) refers to the opinions or observations of the one-hop neighbors (k) of a trustor i pertinent to a trustee j in an IoV network. Since a trustor in this context relies on the opinions or observations of its one-hop neighbors, it is also highly indispensable to take into account a trustor's direct trust pertinent to its respective one-hop neighbor. Therefore, the indirect trust is computed as:

$$T_{indir_{i,j,t}} = \frac{1}{K}\sum_{k=1}^{K}[T_{dir_{k,j,t}} \cdot T_{dir_{i,k,t}}] \qquad \text{Equation 4.9}$$

where, $T_{dir_{k,j,t}}$ is the opinion of a one-hop neighbor (k) of a trustor i pertinent to a trustee j and $T_{dir_{i,k,t}}$ is the direct trust of the trustor i on the respective one-hop neighbor k.

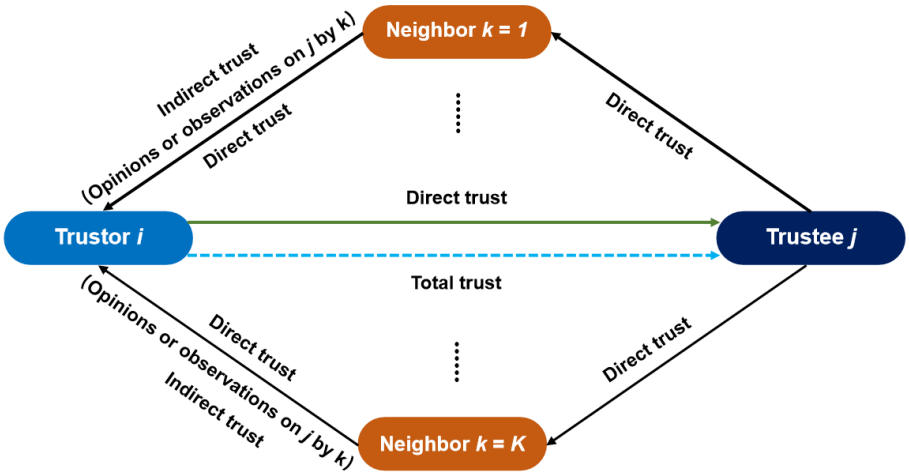

Figure 4.3 The Total Trust of a Trustee in an IoV Network.

4.3.3 Total Trust ($T_{total_{i,j,t}}$)

The total trust of each vehicle at each time instance t is obtained via the weighted sum of its direct trust and indirect trust as portrayed in Figure 4.3 and given as follows:

$$T_{total_{i,j,t}} = w_1 T_{dir_{i,j,t}} + w_2 T_{indir_{i,j,t}} \qquad \text{Equation 4.10}$$

wherein, w_1 and w_2 are the weights of the direct and indirect trust, respectively ($w_1 + w_2 = 1$).

4.4 Simulation Setup and Result Analysis

4.4.1 Simulation Setup

Epinions dataset (Tang et al., 2012) has been utilized to fetch the data traces pertinent to the trust parameters envisaged in Section 4.3. Epinions is a publicly accessible trust dataset encompassing six parameters – $userid$, $productid$, $categoryid$, $rating$, $helpfulness$, and $timestamps$. A reputation segment, [1, 2, 3, 4, 5, 6], in the context of the Epinions dataset suggests that a particular user 1 confers a reputation of 4 to a certain product 2 from category 3 at the timestamp 6. For reference, the process via which the Epinions dataset has been transformed into an IoV dataset is elaborated in Chapter 3. The said dataset encompasses

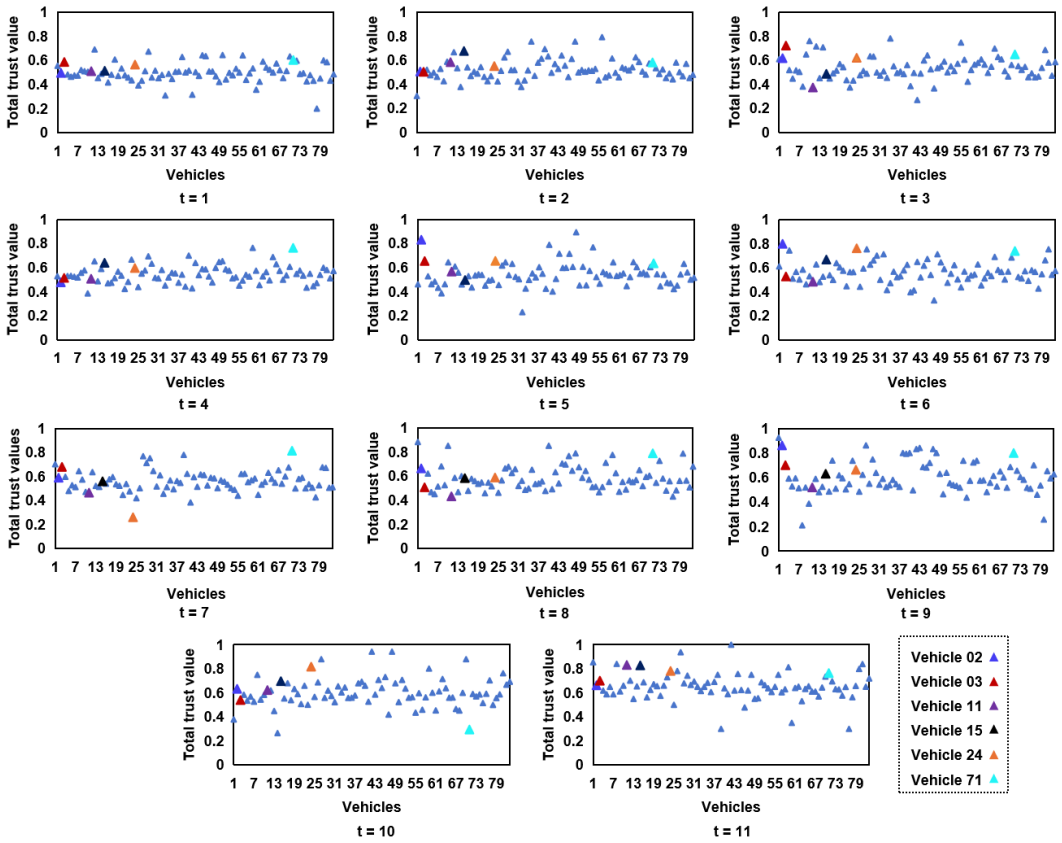

Figure 4.4 Trust Values of 83 Vehicles Over 11 Time Instances in an IoV Network.

83 vehicles which engage in frequent interactions with other vehicles, thereby resulting in 47, 811 pairs of interactions over a duration of 11 time instances. Each vehicle interacted at least once to ascertain the trust parameters discussed in Section 3. The simulations have been carried out using Python 3.9. In order to validate the effectiveness of the envisaged IoV-based trust model, four types of trust-based attacks, namely, zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks, have been injected in the said IoV dataset.

4.4.2 Result Analysis

Figure 4.4 illustrates the changes in the total trust values of 83 vehicles over 11 time instances. Since all vehicles enter the IoV network at the time instance $t = 1$, they possess limited interactions and, accordingly, their respective trust value is comparatively lower. However, over time, with an increasing number of interactions amongst the vehicles,

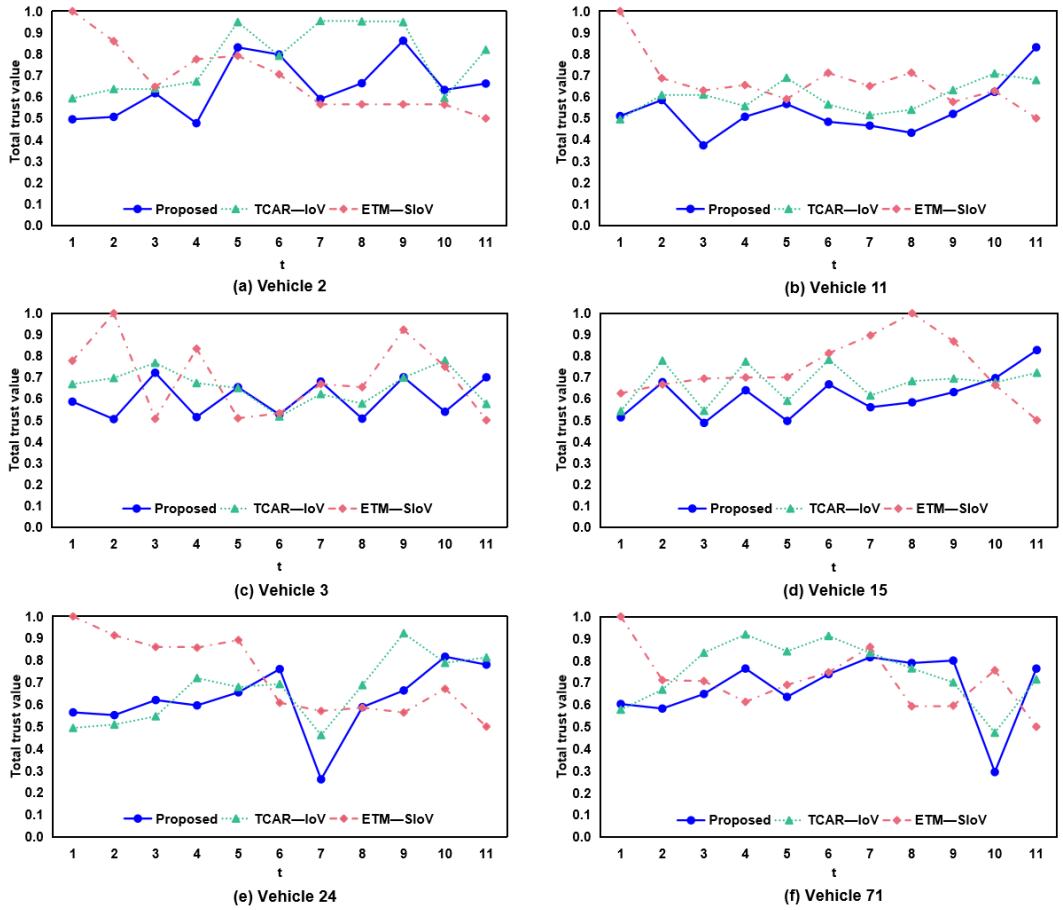

Figure 4.5 Trust Varying Patterns of (a) Vehicle 2, (b) Vehicle 11, (c) Vehicle 3, (d) Vehicle 15, (e) Vehicle 24, and (f) Vehicle 71 Over 11 Time Instances in an IoV Network.

their respective trust value exhibits a gradual change. It is pertinent to mention that owing to spatial constraints, the temporal evolution of trust values for select vehicles has been presented in Table 4.4, thereby facilitating a more intuitive understanding of the changes in their respective trust values. Furthermore, by scrutinizing the dynamics of trust values for all the 83 vehicles, 6 vehicles, i.e., vehicles 2, 3, 11, 15, 24, and 71, whose trust values exhibited more pronounced change over time have been identified. The same are illustrated in Figure 4.5. This identification facilitates in understanding the behavior of vehicles in an IoV network.

Also, owing to the high mobility of vehicles in an IoV network and the absence of a comprehensive infrastructure, IoV networks are susceptible to a number of attacks. The envisaged model demonstrates its capability in identifying four trust-based attacks, i.e., zig-

Table 4.4 Partial Trust Values Pertinent to Trust Parameters (Interaction Experience – $IExp$, Interaction Frequency – $IFre$, Interaction Timeliness – $ITim$, Received Message Quality – RMQ).

Time	Trustor	IExp	IFre	ITim	RMQ
1	1	0.8889	0.2099	0.5119	0.9167
5	1	0.3333	0.5556	0.5752	1.0000
2	8	0.8333	0.1319	0.5251	0.8229
6	8	1.0000	0.5556	0.5973	0.3333
5	12	0.9890	0.5153	0.5752	0.5055
7	12	0.9336	0.6711	0.6238	0.5131
1	16	0.7250	0.1300	0.5119	0.5438
11	16	1.0000	0.5000	1.0000	0.5000
4	23	1.0000	0.5000	0.5563	0.7500
7	23	0.8571	0.2653	0.6238	0.3571
6	32	1.0000	1.0000	0.5973	0.2500
8	32	0.5385	1.0000	0.6569	0.6154
5	38	0.9474	0.2022	0.5752	0.5789
9	38	1.0000	1.0000	0.7011	0.5000
1	41	0.3929	0.4158	0.5119	0.3661
5	41	0.6364	0.2603	0.5752	0.5114
2	45	0.8891	0.5208	0.5251	0.4743
10	45	0.9535	0.5143	0.7683	0.4767
3	52	0.9394	0.4105	0.5397	0.4621
7	52	0.9277	0.1995	0.6238	0.5260
8	57	1.0000	0.6250	0.6569	0.5625
10	57	0.6667	0.1667	0.7683	0.5417
1	63	1.0000	0.5000	0.5119	0.2500
5	63	0.6667	0.2222	0.5772	0.6250
3	72	1.0000	0.1833	0.5397	0.5319
9	72	1.0000	0.3878	0.7011	0.5357
5	80	0.9474	1.0000	0.5752	0.3026
11	80	1.0000	1.0000	1.0000	0.4750

zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks. These four trust-based attacks are delineated as follows:

i. *Zig-zag Attacks and On-off Attacks*: In case of a zig-zag attack and an on-off attack,

malicious vehicles do not consistently manifest malicious behavior. Instead, intelligent malicious vehicles employ a strategic approach via alternating irregularly, i.e., zig-zag attack, or regularly, i.e., on-off attack, between both the honest and the dishonest modes. These intermittent attacks allow perpetrators to inflict considerable damage without being detected and evicted from an IoV network (Chen et al., 2024)(Mao et al., 2021).

ii. *Self-promoting Attacks*: In the context of a self-promoting attack, malicious vehicles consistently augment their respective reputation to gain significant privileges within an IoV network for jeopardizing the entire network for malign gains (Magdich et al., 2022). In order to instigate such an attack, malicious vehicles generate sophisticated pseudonymous (Sybil) identities to manipulate trust and intelligently deceive trust-based mechanisms (Siddiqui et al., 2021b).

iii. *Opportunistic Attacks*: When it comes to an opportunistic attack, a malicious vehicle strategically offers superior services for most of the time to establish a reputable presence in an IoV network. Once it establishes the same, it effectively colludes with other malicious entities to launch various sophisticated attacks, including but not limited to, bad-mouthing attack and ballot stuffing attack (Mahmood et al., 2023), to inflict considerable harm to the IoV entities it interacts with and to the entire IoV network as a whole.

Figures 4.5(a) and 4.5(b) illustrate the trust varying patterns of vehicles 2 and 11 respectively over 11 time instances for the envisaged IoV-based trust model vis-à-vis TCAR–IoV (Siddiqui et al., 2023b) and ETM–SIoV (Shamaeian and Pesch, 2024). It is quite evident that the envisaged IoV-based trust model can ascertain the injected zig-zag attack transpiring in the context of vehicle 2, and a zig-zag and a self-promoting attack in the context of vehicle 11 in an optimal manner in contrast to TCAR–IoV and ETM–SIoV. Whilst TCAR–IoV demonstrate some form of a zig-zag pattern for vehicle 2, the variation in its trust pattern has been unnoticeable for time instances $t = 1 - 4$ and $t = 7 - 9$ and which, therefore, allows the said malicious vehicle to remain undetected over the course of its entire trajectory in the IoV network. Similarly, ETM–SIoV did not demonstrate an optimal pattern for it to be classified

as instigating zig-zag attack. The same is true for vehicle 11 too since both TCAR–IoV and ETM–SIoV could not particularly recognize the self-promoting attack. It is pertinent to mention that the underlying rationale for launching a zig-zag attack lies in a malicious vehicle's ability to deceit the detection thresholds so as to stay for an extended duration of time in an IoV network for realizing its respective malign goals. Similarly, once a malicious vehicle understands the dynamics of an IoV network, it generates pseudonymous, i.e, Sybil (Du et al., 2024)(Li et al., 2022a), identities and employs the same to enhance its trust value, thereby resulting in a self-promoting attack.

