A SCENARIO-BASED TRUST MANAGEMENT APPROACH WITH 3R MESSAGE CATEGORIZATION IN VANETS

by

Sarferoze Shaik

Submitted in partial fulfillment of the requirements
for the degree of Master of Computer Science

at

Dalhousie University
Halifax, Nova Scotia
February 2021

This thesis is dedicated to my beloved family. My hero and father, Khadar Shaik, for always inspiring me with your journey of life which is nothing less than a roller coaster ride, my support system and mother, Pasha begum, for always holding my hand, teaching me right perception of life and guiding me all the way, and to my two main pillars and sisters, Saneema and Sameera, for their unconditional love which made me realize that there exists a world with full of love, care and concern. To my extended family, Neha, for always being my side during my tough phases and holding my hand through dusk till dawn and beyond. To my brother-in-law, AJ for inspiring me with your thoughts. To my dearest friends, Uthej, Vivek, Raghu, Hema Datta, Nikhil, Sairam, Drona and many other colleagues during various stages of life, without whom I wouldn't be the same as I am now. Thanks for all the chats and conversations you gifted me throughout my life. A special mention to all the strong women, Amma, Pedhakka, Chinnakka, Neha, Lalbee akka, Dolly akka, Reshma akka and many other, who inspired and taught me the meaning of life and love.

Contents

List of Tables

List of Figures

Abstract

With the recent advancements in vehicular communications, there has been tremendous growth in the applications supported by Vehicular Ad-hoc Networks (VANETs). To realize the primary objective of Intelligent Transportation System (ITS), the growth and development of VANETs in vehicular communications has been eyed as a preeminent advancement by distinguishing itself from the existing technologies with respect to its unique and stringent characteristics. On the one hand, these distinctive characteristics enhance the application of VANETs in various road-related services. However, on the other hand, they pose tremendous security risks due to the presence and possibility of potential cyber threats.

Besides many potential solutions that have been implemented to address the security and privacy issues, trust management has positioned itself as a promising advancement in the last few years. However, the development of trust management is still in its early stages. But the focus is narrowed in demonstrating the intricate details involved in a trust management scheme. A Scenario-based Trust management Approach with 3R message categorization (STAR) for VANETs is proposed in this thesis to address the above issue. STAR implements a trust management scheme with three main objectives. Firstly, a 3-type classification of messages, namely refresh, rush and revoke, introduces a modular approach to reduce overhead issues on the computational units. Secondly, a scenario-based approach is demonstrated, which details five scenarios involved in performing trust computations. Finally, an efficient and secure model is implemented, limiting one of the prominent security threats, Man-in-the-Middle (MiTM) attack.

STAR has been implemented on Network simulator2 (NS2) with the integration of Simulation of Urban Mobility (SUMO) for simulating the traffic environment. On various simulation runs, the proposed model is compared with existing Ad-hoc On-demand Distance Vector (AODV) routing technology and reference-list trust management scheme and then validated based on various performance metrics such as delay, throughput, detection accuracy, and packet delivery ratio.

List of Abbreviations Used

AODV Ad-hoc On-demand Distance Vector

AR Anamoly Ratio

ART Attack Resistant Trust

AU Application Unit

BARS Blockchain-based Anonymous Reputation System for Trust Management

BI Bayesian Inference

BSM Basic Safety Messages

BTM Beacon-based Trust Management

CA Certificate Authority

CAM Cooperative Awareness Messages

CH Cluster Head

CTA Central Trusted Authority

DMN Detetction of Malicious Nodes

DMV Detection of Malicious Vehicles

DoS Denial of Service

DOT Department of Transportation

DS Digital Signature

DSRC Dedicated Short Range Communication

DT Direct Trust

DT Direct Trust

DTC Data-centric Trust Computations

ECC Elliptic Curve Cryptography

ECDSA Elliptical Curve Digital Signature Algorithm

ERS Event-based Reputation System

ETC Entity-centric Trust Computations

ETSI European Telecommunications Standards Institute

FANET Flying Ad-hoc Network

FT Functional Trust

HR Honest Rating

IBC ID-based Cryptography

ITS Intelligent Transportation System

LEA Legal Enforcement Authority

LSOT Lightweight Self Organized Trust

MANET Mobile Ad-hoc Network

MARINE Man-in-the-middle Attack Resistant trust model in connected vehicles

MDR Message Dissemination Ratio

MiTM Man-in-the-Middle

MTR Message Transmission Ratio

NAM Network Animator

NS2 Network Simulator2

OBU On-Board Unit

OIF Offline Infrastructure Factors

PDR Packet Drop Ratio

PKI Public Key Infrastructure

PPS Payment Punishment Scheme

PTR Packet Transmission Ratio

RaBTM RSU-based Beacon Trust Mangement

RET Role and Experience-based Trust

RGTE Reputation-based Global Trust Establishment

RMC Reputation Management Centre

RREQ Route Request

RSU Road Side Units

RT Recommendation Trust

SNR Signal-to-Noise Ratio

STAR Scenario-based Trust management Approach with 3R message categorization

SUMO Simulation of Urban Mobility

TMEC Trust Management based on Evidence Combination

TR Transmission Range

TRIP Trust and Reputation-based Infrastructure Proposal

TRT Trust Routing Table

TTP Trusted Third Party

TV Threshold Value

V2D Vehicle-to-Device

V2I Vehicle-to-Infrastructure

V2N Vehicle-to-Network

V2P Vehicle-to-Pedestrian

V2R Vehicle-to-RSU

V2V Vehicle-to-Vehicle

V2X Vehicle-to-everything

VANET Vehicular Ad-hoc Network

VCG Vickrey-Clarke-Grooves

VID Vehicle-ID

WAVE Wireless Access in Vehicular Environment

WHO World Health Organization

XML Extensible Markup Language

Acknowledgements

First and foremost, I would like to express my gratitude towards my supervisor Dr. Srinivas Sampalli for his involvement and contribution to my research work. His positive attitude and valuable inputs encouraged me to push my limits further. I should mention the level of support and guidance from him, which has positioned me in a place where I am right now. I want to take this stage to convey my respect for the supervision he rendered to me. Your approach of conducting lab sessions weekly and personally monitoring each student has helped me become strong and confident. Thank you, Dr. Srini.

I would like to thank my readers, Dr. Qiang Ye and Dr. Israat Haque, for accepting to be readers for my defense. I feel glad to have such professionals for my defense.

It was wonderful sharing a space with the people of Mytech lab. You are a bunch of talents, and I hope all positives in your path. Special mention to Masood, Robie, and Reetam for their valuable inputs during my initial stages. Thanks, Sumanth and akanchha, for answering all my queries and giving your support at the right times.

Finally, I would like to use this opportunity to express my gratefulness to my dad, amma, and my two beautiful sisters. You all have been my greatest support system, especially during the process of my thesis completion. Neha, thanks for your constant support and concern always. Sairam, thanks for your companionship, baa. Uthej and Dattu, thanks for all the conversations and acting as my stress busters. Thanks a ton to all my friends throughout various stages of my life. You have supported me like a family.

Chapter 1

Introduction

The development and transformation of cities to metropolises have led to the growth of urbanization, which resulted a rise in traffic on roads to a greater extent. It is estimated that there will be a 60 percent occupancy rate in urban areas by 2030[55]. Besides the socio-economic problems caused by urbanization, transportation systems are adversely affected by congestion, road accidents, and casualties. In a run to make the cities smarter, several traffic-related issues have emerged.[20]. With the recent advancements in vehicular communications, Vehicular Ad-hoc Networks (VANETs) have been identified as a key solution to address the key challenges raised by urbanization. It is also considered as an indispensable component of the Intelligent Transportation System (ITS) due to the demand and need to integrate transportation systems with information technology[49].

ITS comprises a range of transport-specific technologies and applications. The main objective of ITS is to enhance road safety and mobility. It also maximizes the effectiveness of driver's usability and reduces the detrimental effects incurred by road-related problems[33]. To solve the concerns listed above, the system uses many of its technologies and plays a critical role in keeping road travel secure, free of pollution, and environmentally sustainable[57].

1.1 VANET

VANET is a self-organizing, infrastructure-less, and dynamic network which allows vehicles inside the network to share information such as safety and traffic analysis with other vehicles[20]. VANET is a subset of ad-hoc networks and an application of Mobile Ad-hoc Network (MANET) working over a vehicular domain[42]. The basic components of VANETs constitute mobile nodes or vehicles, limited infrastructure such as Road-Side Units (RSU), and wireless interconnection to share information.

Based on the nature of communication involved, VANETs comprise of two domains or environments, namely ad-hoc and infrastructure[49].

1.2 Security Challenges

VANETs form an integral part of ITS and responsible for enhancing road transportation by continuously generating and sharing safety messages, which in turn results in avoidance of accidents, collisions, traffic congestions, and delays that would otherwise be a confusion[42][20]. There are many entities and communication technologies that support VANETs at various stages that help in effective traffic management both in terms of safety and security. VANETs are also responsible for ensuring the security of both communication and content; however, providing a safer and secure environment for such scenarios is most challenging. Nevertheless, VANETs become susceptible to many harmful security attacks that can create confusion in the system, which leads to many accidents, injuries, and even deaths. Many factors make VANETs vulnerable to attacks, and they can be classified into two categories[49], namely technical and security factors.

1.2.1 Technical Factors

Firstly, due to the unique characteristics of VANETs, such as high mobility, rapid change of topology, and intermittent connections, it is prone to many network-related issues[20]. For instance, consider a car whose movement on various parts of the road is highly dynamic due to different speed limits set by traffic authority. This serves as the main reason for a problem that occurs due to very limited and less connectivity time between two nodes, also known as short inter-contact times. The other challenging characteristic is rapid topology change[19] that poses a threat to VANETs. Although the layout, locations, trajectories, and routes are fixed for every vehicle, their relatively high mobility results in the rapid change of topology. For instance, as soon as it establishes a connection with its neighboring node, a node initiates information exchange. However, due to the high mobility of the neighboring node, both vehicles attain different topologies within a second, thereby resulting in connection loss. Many other characteristics such as network fragmentation, energy and bandwidth constraints, different operational environments make the functioning

of VANETs more troublesome[57].

1.2.2 Security Factors

Secondly, as VANETs is responsible for carrying sensitive information, which comes with a prerequisite of secure, reliable, and efficient exchange of information, any discrepancies in transmission might lead to catastrophe. For example, many malicious vehicles may induce attacks by forging messages, initiating false messages, withdrawing services, and few wide range attacks include MiTM, Denial of Service (DoS), malware injection, Sybil and black-hole attacks[33][19][52].

1.2.3 Mitigation approaches

Over the past decade, many approaches and solutions have been identified. They have succeeded in mitigating the issues caused by the unique characteristics of VANETs. For instance, interference caused by peer-to-peer connection can be resolved using multi-hop connections[25]; problems related to rapid change of topology is handled using WAVE; and many other multi-layer problems such as synchronization, congestion control and bandwidth limitations were also addressed [36].

Researchers have identified various solutions to abate the security challenges caused during communication and information exchange in VANETs. Many schemes are related to identity management, message verification, privacy protection, and misbehavior detection. These techniques are supported by traditional cryptography and Public Key Infrastructure (PKI)[51]. They provide various services related to authentication, certification, and digital signatures, but with the implementation of PKI based cryptosystems, only a few security challenges have been addressed. For instance, the drawback of using Wireless Access in Vehicular Environment (WAVE), i.e., the inability to access the security standards provided by 802.11 standards where users are not authenticated before connection establishment, has been mitigated using the PKI systems[49]. It can only defend external attackers that need to be authenticated to enter into the system but proved to be useless, while in the case of internal attackers who are authorized users with valid credentials[9]. This is considered a potential threat to VANETs where researchers are still identifying the best and practical

approach, as a feasible measure, in the form of trust management.

1.3 Motivation and Research Objectives

According to the road crash statistics available from the association for safe international road travel, it is estimated that on average, 35 million people are injured worldwide with a fatality rate of 3.7 percent, which equals 1.3 million. Road traffic accidents are identified as the 9th leading cause of death[49] and predicted to become 5th by the year 2030 according to the reports of World Health Organization (WHO). Few surveys conducted in Germany, the USA and other countries state that 60 percent of accidents could have been avoided if the driver is informed about the incident half a second before it took place[49]. To overcome such shortcomings, many advancements have been developed in vehicular communication with the help of ITS and identified VANET as a potential breakthrough that could enable a wide range of safety, mobility, and commercial applications with utmost significance.

As mentioned earlier, the highest priority is assigned to safety-related applications facilitated by VANET since it involves the transmission of time-sensitive and life-critical information that would serve the purpose of collision avoidance and thereby enhancing traffic management[57]. In the case of information exchange, it is essential to assure two things: content and entity validation. When a connection has been established between two mobile nodes, one node initiates communication by sending a message with limited inter-contact time. On the other hand, the receiver needs to validate the sender, identify the trustworthiness of data, and decide to either accept or deny the message. This whole process is expedited by VANET with proper communication and routing protocols alongside employing appropriate security mechanisms.

Many PKI based traditional security mechanisms have been identified as a potential solution to the drawback of VANETs, but they are limited to only defending external attackers[51]. Researchers have come up with trust management schemes as an extension to current approaches and positioned them as the most suitable ones in mitigating the security issues faced by VANET[55].