Moreover, Figures 4.5(c) and 4.5(d) portray the trust varying patterns of vehicles 3 and 15 over 11 time instances for the envisaged IoV-based trust model vis-à-vis TCAR–IoV and ETM–SIoV. It is once again quite apparent that the envisaged IoV-based trust model can ascertain the injected on-off attack transpiring in respect of vehicle 3, and an on-off attack and a self-promoting attack in respect of vehicle 15 in an optimal manner in contrast to TCAR–IoV and ETM–SIoV. In case of vehicle 3, both TCAR–IoV and ETM–SIoV demonstrate zig-zag attack as opposed to the on-off attack. Moreover, in case of vehicle 15, TCAR–IoV fail to demonstrate the self-promoting attack, whereas, ETM–SIoV was unable to ascertain both on-off attack as well as self-promoting attack. It is noteworthy to mention that similar to that of a zig-zag attack, a malicious vehicle launches an on-off attack with the key aim of evading detection and subsequent eradication from an IoV network. However, a zig-zag attack poses a greater challenge in terms of its detection and can inflict a considerable damage to an IoV network in contrast to an on-off attack primarily as the former launches the attack via irregularly alternating the behavioral patterns, whereas, the latter does the same through regularly alternating the behavioral patterns. Nevertheless, it is highly indispensable for a trust model to identify the right type of attack instigated by a malicious vehicle so as to enable it to apply the optimal mitigation strategy to resist the same.

Furthermore, Figures 4.5(e) and 4.5(f) illustrate the time varying patterns of vehicles 24 and 71 over 11 time instances for the envisaged IoV-based trust model vis-à-vis TCAR–IoV

and ETM–SIoV. It is quite noticeable that the envisaged IoV-based trust model can ascertain the classical opportunistic attack transpiring in the context of vehicles 24 and 71 in an optimal manner in contrast to TCAR–IoV and ETM–SIoV. Whilst TCAR–IoV demonstrate some form of an opportunistic behavior, its trust varying pattern at time instances $t = 6-9$ for vehicle 24 and $t = 6-11$ for vehicle 71 do not reflect a classical opportunistic attack, thereby allowing the said malicious vehicle to remain undetected in an IoV network. Moreover, ETM–SIoV completely fails in detecting the opportunistic attack for vehicles 24 and 71. It is interesting to note here that both vehicles delivered high quality services and established considerable reputation over time in an IoV network. However, once they had ensured strong reputation in an IoV network, they instigated an abrupt sophisticated attack by furnishing bad service.

Table 4.5 delineates the total trust values of vehicles 2, 3, 11, 15, 24, and 71 over 11 time instances in an IoV network. It is pertinent to mention here that vehicles 2 and 3 remain engaged in a zig-zag attack and an on-off attack respectively, and the same is quite apparent from their respective patterns. Vehicles 11 and 15 instigated the multiple trust-based attacks throughout their respective temporal span in an IoV network and the same is manifested in italic cum underlined text, i.e., 0.5202 ($t = 9$) and 0.5835 ($t = 8$) respectively. Vehicles 24 and 71 launched the opportunistic attack and the impact of the same is also delineated in italic cum underlined text, i.e., 0.2607 ($t = 7$) and 0.2947 ($t = 10$) respectively.

Figure 4.6 illustrates the trust varying patterns of the four trust parameters, i.e., interaction experience, interaction frequency, interaction timeliness, and received message quality, vis-à-vis the total trust values of vehicles 15 and 24 over the 11 time instances with the primary objective being to distinguish the particular trust parameters which have been manipulated by the said vehicles for instigating the trust-based attacks. As quite evident from Figure 4.6(a), vehicle 15 instigates an on-off attack between the time instances $1-7$ followed by a self-promoting attack between the time instances $8-11$. The on-off attack, among other factors, primarily transpires due to the regular yet rapid fluctuation in its interaction frequency with the other vehicles in an IoV network. Moreover, while vehicle 15 demonstrated a lower level

Table 4.5 Total Trust Values of Vehicles 2, 3, 11, 15, 24, and 71 Over 11 Time Instances (t) in an IoV network.

t	2	3	11	15	24	71
1	0.4957	0.5867	0.5102	0.5133	0.5646	0.6032
2	0.5070	0.5050	0.5848	0.6778	0.5521	0.5826
3	0.6172	0.7219	0.3734	0.4871	0.6205	0.6488
4	0.4776	0.5144	0.5069	0.6398	0.5963	0.7641
5	0.8313	0.6544	0.5665	0.4963	0.6554	0.6355
6	0.7981	0.5267	0.4834	0.6674	0.761	0.7387
7	0.5904	0.6805	0.4656	0.5605	*0.2607*	0.8153
8	0.6642	0.5072	0.4323	*0.5835*	0.5885	0.7892
9	0.8624	0.7012	*0.5202*	0.6312	0.664	0.8003
10	0.6329	0.5396	0.6229	0.6967	0.8171	*0.2947*
11	0.6625	0.7006	0.8313	0.8278	0.7813	0.7639

of interaction frequency during the last 4 time instances, it manifested a much reasonable interaction-related behavior and higher number of positive interactions with the other vehicles in a bid to enhance its total trust value so as to instigate a self-promoting attack for gaining higher privileges in an IoV network.

Furthermore, vehicle 24, as illustrated in Figure 4.6(b), instigated a classic opportunistic attack at the time instance 7 after demonstrating a reasonably upward trajectory in its total trust value during the time instances $1-6$ with its trajectory particularly at the time instance 6 being promising enough so as to make the vehicles interacting with it to rest their respective faith on it for realizing a number of requisite IoV-related services. This is, therefore, the mere instance, wherein an opportunistic attack is instigated by the malicious vehicles so as to inflict a maximum damage to not only the vehicles interacting with it but to the entire IoV network too. It is noteworthy to mention that an opportunistic attack in most cases remains undetected since it transpires for an extremely short duration of time and the malicious vehicles subsequently disguise themselves as honest vehicles.

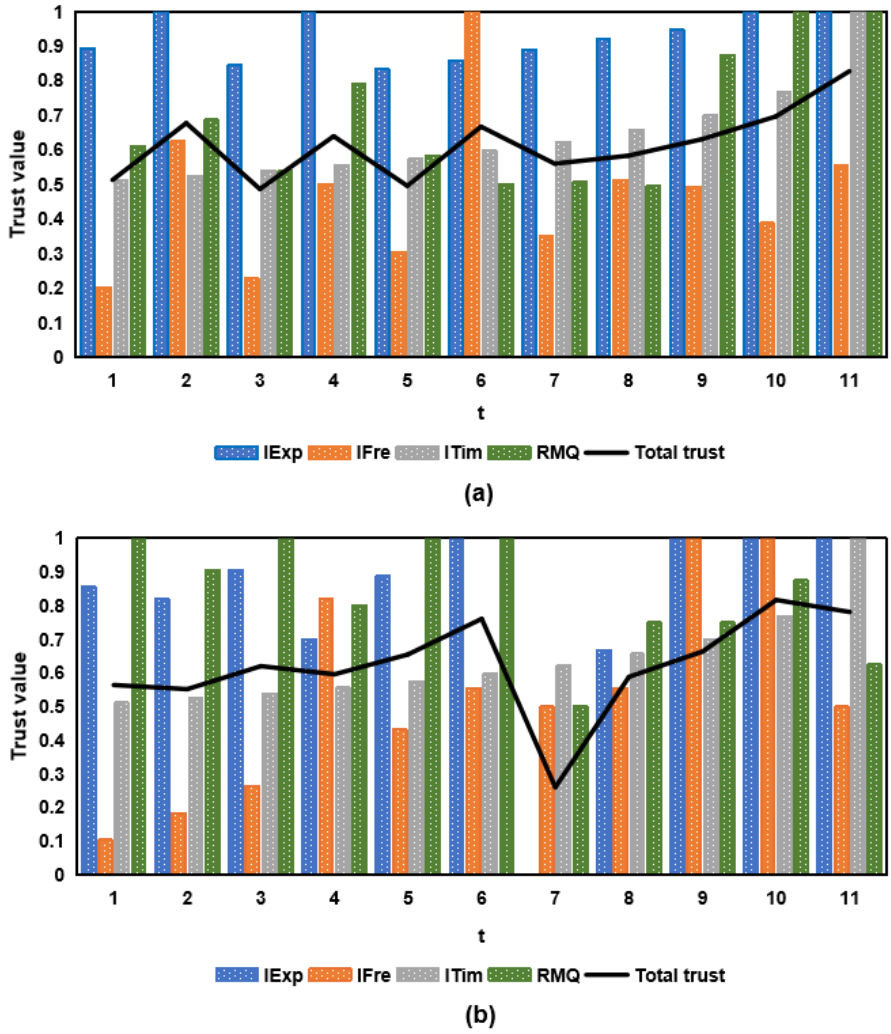

Figure 4.6 Variation in the Total Trust Value, Interaction Experience – $IExp$, Interaction Frequency – $IFre$, Interaction Timeliness – $ITim$, and Received Message Quality – RMQ vis-à-vis Time (t) for (a) Vehicle 15 and (b) Vehicle 24.

4.5 Summary

This particular chapter envisages an IoV-based trust management heuristic that takes into consideration both direct trust and indirect trust to ascertain the behaviors of the vehicles vis-à-vis time so as to detect various trust-based attacks, i.e., zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks, together with the attackers' multiple attacking strategies. The experimental findings demonstrate that the envisaged trust management heuristic exhibits prompt and accurate detection of the trust-based attacks in contrast to

the state-of-the-art trust management mechanisms. Therefore, the proposed time-aware trust model directly strengthens IoV network resilience by enabling the timely and accurate identification of malicious behavioral patterns, thereby ensuring the integrity and reliability of safety-critical communications. In the near future, conceiving of a state-of-the-art IoV-based trust testbed would be contemplated so as to holistically capture and analyze all the possible attack vectors under dynamic realistic network environments along with the feasibility of the mitigation techniques employed to tackle the same. Furthermore, the computational complexity of the trust management heuristics would be considerably minimized.

CHAPTER 5

TM – IoV: A FIRST-OF-ITS-KIND MULTILABELED TRUST PARAMETER DATASET FOR EVALUATING TRUST IN THE INTERNET OF VEHICLES

The emerging and promising paradigm of the Internet of Vehicles (IoV) employ vehicle-to-everything communication for facilitating vehicles to not only communicate with one another but also with the supporting roadside infrastructure, vulnerable pedestrians, and the backbone network in a bid to primarily address a number of safety-critical vehicular applications. Nevertheless, owing to the inherent characteristics of IoV networks, in particular, of being (a) highly dynamic in nature and which results in a continual change in the network topology and (b) non-deterministic owing to the intricate nature of its entities and their interrelationships, they are susceptible to a number of malicious attacks. Such kinds of attacks, if and when materialized, jeopardizes the entire IoV network, thereby putting human lives at risk. Whilst the cryptographic-based mechanisms are capable of mitigating the external attacks, the internal attacks are extremely hard to tackle. Trust, therefore, is an indispensable tool since it facilitates in the timely identification and eradication of malicious entities responsible for launching internal attacks in an IoV network. To date, there is no dataset pertinent to trust management in the context of IoV networks and the same has proven to be a bottleneck for conducting an in-depth research in this domain. The manuscript-at-hand, accordingly, presents a first-of-its-kind trust-based IoV dataset encompassing 96,707 interactions amongst 79 vehicles at different time instances. The dataset involves nine salient trust parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward / punishment, and context, which play a considerable role in ascertaining the trust of a vehicle within an IoV network.

Wang Yingxun, Adnan Mahmood, Mohamad Faizrizwan Mohd Sabri, Hushairi Zen (2024). *TM – IoV: A First-of-its-Kind Multilabeled Trust Parameter Dataset for Evaluating Trust in the Internet of Vehicles*. Data, 9 (9):103 (Q2, Impact Factor: 2.0).

5.1 Overview

Over the past decade or so, the rapid evolution and advancements in a number of cutting-edge technologies, including but not limited to, the Internet of Things (IoT), artificial intelligence, and fifth-generation communication, has led to the transformation of the conventional intelligent transportation systems into Internet of Vehicles (IoV) networks (Cao et al., 2024)(Yang et al., 2023b). The IoV networks facilitate seamless connectivity for a real-time exchange of safety-critical and non-safety information amongst vehicles, and between vehicles and vulnerable pedestrians, supporting roadside infrastructure, and the backbone network via vehicle-to-everything communication (Alagha et al., 2025)(Yang et al., 2024)(Adhikari et al., 2022). Despite the low latency advantages associated with the IoV networks, they are prone to a number of malicious attacks that are not only capable of jeopardizing the entire network but also poses a considerable risk to human lives. Hence, it is of paramount importance to ensure the resilience of IoV networks (Zhang et al., 2025)(Shokrollahi and Dehghan, 2023)(Zhang et al., 2022c). Figure 5.1 portrays an IoV landscape.

A brief glimpse of the state-of-the-art reveals that a number of mechanisms have been proposed over the years in order to strengthen the security of an IoV network. Such mechanisms can be broadly classified into two categories, i.e., cryptography-based approaches and trust-based approaches (Rathee et al., 2024)(Abbas et al., 2022). Whilst the cryptography-based approaches safeguard IoV networks against a number of malicious attacks, including but not limited to data tampering, identity theft, and eavesdropping, they are prone to a number of internal attacks (Ullah et al., 2023b)(Monfared and Shokrollahi, 2023). Trust-based approaches, on the contrary, can intelligently address the challenges pertinent to internal attacks (Guo et al., 2020) since they leverage the reputation of entities within an IoV network in order to guarantee secure communication amongst them, thereby facilitating intelligent traffic flows (Kuang et al., 2022)(Tripathi and Sharma, 2020).

In the context of an IoV network, vehicles are classified as either trusted or untrusted (Li

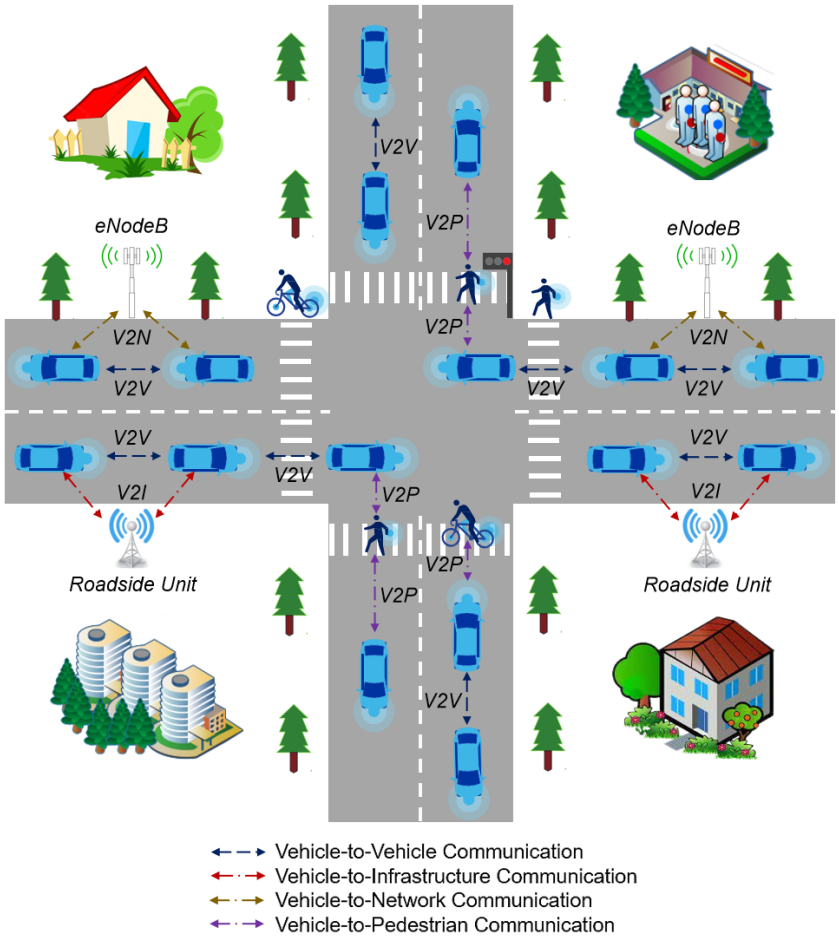

Figure 5.1 An IoV Landscape.

et al., 2022b)(Kaur and Kakkar, 2022). Trusted vehicles exhibit legitimate behavior by primarily disseminating accurate information, whereas, untrusted vehicles engage in malicious activities by intentionally transmitting and facilitating the relay of incorrect information and recommendations in an IoV network in an intelligent manner, thereby posing a grave threat to vehicular passengers and vulnerable pedestrians (Wazid et al., 2022)(Li et al., 2021b). Hence, an accurate and real-time identification of malicious vehicles in such a highly dynamic network is highly indispensable (Fernandes et al., 2023). The state-of-the-art methodologies employed for the identification of such vehicles in an IoV network typically involve threshold-based and decision boundary-based mechanisms (Alalwany and Mahgoub, 2024)(Aslan and Sen, 2023). In the case of threshold-based mechanisms, a vehicle's trust value is compared with a predetermined trust threshold, i.e., if the trust value of a vehicle exceeds the predeter-

mined trust threshold, it is regarded as a trusted vehicle, or else, it is classified as a malicious vehicle. On the contrary, in case of decision boundary-based mechanisms, the trust values derived from vehicular interactions are clustered and classified via learning algorithms, and an optimal decision boundary is subsequently employed to segregate the trusted vehicles from the malicious ones (Nazih et al., 2024)(Zhang et al., 2023a). However, regardless of the methodology employed for the identification of the malicious vehicles in an IoV network, vehicles should have an associated precise trust value. Therefore, trust-related data hold considerable significance for securing highly dynamic IoV networks.