Trust management schemes are categorized into data-oriented, entity-oriented, and hybrid trust models[23]. All the three models perform trust computation based on the revocation targets, among which hybrid trust models have proven to be effective yet challenging[9]. In hybrid trust models, trust is computed on both senders, which transmit the message and the data that is being transmitted[48]. Although the results attained after computing trust will be reliable and accurate, performing both the computations in less interaction time is challenging. Trust computation involves various steps and should demonstrate various scenarios that are specific to particular conditions[23]. Excessive research is being conducted in developing an efficient trust model compared to the state-of-art models, but a demonstration of different scenarios that involve in trust computation has not been explored.

The concept of trust is identified as the most salient security parameter in VANETs, which can disclose the insider attackers who join the system with valid credentials. These attackers behave as honest nodes for a particular amount of time, gain trust, and launch attacks. Since traditional PKI based cryptosystems are unable to identify the insider attackers, reputation-based schemes have been implemented where each vehicular node places a certain unit of trust on other nodes for sharing reliable, authenticated, accurate, and trusted message[9]. It is also essential to compute the trustworthiness of data since it is the primary source of communication.

After surveying literature established in this area, it was identified that more efforts were put in to address the drawbacks of existing trust models and developing a model that enhances the former one. Nevertheless, it is equally important to demonstrate how trust is computed for various scenarios; for instance, each vehicle, after having interaction with the other, computes the level of trust and stores it as a reference for future interactions. If the same vehicle interacts again in the future, the receiver is provided with a trust value that has been computed earlier, which assists in computing trust rapidly. However, if the vehicle is communicating for the first time, there is no such value called trust to quickly and accurately compute the trust value. Trust calculation in this scenario must be different since more care should be taken as there was no past interaction.

Such scenarios exist in various stages of communication. This dissertation provides insights into precisely five scenarios where trust computation for both the entity (sender node) and data (message) is demonstrated. To provide extensive details on trust calculation, a new approach known as message categorization is integrated with the former one alongside the scenario-based approach. This combined approach demonstrates a MiTM based trust management with multiple scenarios that occur at various stages during Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, also demonstrates specific approaches to calculate trust for different scenarios. It also explains the need for categorizing the messages and how they are different from each other. The specific contributions of this thesis and its organization are described in the following sections.

1.4 Thesis Contribution

Most of the work under the category of security and privacy in VANETs have been carried to address the drawbacks of existing trust models by implementing a model that brings forth significant betterment in either detecting an attack or computing trust[27][9][47]. This dissertation, alongside developing a new-age trust management technique in order to identify MiTM attacks, primarily provides insights into various scenarios that come across different stages in the process of calculating trust. These insights are important because of two reasons:

1. Each scenario needs to be dealt with slightly modified versions of the trust management technique. This will resolve the problem of generalizing a common solution to every scenario that occurs on the road.

2. The scenario-based approach works like a distributed system in which every entity such as mobile nodes, RSUs and Certificate Authority (CA) is designated with the individual role of handling different scenarios to reduce interference and attain enhancements in terms of performance.

The primary goal of this research work is to study different scenarios that exist

through various phases of a VANET. Most previous research works were held to design a generic scheme feasible to apply to the whole system at various stages. However, this dissertation provides details on the possibility of applying an accurate and specific scheme for each scenario and enhancing the performance. On the other hand, all these specific schemes collectively form up a framework that helps in identifying MiTM attacker and assists all the mobile nodes in reaching out to the right conclusion on a particular traffic event.

In this dissertation, all the messages that are used for V2V and V2I communication are classified into three main categories, namely, refresh, rush and revoke messages[47]. Refresh messages are related to entertainment and fall under the category of non-safety/user-based applications[57]. These messages include information related to tolls, parking, entertainment, and few others that has the least impact on road accidents. Rush, also known as alert messages, hold the highest priority on the roads as these constitute the vital information that creates a significant impact on road accidents such as collision avoidance, black ice warnings, lane changing assistance, etc.,[9]. Revoke or foreclosure messages belong to security-based applications whose primary motive is to identify the misbehaving nodes in the system and foreclose them to nearby RSU[47]. These RSUs will gather evidence based on the reports made by the foreclosing node and decides on the foreclosed node, whether to revoke its credentials or to reduce its trust percentage in the system[14].

Each mobile node maintains a lookup-database that contains trust information about other vehicular nodes in the system that include unique vehicle ID and respective honest rating. The scenarios in the system are broadly categorized into five types, and they are as follows:

Scenario 1: When a node initiates communication with its neighboring node, the receiver checks the database for any previous interaction. If there is an entry in the database, the sender is either forwarded for trust calculation in step 2 or discarded, based on the rating and Message Transmission Ratio (MTR).

Scenario 2: If there is no entry, since the receiver does not have any information about the sender, it initiates a new concept, Offline Social Factor (OIF), to attain initial trust values and make an entry for the newly interacting vehicle.

Scenario 3: While the two scenarios explain the working of rush messages, this scenario is related to revoke messages, which demonstrates the concept of node-RSU communication.

Scenario 4: Each vehicular node is allotted with either award or penalty points based on their conduct. This scenario explains the possibility of a dishonest node claiming an award or positive rating.

Scenario 5: This scenario illustrates the factors responsible for avoiding assigning punishment or negative rating to an honest node.

All these scenarios form up to build a scenario-based trust management scheme to identify MiTM attacker and maintaining efficient trust management throughout the system that enables significant traffic management.

1.5 Thesis Organization

This thesis is organized as follows:

Chapter 2 Provides an overview of VANET architecture, domains, communication standards, and applications alongside security prerequisites. This section also includes background on traditional PKI based cryptosystems and trust management schemes.

Chapter 3 Provides an insight into various trust management schemes in each category of data-oriented, entity-oriented, and hybrid trust models. It also emphasizes the drawbacks of each approach that led to the development of another.

Chapter 4 Introduces and proposes a scenario-based trust management scheme for various classifications of messages and identifying malicious nodes in the system

present in the form of MiTM attackers. It presents intricate details on the individual scenarios, their respective algorithms, flowcharts, and methodology.

Chapter 5 Explains the implementation process, types of tools used to simulate a vehicular environment, and working of each scenario. It also explains various steps involved in the simulation to test the performance of the proposed trust model. Results obtained from various simulation runs are analyzed by plotting them on a graph and compared with the existing trust model concerning four performance metrics.

Chapter 6 Derives the main conclusion based on the analysis of obtained results and provides future directions towards VANETs privacy and security.

Chapter 2

Background

2.1 VANET Architecture

VANETs are a subgroup of Mobile Ad-hoc Networks (MANET)[38] and forms one of its relevant representations. MANETs are also known as ad-hoc wireless networks, which consist of minimal infrastructure with a set of mobile nodes connected wirelessly to each other in a self-configuring and self-healing environment. The mobility of nodes in a MANET is highly random due to one of its typical characteristics, rapid change of topology, which is inherited by VANET[38]. Alongside, VANET is also known for its uniqueness because of its highly dynamic architecture[20]. Each node in VANET is considered as a communication vehicle whose sole intention is to propagate road safety and traffic-related information to other nodes. It enhances traffic efficiency and safety and provides a safe, secure and sophisticated experience to users.

In the figure 2.1, the architecture of a VANET includes various interconnected entities such as On-Board Unit (OBU), Application Unit (AU), RSU, access network and communication technologies such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)[49][20][19]. All these entities form a part of VANET and apportioned to two domains, ad-hoc and infrastructure[42][19] as depicted in the figure 2.2. As VANET is well known for its limited otherwise minimal infrastructure, RSU and access network constitute the only infrastructure with which VANET is established.

2.1.1 Domains

Ad-hoc domains consists of the mobile nodes embedded with information processing units such as OBU and AU. OBU possess capabilities that facilitate communication among vehicles and the other infrastructure present in the system. AU is responsible

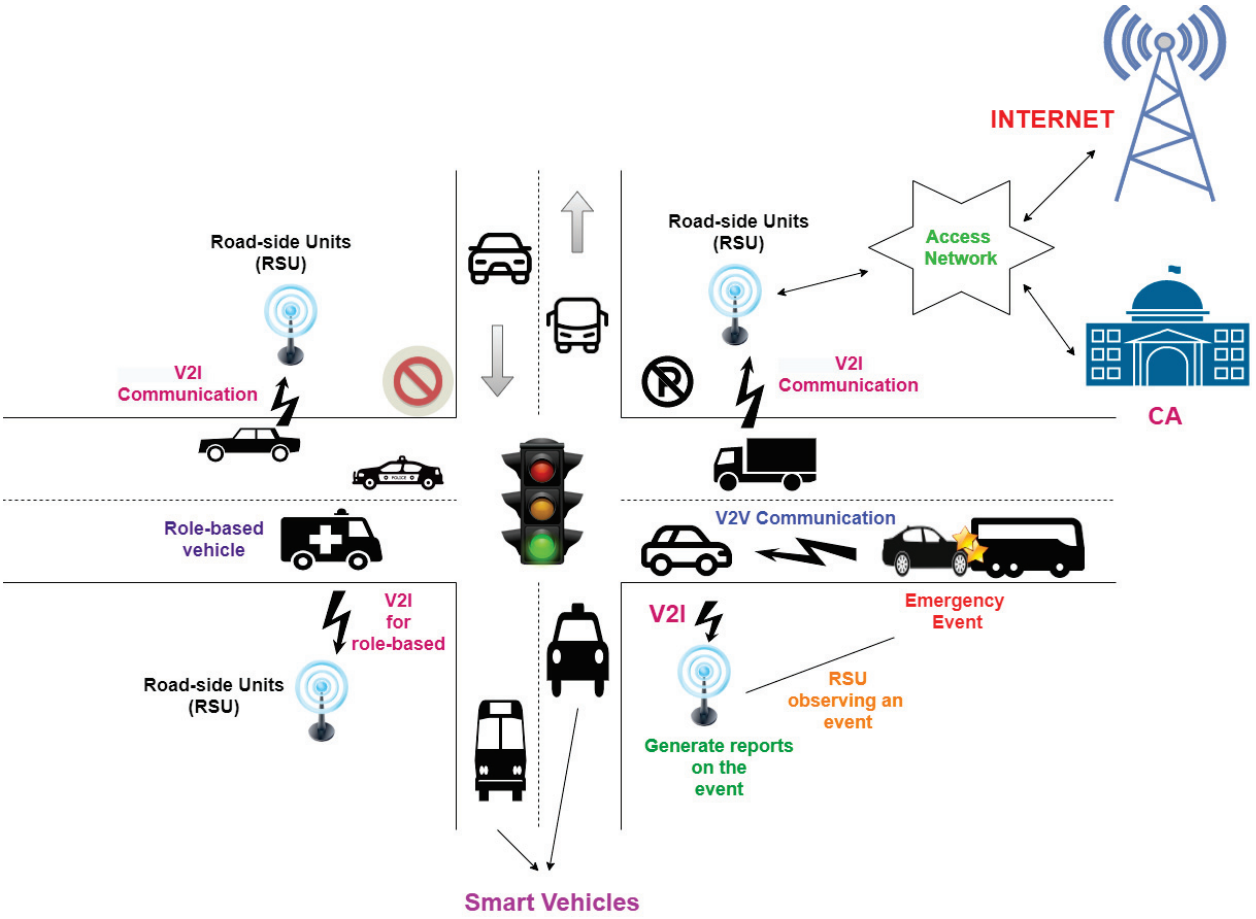

Figure 2.1: Architecture of VANET

for enabling the capabilities of OBU by executing programs required for information exchange[42]. There are two types of communication technologies established in VANET, in order to exchange safety, time sensitive and valuable information, namely vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)[19]. V2V and V2I are responsible for information exchange between vehicles and other infrastructural units such as RSU, respectively and both these approaches are supported by DSRC and WAVE standards[57].

Infrastructure domain consists of entities that manages various activities such as certification, vehicle registration, ID management and certificate revocation and all these are abstracted as VANET Authority[42]. Besides, the infrastructure domain is

deployed with RSU which acts as node access points. The deployment of RSU are limited based on few factors such as cost consideration, road intersections, population density and level of urbanization[5]. VANET facilitate V2I between RSU and mobile nodes as the former is responsible for monitoring the nodes, validating the events occurred on the rod and forwarding the information to certificate authority (CA). In specific, the V2I between RSU and mobile nodes are termed as Vehicle-to-RSU (V2R) and carried using DSRC and WAVE. Since RSU communicates with both vehicular nodes and CA, the latter is conducted using some mature technologies such as WiMAX, 3G, 4G and recently 5G is being implemented[42][22][14].

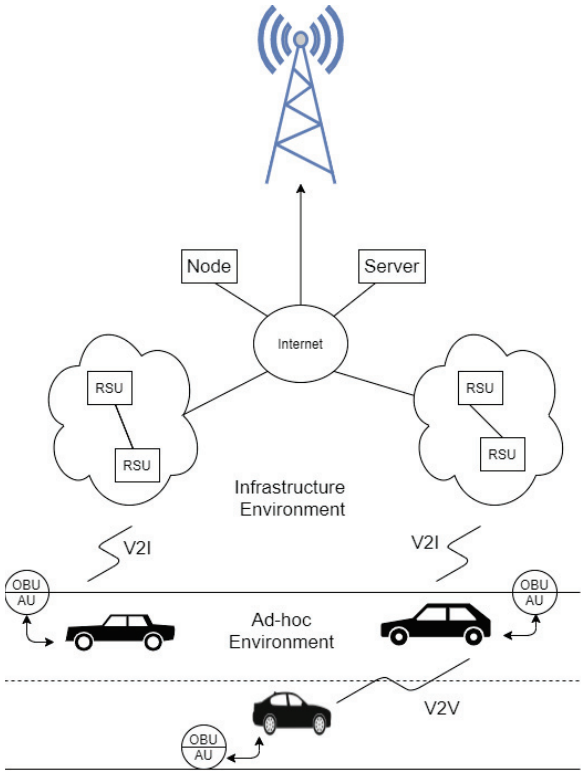

Figure 2.2: Domain view of VANET

2.2 Communication Standards

As mentioned earlier, two types of communication approaches are established in VANET and recent studies identified a new approach, Vehicle-to-everything (V2X),

that enables vehicles to connect with every entity that is related to road transportation which includes Vehicle-to-Pedestrian (V2P)), Vehicle-to-Device (V2D), Vehicle-to-Network (V2N) and to spotlights in the form of V2I [4]. All these approaches are supported by DSRC and WAVE, two standard technologies that enable wireless communication over vehicular domain[42].

2.2.1 DSRC

DSRC is a communication standard established to provide drivers' safety and experience on roads. The primary motivation for deploying DSRC is to enable collision prevention applications. The U.S. Department of Transportation (DOT) has reported that DSRC-based vehicle-to-vehicle (V2V) communication will fix up to 82% of all collisions affecting unimpaired vehicles in the United States, ultimately saving thousands of lives and billions of dollars[34]. It constitutes four standards, IEEE 1609.1 – IEEE 1609.4, each providing various applications, safety services and enhance the experience of road transportation[11]. DSRC also provides many standards that help nodes in VANET to communicate with other entities. Communication between nodes and infrastructure is enabled using messages, and a node can generate 15 types of different messages during their interaction, to name a few, Basic Safety Messages (BSM) and Cooperative Awareness Messages (CAM))[13].

2.2.2 WAVE

Alongside DSRC, WAVE is another prominent technology that is specially used for wireless access in VANET. It is an IEEE 802.11p standard and facilitates both the communication approaches, V2V and V2I, under licensed ITS band of 5.9 GHz[49]. The need for VANETs to quickly establish a vehicular network, enable communication with vehicles of high dynamicity, and rapid change of topology has made WAVE an integral part of it. WAVE provides a platform for nodes in VANET to establish connections without prior authentication and association[49]. This leads to a scenario where security measures provided by 802.11 standards can no longer be applied, resulting in the need for implementing efficient security measures in VANET.

2.3 Applications

The main objective of VANETs is to enable vehicles to establish connections with other vehicles and entities for sharing time-sensitive and life-critical information. This information includes accident-avoidance, black-ice warnings, traffic analysis, and entertainment. To experience the services provided by vehicular communications, several applications have been ideated for VANETs, which are classified and abstracted as security and user-based applications[42][57].

2.3.1 Security based applications

These applications aim to strengthen driver's safety by disseminating information about accidents, collisions, delays, and any other information relative to the safety of drivers and passengers[57]. To support these applications, each mobile node disseminates beacons periodically to specify technical details such as driving status, speed, location, and lane changing decisions, to its neighboring nodes. These nodes will assist them in handling any traffic-related issues ranging from delays to accidents[11]. Since these applications can influence any such incidents, they must be assigned a higher priority in VANETs. Few examples of applications that come under this category are [42][57][58][43]:

1. Blind spot warning
2. Emergency response time reduction
3. Road obstacle detection
4. Intersection coordination
5. Traffic signal violation
6. Lane change assistance
7. Post-crash notification
8. Emergency electronic brake light
9. Left or right turn assistance

One such classification that is part of safety-based applications but deals with traffic congestion issues and delays is the traffic management application. VANETs rely on

V2I and V2V communication to enhance traffic management and traffic monitoring. This will assist RSU in collecting real-time traffic data and sharing it with nodes in its vicinity to enable safer travel and efficient traffic management. The other entities in the infrastructure domain, such as CA take appropriate decisions in case of any security attacks and maintain the system less vulnerable[14]. Many applications under this category have been implemented over time, namely, floating car data collection, Smart traffic routing, and autonomous traffic control that helps VANETs improve traffic efficiency in various regions and multiple scenarios[42].

2.3.2 User based applications

Besides safety, VANET attracts many users from a business and comfort perspective. There are few applications classified under non-safety or user-based applications. The focus is capitalized on improving user experience on roads in terms of comfort by providing uninterrupted internet connectivity for audio and video streaming, entertainment and enhancing traffic efficiency by optimizing routes[42]. However, disseminating advertisements during travel has been identified as a successful formula from a business perspective. The main objective of such applications is to make the user experience entertaining and more enjoyable. Besides entertainment, VANETs also provides a platform to collect statistics related to environmental and weather conditions on the road that help recognize the level of pollution and environmental effects caused by road transportation and thereby identify the appropriate measures to be implemented[3]. A few of the non-safety applications include:

1. On-road entertainment
2. Parking lot management system
3. Digital maps download
4. Advertisement services and discovery
5. Traffic efficiency
6. Road sensing
7. Comfort and entertainment
8. CLARUS for road weather management system
9. Fuel filling stations

10. Restaurant finder

2.4 Characteristics and Features

VANETs incorporate various features and particularities from MANET since they both along with another type of ad-hoc networks such as Flying Ad-hoc Network (FANET) are considered as the classification of wireless ad-hoc networks[35]. Besides few common characteristics shared among these ad-hoc networks, each of them also possesses a set of unique characteristics. On the one hand, these are very extensive and positively influence the development of their envisioned applications. Nevertheless, on the other hand, they also form a challenging part while designing solutions for various wireless architectures. Similarly, VANETs possess few unique features that must be taken into consideration, which would otherwise ruin the primary objective of establishing a wireless vehicular network[49][20][19]. These features are described as follows:

High Mobility: One of the most prominent yet challenging characteristics of VANETs. The movement of mobile nodes in VANETs varies based on the different road situations. For instance, on a highway, each vehicle must maintain a higher speed limit than on regular roads. Similarly, this holds the same for various situations such as lane changing, traffic signals, crossroad intersections, and other vehicles' speed. Although the mobility of vehicular nodes is high, they are predictable since each vehicle is bounded with space since they travel on fixed and pre-established trajectories.

Self-organization: It is the most common feature for any ad-hoc wireless network, where each mobile node in the network does not require any assistance such as infrastructure or a centralized authority to organize and form into a network. Mobile nodes in VANET are challenged with frequent topology changes in which each vehicle shift their topology within seconds. In such scenarios, a mobile node initiating connection establishment requests and depending on a central authority would lead to delays, overheads, inefficiency, and, thereby, creating havoc in the network.

Dynamic Topology: Although the movement of vehicles is controlled using pre-established trajectories, traffic lights, and street layout, the topology of a moving vehicle changes rapidly. This gives a very less inter-contact time to establish a connection and propagate information. For instance, consider two vehicles moving on the same road in the opposite direction. As soon as one vehicle comes out of the other's transmission range or merges into another path, the topology has been changed, resulting in loss of communication. This depicts the importance of maintaining a particular topology for a considerable amount of time and why it becomes more challenging.

Latency control: The information shared between the mobile nodes does not pertain only to lane changing and status updates. Due to rapid changes in environments and delay restrictions introduced by safety applications, the information that is being propagated has become time-sensitive. To achieve control over latency and the timely propagation of these critical data, efficient yet fast cryptographic solutions must be designed.

Operational environments: The scenarios in a VANET varies based on different environments. VANET needs to operate efficiently and effectively at different domains. For instance, the mobility of nodes at certain urban areas is very high, resulting in the rapid change of topologies. However, on roads of rural areas, vehicles' mobility and density are relatively low, which is equally challenging. In such scenarios, communication is quite lacking, and it becomes difficult to validate a particular event.

Energy consumption: Unlike in MANETs, the energy consumption and resource utilization in VANETs is not quite challenging since the building blocks of the vehicular network are built with a sufficient amount of battery and computational power. This characteristic of VANETs is identified as a key advantage while implementing cryptography and trust-based solutions for safety applications.

All the characteristics mentioned above play an important role in enabling and enhancing various potential applications. In contrast, few characteristics still pose a

challenge in building a robust and efficient VANET architecture. Few other characteristics include data consistency, error tolerance, short inter-contact times, Geolocalization capabilities, intermittent communications, bandwidth, and network fragmentation [20][19].

2.5 Security Prerequisites

The primary objective of ITS is to improve the user experience and security of civic life by reducing road accidents and enhancing traffic regulation. In order to fulfill the requirements of ITS, the unique characteristics of VANET has made it as an integral part of ITS[49]. However, the traditional technologies such as DSRC assignment for vehicular communications have brought some significant results in handling the concerns related to the reliability of message transfers and accurate dissemination of emergency messages. With the advancement of technologies and the rising level of new and diversified security attacks, the system's robustness has become a challenge. On the one hand, handling security attacks related to message dissemination, overload, and the delay has become challenging. On the other hand, assuring transmission of information from a trusted source has become a concern.

VANETs are susceptible to attacks that can harm 3 of its basic entities, hardware, software, and users[51]. Hardware and software-related attacks include alteration and damage to the infrastructure, such as attaining illegal access through by-pass control by OBU and RSU, malware injection to leak privacy details of authenticated users, and modify the system certification process. Threats to users can be classified as data threats that include loss of their private data, denial of service, fabricating the messages during communication, impersonating as an authenticated user, and cause delays to emergency messages[33]. Over time, all these attacks have been broadly categorized into five classes, namely network, application, timing, social, and monitoring attacks[33].

All these attacks are primarily performed to break the security of the system. Many attacks are possible in an ad-hoc environment, especially in the vehicular domain. The impact of each attack essentially depends on the intentions of an attacker behind it. Attackers can be grouped based on various factors such as nature, scope,

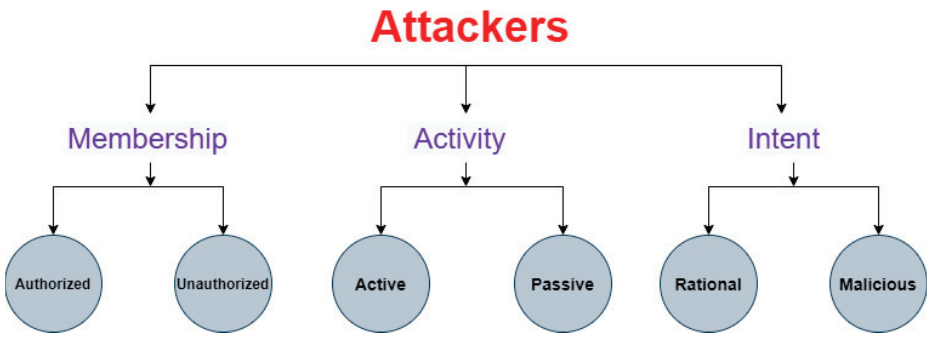

Figure 2.3: Classification of attackers

and behavior[33]. According to Maxim Rayal et al.[54], the attackers are classified based on three factors, and they are based on i)membership, ii)activity, and iii)intentions, as shown in the figure 2.3 Attackers based on membership include authorized and unauthorized users. It is essential to consider this category since various solutions are identified based on whether the attacker performs the attacks by residing in the network or outside. The second category differentiates between the attackers who alter the sensitive information and generates malicious signals, known as active attackers, and the attackers who tend to be tranquil just by sensing the information silently for ensuing attacks, known as passive attackers. The final category of attackers deals with the attackers who possess intentions of either seeking personal benefits or to create disturbance in the functionality of a system[49][33].

Many researchers have implemented security architectures and solutions to mitigate the threats that occur in a VANET system. Each unique characteristic of VANET poses a serious challenge and stringent requirement in developing a reliable, accurate, and efficient security scheme. In general, all these requirements are categorized as five primary security goals, and over the period, few prerequisites have been appended to the current set of goals[52]. Information exchange in VANET is sensitive and critical. It must ensure that these messages are transmitted to the appropriate destination from a trusted source and also make sure that drivers can notify neighbors and thus creating a trusted vehicular environment[33]. To build an algorithm or a system with such efficiency, these requirements must be a primary consideration. Figure 2.4 distinguishes between security prerequisites for VANET and trust management.

1. Authentication: It is very crucial to ensure that the information is generated from a trusted and authenticated source, without which it provides a way for attackers to impersonate themselves as legitimate users and transmit malicious information.

2. Availability: A requirement that is considered as significant and specific to vehicular communications is availability. The network needs to be available all the time to maintain seamless communication between nodes. Delay in reaction time, providing services, and transmitting emergency messages might lead to catastrophe. Few examples include jamming and DoS attacks.

3. Non-repudiation: Attackers try to resist themselves from taking responsibility for sending a malicious message. Non-repudiation ensures that no fraud is performed by refusing any offense caused by dishonest nodes. Cryptographic solutions such as digital signatures have been implemented to attain this goal.