Trust, in essence, implies a degree of belief or disbelief that a trustor has on a trustee in carrying out a particular task or a set of tasks in an anticipated manner (Mahmood et al., 2023). It mandates quantification, and to realize the same, it relies on several trust-based parameters which are not only context-dependent but are also highly dynamic in nature since they transpire as a result of the frequent interactions amongst the vehicles in an IoV network (Sagar et al., 2024a)(Zhang et al., 2023b). Whilst a number of IoV-based trust parameters have already been delineated in the research literature, as of date, there is no dedicated publicly available trust-based IoV dataset that researchers from both academia and industry can predominantly employ in order to carry out an in-depth research and subsequently expand upon within this particular domain. In order to address this particular challenge, the manuscript-at-hand presents a pioneering trust-based IoV dataset, which is discussed in detail in Section 5.2 (Data Description) and Section 5.3 (Methods).

5.2 Data Description

The manuscript-at-hand introduces a trust-based IoV dataset which has been made available for the readers at https://github.com/wangyingxun/IoV. This particular dataset has been employed for not only ascertaining the trust values of vehicles in an IoV network but also for segregating the trustworthy vehicles from the untrustworthy ones by means of an optimal

Figure 5.2 Depicting a Realistic Urban Mobility Scenario for Jinan.

decision boundary. Accordingly, a detailed description of the key features of this particular dataset is indispensable so as to enable researchers in both academia and the industry to employ and extend the same in a bid to investigate open research directions of this emerging and promising domain.

It is pertinent to mention here that, to date, there is no public dataset pertinent to trust management in IoV networks. Therefore, the dataset proposed in the manuscript-at-hand represents a pioneering contribution within this particular domain. In order to realize the same, Java has been employed for designing an IoV-based simulator, whereas, Python was employed for analyzing the simulation results. Figure 5.2 herein depicts a realistic urban mobility scenario for Jinan, i.e., a city in the Shandong province of the People's Republic of China. The IoV simulator, accordingly, takes into account the said urban mobility scenario since it encompasses several interconnected road segments with vehicles traversing on the same along diverse paths at random speeds in disparate directions. Moreover, the speed of a vehicle remains constant throughout its traveling trajectory along a single path and only changes once the respective vehicle opts for a new path. Figure 5.3 illustrates the simulation process employed to generate the TM – IoV dataset. Vehicles, therefore, interact with one another, i.e., the time of interaction amongst them depends on their respective speeds, and frequently exchange indispensable information to realize a number of both safety-critical and

non-safety applications. Moreover, the proposed IoV-based simulator incorporates not only honest vehicles but also intelligent malicious ones that dynamically alternate between honest and dishonest behaviors in a bid to execute malicious acts so as to evade detection by the IoV-based trust models (Qi et al., 2024)(Mahmood et al., 2022).

For the readers' reference, the trust-based IoV dataset proposed in the manuscript-at-hand encompasses 79 vehicles, i.e., trustors and trustees, that engage in a total of 96, 707 interactions over different time instances. In total, nine key trust parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward / punishment, and context have been ascertained. A trust authority (Azizi and Shokrollahi, 2024) here plays an indispensable role as it facilitates in ascertaining the trust parameters, which (a) cannot transpire as a result of the interactions between a trustor and a trustee or (b) requires the opinion of a global entity with an overarching view of the entire IoV network in a bid to determine the credibility of the information exchanged between a trustor and a trustee and their respective recommendations. These parameters thus not only depict the dynamic interactions amongst the trustors and trustees in an IoV network but further offer valuable insights pertinent to the behavior of the same.

5.3 Methods

As discussed above, the proposed trust-based IoV dataset encompasses trustors, trustees, and 9 salient trust parameters. The same are delineated as follows:

5.3.1 Trustor

Trust in an IoV network involves multiple attributes, which can be quantified by considering it as a relational construct involving two entities, i.e., a trustor i and a trustee j. The trustor i assumes the role of an evaluator to assess and ascertain the trustworthiness of a trustee j. In proposed dataset, there are 79 trustors listed in column 1 of the dataset.

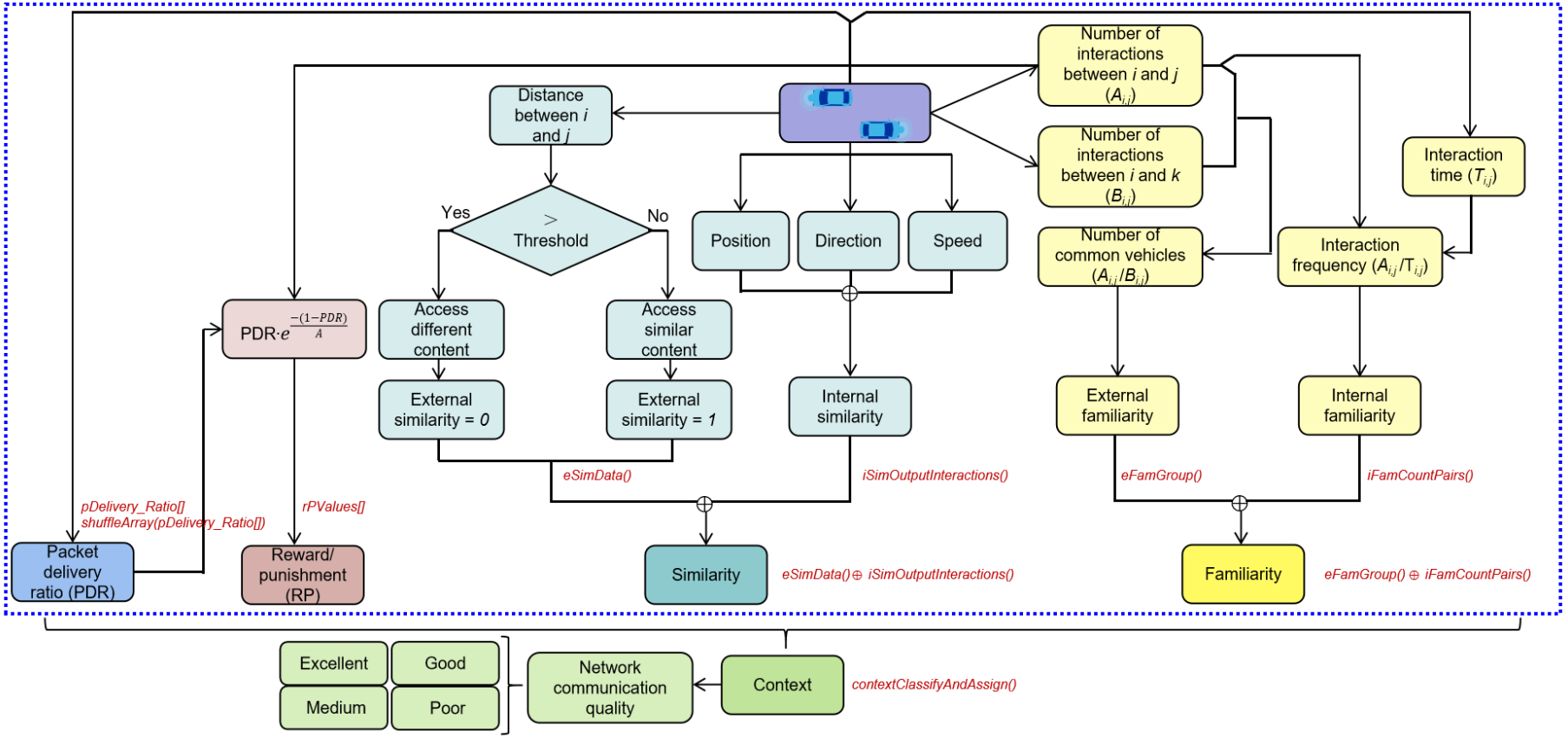

Figure 5.3 Simulation Process of TM – IoV Dataset.

5.3.2 Trustee

The trustee, also referred to as a target node, is an entity that is evaluated by a trustor as either trustworthy or untrustworthy. In the proposed dataset, there are 79 trustees (listed in column 2 of the dataset) that have encountered 96, 707 interactions with the trustors.

5.3.3 Packet Delivery Ratio (PDR)

The packet delivery ratio ($0 \leq PDR \leq 1$) measures the degree of interaction between a trustor i and a trustee j at a time instance t, thereby providing a key understanding of their relationship. In order to ascertain PDR, the total number of messages sent by a trustor i and successfully received by a trustee j at a time instance t, have been collected. The PDR is determined by taking into account the ratio between the aforementioned sent and successfully received messages between a trustor i and a trustee j. The same is listed in column 3 of the dataset.

5.3.4 Similarity (Sim)

The similarity ($0 \leq Sim \leq 1$) between a trustor i and a trustee j at a time instance t encompasses both External Similarity (ES) and Internal Similarity (IS), and is a weighted amalgamation of the two. The same is listed in column 4 of the dataset.

i. *External Similarity (ES)* – The external similarity ($0 \leq ES \leq 1$) suggests the extent to which a trustor i and a trustee j access similar content at a time instance t, and is listed in column 5 of the dataset. ES is deemed to be 1 if the trustor i and a trustee j access similar content. Otherwise, it is regarded as 0.

ii. *Internal Similarity (IS)* – The internal similarity ($0 \leq IS \leq 1$) manifests the degree of similarity in the positions, directions, speeds, and accelerations of a trustor i and trustee j. The same is depicted in column 6 of the dataset.

5.3.5 Familiarity (Fam)

The familiarity ($0 \leq Fam \leq 1$) between a trustor i and a trustee j at a time instance t is also segregated into External Familiarity (EF) and Internal Familiarity (IF). The same is delineated in column 7 of the dataset.

i. *External Familiarity (EF)* – The external familiarity ($0 \leq EF \leq 1$) quantifies the level of the familiarity a trustor possesses towards a trustee, and is listed in column 8 of the dataset. The value of EF is obtained by calculating the ratio between the number of common vehicles that interact with both a trustor i and a trustee j, and the total number of vehicles that interact with a trustor over a given timestamp in an IoV network (Cheong et al., 2024a). In other words, a higher number of shared interacting vehicles (i.e., $EF = 1$) indicates a stronger level of familiarity between a trustor and a trustee.

ii. *Internal Familiarity (IF)* – The internal familiarity ($0 \leq IF \leq 1$) manifests the extent of interaction frequency between a trustor i and a trustee j, and is recorded in column 9 of the dataset. The value of IF is determined by quantifying the frequency of interactions between a trustor and a trustee over a given timestamp in an IoV network. In other words, a higher interaction frequency (i.e., $IF = 1$) indicates a stronger familiarity between the two parties (trustor and trustee).

5.3.6 Reward / Punishment (RP)

The reward / punishment ($0 \leq RP \leq 1$) is employed in order to ascertain the degree of a reward or a penalty allocated to a trustee j based on its conduct in an IoV network. Specifically, a trustee j is rewarded by a trustor i for exhibiting cooperation, honesty, and reporting critical events, whereas, it is penalized for any sort of a misconduct (Sagar et al., 2020b). The RP is determined by taking into consideration the PDR, and a metric that accounts for both positive and negative interactions between a trustor and a trustee. It is thus represented in column 10 of the dataset.

5.3.7 Context

Context plays an indispensable role for ascertaining the trust of a trustee in an IoV network since most of the other trust parameters are directly impacted owing to the same (Mao et al., 2023). It provides specific information regarding the settings, wherein interactions take place between a trustor i and a trustee j in an IoV network, i.e., network stability, and temporal and spatial aspects. In the context of this particular dataset, the context ($0 \leq Context \leq 1$) implies the network communication quality segregated into four classes implying poor, medium, good, and excellent. The corresponding values pertinent to these four classes are depicted in column 11 of the dataset.

Figures 5.4–5.8 depict the packet delivery ratio, similarity, familiarity, reward / punishment, and context-related scores of each of the 79 vehicles in an IoV network at their most recent respective time instance. Additionally, Table 5.1 delineates the values of all of the 9 trust parameters introduced in this particular dataset so as to enable the readers to have a comprehensive understanding of the same.

The TM – IoV dataset comprises multiple parameters with diverse statistical characteristics. Specifically, PDR ranges from 0.1054 to 0.9967 with a mean of 0.5561. The similarity varies between 0.1539 and 0.9078 yielding an average of 0.6891. The ES follows a binary distribution with values of either 0 or 1 and a mean of 0.4682. In contrast, IS spans from 0.2796 to 0.8157 with an average of 0.5935. Familiarity ranges from 0.0835 to 0.6801 resulting in a mean of 0.3548. The EF exhibits a broad range from 0.0061 to 1 with an average of 0.4232, whereas, IF is more constrained and varies between 0.1525 and 0.3602 yielding a mean of 0.2894. The RP ranges from 0.0415 to 0.9934 with an average of 0.5124. Finally, context assumes discrete values of 0, 0.4, 0.6, and 0.8 resulting in a mean of 0.3488.

The mean score across all trust parameters is 0.5124. Amongst these parameters, similarity possesses the highest mean value of 0.6891, whereas, IF records the lowest mean score of 0.2894. With respect to the dispersion, the overall variance is 0.0943. ES demonstrates

the highest variance of 0.2142, thereby reflecting greater variability in its scores, whereas, IS exhibits the lowest variance of 0.0314 thus indicating a more tightly clustered distribution. Overall, the proposed trust-based IoV dataset manifest a standard deviation of 0.3071. These computed statistics provide a detailed overview of the distribution and central tendencies for each trust parameter in the dataset.

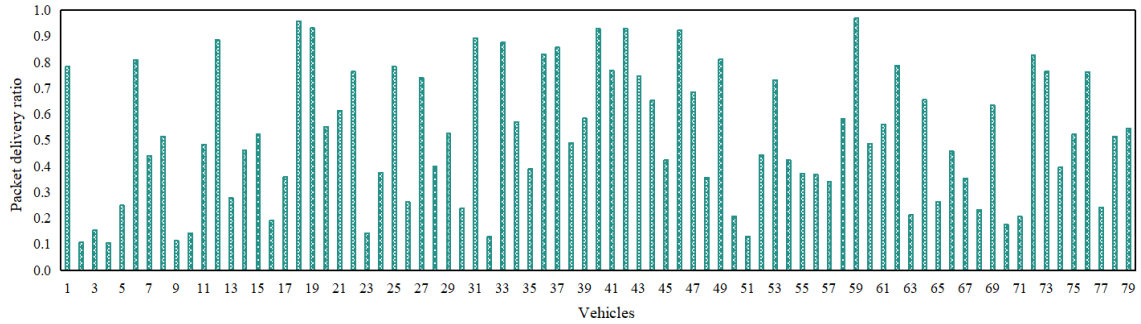

Figure 5.4 Packet Delivery Ratios of 79 Vehicles in an IoV Network.

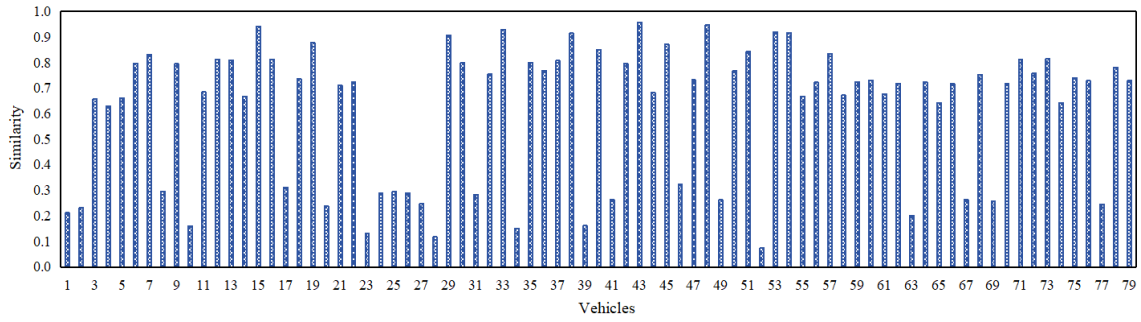

Figure 5.5 Similarity-related Values of 79 Vehicles in an IoV Network.