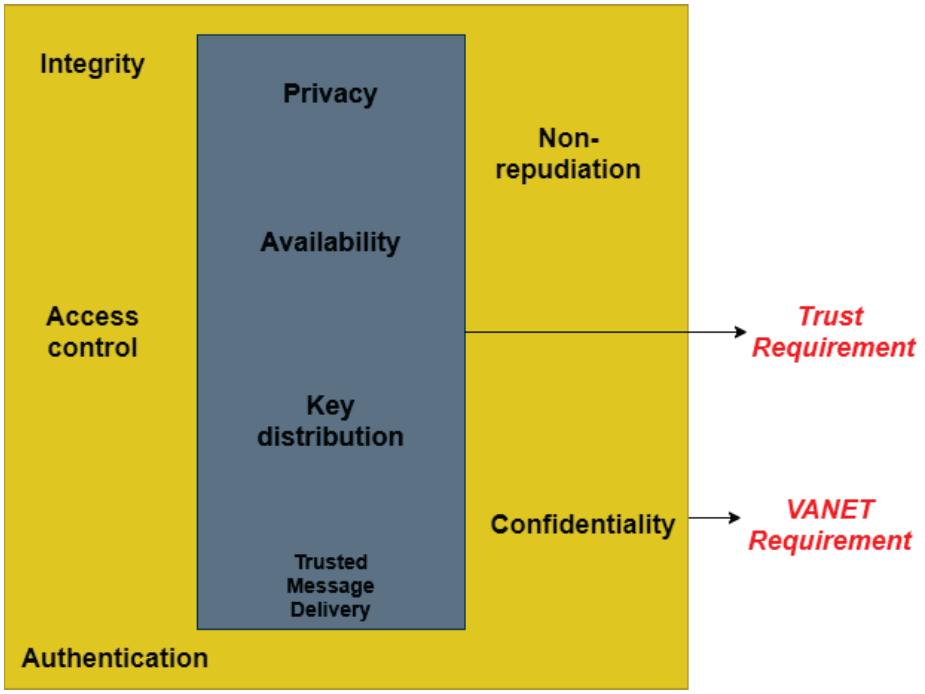

Figure 2.4: Security requirements of VANET

4. Integrity: One of the most common attacks performed in any wireless environment refers to fabrication, modification, or tampering messages. VANET must ensure that the message at sender and receiver must be identical. Traditional DSRC solution provides a way to closely monitor, analyze, and alter the messages. However, only authorized users such as certificate authority has the only right to do so. This is where trust management schemes play a crucial role over traditional solutions.

5. Confidentiality: Besides security, privacy is another key requirement that must be satisfied by VANETs. Although both these factors are contradictory, VANETs have no exception. A VANET architecture can be considered robust and efficient only when it can ensure all the security goals while preserving the privacy requirement of all the nodes.

Alongside the mentioned security goals, VANETs are still susceptible to few other attacks. Researchers have identified a set of other requirements that helps in shunning new-age attacks, which include tamper evidence hardware, electronic license plates, information correlation and verification, and event information recording[33].

2.6 Trust Management and Computation

Over the past few decades, many solutions have been proposed to handle various security attacks that effectuate in VANETs. All these solutions are implemented in the form of various protocols, algorithms, schemes, and architectures. Beginning with traditional communication technologies, DSRC and WAVE standards have provided basic functionalities for vehicular communication but failed in providing a secure environment for nodes to communicate[42]. With the advancement in technologies, cryptography-based solutions have been implemented to meet the security requirements designed for VANETs[25][51]. These solutions created a significant impact in handling the security issues to a particular extent. The drawbacks of one solution have given scope to the development of another solution. Nevertheless, all the solutions based on cryptography were deteriorated in meeting the privacy requirements of VANETs[55]. All the cryptography-based solutions are categorized into three main categories, PKI-based, ID-based and Situational Modelling[51]. To enable

authentication in VANETs and thereby assisting receivers in identifying the sender of the message and assuring them with the right content, few PKI based solution was implemented[51][52].

With time, Digital Signature (DS) made their way to enhance the current security of VANETs. Alongside authentication, DS ensured integrity and non-repudiation of messages. However, a sole DS scheme has its shortcomings, such as long verification times to validate the signatures and heavy computational overheads[52]. This led to the development of DS algorithms, which are classified as symmetric and asymmetric cryptography, also known as private and public-key cryptography, respectively. Each of these cryptography solutions has its disadvantage. Symmetric cryptography is vulnerable since it is easy to intercept or discover the secret key, which will decrypt the message. However, it works comparatively fast due to less complexity in the encryption process[52]. On the other hand, despite its computational overhead, asymmetric cryptography solutions are more reliable and secure. Few asymmetric cryptography solutions include RSA, Elliptical Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Cryptography (ECC). Alongside few ID-based Cryptography (IBC) schemes have been developed as a countermeasure for the existing PKI-based solutions[52].

A majority of the existing security solutions depend on PKI-based and traditional cryptography solutions. Perhaps, these solutions play a crucial role in identifying various security threats that can disturb and destroy the functionality of a VANET system. However, the potentiality of these solutions is limited to a particular extent, such as successfully identifying only external attackers. The most important drawback of a PKI-based cryptographic solution is the inability to catch hold of malicious nodes operating from inside a network[51]. Insider attackers reside and perform attacks from inside the system as they are valid and registered clients. All these attackers attain valid credentials from either Trusted Third Party (TTP) or Certificate Authority (CA) and behave as a legitimate user for a particular time to launch an attack. Such attacks are identified as a serious threat in the current VANET system. To overcome these shortcomings, VANET has identified a key concept, trust, that

possess the ability to successfully identify external attackers while evaluating shared messages for consistency[9].

There have been severe implications on security and privacy mechanisms during the transformation of vehicular environments from a centralized to distributed approach. Communication in a vehicular environment involves at least two parties, sender and receiver, to exchange or transmit road-related information. When a message arrives from an unknown computing source, there is always a certain amount of risk involved at the receiver end. To address and mitigate such types of risks, a secure parameter is known as trust has been introduced in the current VANET systems. According to[8][27], trust is defined as the amount of faith one vehicle places on other vehicles for sharing trusted, reliable and accurate messages. There are many versions of trust definitions, one of which states that trust is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his action[24].

Many trust management schemes have been implemented as an extension to the traditional cryptographic solutions[18][27][23][9][55]. Each scheme performs better over the other in terms of various performance metrics such as delay, event detection probability, error detection, false-positive rate, and few others. Nevertheless, the primary goal of every trust management scheme is to calculate the trustworthiness of either the entity (node) or the data (message) or sometimes both. By successfully performing trust computation, it enables the local entities such as mobile nodes and RSU to assess other entities' trustworthiness and thereby abate the centralized approach. Trust calculation in VANETs involve two steps in which; the first step includes the receiver collecting appropriate data about an event in the form of trust evidence. The second step involves trust computation on the gathered trust evidence. The result is in the form of trust values ranging from -1 to 1, where -1 refers to un-trusted data, and 1 refers to trusted data[23].

VANET entails two primary revocation targets: network entities or mobile nodes

and exchanged data or messages. Based on these revocation targets, trust models are categorized into three categories[9] They are as follows:

1. Entity-centric: It refers to calculating the trustworthiness of a sender vehicle to accept the sent message. If the trust values are positive, then the receiver is suggested to accept the message without any validations on the data. These trust models help in identifying the malicious and differentiate them from the legitimate nodes.

2. Data-centric: It refers to the computation of trustworthiness of data by various plausibility checks. Based on few scenarios and the unique characteristics of VANET, it is always difficult to calculate the trust of a particular vehicular node. These trust models play a vital role in such situations and assist the receiver in making a decision.

3. Hybrid: One of the significant and most efficient models that enables a way to accurately make decisions based on both factors, entity and data trust. In hybrid trust models, the trustworthiness of a node is calculated initially. If the trust values are positive, the process is forwarded to the next step for data trust computation. Although performing two types of trust with short inter-contact times is challenging, most of the research has been undergoing in this field.

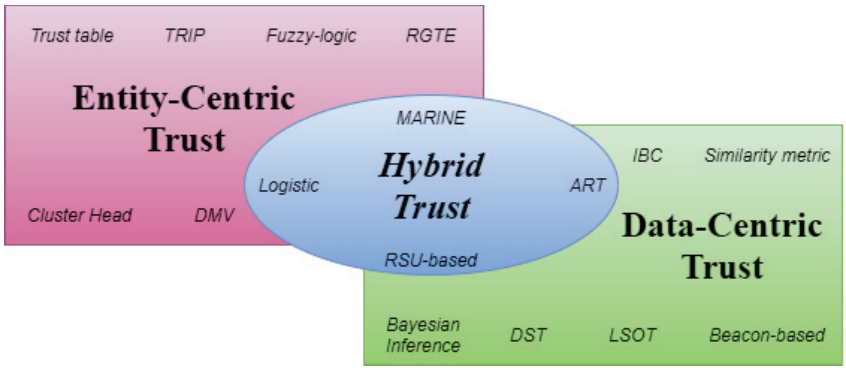

Figure 2.5: Classification of trust computation

Each model has its way of approaching the trust issues in VANET and various

metrics were introduced for calculating trust values. These metrics include plausibility checks, similarity measuring techniques, neighbor recommendations, message transmission range, mutual interaction evaluation, to name a few. Both the categories perform significantly better than the other based on various metrics. For instance, data trust models can perform accurately, while entity models can address sparse traffic effectively. This thesis focuses mainly on integrating two trust models and forming a hybrid trust model that improves the performance compared with the state-of-the-art model and can explain trust calculation during various road scenarios.

Chapter 3

Related Work

This chapter focuses on the state-of-the-art models related to trust management in VANETs. Many researchers have implemented various schemes, techniques, and models, to address the security aspects concerning VANET, s especially during the communication. However, this dissertation focuses on various trust management schemes that have been introduced over the past two decades, their contribution, and drawbacks that led to the development of new and contemporary schemes. The primary objective of a trust model or a reputation-based system is to distinguish between honest and dishonest nodes and ensure the dissemination of accurate and authentic messages, thus enabling road safety. The two fundamental revocation targets that influence the safety of mobile nodes constitute: 1)The information that is exchanged between the entities in the form of messages and 2)The entities responsible for transmitting the information. Based on these two factors, the trust models are categorized as a)entity-centric, b)data-centric, and c)hybrid trust models. Although the proposed model belongs to the category of hybrid trust model, a literature survey is also performed on entity-centric and data-centric trust models to elevate the importance and depict the reason for considering the combination of both these categories. Besides these trust models, a considerable amount of background work is performed on the significance of RSUs, their role in accomplishing trust evaluations, and enhancing security and efficiency in the system. This section begins with the related work from all three categories and concludes with a summary.

3.1 Entity-centric trust models

The entity-based trust schemes mainly emphasize identifying the malicious node that intends to curb the functionalities of VANETs. Such nodes are also termed as insider attackers who perform attacks after legitimately entering the system with valid credentials. Each malicious node has diversified behavior based on the security measures

that are designed in the system. Few dishonest nodes try to attack as soon as it enters the system, while few nodes delay the attacks to attain a considerable amount of trust in the system. Similarly, few nodes behave honestly during the dissemination process but perform attacks by inappropriately disclosing an honest node as dishonest to the central authority. A malicious node is responsible for spoofing, modifying, tampering, and blocking routing and life-critical information, resulting in connectivity issues, bandwidth consumption problems, inappropriate dissemination of messages, and leading to denial-of-service. Hence, evaluating a sender node's trustworthiness is highly necessary, and various credit and reputation-based entity-centric trust models are discussed below.

Hanin Almutairi et al. [12] proposed a trust-based scheme for the detection of new black hole attackers. A black hole attack is considered as one of the prominent routing attacks in which a malicious node executes an attack by attracting the sender node to propagate the message through itself. The malicious node sends a route reply with the shortest route passing from itself to the destination node to gain trust. In response to the route reply packet, the sender node transmits the messages through the malicious node resulting in a black hole attack where this malicious node drops the packet and prevents message dissemination. To avoid trusting such attacker nodes, this model implements a trust scheme where each vehicle maintains a Trust Routing Table (TRT) for its neighboring vehicles and updates it based on the acknowledgment received from the destination. A TRT of a source node contains an entry for each neighboring vehicle and two columns for each entry. The first column represents the trust value of that neighboring vehicle and the second column represents the progress, which means the difference between the distance from neighbor to the destination. Each source node selects its neighbor with the help of progress value, the lesser the value, the shorter the distance. If the destination node receives the packet, it sends back an acknowledgment to the source node. The source node then updates the corresponding neighboring node's trust value in its TRT. A black-hole attack node is identified based on the acknowledgment packet received from the destination node. If no such packet is received, the neighboring node is identified as malicious, and the

trust value is reduced by 1 unit.

Marmol et al. [26] proposed Trust and Reputation-based Infrastructure Proposal (TRIP) model that was designed primarily to meet the design requirements of any trust and reputation-based models such as accuracy, scalability, simplicity, light, and fast, resilience, and non-dependency on mobility patterns. The proposed model is described as a reputation-based model in which, on receiving a traffic warning message from a sender node, the receiver node determines whether to reject or accept and forward the message based on three trust levels represented with fuzzy sets. The three trust factors include direct historical interaction with the sender node, a recommendation from neighboring vehicles, and recommendations from central authorities. Each message is associated with a different severity level, which is attached by the issuer or sender of that message. Upon receiving the message, based on the severity and the three trust factors, the receiver node computes trust scores for the sender node and decides whether to drop or forward it to its neighboring nodes.

In [41], Xiaoqing Li et al. proposed a Reputation-based Global Trust Establishment (RGTE) in VANETs scheme, which introduces a solution for efficiently and accurately establishing a trust for entities in rapidly changing conditions by applying statistical laws. RGTE is a centralized approach in which a central authority, Reputation Management Centre (RMC), evaluates the reputation list and updates the information in the system. Upon identifying another node, each node sends a query about the reputation of its neighboring node to RMC through RSU. RMC maintains an updated list of reputations about all the nodes in the system. This list is updated on a timely basis and is forwarded when a request is generated through RSUs. Upon receiving a query message from a node, each RSU validates the message by decrypting it using a shared private key between RSU and RMC and evaluating the attached signature. If valid, RSU is responsible for gathering the trust data from RMC, computing trust, and forwarding it to the corresponding node.

Similarly, two other centralized approaches based on the cluster-based mechanism

are proposed by Uzma et al. [37] and Sulaiman et al. [31]. Both the proposed models address the lack of infrastructure and centralized administration, resulting in inefficiency in detecting malicious nodes in the network. In [37], Detetction of Malicious Nodes (DMN) algorithm is proposed which is an enhanced version of Detection of Malicious Vehicles (DMV) algorithm which facilitates the efficient selection of verifiers for detecting dishonest nodes. In this model, a Cluster Head (CH) is elected by participating entities, which implement a watch-dog mechanism in which a set of verifiers are assigned by CH for multiple regions in its vicinity. This set of verifiers monitors all the nodes in that region. Each verifier is responsible for closely monitoring the behavior of each node upon receiving a message. Based on the node's activity, the verifier reports its decision to CH, which finally reports it to Central Trusted Authority (CTA) to revoke the credentials of the detected malicious node. A slightly similar approach has been implemented in [31] where a Payment Punishment Scheme (PPS) and Vickrey-Clarke-Grooves (VCG) mechanism models are employed in detecting dishonest nodes. The primary objective of this model is to engage the mobile nodes actively in network activities such as monitoring, forwarding, and reporting any malicious behavior to a central entity. To encourage mobile nodes to participate actively, the researchers have employed the cluster-based approach. Each node is motivated by providing incentives (trust values) to perform the above activities and participate in elections. VCG employs a truth-telling approach as a dominant behavior strategy for nodes and thus enables each node to forward honest information in the run to gain incentives. During the election process of CH, the reputation of each vehicle is evaluated. Thus CH only accepts/trusts a node that attains the required reputation during the election.

Daeinabi et al. [18] has proposed an entity-centric trust scheme for Detection of Malicious Vehicle (DMV) which served as base paper for [37]. DMV is an algorithm for identifying malicious vehicles that drop and duplicate received packets/messages, thus causing a disturbance in the network. In this model, a cluster head is selected for a particular region and employed with verifiers to monitor each node in that region to detect any abnormal behaviors during message transmission. Each CH maintains two

lists, a white list, and a black list. The white list contains honest vehicles whose trust value is less than the threshold level, and the black list contains malicious vehicles with trust values higher than the threshold level. These two lists are evaluated by CA and updated at CH. Based on the observations reported by verifiers, CH verifies the information and forwards it to CA, which can isolate the reported vehicles from honest vehicles and revoke their credentials.

In [28], Haddadou et al. has proposed an economic incentive scheme adopted from the job market signaling model. Unlike the models mentioned above, this is a distributed trust model. Each vehicle is assigned with defined credit values and forced to maintain or increase its credit value for performing any activity in the system. To access any data in the system, the proposed model requires each vehicle to attain a particular level of credits, which would otherwise refrain the node from doing so. Moreover, each vehicle should possess credits concerning the severity of the activity. Therefore, the more severity tagged to the activity, the higher it should possess the credits. This will restrict any malicious node from performing attacks that cause the highest impact on the network. Credit management is implemented similarly to all other models. The node with honest behavior gets an increment in its credit value, and the node with malicious behavior suffers a decrement in its credit value. If the credit value falls below 0, it is categorized as malicious and removed from the network.

Most of the trust models employed for calculating entity-centric trust are centralized. Due to the unique characteristics possessed by VANET, it is quite challenging to rely completely on a single entity, which therefore becomes vulnerable to many attacks. In the case of VANETs, a distributed approach renders better outcomes but with the appropriate assignation of responsibilities based on their capacity and compromising factors. Besides these drawbacks, few limitations such as extra overhead generation due to the presence of multiple sources for trust evaluation, inefficient approach in case of rural scenarios and high mobility, and delays involved in updating trust tables to all the participant entities such as in RMC and CA. A node can be identified as dishonest only when it deliberately performs an attack, and until then,

it is considered as an honest node. This stands as one of the significant reasons that demonstrate more focus should be emphasized on identifying the trustworthiness of exchanged information.

3.2 Data-centric trust models

Data-centric trust models primarily focus on evaluating the trustworthiness of the information exchanged among the vehicles. Identifying the data trust is considered the utmost important factor since the information circulated in VANETs are life-critical, time and delay-sensitive. The majority of attackers prioritize their attacks on fabricating, tampering, and causing delays in disseminating data since the data/information is the most pivotal and the vulnerable component of VANETs. Research has been conducted for introducing a trust-based scheme that implements a solution to efficiently identify and eliminate the dissemination of malicious data and assure honest vehicles with the propagation of accurate and legitimate information. These solutions consist of both centralized and distributed approaches. These include calculating similar events, probabilistic and deterministic approaches, and an intrusion-aware trust scheme. The remaining part of this section consists of a literature survey on various data-centric trust models.

Yue Wu et al. [61] has proposed a new data-centric trust model based on Dempster-Shafer theory to verify road information accurately. It also employed a general voting algorithm based on DS theory to validate the trustworthiness of exchanged information with the maximum vote count. The proposed model does not employ any trust scheme for evaluating entity trust; instead, it implements an IBC for validating a node at the receiver end. Each vehicle is categorized as equipped and unequipped vehicles, and further, unequipped vehicles constitute common, malicious, and trusted vehicles based on predefined responsibilities. When one of these equipped vehicles transmits a message, the receiver vehicle authenticates the sender vehicle based on IBC, and the information is compared with the local database. This local database contains information about all the events that occur in its segment (vicinity). The receiver vehicle checks the similarity between the information, verifies the time stamp, and updates the database with the newest information. To avoid inserting malicious data

into the database and updating it to the local maps, the proposed model employs DS theory to evaluate the trustworthiness of received information.

In [39], a data-centric trust model based on similarity metric, which is aided by infrastructure such as RSUs, has been proposed. The principle of this model is to calculate the trust of a message instead of a node that transmitted it since a node makes a decision based on the received information, which can be critical, and hence consequence of the decision is highly dependent on that exchanged data. The proposed model emphasizes preventing attacks that are performed by malicious vehicles that act as trustworthy nodes. It implements two tables, neighbor similarity and trust table. The former evaluates the similarity factor to either 1 or 0 based on the speed range of the sender node and its recently traversed RSU. The latter is updated by calculating and assigning trust values to the sender nodes based on similarity and historical interaction. If the sender vehicle's ID is not present in the trust table and its similarity value is 0, then the node is added to the debarred list and marked as malicious nodes.

A combined probabilistic and deterministic approach has been proposed by Rawat et al. in [53]. It aims to prevent VANETs from harmful messages by determining the trust level of a received message based on few factors and decides whether to forward or discard it. Two scenarios are considered in the probabilistic approach, such as single malicious and multiple malicious drivers' detections. In both cases, all the vehicles' suspicious level and trust level are evaluated by making observations on a timely basis. Once the trust values are obtained, it is compared with a predefined threshold value, Signal-to-Noise Ratio (SNR) and if a vehicle is computed as trustworthy, then the transmitted message is forwarded to the next step. In the deterministic approach, the trustworthiness of the message in step-1 is evaluated based on two distance factors, location coordinates and received signal strength. Finally, the overall distance computed is compared with the predefined threshold value, tolerance for deciding on the trustworthiness of the received message.

In [46], Wei Lo et al. has proposed a dynamic Event-based Reputation System (ERS)

to prevent the propagation of inaccurate and false traffic messages from saving time and fuel for the drivers. ERS is based on the collaborative enforcement technique of MANETs to closely observe inappropriate behavior, disclose the malicious vehicles, and broadcast warnings to the neighboring nodes. ERS possesses four functions such as event management, reputation value adaption, event confidence list, and reputation value collection. The first two functions are designed to control the events that occur in the network and handle the corresponding reputation values of a detected event. The latter two functions define an event's intensity and the event's reliability, respectively. Based on the predefined threshold limits, the intensity and reliability of a detected event are evaluated and thus helps the honest vehicles distinguish between safety and malicious messages. On the whole, ERS follows an event observation scheme to control the events and a reputation-based scheme to evaluate confidence and reliability on the exchanged information.

Dynamic routing assists vehicular nodes in VANETs to reroute around the congested areas based on the road information propagated in the network. However, due to the presence of malicious nodes, honest nodes are deceived by the false information that led to serious accidents. To handle this scenario, Wang et al. [59] have proposed a data-centric trust model that utilizes Bayesian Inference (BI) in the voting scheme. The proposed model is similar to [61], but the difference lies in the algorithm integrated with the voting scheme. In [61], Dempster Shafer theory is implemented in collaboration with voting scheme whereas in [59], BI is implemented. The main difference between DS theory and BI algorithm is, during the scenario where the number of malicious and normal messages are the same, the former employs an evaluation scheme based on two groups. It calculates a mutual trust from these two groups, which is then compared with the threshold value for trustworthiness. In the latter case, high probability and low probability values between the malicious and normal messages are calculated, combined, and compared with the threshold value. The reason behind integrating both these algorithms with the traditional weighted voting scheme because in the scenario mentioned above, with the weighted voting scheme, the receiver node tends to select a malicious message due to their number advantage instead of a normal message.

To overcome the limitations of historical recommendations and privacy concerns in VANETs, Alzahrani et al. [56], have proposed an identity anonymous based trust model functions in three phases. In the first phase, each node evaluates their confidence in the received message based on four factors such as location closeness and verification and time closeness and verification. These confidence values are forwarded to phase-2, in which the proposed model measures the trust of each message based on confidence. In the third phase, the method evaluates a decision in two steps. The first step selects the message with a higher trust value than the other messages in the pool. The second step compares the trust value with the minimum acceptable threshold value to determine the data's trustworthiness.

A Lightweight Self Organized Trust (LSOT) model is proposed by Liu et al. [62] which aims to address the unique and challenging characteristics of VANETs such as high mobility and random distribution. LSOT functions in two phases, including trust certificate-based trust evaluation and recommendation-based trust evaluation. Upon interacting with their neighboring vehicle (trustee), each vehicle (certifiers) forms an opinion based on its behavior and stores the trust information in its local storage. When the trustee tries to interact with a new vehicle (trustor), the trustor needs to establish trust information about the trustee. Due to high mobility, the trustor is unable to receive the trust information from certifiers. The trustor needs to generate trust information about the trustee, which is already generated by certifiers. To overcome this situation, a trust certificate-based trust evaluation scheme is implemented. A set of certifiers generates a trusted certificate based on locally stored trust information and forwards it to the corresponding trustee. Whenever a trustor tries to contact a trustee, it is provided with a trusted certificate. To evaluate the trustworthiness of the certificate, the proposed model employs three factors, number weight, time decay weight, and context weight. Alongside these weight calculations, in the second phase, recommendation trust evaluation, a set of recommenders generate opinions about the trustee and forward them to the trustor. Based on these recommendations and weight evaluations, the trustor can determine the trustworthiness of the information sent by the trustee.

All the data-centric trust models mentioned above focused on implementing a trust scheme based on recommendations, weighted voting, or calculating similarity between the events. Despite their advantages, each model has its limitations. In scenarios related to the evaluator node, the time taken to assess the evidence, decide and share the trusted data to all the vehicles in its vicinity is most challenging. Approaches related to preserving location and privacy data face many geographical challenges, such as overwhelming redundant data describing a similar event, which affects the processing time at the evaluator node. Few solutions have limitations, such as lack of availability of neighboring vehicles and infrastructure, for instance, in rural scenarios. The common drawback with all these solutions is that they do not consider evaluating the trustworthiness of an entity and completely rely on data trust. The other major drawback is not considering two types of trust metrics: direct and indirect trust, which disseminates accurate results compared with single metric trust calculation.

3.3 Hybrid trust models

Hybrid or combined trust models inherit the characteristics of both entity and data-centric trust models. They aim to identify the honesty of a sender node by evaluating the trustworthiness of the transmitted information. According to the statistics, hybrid trust models are considered a prominent approach that generates accurate results since trust computation is performed on the information, which provides a means to identify the reputation of an entity. Various hybrid trust models are proposed that have functionality in two dependent phases. The first phase carries the trust computation of a sender node. A decision is obtained whether to forward it for the next phase for computing data trust or discard it and prevent disseminating malicious data in the network. In the second phase, the trustworthiness of the transmitted data is calculated based on various factors such as functional and recommendation trust, direct and indirect trust, the similarity between data, and many plausibility checks. A final decision is obtained on whether to broadcast the data in the network or discard it safely.

A Beacon-based Trust Management (BTM) scheme is proposed by Chen et al.[17], which focuses on enhancing location privacy for the drivers alongside restricting internal attackers from propagating false information in the network. BTM implement a hybrid trust model in which entity trust is computed from beacon messages and directly received event messages. Data trust is calculated using the traditional event trust recommendation method. Beacon-based trust is calculated using the vehicle's position, driving direction, and velocity. Direct event-based trust is calculated by using a position and movement verification mechanism. Applying these two-trust metrics, beacon-based and direct event-based trust, the trustworthiness of a sender node is calculated. The trustworthiness of the event or the event message is calculated using indirect trust-based trust. The receiver establishes a trust relationship on the received information based on the recommendation from the neighboring vehicles. After combing all the obtained trust values, the overall trust is calculated and compared with a defined threshold value to accept or discard the event message.