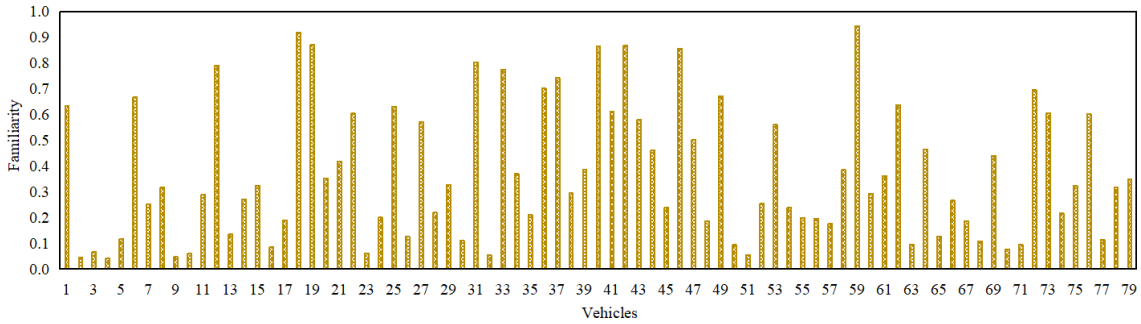

Figure 5.6 Familiarity-related Values of 79 Vehicles in an IoV Network.

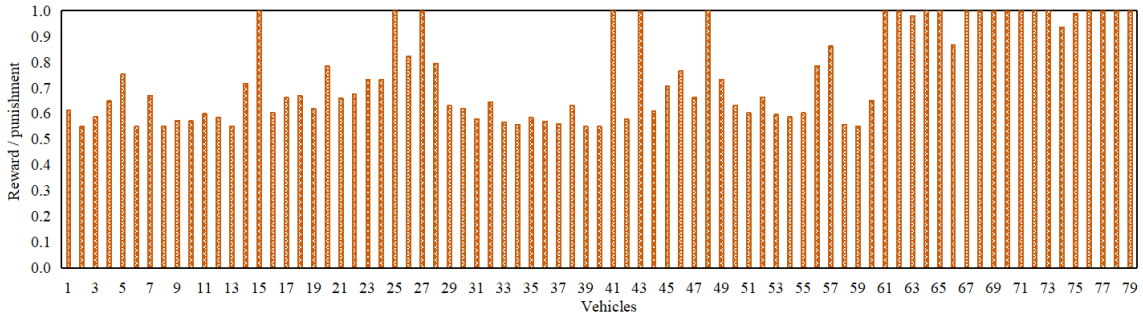

Figure 5.7 Reward / Punishment-related Values of 79 Vehicles in an IoV Network.

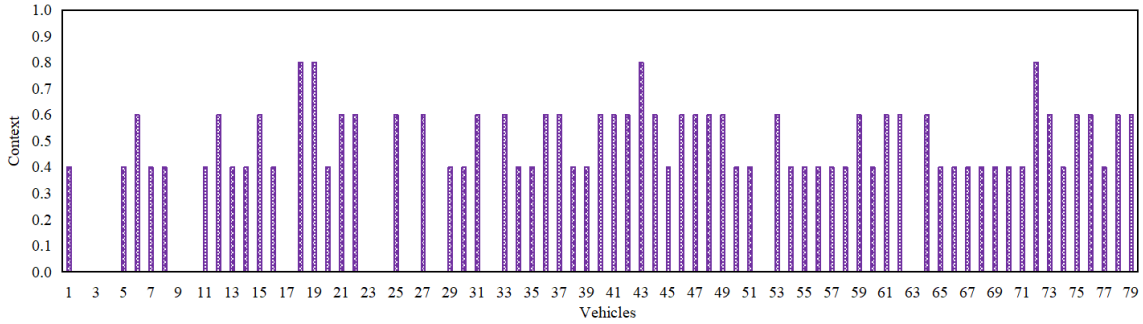

Figure 5.8 Context-related Values of 79 Vehicles in an IoV Network.

5.4 Summary

The manuscript-at-hand employs Java to design a trust-based IoV simulator which ascertains the trust values of vehicles in an IoV network. The trust-based IoV dataset obtained via this simulator is the first of its kind and encompasses nine salient trust parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward / punishment, and context. The underlying rationale of the said trust parameters lies in their effectiveness to investigate dynamic interactions between trustors and trustees in an IoV network, thereby offering valuable insights into the behavior of the same and a foundation for researchers from both academia and industry to utilize and expand upon. In the near future, a trust-based IoV testbed would be employed to (a) ascertain the parameters introduced in this dataset via realistic interactions and (b) simulate various intricate IoV-based trust attacks, i.e., self-promoting attacks, on-off attacks, opportunistic service attacks, bad mouthing attacks, and good mouthing attacks.

Table 5.1 A Snapshot of Values Pertinent to the Trust Parameters, i.e., Packet Delivery Ratio – PDR, Similarity – Sim, External Similarity – ES, Internal Similarity – IS, Familiarity – Fam, External Familiarity – EF, Internal Familiarity – IF, Reward / Punishment – RP, and Context, in the Trust-based IoV Dataset.

Trustor	Trustee	PDR	Sim	ES	IS	Fam	EF	IF	RP	Context
0	1	0.7113	0.6833	1	0.3666	0.6801	1.0000	0.3602	0.5329	0.6
0	10	0.9625	0.9047	1	0.8094	0.6083	1.0000	0.2166	0.9271	0.8
0	78	0.7849	0.2117	0	0.4235	0.6138	1.0000	0.2276	0.6330	0.4
5	9	0.7617	0.7646	1	0.5292	0.7765	1.0000	0.5529	0.6002	0.6
5	25	0.1275	0.7946	1	0.5892	0.6257	1.0000	0.2513	0.0533	0.4
5	65	0.9199	0.7658	1	0.5315	0.5569	1.0000	0.1138	0.8491	0.6
9	10	0.7832	0.4056	0	0.8112	1.0000	1.0000	1.0000	0.6305	0.6
9	37	0.1610	0.9599	1	0.9199	0.5500	1.0000	0.1000	0.0696	0.4
9	70	0.4428	0.8090	1	0.6581	0.6116	1.0000	0.2232	0.2536	0.4
17	21	0.2089	0.4289	0	0.8578	0.9807	1.0000	0.9614	0.0947	0.4
17	53	0.8233	0.7468	1	0.4935	0.6421	1.0000	0.2841	0.6900	0.6

Table 5.1 continued

Trustor	Trustee	PDR	Sim	ES	IS	Fam	EF	IF	RP	Context
17	59	0.6767	0.6915	1	0.3830	0.6421	1.0000	0.2841	0.4898	0.6
23	24	0.9312	0.8760	1	0.7519	1.0000	1.0000	1.0000	0.8693	0.8
23	67	0.3746	0.2880	0	0.5760	0.7328	1.0000	0.4656	0.2004	0.0
23	70	0.8733	0.7228	1	0.4456	0.6758	1.0000	0.3516	0.7694	0.6
27	40	0.9835	0.8466	1	0.6933	0.8098	1.0000	0.6196	0.9674	0.8
27	53	0.3995	0.1174	0	0.2348	0.7963	1.0000	0.5926	0.2191	0.0
27	74	0.7684	0.7259	1	0.4519	0.7694	1.0000	0.5388	0.6095	0.6
35	36	0.7692	0.1149	0	0.2298	0.6487	1.0000	0.2973	0.6107	0.4
35	37	0.5302	0.8996	1	0.7993	0.8904	1.0000	0.7807	0.3314	0.6
35	54	0.1979	0.7465	1	0.4929	0.6607	1.0000	0.3213	0.0887	0.4
40	41	0.5738	0.7033	1	0.4067	0.5661	1.0000	0.1321	0.3747	0.6
40	45	0.3765	0.6316	1	0.2632	0.6867	1.0000	0.3733	0.2018	0.4

Table 5.1 continued

Trustor	Trustee	PDR	Sim	ES	IS	Fam	EF	IF	RP	Context
40	59	0.7693	0.2638	0	0.5276	1.0000	1.0000	1.0000	0.6108	0.6
43	45	0.4167	0.8005	1	0.6009	0.5899	1.0000	0.1797	0.2325	0.4
43	52	0.2337	0.7170	1	0.4339	0.6113	1.0000	0.2225	0.1086	0.4
43	58	0.9459	0.6806	1	0.3611	0.8295	1.0000	0.6590	0.8961	0.8
50	52	0.4822	0.7346	1	0.4692	1.0000	1.0000	1.0000	0.2873	0.6
50	55	0.5339	0.8764	1	0.7527	1.0000	1.0000	1.0000	0.3350	0.6
50	62	0.7857	0.8393	1	0.6785	0.6659	1.0000	0.3317	0.6341	0.6
54	57	0.6790	0.8617	1	0.7234	1.0000	1.0000	1.0000	0.4926	0.6
54	61	0.5491	0.8709	1	0.7417	0.7000	1.0000	0.4000	0.3498	0.6
54	75	0.3732	0.6680	1	0.3360	0.6025	1.0000	0.2049	0.1944	0.4
60	61	0.6867	0.9094	1	0.8187	1.0000	1.0000	1.0000	0.5020	0.6
60	63	0.4465	0.8510	1	0.7020	0.6292	1.0000	0.2583	0.2567	0.4

Table 5.1 continued

Trustor	Trustee	PDR	Sim	ES	IS	Fam	EF	IF	RP	Context
60	75	0.3603	0.9066	1	0.8131	0.6722	1.0000	0.3444	0.1900	0.4
63	65	0.8792	0.7572	1	0.5145	1.0000	1.0000	1.0000	0.7792	0.8
63	67	0.6562	0.7231	1	0.4462	1.0000	1.0000	1.0000	0.4653	0.6
63	74	0.4972	0.9154	1	0.8307	0.6249	1.0000	0.2497	0.3007	0.4
70	71	0.5665	0.7666	1	0.5332	0.5753	1.0000	0.1505	0.3672	0.4
70	73	0.5879	0.7530	1	0.5059	0.6969	1.0000	0.3937	0.3893	0.6
70	76	0.9644	0.1530	0	0.3060	0.9343	1.0000	0.8685	0.9307	0.6
74	75	0.1220	0.7480	1	0.4960	0.5500	1.0000	0.1000	0.0507	0.0
74	77	0.5229	0.7413	1	0.4826	0.9888	1.0000	0.9775	0.3245	0.6
74	78	0.2091	0.7263	1	0.4526	1.0000	1.0000	1.0000	0.0948	0.4

CHAPTER 6

CONCLUDING REMARKS AND FUTURE WORKS

This chapter summarizes the salient research contributions pertinent to this PhD dissertation and subsequently delineates future works in the context of the Internet of Vehicles (IoV)-based trust management.

6.1 Concluding Remarks

The IoV is an indispensable constituent of the Internet of Things, wherein vehicles not only interact amongst one another but also with various network entities in order to realize a number of safety-critical and non-safety (infotainment) applications via vehicle-to-everything communication. The resilience of such a network is, therefore, of the utmost essence to ensure safety, reliability, and efficacy of the modern-day transportation systems. However, this is itself an extremely challenging chore since IoV networks are highly dynamic and distributed in nature, and are prone to a number of both external and internal attacks. Whilst the external attacks can be tackled by the conventional cryptography-based schemes, the internal attacks are the ones that are capable of jeopardizing the entire IoV network, thereby putting the life of the drivers, passengers, and the vulnerable pedestrians at high risk. This PhD dissertation, accordingly, aims to enhance the resilience of an IoV network from the perspective of trust management in order to ascertain the trustworthiness of vehicles in an IoV network so as to mitigate the internal attacks.

Chapter 2 of this PhD dissertation presented a comprehensive discussion pertinent to the notion of trust in an IoV network followed by an in-depth analysis of the trust management process. It further succinctly offered a comparative analysis of the strengths and limitations of the state-of-the-art trust management models. Chapter 3 envisaged an intelligent state-of-the-art machine learning-based trust management mechanism, MESMERIC, for an IoV network

that takes into account direct trust, indirect trust, and context to ascertain the trustworthiness of vehicles so as to segregate the trustworthy vehicles from the untrustworthy ones by means of an optimal decision boundary. Experimental results demonstrated that the envisaged trust mechanism significantly outperformed both machine learning-based trust mechanisms that do not consider context (El-Sayed et al., 2020)(Gyawali et al., 2020) and conventional (weighted sum) trust-based mechanisms (Fabi and Thampi, 2022a) in terms of precision.

Chapter 4 introduced an IoV-based trust model encompassing both direct trust and indirect trust for distinguishing the trust-based attacks in an IoV network. The behavior of the vehicles has been analyzed vis-à-vis time in a bid to ascertain several trust-based attacks, i.e., zig-zag attacks, self-promoting attacks, on-off attacks, and opportunistic attacks. The experimental results demonstrate that the envisaged trust-based model can ascertain the impact of multiple trust-based attacks on the vehicles across the entire time span of an IoV network in a highly efficacious manner. Finally, Chapter 5 introduced a first-of-its-kind dedicated public trust-based IoV dataset encompassing 96,707 interactions among 79 vehicles, i.e., both honest and intelligent malicious ones. Nine key trust parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward / punishment, and context, have been identified in the said IoV dataset. The availability of this dataset facilitates subsequent research in this emerging and promising domain. In summary, this PhD dissertation has successfully achieved its three primary research objectives.

6.2 Future Works

Whilst the notion of trust in the context of IoV networks has gained considerable research attention by researchers in both academia and industry in the past decade or so, there are still a number of prevailing issues which mandates careful consideration. This section, therefore, is an effort to outline salient open research directions pertinent to IoV-based trust management.

6.2.1 Intelligent Trust Aggregation

Trust aggregation involves aggregating several context-dependent trust attributes (parameters) into a single optimal trust score in a bid to ascertain the trustworthiness of a particular vehicle or vehicles in an IoV network. Accordingly, conventional trust-based mechanisms primarily employ static weights for the said purpose. However, static weights cannot realize the impact of the influential trust attributes in the trust aggregation process (Sagar et al., 2024a)(Azizi and Shokrollahi, 2024). Owing to the same, learning-based trust aggregation mechanisms have been recently envisaged in the research literature (Siddiqui et al., 2023a)(Wang et al., 2023a). Nevertheless, learning-based trust mechanisms require substantial data and are prone to data bias too. It is, therefore, indispensable to design intelligent trust aggregation mechanisms that are not only robust but can further take into consideration the underlying dynamic context for ascertaining optimal trust scores in an IoV network (Alalwany and Mahgoub, 2024).

6.2.2 Intelligent Adaptive Trust Thresholds

Existing trust-based management mechanisms primarily rely on predefined trust thresholds for segregating the trustworthy vehicles from the untrustworthy ones. Accordingly, a vehicle with trust above the predefined threshold is regarded as trustworthy, whereas, the one below the predefined threshold is considered as untrustworthy (Chen et al., 2024)(Qi et al., 2024). Therefore, an optimal and intelligent trust threshold is indispensable for not only detecting the malicious vehicles but to subsequently evict them as soon as possible from an IoV network. This is particularly of the essence since (a) if a predefined threshold is set unrealistically high, it would result in mistakenly evicting the honest vehicles or (b) if a predefined threshold is set unnecessarily low, it would allow the malicious vehicles to realize their respective malicious gains. An adaptive trust threshold is thus one of the possible solutions for addressing this issue, however, the same would also result in an excessive network

management overhead since it involves monitoring and adaptively adjusting the threshold for each vehicle at regular intervals. Therefore, there is a dire need of envisaging intelligent adaptive threshold mechanisms so as to tackle this critical challenge (AlMarshoud et al., 2024)(Wang et al., 2023d).

6.2.3 Lifespan of the Trust

Owing to the highly dynamic and distributed nature of an IoV network, vehicles interact with and subsequently assign trust to numerous other vehicles during the course of their respective trajectory. Accordingly, it is not possible for a particular vehicle to store the trust of all the vehicles it has interacted with primarily due to the onboard storage constraints. Moreover, a vehicle might interact with another vehicle merely once, thereby making it highly impractical to keep a record of such an interaction after a certain duration of time. Therefore, intelligent lifespan- and decay-related mechanisms should be envisaged for (a) not only ascertaining the lifetime of the trust vis-à-vis context but (b) to also decay the same by an optimal proportion in case of no recent further interactions (Huber and Kandah, 2024)(Mahmood, 2021).

6.2.4 Resiliency vis-à-vis Dynamic Attack Vectors

Whilst trust remains an optimal solution for mitigating internal attacks in an IoV network, it is itself prone to a number of trust-based attacks, including but not limited to, self-promoting attacks, on-off attacks, zig-zag attacks, opportunistic attacks, ballot stuffing attacks (good-mouthing attacks), and bad-mouthing attacks that are instigated by the malicious vehicles to attain considerable privileges so as to jeopardize the entire IoV network for their respective malicious gains. This becomes even more critical if and when an attacker (malicious vehicle) launches multiple dynamic attacks vis-à-vis dynamic contexts in order to avoid detection and subsequent eviction from an IoV network. It is, therefore, indispensable to

devise intelligent threat models that have the potential to identify the underlying vulnerabilities within an IoV network that are exploited by the attackers to instigate such sort of sophisticated attacks (Qi et al., 2024)(Sagar, 2023).

6.2.5 IoV-based Trust Testbed

An IoV-based trust testbed is paramount for evaluating trust models in this particular domain. Whilst numerous trust models have already been envisaged and subsequently evaluated via a wide range of simulation techniques, these simulations often do not reflect the real-world realistic environment pertinent to an IoV network. Also, existing trust models take into consideration multiple static trust attributes and are evaluated via standardized metrics, however, they lack a comprehensive and realistic trust testbed that can ascertain their respective performance vis-à-vis dynamic contexts and subsequently compare their respective performance vis-à-vis several other prevailing trust models. Hence, designing of an IoV-based trust testbed that not only takes into account the underlying environmental considerations but can also intelligently evaluate the complex interactions between the dynamic network entities is imperative for strengthening the resiliency of an IoV network (Drobot et al., 2023).

6.2.6 Leveraging Large Language Models for Advanced Trust Management

The emergence of the Large Language Models (LLMs) presents a promising opportunity for strengthening the resilience of the IoV-based trust management systems. Leveraging their advanced natural language understanding and contextual reasoning capabilities, LLMs can intelligently interpret complex, multi-modal data, i.e., ranging from vehicular sensor readings and traffic reports to driver and passenger intent, across diverse IoV environments. A critical research gap remains in exploring how LLMs can dynamically adapt trust evaluation policies in response to unstructured incident reports and real-time risk assessments. Recent studies highlight the potential of LLMs to directly analyze sequences of vehicle safety mes-

sages for real-time misbehavior detection, thereby achieving high accuracy and underscoring their role as key security analysis engines (Hamhoum and Cherkaoui, 2025). Nevertheless, integrating LLMs in resource-constrained and latency-sensitive IoV settings mandates designing lightweight LLM architectures for the on-board units and the development of secure, privacy-preserving mechanisms for querying cloud-based LLMs (Shu et al., 2024)(Huang et al., 2025).

6.2.7 Integration with Emerging Technologies

Future work should focus on integrating trust management mechanisms with emerging and promising paradigm of 6G networks to address scalability, security, and resilience at unprecedented scales. The ultra-high data rates, ultra-low latency, and pervasive connectivity of 6G would enable the real-time exchange of rich, multi-dimensional trust evidence for supporting more fine-grained and adaptive trust computations. Moreover, network-native AI in 6G could optimize trust dissemination by intelligently selecting reliable and context-aware nodes for indirect trust aggregation, in turn, enhancing both efficacy and accuracy (Saha and Chandrakar, 2025). In parallel, blockchain technology offers a decentralized and tamper-resistant trust infrastructure for IoV for securely recording vehicle interactions and reputation histories. By improving transparency and mitigating risks from central failures, data tampering, and collusion, blockchain, coupled with smart contracts, could automate trust management processes encompassing rewards, penalties, and trust score updates in a reliable and auditable manner (Surapaneni et al., 2025). Additionally, quantum computing is also capable of revolutionizing IoV-based trust management by enabling ultra-fast optimization and inference over massive, high-dimensional trust graphs, thereby allowing real-time, globally optimal trust evaluation across vehicles and infrastructure.

This PhD research yielded several key lessons regarding the security of highly dynamic and distributed IoV networks. First, trust management is not an auxiliary mechanism but a

core security primitive indispensable for real-time differentiation between honest and malicious vehicles. Second, effective trust assessment requires the aggregation of heterogeneous and context-aware evidence rather than reliance on single-factor metrics. Third, trust models must be adaptive and time-aware to remain effective against sophisticated trust-based attacks which evolve over time. Finally, the development of a comprehensive, parameter-rich dataset demonstrated that empirically grounded, data-driven approaches are critical for building resilient and practical IoV security solutions. Collectively, these insights indicate that system resilience emerges from continuous, intelligent trust evaluation rather than static architectural robustness alone.

Beyond the specific domain of IoV, the principles, methodologies, and frameworks developed in this PhD dissertation demonstrate considerable cross-domain applicability. The fundamental challenge of establishing trust among distributed, dynamic, and potentially untrustworthy entities is common to a wide range of cyber-physical systems. Accordingly, the contributions of this PhD dissertation can be directly adapted to enhance security and reliability in general Internet of Things (IoT) deployments, regulate socially-aware interactions in the Social Internet of Things (SIoT), and safeguard critical communications in Industry 4.0 environments, i.e., smart factories and automated supply chains. Moreover, the envisaged models are applicable to various emerging domains, e.g., smart grids, collaborative drone networks, and edge computing ecosystems, thereby highlighting the broad relevance and transformative potential of the research-at-hand for the development of resilient and trustworthy intelligent systems.

REFERENCES

Aalibagi, S., Mahyar, H., Movaghar, A., & Stanley, H. E. (2022). A Matrix Factorization Model for Hellinger-Based Trust Management in Social Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2274-2285.

Abbas, G., Ullah, S., Waqas, M., Abbas, Z. H., & Bilal, M. (2022). A Position-Based Reliable Emergency Message Routing Scheme for Road Safety in VANETs. *Computer Networks*, *213,* 109097.

Abdel-Hakim, A. E., Deabes, W., Bouazza, K. E., & Hedar, A.-R. (2024). Dynamic Deployment of Mobile Roadside Units in Internet of Vehicles. *IEEE Access*, *12,* 155534-155548.

Abualigah, L., Yousri, D., Abd Elaziz, M., Ewees, A. A., Al-qaness, M. A., & Gandomi, A. H. (2021). Aquila Optimizer: A Novel Meta-Heuristic Optimization Algorithm. *Computers Industrial Engineering*, *157,* 107250.

Adhikari, M., Munusamy, A., Hazra, A., Menon, V. G., Anavangot, V., & Puthal, D. (2022). Security in Edge-Centric Intelligent Internet of Vehicles: Issues and Remedies. *IEEE Consumer Electronics Magazine*, *11*(6), 24-31.

Afrin, T. & Yodo, N. (2020). A Survey of Road Traffic Congestion Measures Towards a Sustainable and Resilient Transportation System. *Sustainability*, *12*(11), 4660.

Ahmad, F., Franqueira, V. N. L., & Adnane, A. (2018). TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks. *IEEE Access*, *6,* 28643-28660.

Ahmad, F., Kurugollu, F., Adnane, A., Hussain, R., & Hussain, F. (2020). MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles. *IEEE Internet of Things Journal*, *7*(4), 3310-3322.

Ahmad, F., Kurugollu, F., Kerrache, C. A., Sezer, S., & Liu, L. (2021). NOTRINO: A NOvel Hybrid TRust Management Scheme for INternet-of-Vehicles. *IEEE Transactions on Vehicular Technology*, *70*(9), 9244-9257.

Ahmad, U., Han, M., Jolfaei, A., Jabbar, S., Ibrar, M., Erbad, A., Herbert Song, H., & Alkhrijah, Y. (2024). A Comprehensive Survey and Tutorial on Smart Vehicles: Emerging Technologies, Security Issues, and Solutions Using Machine Learning. *IEEE Transactions on Intelligent Transportation Systems*, *25*(11), 15314-15341.

Akwirry, B., Bessis, N., Malik, H., & McHale, S. (2022). A Multi-Tier Trust-Based Security Mechanism for Vehicular Ad-Hoc Network Communications. *Sensors*, *22*(21).

Alagha, A., Kadadha, M., Mizouni, R., Singh, S., Bentahar, J., & Otrok, H. (2025). UAV-Assisted Internet of Vehicles: A Framework Empowered by Reinforcement Learning and Blockchain. *Vehicular Communications*, *52,* 100874.

Alalwany, E. & Mahgoub, I. (2024). Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions. *Sensors*, *24*(2).

Alam, I., Manjul, M., Pathak, V., Mala, V., Mangal, A., Thakur, H. K., & Sharma, D. K. (2024). Efficient and Secure Graph-Based Trust-Enabled Routing in Vehicular Ad-Hoc Networks. *Mobile Networks and Applications*, *29*(2), 786-801.

Aldhanhani, T., Abraham, A., Hamidouche, W., & Shaaban, M. (2024). Future Trends in Smart Green IoV: Vehicle-to-Everything in the Era of Electric Vehicles. *IEEE Open Journal of Vehicular Technology*, *5,* 278-297.

AlMarshoud, M., Sabir Kiraz, M., & H. Al-Bayatti, A. (2024). Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions. *ACM Computing Surveys*, *56*(10).

Alnasser, A., Sun, H., & Jiang, J. (2020). Recommendation-Based Trust Model for Vehicle-to-Everything (V2X). *IEEE Internet of Things Journal*, *7*(1), 440-450.

Alshahrani, M. M. (2024). A Verifiable Discrete Trust Model (VDTM) Using Congruent Federated Learning (CFL) for Social Internet of Vehicles. *IEEE Open Journal of Vehicular Technology*, *5,* 1441-1456.

Aman, M. N., Javaid, U., & Sikdar, B. (2021). A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles. *IEEE Internet of Things Journal*, *8*(2), 1123-1139.

Amari, H., Houda, Z. A. E., Khoukhi, L., & Belguith, L. H. (2023). Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey. *IEEE Access*, *11,* 47659-47680.

Anupama, K. & Nagaraj, R. (2025). Secure Vehicle-to-Vehicle Communication Using Routing Protocol Based on Trust Authentication Secure Sugeno Fuzzy Inference System Scheme. *Recent Patents on Engineering*, *19*(1).

Arthurs, P., Gillam, L., Krause, P., Wang, N., Halder, K., & Mouzakitis, A. (2022). A Taxonomy and Survey of Edge Cloud Computing for Intelligent Transportation Systems and Connected Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 6206-6221.

Aslan, M. & Sen, S. (2023). A Dynamic Trust Management Model for Vehicular Ad Hoc Networks. *Vehicular Communications*, *41,* 100608.

Atwa, R. J., Flocchini, P., & Nayak, A. (2021a). A Fog-Based Reputation Evaluation Model for VANETs. In *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–7.

Atwa, R. J., Flocchini, P., & Nayak, A. (2021b). RTEAM: Risk-Based Trust Evaluation Advanced Model for VANETs. *IEEE Access*, *9,* 117772-117783.

Awotunde, J. B. et al. (2023). A Multi-level Random Forest Model-based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks. *International Journal of Computational Intelligence Systems*, *16*(1), 31.

Ayed, S., Hbaieb, A., & Chaari, L. (2023). Blockchain and Trust-Based Clustering Scheme for the IoV. *Ad Hoc Networks*, *142,* 103093.

Azizi, M. & Shokrollahi, S. (2024). RTRV: An RSU-Assisted Trust-Based Routing Protocol for VANETs. *Ad Hoc Networks*, *154,* 103387.

Bhargava, A. & Verma, S. (2022). DUEL: Dempster Uncertainty-Based Enhanced- Trust Level Scheme for VANET. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), 15079-15090.

Bozkurt, E. et al. (2025). Robust Classification Under Noisy Labels: A Geometry-aware Reliability Framework for Foundation Models. *arXiv preprint arXiv:2508.00202*.

Byeon, H., Seno, M. E., Srivastava, A. K., AlGhamdi, A., Keshta, I., Soni, M., Prasad, K. D. V., Abdurakhimova, D., & Bhatt, M. W. (2025). Trust Management Scheme for Securing Vehicular Ad Hoc Networks Against Malicious Nodes and False Message Anomaly. *Transactions on Emerging Telecommunications Technologies*, *36*(4), e70110.

Cao, T., Yi, J., Wang, X., Xiao, H., & Xu, C. (2024). Interaction Trust-Driven Data Distribution for Vehicle Social Networks: A Matching Theory Approach. *IEEE Transactions on Computational Social Systems*, *11*(3), 4071-4086.

Che, H., Duan, Y., Li, C., & Yu, L. (2022). On Trust Management in Vehicular Ad-Hoc Networks: A Comprehensive Review. *Frontiers in the Internet of Things*, *1,* 995233.

Chen, C., Wang, L., & Shi, Q. (2026). Integration of Blockchain and Federated Learning for Data Sharing in Internet of Vehicles. *IEEE Internet of Things Journal*, *13*(1), 678-694.

Chen, C.-M., Li, Z., Kumari, S., Srivastava, G., Lakshmanna, K., & Gadekallu, T. R. (2023a). A Provably Secure Key Transfer Protocol for the Fog-Enabled Social Internet of Vehicles Based on a Confidential Computing Environment. *Vehicular Communications*, *39,* 100567.

Chen, I.-R., Bao, F., & Guo, J. (2016a). Trust-Based Service Management for Social Internet of Things Systems. *IEEE Transactions on Dependable and Secure Computing*, *13*(6), 684-696.

Chen, I.-R., Guo, J., & Bao, F. (2016b). Trust Management for SOA-Based IoT and Its Application to Service Composition. *IEEE Transactions on Services Computing*, *9*(3), 482-495.

Chen, J. & Wang, X. (2021). TCNS: An Efficient Trusted Cooperative Node Selection Model for Internet of Vehicles. In *2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–6.

Chen, J., Wang, X., & Shen, X. (2024). RTE: Rapid and Reliable Trust Evaluation for Collaborator Selection and Time-Sensitive Task Handling in Internet of Vehicles. *IEEE Internet of Things Journal*, *11*(7), 12278-12291.

Chen, J.-M., Li, T.-T., & Panneerselvam, J. (2019). TMEC: A Trust Management Based on Evidence Combination on Attack-Resistant and Collaborative Internet of Vehicles. *IEEE Access*, *7,* 148913-148922.

Chen, Y.-C., Jhong, S.-Y., & Hsia, C.-H. (2023b). Roadside Unit-Based Unknown Object Detection in Adverse Weather Conditions for Smart Internet of Vehicles. *ACM Transactions on Management Information Systems*, *13*(4).

Chen, Z., Ling, R., Huang, C.-M., & Zhu, X. (2016c). A Scheme of Access Service Recommendation for the Social Internet of Things. *International Journal of Communication Systems*, *29*(4), 694-706.

Cheong, C., Song, Y., Cao, Y., Zhang, Y., Cai, B., & Ni, Q. (2024a). Multidimensional Trust Evidence Fusion and Path-Backtracking Mechanism for Trust Management in VANETs. *IEEE Internet of Things Journal*, *11*(10), 18619-18634.

Cheong, C., Song, Y., Cao, Y., Zhang, Y., Wang, H., & Ni, Q. (2024b). DCACA: Dual-Model Consensus-Based Anti-Risk Confidence Allocation Trust Management in IoVs. *IEEE Internet of Things Journal*, *12*(2), 1890-1906.

Cheong, C., Song, Y., Zhang, Y., Cao, Y., Leow, C. Y., & Wang, X. (2024c). A Path-Backtracking-Based Trust Management Scheme for VANETs. In *2024 IEEE* 99^{th} *Vehicular Technology Conference (VTC2024-Spring)*, pages 1–6.

Choukhairi, M., Fakhri, Y., & Amnai, M. (2022). TTIDS : A Time-Driven Trust Based Intrusion Detection System for IoT Networks. In *2022* 9^{th} *International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pages 1–8.

Cui, H. & Yi, X. (2024). Secure Internet of Things in Cloud Computing via Puncturable Attribute-Based Encryption With User Revocation. *IEEE Internet of Things Journal*, *11*(2), 3662-3670.

Dai, S., Li, S., Tang, H., Ning, X., Fang, F., Fu, Y., Wang, Q., & Cheng, L. (2024). MARP: A Cooperative Multiagent DRL System for Connected Autonomous Vehicle Platooning. *IEEE Internet of Things Journal*, *11*(20), 32454-32463.

Dang, X., Zhang, G., Sun, K., & Li, Y. (2025). A Trust Model for VANETs Using Malicious-Aware Multiple Routing. *Computers Security*, *148,* 104145.

Di Pietro, R., Guarino, S., Verde, N., & Domingo-Ferrer, J. (2014). Security in Wireless Ad-Hoc Networks – A Survey. *Computer Communications*, *51,* 1-20.

Ding, F., Lin, H., Wen, C., Liu, G., & Li, Z. (2024). Research on Internet of Vehicles Computing Resource Allocation Algorithm Based on Edge Computing. In *2024* 4^{th} *International*

Conference on Neural Networks, Information and Communication Engineering (NNICE), pages 1043–1047.