A logistic trust-based approach is proposed in [10] by Saneeha et al., which describes a learning-based scheme for determining the truthfulness of the events. These learning are further integrated with neighbors' opinions to assess the trustworthiness and behavior of the sender nodes. The proposed model claims to combine the opinions and observed behavior using a logistic trust model and attain over 99 percent accuracy with rapidly changing events. This model carries in two phases. In the first phase, upon receiving an event message, each vehicle tries to identify the authenticity of the message by a weighted voting scheme in which each message is divided into two bins, one containing positive claims and the other one with negative claims. The average value of both bins determines the trustworthiness of the message. Therefore all the nodes who learned about the authenticity of the message can detect the malicious nodes. For instance, if the receiver node has computed the information as safe and any vehicle claiming it to be malicious, known as Anamoly Ratio (AR), is considered dishonest. A proposed logistic approach is applied to generate opinions about the neighboring vehicle, which overcomes the limitation of AR and allows the receiver node to identify the malicious nodes.

Hussain et al. [29] has proposed a trust management scheme for emerging vehicular social networks. In this model, two trust establishment and management schemes are proposed, such as an email-based social trust for identifying the trustworthiness of the vehicle and social networks-based trust for calculating the trustworthiness of the information. The proposed trust mechanism is divided into three steps, trust bootstrap, trust calculation, and evaluation and trust query. The first step involves the initialization of user lists where each node constitutes three lists based on their previous interaction through emails, social networks, and random encounters. The second step includes evaluating trust based on local trust and recommendation trust, which are computed for both email and social network schemes. The final step includes a bonus step, which allows any node in the network to pose a query to its neighbor about another node's trust information. This will facilitate any node's ability to attain any other node's trust information without performing any trust computations.

Li et al. [40] has proposed an Attack Resistant Trust (ART), which employs a hybrid approach to identify the presence of malicious nodes and propagate false information alongside coping up with malicious attacks. The proposed model detects the authenticity of a message by applying Bayesian inference (BI) on the sensed data, which is collected from multiple nodes, and the trustworthiness of a node is calculated using Functional Trust (FT) and Recommendation Trust (RT). FT indicates the level of honesty the sender node displays while fulfilling its functionalities, and RT includes the calculation trustworthiness of a node to accept the recommendations forwarded by it.

A hybrid trust management scheme based on beacons and RSU is proposed by Wei et al. in [60]. RSU-based Beacon Trust Mangement (RaBTM) aims to prevent internal attackers from broadcasting malicious messages in the network by enabling quick propagation of opinions and recommendations. In this model, RSU plays a vital role in assisting vehicular nodes in detecting malicious nodes and information. Each vehicle propagates its opinions to its neighboring vehicle upon detecting an event. During this point, the attacker nodes disturb the adjacent node by sending false or opposite

information in counter to the information sent by honest nodes. RSUs, which are installed at the roadside and corners of the road, can learn about the correctness of the event with the help of other RSUs. Hence, RSU evaluates the correctness of the data using position verification and opinions from other RSUs and forwards it to nearby vehicles. Once the overall trust value is calculated at the evaluator node, it employs Dempster-Shafer theory to formulate a threshold value to perform comparisons and draw a conclusion.

Mahmood et al. [48], has proposed a hybrid trust management scheme that restrains the network from electing a malicious node as cluster head (CH) and detect such nodes by identifying the trustworthiness of the information transmitted by them. In the proposed model, each node forms a part of a vehicular cluster with a hop distance of 1. Trust values for each node are assigned by its one-hop neighbor based on their behavior, determined by the content of transmitted data. Furthermore, based on the node's resource availability, a trust value is computed to determine whether the corresponding can be able to fulfill its minimum requirement or not. Based on the computed trust score and resource availability, a cluster head is elected. CH election is carried on a timely basis, and if a node's resource capacity is less than the threshold level, a new CH will be elected. During this process, if the composite metric values of a node from past interactions are less than the minimum threshold value, it is tagged as malicious and prohibited from being elected as CH.

In [16], an evidence-based trust management scheme has proposed by Chen et al., which aims to early detection of malicious nodes and prevent them from propagating harmful data. The proposed model, Trust Management based on Evidence Combination (TMEC), includes three steps to compute the trust values and attain a global trust. In the first step, data trust is calculated by Dempster- Shafer theory, which is used to combine pieces of gathered evidence on a particular event with belief and plausibility function. Once the data trust is obtained, recommendation trust and direct trust metrics are employed to validate the sender node's honesty. Finally, a global trust value is computed by the receiver/neighboring vehicle using direct, indirect, and data trust.

The key challenge with hybrid trust models includes the calculation of entity and data trust, which results in a higher probability of infusing computational overhead in the network. Alongside, all the approaches that involve electing a CH face challenges related to biased selection of CH through weighted voting. In scenarios where the network is flooded with dishonest vehicles, the elected CH turns out to be the malicious node. Few approaches rely on neighbors to gather opinions about the sender nodes, and in such scenarios, the lack of presence of neighboring vehicles results in uncertainty.

3.4 Research Gap

This section illustrates the research gap that has been identified after surveying literature established in the previous works.

1. While performing entity-centric trust computations, a database or a lookup table can help the receiver nodes check for any past interactions with the sender nodes. If there is any past interaction, the receiver node computes trust with the available trust information and tags it as a malicious or honest node. If there is no entry, an efficient technique must be implemented to create an entry for the newly interacting vehicle and attain initial trust values, which will assist the receiver node to identify the malicious nodes at the lower levels. The implementation of the lookup table differentiates between two scenarios, such as communication with i) previously interacted vehicle and ii) newly interacting vehicle. These two scenarios must be considered mandatory because for a network that possesses characteristics such as high mobility and rapid topology change, and exchange information that is time-sensitive and life-critical, the implementation of a lookup table proves to be efficient as it can identify and eliminate malicious nodes at the lower levels which makes the network fast and secure.

2. In data-centric trust computation, various trust metrics have been implemented to compute direct and indirect trust. Nevertheless, it would be more efficient

and accurate if the opinions and recommendations about a particular traffic event are gathered from the most trusted vehicles in the network.

3. RSUs are considered the heart of VANETs. Although they possess more priority than mobile nodes, the deployment of RSUs is limited in rural areas. They have built-in responsibilities such as monitoring the overall network, communicating with neighboring RSUs, thereby extending the communication range and supporting various user-based applications. Since RSUs are assigned with various tasks, all the mobile nodes must be designated with the role of carrying the entity-centric and data-centric trust computations. Using this approach, the network's roles and responsibilities are modularized and efficiently shared among different entities, which would create a positive impact in reducing overheads.

4. Different types of scenarios such as previously and newly interacted vehicles, challenges that occur while assigning positive and negative ratings, and identifying misbehaving nodes with the help of mobile node and RSU communication have the least consideration.

5. Each node can generate 15 types of messages which include basic safety messages (BSM), periodic beacons, cooperative awareness messages (CAM), and also non-safety messages related to infotainment and parking tolls, etc. Trust computation is not required for all types of messages, which would increase the overheads and delays. Hence, messages should be categorized based on severity level, and trust must be computed for highly prioritized messages.

3.5 Summary

Although a wide range of solutions has been introduced to efficiently handle trust management issues in VANET, very few techniques attempted to explain different scenarios that occur during V2I and V2V communication. Most of the work is related to calculating the trustworthiness of the sender node and transmitted data by implementing one or two schemes. All the above-mentioned problems are integrated and addressed using a framework that includes a hybrid trust management model

that ensures reliable communication and restricting malicious nodes from performing MiTM attacks besides demonstrating five scenarios and three categorizations of messages. Finally, the results are obtained by simulating two scenarios: i) the number of malicious nodes is kept constant, and honest nodes are varied, and ii) the number of honest nodes is fixed, and malicious nodes are varied.

Chapter 4

Proposed Methodology

This section provides insight into the proposed trust management scheme which is a partial integration of two trust calculation techniques in VANETs such as Blockchain-based Anonymous Reputation System for Trust Management (BARS)[47] and Man-in-the-middle Attack Resistant trust model in connected vehicles (MARINE)[9]. The proposed model's novelty comes from a scenario-based approach, which walks through different scenarios while calculating trust values that are salient for a vehicular node to decide on the trustworthiness of received information and the sender of it. The idea adopted from these two techniques has been improvised according to the requirements of the proposed scheme. As stated in chapter 1, five scenarios are considered, which occur at different stages during a communication between a sender and one or more receivers. Every mobile node encounters different scenarios during packet forwarding and message exchange due to the large scale of VANETs and high mobility of vehicular nodes. These scenarios are specific to the situation and they play a vital role in calculating trust. Their impact is high on avoiding road accidents and enabling a reliable communication between vehicular nodes in the presence of malicious nodes. This is because, different type of attackers reside in the VANET and the level of attacks they perform can be distinguished based on the severity. Few attacks, for instance, delaying packet transmission by few seconds might lead to collisions due to the time-sensitive nature of the information. On the other hand, attacks such as dropping the packets and forging the messages can lead to accidents which cause threat to the life. Besides, few malicious nodes tends to misbehave occasionally and act as honest node for most of the time which is known as On-off attacks [11]. These type of attackers must be addressed with a specific and suitable security approach rather than employing traditional trust validation techniques. Therefore, employing a generic trust validation technique for all the scenarios might not provide the required level of efficiency, especially while validating trust for time-sensitive and life-critical

data. The main objective of this scheme is to show the necessity of implementing different approaches for each scenario rather than a generalized approach yet enhancing the performance of the current system.

The proposed model also demonstrates a 3R message categorization approach in which all messages are categorized based on few key factors. According to the specifications mentioned in one of the DSRC security standards, Society of Automotive Engineers - SAE J2735, each vehicular node can generate up to 15 different types of messages ranging from safety to non-safety messages. These messages include life-critical, alert, periodic beacons, status updates, and infotainment data [11]. Trust computation is not necessary for all messages that transmit in the network because not all messages are confined to enhancing safety. Messages related to user-based applications focus on improving user experience, and these do not contain any safety-related data. Few other messages include neither accident alerts nor infotainment data. Such types of messages enable vehicular nodes to disclose any malicious node's identity to central authorities. Trust computation for these types of messages must be different since they require validation of the node's behavior. In order to address the mentioned problems, a 3R message categorization approach has been implemented in the proposed work, which categorizes messages into three types, namely rush, revoke and refresh, based on the severity and role of each message. Refresh messages are related to entertainment and fall under the category of non-safety/user-based applications. These messages constitute data related to tolls, parking, and entertainment. Rush messages are alert messages and fall under the category of safety applications. These messages include collision avoidance, black ice warnings, and lane changing assistance. Revoke, or foreclosure messages, are also a category of safety-based applications whose primary motive is to identify the misbehaving nodes in the system and foreclose them to nearby RSU. Without these messages, an efficient routing protocol cannot be implemented. The first two messages avoid packet dropping due to few network conditions, such as collision. Scenario 1 and 2 implements the application of rush messages, while scenario 3 implement revoke messages. Using such an approach, the ability of the proposed model is enhanced to identify the attackers accurately.

This section also contains information about various concepts that are implemented such as OIF, data and node trust computations, algorithms and flowcharts, infrastructure computation, and enhanced performance with man-in-the-middle(MiTM) attacks. The details of implementation and performance evaluation are precisely explained in the next chapter.

.

4.1 Scope and Assumptions

The state-of-the-art models designed for addressing the security issues involved in VANETs, during information exchange between two or more entities, are mostly based on trust or reputation management schemes. With the advancement of new technologies, solutions based on traditional identity management and PKI cryptosystems are limited to identify only the external attackers. Rise of security standards and presence of central authorities, such as Trusted third party (TTP), certificate authority (CA) and Legal Enforcement Authority (LEA), in VANETs, have strengthened the security measures on the one hand but engendered a scope for advanced security threats on the other hand. These strengthened security measures refer to the development of various trust management schemes, which have been implemented to address the drawbacks of the existing cryptography solutions. These trust schemes are built in coalition with existing solutions and work as extended security measures for current security issues. Similarly, the proposed methodology is built to address the issue of internal attackers, who perform attacks after registering as a legitimate user, assuming the concerns of external attackers are handled using the traditional security solutions.

This paper illustrates a hybrid trust management scheme designed to handle one of the crucial security concerns, namely MiTM attack. Many trust management techniques address only security or privacy concerns due to many constraints, the primary being the rapid change of topology and short inter-contact times. Technology like BARS[47], has implemented the concept of blockchain to preserve the privacy of user information efficiently. Likewise, the proposed methodology focuses on implementing a trust model to render a secured environment for the users. As mentioned previously, the primary objective of the proposed model is to provide insights into

multiple scenarios that occur during V2V and V2I communication. The state-of-the-art models have succeeded in obtaining a generalized solution. This dissertation identifies the necessity in proposing slightly different approaches for each scenario and enhancing the system's performance with respect to four performance metrics. Considering various situation that occur at different stages during the information exchange, five scenarios are considered and addressed using different approaches.

As mentioned earlier, the proposed model's novelty lies with the scenario-based approach, where the first scenario has been addressed previously by multiple researchers with different trust management schemes. In contrast, the other four have not been demonstrated. The first and second scenarios illustrate the trust calculation of a sender vehicle based on the previous interaction. Few trust management schemes have implemented the database concept to store interactions with neighboring vehicles [9]. If the same vehicle encounters in the future, the database will help distinguish between i) a previously interacted vehicle and ii) a newly interacting vehicle. The former has been considered in many previous works, but no approach has been implemented for the latter one. This dissertation introduces a new concept called OIF, which helps the receiver node attain initial trust values if a newly interacting vehicle forwards a packet. Scenario 3 demonstrates the advantage of RSU's deployment in the network and implements the concept of revoke messages that can be achieved through the node-RSU communication. Using the revoke messages, dishonest nodes can be identified without even establishing any connection with them. However, with the level of priority that RSU possesses in the network, they gather the required evidence and make a decision. Scenarios 4 and 5 address the challenges that occur while assigning ratings to the sender node based on their conduct, especially in the presence of misbehaving and deceiving nodes.

4.2 Baseline

The proposed model involves multiple stages that begin with event detection followed by connection establishment, propagation of different types of messages, identifying

the trustworthiness of both sender and the information using a two-dimensional approach, and concluding with a receiver's decision to either accept or reject the information. The trust evaluation is carried in two steps- entity-centric and data-centric computations. In the first phase, entity-centric computation, a vehicle's honesty is calculated based on the previously available information such as past or historical interactions and comparing with a predefined threshold range. The second phase, data-centric computation, includes calculating the trustworthiness of the received information based on direct and indirect trust. If the final trust value falls within a threshold level, it is recommended to accept the information. In the other case, the receiving node drops the data. The proposed model relies on the hybrid trust model approach which calculates the trustworthiness of data and entity and enables reliable communication between the vehicular nodes in the presence of malicious nodes such as MiTM attackers that perform attacks in the form of dropping the packets.

Before delineating the experiment, few concepts are introduced here. At the beginning of the experiment, each vehicle is assumed to be part of VANET system only after registering at CA or TTP and attaining valid credentials and certificates. These certificates can be revoked based on the level of malicious acts performed by a respective entity. As soon as the experiment is started, each vehicle moves on a defined path. Besides traveling, each vehicle is programmed to identify various kinds of traffic-related events and propagate safety and beacon messages to its neighbors. Since the information can also include non-safety information, it is not ideal to forward every message for calculating trust. Based on the severity and role of each entity, the messages are characterized into three types such as refresh, rush, and revoke messages. Refresh messages are considered less severe, including periodic updates on vehicle status and infotainment-related infotainment-related data. Rush messages are highly prioritized and identified as emergency warnings. These messages include accident-warnings, collision avoidance, black-ice warnings, and other life-critical data. Revoke messages are broadcasted to disclose a node's identity after recognizing any malicious behavior. Each message is prioritized based on the severity of the information and is broadcasted to various entities to overcome the fundamental problems of a VANET system, such as overload and delays.

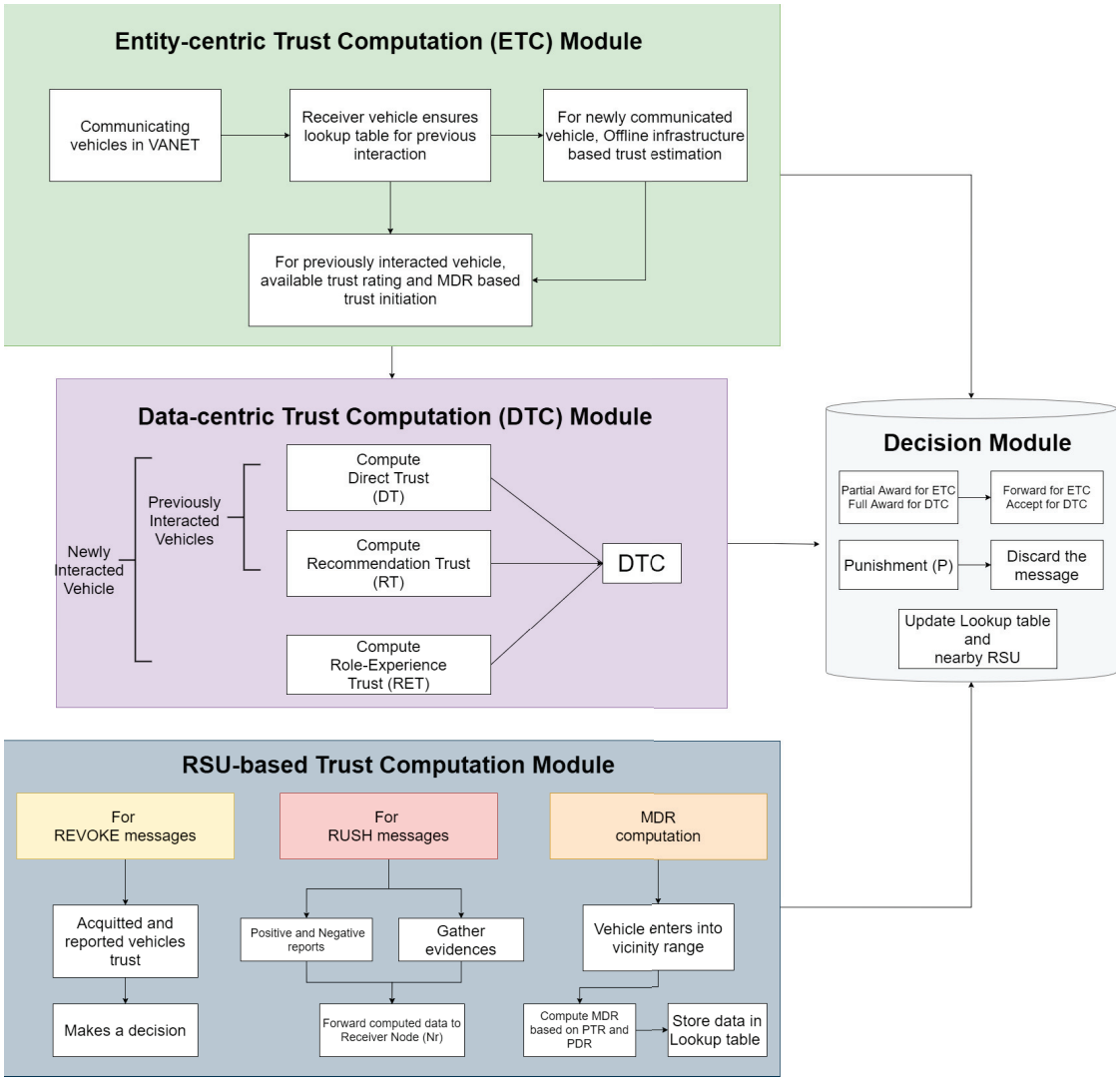

Figure 4.1: Overview of the Proposed Methodology

The proposed model is claimed to perform competently since the system is distributed. Refresh messages are only broadcasted to other vehicles as a part of V2V communication since they pose the least level of security concerns. Revoke messages are only forwarded to RSUs since the role of RSUs are higher than the mobile nodes. RSUs gathers evidence, validates the message, and registers a complaint at CA or TTP for revocation of dishonest node's credentials. Rush messages are forwarded to neighboring vehicles to calculate trust and to RSUs to store the data and use it for validating revoke messages. In each situation, computation is done by only one entity, either the mobile nodes or RSUs, thereby lowering the computational overhead

and delays caused in the system. Each entity in the system maintains a record that contains information about past interactions such as vehicle ID and their respective rating. This record is considered as a lookup table for the receiver node when a sender node initiates communication. These ratings are one of the key factors in computing node-centric and infrastructure trust calculation. The remaining sections brief the different scenarios and two types of trust calculations in each scenario.

Table 4.1: Lookup Table

Vehicle ID(VID)	Honest Rating (HR)	(A, P)	MDR

4.3 Entity-centric trust computation

Each vehicle in the system can identify any emergency event on the road based on high vehicle density and then broadcast rush messages to its neighboring vehicles. Every vehicle possesses a message Transmission Range (TR) which is dependent on the positioning of antenna[21][32]. A transmission range of 250m is defined for every vehicle, which is also considered as a threshold range in the case of entity-centric trust computation. Based on this TR, the sender node(Ns) broadcasts rush messages to its neighboring node. On the other hand, zero or more receiver nodes(Nr) acquire information and initiates the computation. Since each node maintains a lookup table, the receiver node checks its table for any record of past interaction with the sender node. The scenarios are apportioned during this phase; scenario-I(S1) explains the case in which a previous interaction between sender and receiver exists, and scenario-II(S2) explains the case of no previous interaction between sender ad receiver nodes. For each scenario, ETC and DTC are carried with few changes in the approaches as per the requirement.

Table 4.2: Message Format

Vehicle ID	Payload	Timestamp	Signature

4.3.1 SCENARIO- I

This scenario is straightforward since a previous interaction between Nr and Ns is identified, indicating that information about Ns is present in the form of ratings. Availability of such information can improve the processing time and lower the delays. The content of a message includes Vehicle-ID (VID), payload, timestamp, and signature[52]. Each lookup table has an entry for a previously interacted node in the form of VID, a trust value or Honest Rating (HR) which can be either positive or negative, recent rating information in the form of award and punishment values, and MDR. These ratings are obtained as part of computations performed during previous interactions, including adding an award(A) value or subtracting a punishment (P) value to the current trust rating. Each vehicle is subjected to either award(A) or punishment(P) factors. These factors depend on the dissemination of proper messages and exhibiting honest behavior. MDR is defined as the node's ability to propagate the information to its neighboring vehicles. Computation of these factors and MDR, updating lookup table with positive or negative ratings will be discussed during data-centric computation. Meanwhile, Nr confirms the trustworthiness of Ns by checking whether Ns falls in its transmission range, which is calculated using a factor called tThreshold Value (TV). If TV of Ns is less than pre-defined TR, then the node-centric computation for Ns is positive, and hence its rating and MDR from the lookup table is forwarded to step-2 for data-centric trust computation. Also, in this case, Ns is assigned with partial award value (A). Suppose the resultant TV of Ns turns out to be negative, which indicates that the Ns is outside the TR of Nr. Then the message is discarded, and a penalty value (P) is assigned to Ns. This value is reflected in Nr's lookup table and forwarded to the nearest RSU for further calculations.

For malicious vehicle: HR = HR - P

For honest vehicle : HR = HR + A

According to [9], the TV of each vehicle is calculated using a function of three parameters, which include the distance between Ns and Nr(D), antenna height of Ns(AHs), and antenna height of Nr(AHr).

$$TV = \sqrt{D^2 + (AH_s + AH_r)^2} \tag{4.1}$$

MDR is calculated using Packet Transmission Ratio (PTR), which indicates the node's ability to successfully transmit the message to its neighbors, and Packet Drop Ratio (PDR), which is the representation of node's malicious behavior in the form of dropping the packets and ceasing the propagation of information. These are categorized as MiTM attacks and such nodes possess high PDR and low PTR. In contrary, honest vehicles possess high PTR and low PDR, thereby attaining positive MDR. While calculating MDR also includes two other factors such as award(A) and penalty(P). A is associated with PTR and P with PDR since A is assigned based on node's honesty in propagating accurate information, which is similar to PTR and P is assigned based on node's malicious behavior, similar to PDR. MDR of a particular node is calculated by RSU since it has access to a wide range of information compared with vehicular nodes. When a vehicle enters the transmission range of a RSU, it calculates MDR [9] of that vehicle and updates nearby vehicles' lookup table.

$$MDR = \sum_{i=1}^{n} \frac{(A \times PTR)}{(A \times PTR) + (P \times PDR)} \tag{4.2}$$

4.3.2 SCENARIO- II

Due to the high mobility of vehicles in VANETs, it is possible for any two vehicles not to possess any historical interaction, leading to unavailability of trust information of one vehicle to another vice-versa. The non-existence of entry in the lookup table would make entity-centric trust computation less efficient and accurate. Very few solutions have been proposed in the past to address this scenario but with minimal details. In the proposed model, this problem is addressed with a unique approach, termed as Offline Infrastructure Factor (OIF), which stands out to be efficient, accurate, and reliable, comparatively with state-of-the-art models.

Upon receiving a rush message, Nr performs a regular check of the lookup table for any past interaction with Ns. If there is no entry in the table, with the help of OIF, Nr will receive the initial trust numbers required for creating an entry in the lookup table and forwarding Ns to further step for data-trust computation. OIF is computed with the help of RSU whenever the vehicle enters its vicinity range. Each

Algorithm 1 Entity-centric trust computation for Scenario I and II

Initialize the system with eight inputs.
Honest rating (HR); award (A) and punishment (P) pair; message dissemination ration (MDR); vehicle ID (V_{ID}); defined threshold value ($TV_{defined}$); antenna height of receiver (AH_r); antenna height of sender (AH_s); and distance between sender and receiver nodes (D).
Upon receiving a message, receiver node (Nr) checks the database for an entry belonging to sender node (Ns).
procedure ETC
    if ($V_{ID} \in lookup$) **then**
        Compute threshold value (TV) for Ns
        if ($TV \in TV_{defined}$) **then**
            Assign award (A) and forward Ns for data trust computation
            Forward the lookup table information corresponding to Ns.
        else
            Tag as a malicious node
            Assign punishment (P) and discard from further computation
        end if
    else
        Initiate offline infrastructure factors (OIF)
        Request trust data from nearby RSU
        if ($data\ available$) **then**
            Create an entry in the lookup table for Ns
            Assign the OIF value for Ns
            Compute threshold value
            Forward or discard based on resultant TV
        else
            Assign sample numbers using initial numbering scheme
            Forward or discard based on TV
        end if
    end if
end procedure

RSU can interact with another RSU through the infrastructure communication technology employed in VANETs. Therefore, whenever a vehicle enters the vicinity range of a RSU, it immediately collects the information about the vehicle from the neighboring RSU and stores it in its lookup table. Thus, upon identifying the non-existence of trust information about Ns, Nr sends a request to nearby RSU and collects the required data. After receiving the trust information, Nr creates an entry for Ns in its lookup table and assigns the received trust data. In the next step, Nr verifies whether Ns falls in its transmission range or not and decides to forward it or discard it, as mentioned in the scenario I.