Drobot, A., Zhang, T., Buonarosa, M. L., Kargl, F., Schwinke, S., & Sikdar, B. (2023). The Internet of Vehicles (IoV) – Security, Privacy, Trust, and Reputation Management for Connected Vehicles. *IEEE Internet of Things Magazine*, *6*(2), 6-16.

Du, G., Cao, Y., Li, J., Zhuang, Y., Chen, X., Li, Y., & Chen, J. (2024). A Blockchain-Based Trust-Value Management Approach for Secure Information Sharing in Internet of Vehicles. *IEEE Internet of Things Journal*, *11*(1), 333-344.

Dutta, A., Samaniego Campoverde, L. M., Tropea, M., & De Rango, F. (2024). A Comprehensive Review of Recent Developments in VANET for Traffic, Safety & Remote Monitoring Applications. *Journal of Network and Systems Management*, *32*(4), 73.

El-Sayed, H., Alexander, H., Kulkarni, P., Khan, M. A., Noor, R. M., & Trabelsi, Z. (2022). A Novel Multifaceted Trust Management Framework for Vehicular Networks. *IEEE Transactions on Intelligent Transportation Systems*, *23*(11), 20084-20097.

El-Sayed, H., Ignatious, H. A., Kulkarni, P., & Bouktif, S. (2020). Machine Learning Based Trust Management Framework for Vehicular Networks. *Vehicular Communications*, *25,* 100256.

Elsagheer, M. S. A. & AlShalfan, K. A. (2021). Intelligent Traffic Management System Based on the Internet of Vehicles (IoV). *Journal of Advanced Transportation*, *2021*(1), 4037533.

Fabi, A. & Thampi, S. M. (2022a). A Trust Management Framework Using Forest Fire Model to Propagate Emergency Messages in the Internet of Vehicles (IoV). *Vehicular Communications*, *33,* 100404.

Fabi, A. K. & Thampi, S. M. (2022b). A Psychology-Inspired Trust Model for Emergency Message Transmission on the Internet of Vehicles (IoV). *International Journal of Computers and Applications*, *44*(5), 480-490.

Fang, W., Zhang, W., Liu, Y., Yang, W., & Gao, Z. (2020). BTDS: Bayesian-Based Trust Decision Scheme for Intelligent Connected Vehicles in VANETs. *Transactions on Emerging Telecommunications Technologies*, *31*(12), e3879.

Farahbakhsh, B., Fanian, A., & Manshaei, M. H. (2021). TGSM: Towards Trustworthy Group-Based Service Management for Social IoT. *Internet of Things*, *13,* 100312.

Feng, C., Xu, Z., Zhu, X., Klaine, P. V., & Zhang, L. (2023). Wireless Distributed Consensus in Vehicle to Vehicle Networks for Autonomous Driving. *IEEE Transactions on Vehicular Technology*, *72*(6), 8061-8073.

Feng, X., Shi, Q., Xie, Q., & Wang, L. (2021). P2BA: A Privacy-Preserving Protocol With Batch Authentication Against Semi-Trusted RSUs in Vehicular Ad Hoc Networks. *IEEE Transactions on Information Forensics and Security*, *16,* 3888-3899.

Fernandes, C. P., Montez, C., Adriano, D. D., Boukerche, A., & Wangham, M. S. (2023). A Blockchain-Based Reputation System for Trusted VANET Nodes. *Ad Hoc Networks*, *140,* 103071.

Gao, H., Liu, C., Yin, Y., Xu, Y., & Li, Y. (2022). A Hybrid Approach to Trust Node Assessment and Management for VANETs Cooperative Data Communication: Historical Interaction Perspective. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), 16504-16513.

García-Magariño, I., Sendra, S., Lacuesta, R., & Lloret, J. (2019). Security in Vehicles with IoT by Prioritization Rules, Vehicle Certificates, and Trust Management. *IEEE Internet of Things Journal*, *6*(4), 5927-5934.

Gu, W., Liu, Y., Wang, C.-X., Xu, W., Yu, Y., Lu, W.-J., & Zhu, H.-B. (2024). A General 3-D Geometry-Based Stochastic Channel Model for B5G mmWave IIoT. *IEEE Internet of Things Journal*, *11*(2), 3362-3376.

Guo, J., Bilal, M., Qiu, Y., Qian, C., Xu, X., & Raymond Choo, K.-K. (2024). Survey on Digital Twins for Internet of Vehicles: Fundamentals, Challenges, and Opportunities. *Digital Communications and Networks*, *10*(2), 237-247.

Guo, J., Li, X., Liu, Z., Ma, J., Yang, C., Zhang, J., & Wu, D. (2020). TROVE: A Context-Awareness Trust Model for VANETs Using Reinforcement Learning. *IEEE Internet of Things Journal*, *7*(7), 6647-6662.

Gupta, M., Patel, R. B., Jain, S., Garg, H., & Sharma, B. (2023). Lightweight Branched Blockchain Security Framework for Internet of Vehicles. *Transactions on Emerging Telecommunications Technologies*, *34*(11), e4520.

Gyawali, S., Qian, Y., & Hu, R. Q. (2020). Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks. *IEEE Transactions on Vehicular Technology*, *69*(8), 8871-8885.

Haddaji, A., Ayed, S., & Chaari, L. (2022). Federated Learning with Blockchain Approach for Trust Management in IoV. In Barolli, L., Hussain, F., & Enokido, T., editors, *Advanced Information Networking and Applications*, pages 411–423, Cham. Springer International Publishing.

Haider, Z. A., Zeb, A., Islam, A., Rahman, T., Arishi, A., & Ullah, I. (2026). Enhancing IoT Security with Resource-Efficient Cryptography: A Comprehensive Review of Lightweight and Hybrid Algorithms. *Computer Science Review*, *59,* 100861.

Hamhoum, W. & Cherkaoui, S. (2025). MistralBSM: Leveraging Mistral-7B for Vehicular Networks Misbehavior Detection. arXiv. https://arxiv.org/abs/2407.18462.

Han, H., Zhang, M., Xu, Z., Dong, X., & Wang, Z. (2024). Decentralized Trust Management and Incentive Mechanisms for Secure Information Sharing in VANET. *IEEE Access*, *12,* 124414-124427.

Han, S., Wang, F.-Y., Luo, G., Li, L., & Qu, F. (2023). Parallel Surfaces: Service-Oriented V2X Communications for Autonomous Vehicles. *IEEE Transactions on Intelligent Vehicles*, *8*(11), 4536-4545.

Hbaieb, A., Ayed, S., & Chaari, L. (2022). A Survey of Trust Management in the Internet of Vehicles. *Computer Networks*, *203,* 108558.

Honarmand, F. & Keshavarz-Haddad, A. (2024). T-AODV: A Trust-Based Routing Against Black-Hole Attacks in VANETs. *Peer-to-Peer Networking and Applications*, *17*(3), 1309-1321.

Hossain, S., Senouci, S.-M., Brik, B., & Boualouache, A. (2025). A Privacy-Preserving Self-Supervised Learning-Based Intrusion Detection System for 5G-V2X Networks. *Ad Hoc Networks*, *166,* 103674.

Huang, D., Zhang, L., Na, Y., Bu, F., & Li, Z. (2026). A Trust Assessment Method for Intelligent Connected Vehicles Based on Data Consistency Verification Matched with Adaptive Leader Election in a Zero-Trust Framework. *IEEE Transactions on Dependable and Secure Computing*, 1-16.

Huang, F., Li, Q., & Zhao, J. (2022). Trust Management Model of VANETs Based on Machine Learning and Active Detection Technology. In *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pages 412–416.

Huang, S., Li, H., Gu, Y., Hu, X., Li, Q., & Xu, G. (2025). HyperG: Hypergraph-Enhanced LLMs for Structured Knowledge. In *Proceedings of the* 48^{th} *International ACM SIGIR*

Conference on Research and Development in Information Retrieval, SIGIR '25, page 1218–1228, New York, NY, USA. Association for Computing Machinery.

Huber, B. & Kandah, F. (2024). DECAY: Dynamic Evaluation and Component Analysis for Enhancing Trust Management. In *2024 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–6.

Humayun, M., Afsar, S., Almufareh, M. F., Jhanjhi, N. Z., & AlSuwailem, M. (2022). Smart Traffic Management System for Metropolitan Cities of Kingdom Using Cutting Edge Technologies. *Journal of Advanced Transportation*, *2022*(1), 4687319.

Hussain, R., Lee, J., & Zeadally, S. (2021). Trust in VANET: A Survey of Current Solutions and Future Research Opportunities. *IEEE Transactions on Intelligent Transportation Systems*, *22*(5), 2553-2571.

Iqbal, M., Suhail, S., Matulevičius, R., Shah, F. A., Malik, S. U. R., & McLaughlin, K. (2025). IoV-TwinChain: Predictive Maintenance of Vehicles in Internet of Vehicles Through Digital Twin and Blockchain. *Internet of Things*, *30,* 101514.

Ismail, S., Hammad, E., & Iqbal, R. (2025). Towards Holochain-Based Adaptive Trust Management in Social Internet of Vehicles. In *2025 IEEE* 15^{th} *Annual Computing and Communication Workshop and Conference (CCWC)*, pages 878–884.

Jain, A., Kumar, A., Mahadev, Chaudhary, J. K., & Singh, S. (2025). Trust-Based Reliability Scheme for Secure Data Sharing With Internet of Vehicles Networks. *Internet Technology Letters*, *8*(2), e70000.

Jamil, M., Farhan, M., Ullah, F., & Srivastava, G. (2024). A Lightweight Zero Trust Framework for Secure 5G VANET Vehicular Communication. *IEEE Wireless Communications*, *31*(6), 136-141.

Jayasinghe, U., Lee, G. M., Um, T.-W., & Shi, Q. (2019). Machine Learning Based Trust Computational Model for IoT Services. *IEEE Transactions on Sustainable Computing*, *4*(1), 39-52.

Jegatheesan, D. & Arumugam, C. (2024). SIoV-FTFSA-CAOA: A Fuzzy Trust-Based Approach for Enhancing Security and Energy Efficiency in Social Internet of Vehicles. *Wireless Networks*, *30*(4), 2061-2080.

Ji, B., Zhang, X., Mumtaz, S., Han, C., Li, C., Wen, H., & Wang, D. (2020). Survey on the Internet of Vehicles: Network Architectures and Applications. *IEEE Communications Standards Magazine*, *4*(1), 34-41.

Jing, T., Liu, Y., Wang, X., & Gao, Q. (2022). Joint Trust Management and Sharing Provisioning in IoV-Based Urban Road Network. *Wireless Communications and Mobile Computing*, *2022*(1), 6942120.

Junejo, M. H., Rahman, A. A.-H. B. A., Shaikh, R. A., Yusof, K. M., & Sadiah, S. (2023). Trust Model for Reliable Grouping-Based Communications in Vehicular Ad-Hoc Networks. *IEEE Access*, *11,* 124584-124596.

Kaffash, S., Nguyen, A. T., & Zhu, J. (2021). Big Data Algorithms and Applications in Intelligent Transportation System: A Review and Bibliometric Analysis. *International Journal of Production Economics*, *231,* 107868.

Kang, H.-S., Chai, Z.-Y., Li, Y.-L., Huang, H., & Zhao, Y.-J. (2025). Edge Computing in Internet of Vehicles: A Federated Learning Method Based on Stackelberg Dynamic Game. *Information Sciences*, *689,* 121452.

Kaur, G. & Kakkar, D. (2022). Hybrid Optimization Enabled Trust-Based Secure Routing with Deep Learning-Based Attack Detection in VANET. *Ad Hoc Networks*, *136,* 102961.

Kchaou, A., Abassi, R., & Guemara, S. (2020). Towards the performance evaluation of a clustering and trust based security mechanism for vanet. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pages 1–6, Virtual Event, Ireland. ACM.

Kerrache, C. A., Lagraa, N., Hussain, R., Ahmed, S. H., Benslimane, A., Calafate, C. T., Cano, J.-C., & Vegni, A. M. (2019). TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles. *IEEE Internet of Things Journal*, *6*(4), 5870-5877.

Khezri, E., Hassanzadeh, H., Yahya, R. O., & Mir, M. (2025). Security Challenges in Internet of Vehicles (IoV) for ITS: A Survey. *Tsinghua Science and Technology*, *30*(4), 1700-1723.

Kuang, Y., Xu, H., Jiang, R., & Liu, Z. (2022). GTMS: A Gated Linear Unit Based Trust Management System for Internet of Vehicles Using Blockchain Technology. In *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 28–35.

Leng, K. & Li, S. (2022). Distribution Path Optimization for Intelligent Logistics Vehicles of Urban Rail Transportation Using VRP Optimization Model. *IEEE Transactions on Intelligent Transportation Systems*, *23*(2), 1661-1669.

Li, B., Song, X., Dai, T., Wu, W., Zhu, D., Zhai, X., Wen, H., Lin, Q., Chen, H., & Cai, K. (2023a). Trust Management Strategy for Digital Twins in Vehicular Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, *41*(10), 3279-3292.

Li, H., Shan, Q., Zhan, J., & Wang, D. (2021a). A Trust Evaluation Method Based on Environmental Assessment in the Perception Layer of Internet of Vehicles. In *2021* 13^{th} *International Conference on Communication Software and Networks (ICCSN)*, pages 49–54.

Li, J., Li, Y., Cao, C., & Lam, K.-Y. (2022a). Conditional Anonymous Authentication With Abuse-Resistant Tracing and Distributed Trust for Internet of Vehicles. *IEEE Internet of Things Journal*, *9*(11), 8749-8762.

Li, T., Li, C., Luo, J., & Song, L. (2020). Wireless Recommendations for Internet of Vehicles: Recent Advances, Challenges, and Oportunities. *Intelligent and Converged Networks*, *1*(1), 1-17.

Li, W., Meng, W., & Kwok, L. F. (2022b). Surveying Trust-Based Collaborative Intrusion Detection: State-of-the-Art, Challenges and Future Directions. *IEEE Communications Surveys Tutorials*, *24*(1), 280-305.

Li, W., Meng, W., & Yang, L. T. (2021b). Enhancing Trust-Based Medical Smartphone Networks via Blockchain-Based Traffic Sampling. In *IEEE* 20^{th} *International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 122–129.

Li, W., Song, H., & Zeng, F. (2018). Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities. *IEEE Internet of Things Journal*, *5*(2), 716-723.

Li, X., Yin, X., & Ning, J. (2023b). Trustworthy Announcement Dissemination Scheme with Blockchain-Assisted Vehicular Cloud. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 1786-1800.

Liang, W., Long, J., Weng, T.-H., Chen, X., Li, K.-C., & Zomaya, A. Y. (2019). TBRS: A Trust Based Recommendation Scheme for Vehicular CPS Network. *Future Generation Computer Systems*, *92,* 383-398.

Lin, Z., Cui, H., & Liu, Y. (2024). Distributed Deep Learning Based on Edge Computing Over Internet of Vehicles: Overview, Applications, and Challenges. *IEEE Access*, *12,* 133734-133747.

Liu, X., Liang, L., Tan, Z., Chen, J., & Li, G. (2025a). An Adaptive Trust Threshold Based on Q-Learning for Detecting Intelligent Attacks in Vehicular Ad-Hoc Networks. *Ad Hoc Networks*, *175,* 103865.

Liu, X., Wang, S., & Chen, Y. (2025b). Adaptive Scheduling for Internet of Vehicles Using Deconfounded Graph Transfer Learning. *Computer Networks*, *256,* 110899.

Lu, L., Gu, W., Xu, X., Wang, M., Liu, S., & Wu, F. (2024). Cross-Chain Protocol Lightning-C for Internet of Vehicles Environment. *IEEE Access*, *12,* 111932-111941.

Lu, X. & Song, W. (2025). Improved Trajectory Data Encryption Method for Internet of Vehicles Using GAN-Based Chaotic Logistic Algorithm. *Alexandria Engineering Journal*, *114,* 719-727.

Lu, Y., Zhang, G., Wang, X., & Li, X. (2023). Trust-Based Reliability Enhancements Provisioning With Resilience Under Information Asymmetry in IoV System. *IEEE Access*, *11,* 82362-82376.

Madani, S. E., Motahhir, S., & Ghzizal, A. E. (2022). Internet of Vehicles: Concept, Process, Security Aspects and Solutions. *Multimedia Tools and Applications*, *81*(12), 16563-16587.

Magdich, R., Jemal, H., & Ayed, M. B. (2022). A Resilient Trust Management Framework Towards Trust Related Attacks in the Social Internet of Things. *Computer Communications*, *191,* 92-107.

Mahmood, A. (2021). *Trust on Wheels – Towards Trust Management in the Internet of Vehicles*. PhD thesis, Macquarie University, Sydney, New South Wales, Australia.

Mahmood, A., Sheng, Q. Z., Zhang, W. E., Wang, Y., & Sagar, S. (2023). Toward a Distributed Trust Management System for Misbehavior Detection in the Internet of Vehicles. *ACM Transactions on Cyber-Physical Systems*, *7*(3), 2378-962X.

Mahmood, A., Siddiqui, S. A., Sheng, Q. Z., Zhang, W. E., Suzuki, H., & Ni, W. (2022). Trust on Wheels: Towards Secure and Resource Efficient IoV Networks. *Computing*, *104*(6),1337-1358.

Mahmood, A., Zhang, W. E., Sheng, Q. Z., Siddiqui, S. A., & Aljubairy, A. (2019). *Trust Management for Software-Defined Heterogeneous Vehicular Ad Hoc Networks*, pages 203–226. Springer International Publishing, Cham.

Mao, M., Hu, T., & Zhao, W. (2023). Reliable Task Offloading Mechanism Based on Trusted Roadside Unit Service for Internet of Vehicles. *Ad Hoc Networks*, *139,* 103045.

Mao, M., Yi, P., Hu, T., Zhang, Z., Lu, X., & Lei, J. (2021). Hierarchical Hybrid Trust Management Scheme in SDN-Enabled VANETs. *Mobile Information Systems*, *2021*(1), 7611619.

Marche, C. & Nitti, M. (2021). Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT. *IEEE Transactions on Network and Service Management*, *18*(3), 3297-3308.

Marwein, P. S., Nath Sur, S., Gao, X.-Z., & Kandar, D. (2024). Recent Survey on Internet of Vehicles: Architecture, Applications, Challenges, and Its Solutions. *Journal of Testing and Evaluation*, *52*(1), 731-753.

Miao, J., Wang, Z., Ning, X., Shankar, A., Maple, C., & Rodrigues, J. J. P. C. (2024). A UAV-Assisted Authentication Protocol for Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *25*(8), 10286-10297.

Mirzadeh, I., Sayad Haghighi, M., & Jolfaei, A. (2023). Filtering Malicious Messages by Trust-Aware Cognitive Routing in Vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*, *24*(1), 1134-1143.

Mishra, P. & Singh, G. (2023). Energy Management Systems in Sustainable Smart Cities Based on the Internet of Energy: A Technical Review. *Energies*, *16*(19).

Mo, W., Liu, W., Huang, G., Xiong, N. N., Liu, A., & Zhang, S. (2022). A Cloud-Assisted Reliable Trust Computing Scheme for Data Collection in Internet of Things. *IEEE Transactions on Industrial Informatics*, *18*(7), 4969-4980.

Monfared, S. K. & Shokrollahi, S. (2023). DARVAN: A Fully Decentralized Anonymous and Reliable Routing for VANets. *Computer Networks*, *223,* 109561.

Muhammad, M. & Safdar, G. A. (2025). V2X Application Server and Vehicle Centric Distribution of Commitments for V2V Message Authentication. *Ad Hoc Networks*, *167,* 103701.

Nagaraju, L. & Saini, I. (2025). Trust-Centric Detection of Roadside Unit Misbehaviour in VANETs. In *2025 International Wireless Communications and Mobile Computing (IWCMC)*, pages 361–366.

Naik, D. S. B. & Dondeti, V. (2025). Trust-Based Secure Federated Learning Framework to Mitigate Internal Sttacks for Intelligent Vehicular Networks. *Peer-to-Peer Networking and Applications*, *18*(2), 10.

Najafi, M., Khoukhi, L., & Lemercier, M. (2022). Decentralized Prediction and Reputation Approach in Vehicular Networks. *Transactions on Emerging Telecommunications Technologies*, *33*(7), e4456.

Nazih, O., Benamar, N., Lamaazi, H., & Chaoui, H. (2024). Toward Secure and Trustworthy Vehicular Fog Computing: A Survey. *IEEE Access*, *12,* 35154-35171.

Noor-A-Rahim, M., Liu, Z., Lee, H., Khyam, M. O., He, J., Pesch, D., Moessner, K., Saad, W., & Poor, H. V. (2022). 6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities. *Proceedings of the IEEE*, *110*(6), 712-734.

Osorio, D. P. M., Ahmad, I., Sánchez, J. D. V., Gurtov, A., Scholliers, J., Kutila, M., & Porambage, P. (2022). Towards 6G-Enabled Internet of Vehicles: Security and Privacy. *IEEE Open Journal of the Communications Society*, *3,* 82-105.

Oubabas, S., Aoudjit, R., Rodrigues, J. J. P. C., & Talbi, S. (2018). Secure and Stable Vehicular Ad Hoc Network Clustering Algorithm Based on Hybrid Mobility Similarities and Trust Management Scheme. *Vehicular Communications*, *13,* 128-138.

Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Stern, J., editor, *Advances in Cryptology — EUROCRYPT'99*, pages 223–238, Berlin, Heidelberg. Springer Berlin Heidelberg.

Partani, S., Zentarra, M., Kiggundu, A., & Schotten, H. D. (2025). Improving QoS Prediction in Urban V2X Networks by Leveraging Data from Leading Vehicles and Historical Trends. In *2025 IEEE 101st Vehicular Technology Conference (VTC2025-Spring)*, pages 1–6.

Partovi, Z., Zarei, M., & Rahmani, A. M. (2023). Data-Centric Approaches in the Internet of Vehicles: A Systematic Review on Techniques, Open Issues, and Future Directions. *International Journal of Communication Systems*, *36*(3), e5383.

Philip, A. O., Sreeja, M., Paul, R., & Saravanaguru, R. (2024). Towards Intelligent Trust-Based Incident and Evidence Management Models for Internet of Vehicles: A Survey. *Computers and Electrical Engineering*, *117,* 109284.

Qi, J., Zheng, N., Xu, M., Chen, P., & Li, W. (2024). A Hybrid-Trust-Based Emergency Message Dissemination Model for Vehicular Ad Hoc Networks. *Journal of Information Security and Applications*, *81,* 103699.

Qi, J., Zheng, N., Xu, M., Wang, X., & Chen, Y. (2023a). A Multi-Dimensional Trust Model for Misbehavior Detection in Vehicular Ad Hoc Networks. *Journal of Information Security and Applications*, *76,* 103528.

Qi, L., Tian, J., Chai, M., & Cai, H. (2023b). LightPoW: A Trust Based Time-Constrained PoW for Blockchain in Internet of Things. *Computer Networks*, *220,* 109480.

Qin, H., Tan, Y., Chen, Y., Ren, W., & Choo, K.-K. R. (2024). TriBoDeS: A Tri-Blockchain-Based Detection and Sharing Scheme for Dangerous Road Condition Information in Internet of Vehicles. *IEEE Internet of Things Journal*, *11*(2), 3563-3577.

Qiong, W., Shuai, S., Ziyang, W., Qiang, F., Pingyi, F., & Cui, Z. (2023). Towards V2I Age-Aware Fairness Access: A DQN Based Intelligent Vehicular Node Training and Test Method. *Chinese Journal of Electronics*, *32*(6), 1230-1244.

Qureshi, K. N., Din, S., Jeon, G., & Piccialli, F. (2021). Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges With Future Aspects. *IEEE Transactions on Intelligent Transportation Systems*, *22*(3), 1777-1786.

Rai, I. A., Shaikh, R. A., & Hassan, S. R. (2020). A Hybrid Dual-Mode Trust Management Scheme for Vehicular Networks. *International Journal of Distributed Sensor Networks*, *16*(7), 1550147720939372.

Rani, P. & Sharma, R. (2023). Intelligent Transportation System for Internet of Vehicles Based Vehicular Networks for Smart Cities. *Computers and Electrical Engineering*, *105,* 108543.

Rani, P. & Sharma, R. (2024). Intelligent Transportation System Performance Analysis of Indoor and Outdoor Internet of Vehicle (IoV) Applications Towards 5G. *Tsinghua Science and Technology*, *29*(6), 1785-1795.

Rathee, G., Kumar, A., Kerrache, C. A., & Calafate, C. T. (2024). A Trust Management Solution for 5G-Based Future Generation Internet of Vehicles. *Computer Networks*, *248,* 110501.

Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., Osamor, J., & Hamdi, M. (2022). A Novel Trust-Based Security and Privacy Model for Internet of Vehicles Using Encryption and Steganography. *Computers and Electrical Engineering*, *102,* 108205.

Raya, M., Papadimitratos, P., Gligor, V. D., & Hubaux, J.-P. (2008). On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In *IEEE INFOCOM 2008 - The* 27^{th} *Conference on Computer Communications*, pages 1238–1246.

Raza, A. & Badidi, E. (2025). A Trust-Based Client Selection Framework for Federated Learning in the Internet of Vehicles. In *2025 International Wireless Communications and Mobile Computing (IWCMC)*, pages 1180–1185.

Razafimanjato, M., Saad, M. M., & Kim, D. (2025). Blockchain-Based Trust Management Systems in the Internet of Vehicles: A Comprehensive Survey. *ICT Express*, *11*(6), 1265-1285.

Rehman, A., Hassan, M. F., Hooi, Y. K., Qureshi, M. A., Chung, T. D., Akbar, R., & Safdar, S. (2021). Context and Machine Learning Based Trust Management Framework for Internet of Vehicles. *Computers, Materials & Continua*, *68*(3), 4125-4142.

Rehman, A., Hassan, M. F., Yew, K. H., Paputungan, I., & Tran, D. C. (2020). State-of-the-Art IoV Trust Management: A Meta-Synthesis Systematic Literature Review (SLR). *PeerJ Computer Science*, *6,* e334.

Ren, Y., Li, Z., Yang, Y., Yu, H., Zhao, Y., & Wei, X. (2025). A Dynamic Trust Evaluation Scheme Based on Cross-Domain Trust Inheritance for VANETs. *Ad Hoc Networks*, *175,* 103872.

Rezvi Shahariar, C. P. (2023). A Trust Management Framework for Vehicular Ad Hoc Networks. *International Journal of Security, Privacy and Trust Management*, *12*(1), 1-10.

Riley, G. F. & Henderson, T. R. (2010). The NS-3 Network Simulator. In *Modeling and Tools for Network Simulation*, pages 15–34. Springer.

Rishiwal, V., Agarwal, U., Alotaibi, A., Tanwar, S., Yadav, P., & Yadav, M. (2024). Exploring Secure V2X Communication Networks for Human-Centric Security and Privacy in Smart Cities. *IEEE Access*, *12,* 138763-138788.

Rjoub, G., Bentahar, J., & Wahab, O. A. (2023). Explainable Trust-Aware Selection of Autonomous Vehicles Using LIME for One-Shot Federated Learning. In *2023 International Wireless Communications and Mobile Computing (IWCMC)*, pages 524–529.

Sagar, S. (2023). *Trust Computational Heuristics for Social Internet of Things*. PhD thesis, Macquarie University, Sydney, New South Wales, Australia.

Sagar, S., Mahmood, A., Kumar, J., & Sheng, Q. Z. (2020a). A Time-Aware Similarity-Based Trust Computational Model for Social Internet of Things. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pages 1–6.

Sagar, S., Mahmood, A., Sheng, M., Zaib, M., & Zhang, W. (2021). Towards a Machine Learning-driven Trust Evaluation Model for Social Internet of Things: A Time-aware Approach. In *MobiQuitous 2020 - 17^{th} EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, MobiQuitous '20, page 283–290, New York, NY, USA. Association for Computing Machinery.

Sagar, S., Mahmood, A., Sheng, Q. Z., Zaib, M., & Sufyan, F. (2024a). Can We Quantify Trust? Towards a Trust-Based Resilient SIoT Network. *Computing*, *106*(2), 557-577.

Sagar, S., Mahmood, A., Sheng, Q. Z., & Zhang, W. E. (2020b). Trust Computational Heuristic for Social Internet of Things: A Machine Learning-Based Approach. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pages 1–6.

Sagar, S., Mahmood, A., Sheng, Q. Z., Zhang, W. E., Zhang, Y., & Pabani, J. K. (2024b). Understanding the Trustworthiness Management in the Social Internet of Things: A Survey. *Computer Networks*, *251,* 110611.

Sagar, S., Mahmood, A., Wang, K., Sheng, Q. Z., Pabani, J. K., & Zhang, W. E. (2023). Trust–SIoT: Toward Trustworthy Object Classification in the Social Internet of Things. *IEEE Transactions on Network and Service Management*, *20*(2), 1210-1223.

Saha, S. & Chandrakar, P. (2025). A Blockchain-Enhanced Authentication Framework for 6G-Enabled Internet of Vehicles. In *2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0*, pages 1–8.

Sasikumar, A., Vairavasundaram, S., Kotecha, K., Indragandhi, V., Ravi, L., & Selvachandran, G. & Abraham, A. (2023). Blockchain-Based Trust Mechanism for Digital Twin Empowered Industrial Internet of Things. *Future Generation Computer Systems*, *141,* 16-27.

Shamaeian, N. & Pesch, D. (2024). Evidence Theory-Based Trust Management for the Social Internet of Vehicles. In *2024 IEEE* 49^{th} *Conference on Local Computer Networks (LCN)*, pages 1–7.

Shang, F. & Deng, X. (2025). A Data Sharing Scheme Based on Blockchain for Privacy Protection Certification of Internet of Vehicles. *Vehicular Communications*, *51,* 100864.

Sharma, A., Pilli, E. S., Mazumdar, A. P., & Gera, P. (2020). Towards Trustworthy Internet of Things: A Survey on Trust Management Applications and Schemes. *Computer Communications*, *160,* 475-493.

Sharma, J., Bhardwaj, M., & Chantola, N. (2024). *Emerging Applications and Future Scope of Internet of Vehicles for Smart Cities*. CRC Press, 1^{st} edition.

Shen, Z., Wang, Y., Wang, H., Liu, P., Liu, K., & Zhang, J. (2024). Trust Mechanism Privacy Protection Scheme Combining Blockchain and Multi-Party Evaluation. *IEEE Transactions on Intelligent Vehicles*, *9*(2), 3885-3894.

Shokrollahi, S. & Dehghan, M. (2023). TGRV: A Trust-Based Geographic Routing Protocol for VANETs. *Ad Hoc Networks*, *140,* 103062.

Shokrollahi, S. & Dehghan, M. (2025). CTVAN: A Cooperation-Based RSU-Assisted Trust Management Model for Reliable Communication in VANETs. *Cluster Computing*, *28*(4), 227.

Shu, Z., Sun, X., & Cheng, H. (2024). When LLM Meets Hypergraph: A Sociological Analysis on Personality via Online Social Networks. In *Proceedings of the* 33^{rd} *ACM International Conference on Information and Knowledge Management*, CIKM '24, page 2087–2096, New York, NY, USA. Association for Computing Machinery.

Siddiqui, S. A., Mahmood, A., Sheng, Q. Z., Suzuki, H., & Ni, W. (2021a). A Survey of Trust Management in the Internet of Vehicles. *Electronics*, *10*(18), 2223.

Siddiqui, S. A., Mahmood, A., Sheng, Q. Z., Suzuki, H., & Ni, W. (2021b). A Time-Aware Trust Management Heuristic for the Internet of Vehicles. In *2021 IEEE* 20^{th} *International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1–8.

Siddiqui, S. A., Mahmood, A., Sheng, Q. Z., Suzuki, H., & Ni, W. (2023a). Towards a Machine Learning Driven Trust Management Heuristic for the Internet of Vehicles. *Sensors*, *23*(4).

Siddiqui, S. A., Mahmood, A., Sheng, Q. Z., Suzuki, H., & Ni, W. (2023b). Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *24*(9), 9546-9560.

Siddiqui, S. A., Mahmood, A., Zhang, W. E., & Sheng, Q. Z. (2019). Machine Learning Based Trust Model for Misbehaviour Detection in Internet-of-Vehicles. In Gedeon, T., Wong, K. W., & Lee, M., editors, *Neural Information Processing*, pages 512–520, Cham. Springer International Publishing.

Singh, M., Limbasiya, T., & Das, D. (2019). Pseudo-identity Based Secure Communication Scheme for Vehicular Ad-Hoc Networks. In *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6.

Sivanantham, T. & Sethuraman, S. C. (2026). Securing Vehicle-to-Everything (V2X) Communication: Challenges, Mechanisms, and Future Directions. *Wireless Personal Communications*, *146*(2), 537-643.

Song, Y., Cao, Y., Cheong, C., He, D., Raymond Choo, K.-K., & Wang, J. (2024). CAT: A Consensus-Adaptive Trust Management Based on the Group Decision Making in IoVs. *IEEE Transactions on Information Forensics and Security*, *19,* 7730-7743.

Su, B. & Tong, L. (2023). Transmission Protocol of Emergency Messages in VANET Based on the Trust Level of Nodes. *IEEE Access*, *11,* 68243-68256.

Su, R., Jin, Y., & Song, Y.-Q. (2024). Assessing Trustworthiness of V2X Messages: a Cooperative Trust Model Against CAM- and CPM-Based Ghost Vehicles in IoV. In *Proceedings of the* 10^{th} *International Conference on Vehicle Technology and Intelligent Transport Systems*, pages 276–283.

Sun, G., Wang, Z., Su, H., Yu, H., Lei, B., & Guizani, M. (2024). Profit Maximization of Independent Task Offloading in MEC-Enabled 5G Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *25*(11), 16449-16461.

Sun, N., Wang, W., Liu, K., Li, D., & Lü, J. (2025). Hybrid Framework for Security Evaluation in Internet of Vehicles. *Computers Security*, *153,* 136-141:x.

Sun, S., Fan, X., & Xiao, Y. (2023). Trust Model Based on Recommendation Filtering in Internet of Vehicles. In *2023 2nd International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT)*, pages 364–369.

Suo, D. & Sarma, S. E. (2019). Real-time Trust-Building Schemes for Mitigating Malicious Behaviors in Connected and Automated Vehicles. In *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, pages 1142–1149.

Surapaneni, P., Bojjagani, S., & Khurram Khan, M. (2025). DYNAMIC-TRUST: Blockchain-Enhanced Trust for Secure Vehicle Transitions in Intelligent Transport Systems. *IEEE Transactions on Intelligent Transportation Systems*, *26*(7), 10918-10932.

Tang, J., Gao, H., Liu, H., & Das Sarma, A. (2012). eTrust: Understanding Trust Evolution in an Online World. In *Proceedings of the* 18th *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD'12, page 253–261, New York, NY, USA. Association for Computing Machinery.

Taslimasa, H., Dadkhah, S., Neto, E. C. P., Xiong, P., Ray, S., & Ghorbani, A. A. (2023). Security Issues in Internet of Vehicles (IoV): A Comprehensive Survey. *Internet of Things*, *22,* 100809.

Tripathi, K. N. & Sharma, S. C. (2020). A Trust Based Model (TBM) to Detect Rogue Nodes in Vehicular Ad-Hoc Networks (VANETS). *International Journal of System Assurance Engineering and Management*, *11*(2), 426-440.

Tripathi, K. N., Yadav, A. M., Nagar, S., & Sharma, S. C. (2023). ReTrust: Reliability and Recommendation Trust-Based Scheme for Secure Data Sharing Among Internet of Vehicles (IoV). *Wireless Networks*, *29*(6), 2551-2575.

Truong, N. B., Um, T.-W., Zhou, B., & Lee, G. M. (2017). From Personal Experience to

Global Reputation for Trust Evaluation in the Social Internet of Things. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pages 1–7.

Ullah, I., Khan, M. A., Kumar, N., Abdullah, A. M., AlSanad, A. A., & Noor, F. (2023a). A Conditional Privacy Preserving Heterogeneous Signcryption Scheme for Internet of Vehicles. *IEEE Transactions on Vehicular Technology*, *72*(3), 3989-3998.

Ullah, S., Abbas, G., Waqas, M., Abbas, Z. H., & Khan, A. U. (2023b). RSU Assisted Reliable Relay Selection for Emergency Message Routing in Intermittently Connected VANETs. *Wireless Networks*, *29*(3), 1311-1332.

Vidhya, B., Harshene, H., & Abimathi, N. (2025). *Introduction to Next Generation Networks 5G and Beyond*, chapter 1, pages 1–18. John Wiley & Sons, Ltd.

Wan, N. & Wang, D. (2024). A Novel Federated Learning Framework Based on Trust Evaluation in Internet of Vehicles. *Adhoc & Sensor Wireless Networks*, *58*(3/4), 321.

Wang, D., Chen, X., Wu, H., Yu, R., & Zhao, Y. (2020). A Blockchain-Based Vehicle-Trust Management Framework Under a Crowdsourcing Environment. In *2020 IEEE* 19^{th} *International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1950–1955.

Wang, D., Yi, Y., Yan, S., Wan, N., & Zhao, J. (2023a). A Node Trust Evaluation Method of Vehicle-Road-Cloud Collaborative System Based on Federated Learning. *Ad Hoc Networks*, *138,* 103013.

Wang, N., Yang, W., Wang, X., Wu, L., Guan, Z., Du, X., & Guizani, M. (2024a). A Blockchain Based Privacy-Preserving Federated Learning Scheme for Internet of Vehicles. *Digital Communications and Networks*, *10*(1), 126-134.

Wang, X., Zhu, H., Ning, Z., Guo, L., & Zhang, Y. (2023b). Blockchain Intelligence for Internet of Vehicles: Challenges and Solutions. *IEEE Communications Surveys & Tutorials*, *25*(4), 2325-2355.

Wang, Y., Cao, Y., Lv, C., Zhang, Y., Zhou, B., & Wan, S. (2023c). PDTM: A Provenance-Driven Dynamic Trust Management model for IoVs. *Sustainable Energy Technologies and Assessments*, *60,* 103496.

Wang, Y., Mahmood, A., Sabri, M. F. M., & Zen, H. (2024b). TM–IoV: A First-of-Its-Kind Multilabeled Trust Parameter Dataset for Evaluating Trust in the Internet of Vehicles. *Data*, *9*(9).

Wang, Y., Zhang, Y., Song, Y., Cao, Y., Zhang, L., & Ren, X. (2023d). Appeal-Based Distributed Trust Management Model in VANETs Concerning Untrustworthy RSUs. In *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6.

Wazid, M., Das, A. K., & Shetty, S. (2022). TACAS-IoT: Trust Aggregation Certificate-Based Authentication Scheme for Edge-Enabled IoT Systems. *IEEE Internet of Things Journal*, *9*(22), 22643-22656.

Wei, S., Li, X., Ji, H., & Zhang, H. (2024). Anti-attack Trust Evaluation Algorithm Based on Bayesian Inference in VANET. In Gao, F., Wu, J., Li, Y., Gao, H., & Wang, S., editors, *Communications and Networking*, pages 142–161, Cham. Springer Nature Switzerland.

Wei, X. (2024). Enhancing Road Safety in Internet of Vehicles Using Deep Learning Approach for Real-Time Accident Prediction and Prevention. *International Journal of Intelligent Networks*, *5,* 212-223.

Wilensky, U. (1999). NetLogo. Online; Accessed 10-March-2021.

Xia, H., Xiao, F., Zhang, S.-s., Hu, C.-q., & Cheng, X.-z. (2019a). Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pages 838–846.

Xia, H., Zhang, S.-s., Li, Y., Pan, Z.-k., Peng, X., & Cheng, X.-z. (2019b). An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks. *IEEE Transactions on Vehicular Technology*, *68*(7), 7108-7120.

Xiao, Y. & Liu, Y. (2019). BayesTrust and VehicleRank: Constructing an Implicit Web of Trust in VANET. *IEEE Transactions on Vehicular Technology*, *68*(3), 2850-2864.

Xie, Q., Ding, Z., Xie, Q., Tan, X., He, D., & Tang, W. (2024). Blockchain-Based Traffic Accident Handling Protocol Without Third Party for VANETs. *IEEE Internet of Things Journal*, *11*(19), 31068-31079.

Xing, L., Zhao, P., Gao, J., Wu, H., & Ma, H. (2023). A Survey of the Social Internet of Vehicles: Secure Data Issues, Solutions, and Federated Learning. *IEEE Intelligent Transportation Systems Magazine*, *15*(2), 70-84.

Xu, B., Zhao, J., Wang, B., & He, G. (2025a). Detection of Zero-Day Attacks Via Sample Augmentation for the Internet of Vehicles. *Vehicular Communications*, *52,* 100887.

Xu, Q., Zhang, L., & Liu, Y. (2025b). Enhancing Trust Management System for Connected and Autonomous Vehicles Using Machine Learning Methods: A Survey. *arXiv preprint*. arXiv:2505.07882.

Xu, W., Zhang, Y., Wang, F., Qin, Z., Liu, C., & Zhang, P. (2023). Semantic Communication for the Internet of Vehicles: A Multiuser Cooperative Approach. *IEEE Vehicular Technology Magazine*, *18*(1), 100-109.

Xu, X., Li, H., Xu, W., Liu, Z., Yao, L., & Dai, F. (2022). Artificial Intelligence for Edge Service Optimization in Internet of Vehicles: A Survey. *Tsinghua Science and Technology*, *27*(2), 270-287.

Yadav, S., Singh, K., Yadav, A. K., Shariq, M., Chaudhry, S. A., Das, A. K., & Manjul, M. (2025). Efficient and Reliable Information Sharing for Internet of Vehicles using Trust and Blockchain. *IEEE Transactions on Vehicular Technology*, *11*(1), 333-344.

Yang, J., Ni, Q., Luo, G., Cheng, Q., Oukhellou, L., & Han, S. (2023a). A Trustworthy Internet of Vehicles: The DAO to Safe, Secure, and Collaborative Autonomous Driving. *IEEE Transactions on Intelligent Vehicles*, *8*(12), 4678-4681.

Yang, X., Zhu, F., Yang, X., Luo, J., Yi, X., Ning, J., & Huang, X. (2024). Secure Reputation-Based Authentication With Malicious Detection in VANETs. *IEEE Transactions on Dependable and Secure Computing*, *22*(1), 359-372.

Yang, Z. & Tao, Q. (2026). A Survey of Trust Management Mechanisms in the Internet of Vehicles. *Ad Hoc Networks*, *183,* 104131.

Yang, Z., Wang, R., Wu, D., Yang, B., & Zhang, P. (2023b). Blockchain-Enabled Trust Management Model for the Internet of Vehicles. *IEEE Internet of Things Journal*, *10*(14), 12044-12054.

Yin, D. & Gong, B. (2022). Auto-Adaptive Trust Measurement Model Based on Multidimensional Decision-Making Attributes for Internet of Vehicles. *Wireless Communications and Mobile Computing*, *2022*(1), 3537771.

Yong-hao, W. (2020). A Trust Management Model for Internet of Vehicles. In *Proceedings of the 2020 4^{th} International Conference on Cryptography, Security and Privacy*, ICCSP 2020, page 136–140, New York, NY, USA. Association for Computing Machinery.

Yu, Y., Jia, Z., Tao, W., Xue, B., & Lee, C. (2017). An Efficient Trust Evaluation Scheme for Node Behavior Detection in the Internet of Things. *Wireless Personal Communications*, *93*(2), 571-587.

Yuan, M., Xu, Y., Zhang, C., Tan, Y., Wang, Y., Ren, J., & Zhang, Y. (2023). TRUCON: Blockchain-Based Trusted Data Sharing With Congestion Control in Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *24*(3), 3489-3500.

Zeng, J., Liang, Z., Zhang, J., Zhang, X., & Long, Z. (2022). Research on Cloud Side Collaboration Under Internet of Vehicles. In *2022 IEEE* 6^{th} *Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pages 245–248.

Zhang, C., Li, W., Luo, Y., & Hu, Y. (2021). AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology. *IEEE Internet of Things Journal*, *8*(5), 3157-3169.

Zhang, C., Zhu, L., Xu, C., Sharif, K., Ding, K., Liu, X., Du, X., & Guizani, M. (2022a). TPPR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in VANET. *IEEE Transactions on Services Computing*, *15*(2), 806-818.

Zhang, H. & Li, M. (2025). Towards an Intelligent and Automatic Irrigation System Based on Internet of Things with Authentication Feature in VANET. *Journal of Information Security and Applications*, *88,* 103927.

Zhang, J., Zheng, K., Zhang, D., & Yan, B. (2020). AATMS: An Anti-Attack Trust Management Scheme in VANET. *IEEE Access*, *8,* 21077-21090.

Zhang, P., Shao, S., Wu, C., Yang, Z., & Zhang, R. (2025). Fine-Grained Personalized Hierarchical Federated Learning towards Heterogeneous Internet of Vehicles. *IEEE Internet of Things Journal*, *12*(11), 16349–16362.

Zhang, S., He, R., Xiao, Y., & Liu, Y. (2023a). A Three-Factor Based Trust Model for Anonymous Bacon Message in VANETs. *IEEE Transactions on Vehicular Technology*, *72*(9), 11304-11317.

Zhang, S., Zhang, D., Wu, Y., & Zhong, H. (2023b). Service Recommendation Model Based on Trust and QoS for Social Internet of Things. *IEEE Transactions on Services Computing*, *16*(5), 3736-3750.

Zhang, Y., Jiang, C., & Zhang, P. (2024). Security-Aware Resource Allocation Scheme Based on DRL in Cloud–Edge–Terminal Cooperative Vehicular Network. *IEEE Internet of Things Journal*, *11*(1), 95-104.

Zhang, Y., Song, Y., Wang, Y., Cao, Y., Ren, X., & Yan, F. (2022b). TECS: A Trust Model for VANETs Using Eigenvector Centrality and Social Metrics. In *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 36–43.

Zhang, Y., Zhao, Y., & Zhou, Y. (2022c). User-Centered Cooperative-Communication Strategy for 5G Internet of Vehicles. *IEEE Internet of Things Journal*, *9*(15), 13486-13497.

Zhao, P.-C., Huang, Y.-H., Zhang, D.-X., Xing, L., Wu, H.-H., & Gao, J.-P. (2023). CCP-Federated Deep Learning Based on User Trust Chain in Social IoV. *Wireless Networks*, *29*(4), 1555-1566.

Zhao, Y., Liu, W., Li, B., Zhou, X., Ning, Z., Qiu, T., & Atiquzzaman, M. (2022). Entity and Sociality Trust-Aware Model for Content Distribution in Social Internet of Vehicles. *IEEE Transactions on Vehicular Technology*, *71*(12), 12511-12522.

Zhu, C., Xie, X., Ding, C., Zhou, Y., Gao, X., & An, J. (2024). Terahertz Empowered

Vehicular Fog Computing: Opportunities, Feasibility, and Enhancements. *IEEE Wireless Communications*, *31*(4), 315-323.

APPENDIX A

ACADEMIC SUPERVISORS

Principal Academic Supervisor:

Ts. Dr. Mohamad Faizrizwan Bin Mohd Sabri

Senior Lecturer

Department of Electrical and Electronics Engineering, Faculty of Engineering

Universiti Malaysia Sarawak, Sarawak, Malaysia

Academic Co-supervisors:

Dr. Adnan Mahmood

Senior Lecturer

School of Computing, Faculty of Science and Engineering

Macquarie University, Sydney, Australia

Professor Dr. Hushairi Zen

Dean of Faculty of Engineering and Technology

i-CATS University College, Sarawak, Malaysia

APPENDIX B

LIST OF PUBLICATIONS

Published

- Wang Yingxun, Hushairi Zen, Mohamad Faizrizwan Mohd Sabri, Wang Xiang, and Kho Lee Chin (2022). Towards Strengthening the Resilience of IoV Networks – A Trust Management Perspective. *Future Internet*, 14(7):202 (Q2, Impact Factor: 3.6).
- Wang Yingxun, Adnan Mahmood, Mohamad Faizrizwan Mohd Sabri, Hushairi Zen, and Kho Lee Chin (2024). MESMERIC: Machine Learning-based Trust Management Mechanism for the Internet of Vehicles. *Sensors*, 24(3):863 (Q2, Impact Factor: 3.5).
- Wang Yingxun, Adnan Mahmood, Mohamad Faizrizwan Mohd Sabri, and Hushairi Zen (2024). TM – IoV: A First-of-its-Kind Multilabeled Trust Parameter Dataset for Evaluating Trust in the Internet of Vehicles. *Data*, 9(9):103 (Q2, Impact Factor: 2.0).
- Wang Yingxun, Adnan Mahmood, Mohamad Faizrizwan Mohd Sabri, and Hushairi Zen (2025). Towards Distinguishing Trust-based Attacks in an IoV Network. *Journal of King Saud University – Computer and Information Sciences*, 37:39 (Q1, Impact Factor: 6.1).
- Wang Yingxun, Adnan Mahmood, Mohamad Faizrizwan Mohd Sabri, and Hushairi Zen (2026). Trust Management in the Internet of Vehicles: A Survey of the State-of-the-Art. *IEEE Open Journal of Intelligent Transportation Systems*, 7 (Q1, Impact Factor: 5.3).