4.4 Data centric trust computation

In this step, Data-Centric Trust (DTC) is performed on the nodes that obtained positive TV. Firstly, this step is required for two main reasons explained in scenarios IV and V. Since the trustworthiness of Ns is evaluated in step- 1, it is equally important to identify the trustworthiness of the transmitted information. There are various factors to calculate the trustworthiness of a propagated information, such as weighted voting, watchdog mechanism, functional trust, to name a few. In this proposed model, the trustworthiness of data is calculated using a 3-step approach. In step-1, the trust value is calculated based on direct trust(Direct Trust (DT)) that includes computation involving the sender and receiver of the message. In step- 2, a Recommendation Trust(RT) in the form of recommendations and opinions from the neighboring vehicles are calculated, enhancing the quality and accuracy of the data-centric computation. In step-3, a new concept known as Role and Experience-based Trust (RET) is implemented, in which opinions from the role and experience-oriented vehicles are considered.

VANET is a medium for diversified vehicles that include bicycles, motor vehicles, cars, buses, public taxis, and so on, which serve the purpose of transportation. Apart from public vehicles, few other vehicles provide various services to each individual and are registered as government vehicles. These vehicles are authorized and regulated by governing bodies such as CA and LEA. Such vehicles are assigned with the highest priority since they are role-oriented (Ro), perpetually monitored by a central entity, and supposed to propagate accurate information. Similarly, few vehicles

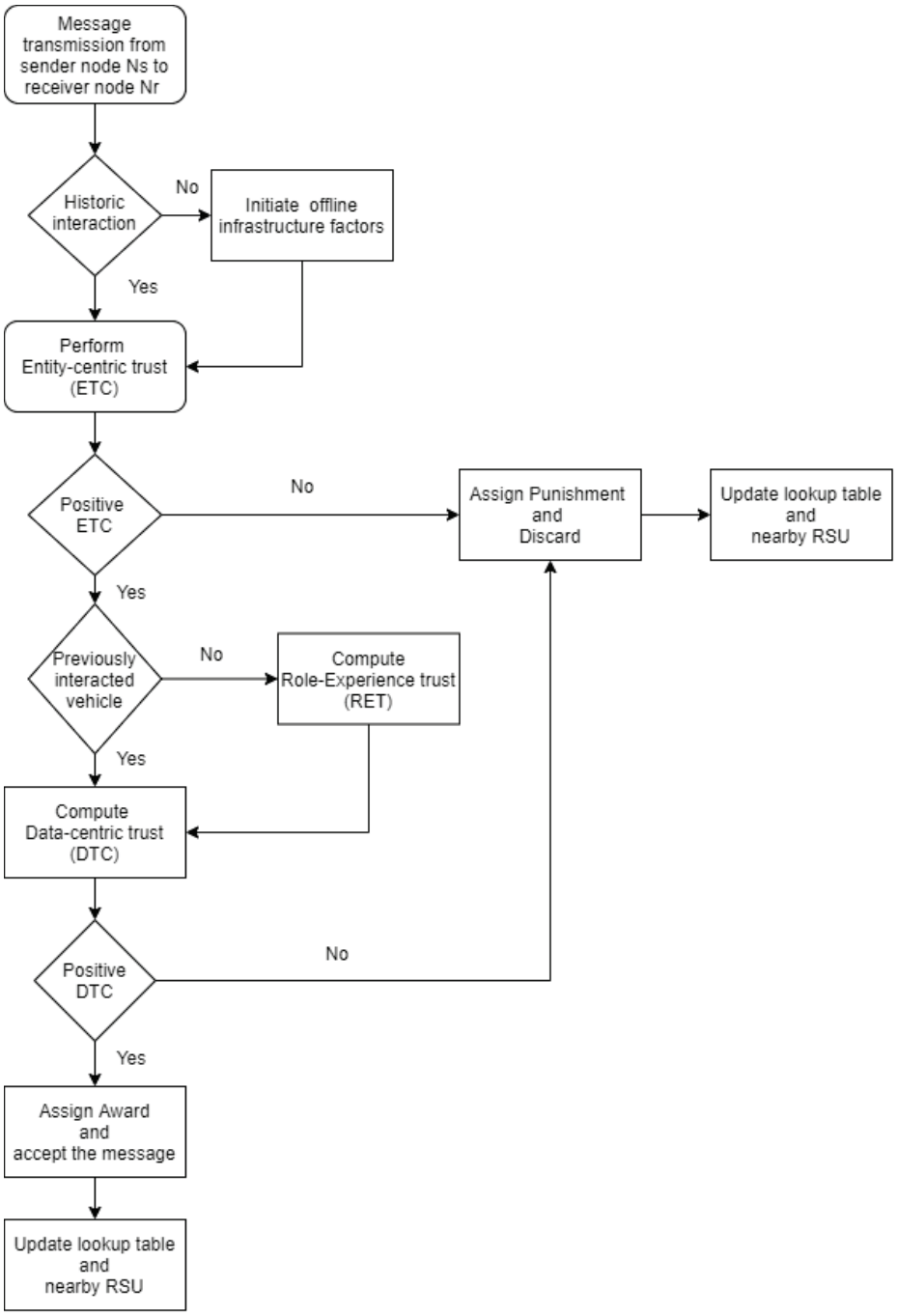

Figure 4.2: Flowchart for ETC and DTC

are registered in the system for a long time yet maintaining a positive rating in the lookup tables of nodes and RSUs. These vehicles are named experience-based(Eo) vehicles, and their decisions are assigned priority next to role-oriented vehicles. Using this 3-step approach, the proposed model carries data-centric trust computation with

utmost accuracy and supports the receiver node in identifying the honest node and information. Here data-centric computation for both the scenarios, S1 and S2, are explained.

4.4.1 SCENARIO- I

This section is a continuation step for the process held in scenario- I of entity-centric trust computation. On the successful computation of trustworthiness of Ns, it is forwarded to this step for calculating the trustworthiness of the transmitted information. Firstly, direct trust (DT) of Ns is calculated from the distance between sender and receiver (DistSR). The accuracy of transmitted information is highly dependent on the distance between Ns and Nr (European Telecommunications Standards Institute (ETSI))[2]. In the proposed model, the transmission range (TR) of Nr is divided into four equal-sized layers, and each layer is assigned with values ranging from 0.25 to 1, 0.25 being the farthest layer and 1 being the nearest layer. Each Ns is assigned with one of these values based on its positioning during the propagation of the message. This layered approach is a slightly modified version of the tier-based threshold approach from MARINE[9]. The main aim DT is to validate the trustworthiness of two primary entities involved in the communication, i.e., node and data, with respect to its physical characteristics. So the computation of direct trust involves the message disseminating ability of the sender node and the distance from which the message is transmitted. The MDR value for a sender node is calculated by nearby RSU and stored in the lookup table. The value of MDR is low, when the malicious node is present in the communication, since the MDR provides more important to the PTR in its equation. The message quality depends on the distance between the sender and receiver nodes and is calculated from the layered approach. If the message originated from the first four layers, a respective trust value is assigned, while the message originating from outside the range is assigned a trust value of 0. With the given equation, the value of DT can be non-zero only if the message originates from within the range. Since the trust value lies between 0 and 1, the equation ensures a final value between 0 and 1 as the denominator is always greater than the numerator in this case. Therefore, the DT value is high for the nearby node with good behavior.

$$DT = \frac{1}{2} \times \left(\frac{Dist_{SR} \times MDR}{Dist_{SR} + MDR}\right) \tag{4.3}$$

Secondly, the recommendation trust (RT) is calculated using the recommendations and opinions generated by neighboring vehicles on the current event. Each vehicle involves in the process of validating an event as soon as identifying it or acquiring it from their neighbors. Before Nr could perform the computation, any of its neighboring vehicle might possess information about it or could have evaluated the trust value. Considering such metric will enhance the trust computation process even better. Similar to MDR, RT is calculated in association with A and P. According to[9], RT is formulated as,

$$RT = \left[\left(\frac{A}{A+P} \times \sum_{i=1}^{n} Pos\right) + \left(\frac{P}{A+P} \times \sum_{i=1}^{n} Neg\right)\right]^{\frac{1}{n}} \tag{4.4}$$

where n represents no. of neighboring vehicles, Pos represent positive opinions, and Neg represents negative opinions.

Since the information about Ns is available in the form of honest rating (HR) and MDR, only DT and RT are computed for calculating trustworthiness of data sent by Ns. Data trust computation (DTC) in the case of previously interacted vehicle is computed as follows:

$$DTC = \sqrt{(DT + RT)^{HR}} \tag{4.5}$$

4.4.2 SCENARIO- II

In the case of a previously interacted vehicle, there is no such step involving RET computation. Information about such vehicles is available at a level where the final trust value obtained is accurate and efficient. But in Scenario- II, Nr carries minimal information about Ns and requires extra metrics when compared to S1, which is why an extra step of computation in the form of RET is implemented.

This is a continuation step for process held in Scenario- II of entity centric trust computation. At this point, Ns is forwarded for data-centric trust computation with only minimal data i.e., the initial values set for rating and MDR. Using the available information, in similar to S1, DT and RT are calculated. Since the accuracy of entity centric trust for S2 is not so accurate, RET is computed alongside DT and RT. Since role-based vehicle are assigned highest priority, the opinions generated by a role-based vehicle (Ro) is calculated as 0.8 and the opinions generated by an experience-based vehicle (Eo) is calculated as 0.5. DTC [9] for Ns is computed as follows,

$$DTC = (R_0 + E_0) \times \sqrt{(DT + RT)^{HR}} \tag{4.6}$$

Once DTC values are obtained for both the scenarios, it is compared with a pre-defined threshold value to confirm Ns' trustworthiness and its propagated information. The threshold value for DTC is initially set to 1. Over time, the threshold value is set to the minimum DTC of Ns. This will assist Nr in estimating whether the current behavior of Ns is better or not, comparatively.

4.5 RSU-based trust computation

Considering the minimal infrastructure, RSU plays a vital role in the functioning of VANETs by facilitating V2I communication with mobile nodes. The role of RSU is to monitor the vehicles extend their services to broadcast safety-related data. It also provides internet access to mobile nodes, thus serving user applications and extending communication between vehicular nodes. With the advancement of technology, RSUs have been upgraded from fixed to mobile. The main drawbacks of fixed RSUs include expensive deployment cost, restricted connection time, interrupted connectivity, to name a few. Researchers have implemented a solution to overcome such issues, such as mobile RSUs, which can maximize the connection probability, thereby reducing the response time and cost[22]. With the mobile RSUs, mobile nodes possess the provision of accessing safety information even though they get disconnected with a fixed RSU due to vicinity range issues. New solutions have been proposed to introduce 3 variants of RSUs which consists of fixed RSU, mobile RSU but not controllable and mobile RSU with full control[22]. The new variant includes busses, public taxis, post

Algorithm 2 Data-centric trust computation for Scenario I and II

1: Initialize the system with inputs
2: Honest rating(HR); (A,P); MDR; $TV_{defined}$; distance range between Ns and Nr(DistSR), positive(Pos) and Negative(Neg) recommendations, number of distinct vehicles(n), role-based(R0) and experience-based(E0) vehicles.
3: Data-centric trust (DTC) is computed for the vehicles that possess positive ETC.
4: **procedure** DTC
5: Calculate the distance range between Ns and Nr.
6: **if** ($Distance\ range \in TR$) **then**
7: Assign corresponding value to $Dist_{SR}$
8: Calculate DT based on $Dist_{SR}$ and MDR
9: **else**
10: Tag as malicious vehicle
11: Assign punishment and discard
12: **end if**
13: **if** ($not\ malicious$) **then**
14: Initiate Recommendation Trust (RT) computation
15: Request recommendations from neighboring vehicles and RSU
16: Calculate RT using A,P,n,Pos and Neg values
17: Compute DTC
18: **end if**
19: **if** $newly\ interacted\ vehicle$ **then**
20: Request event confirmation from R0 and E0 vehicles
21: Compute DTC and compare with $TV_{defined}$
22: **if** $DTC\ is\ positive$ **then**
23: Accept the message and assign award
24: **else**
25: Discard the message and assign punishment
26: **end if**

```
27:     else if previously interacted vehicle then
28:         Compare DTC with TV_defined
29:         if DTC is positive then
30:             Accept the message and assign award
31:         else
32:             Discard the message and assign punishment
33:         end if
34:     end if
35: end procedure
```

vans, and ambulances as mobile RSUs that can serve the only partial purpose of an RSU, such as extending the communication range and propagating safety information, because such vehicles are being controlled by a CA and exists on the transportation system to serve public.

According to [9], RSUs possess the capability of providing a quasi-global view of the overall network. As mentioned above, with all other abilities, RSU can calculate the trustworthiness of both entity and data. But the deployment of RSUs, especially in rural areas compared with urban areas, is supremely challenging due to cost, connectivity issues, and obstacles. Considering this fact, the overhead caused at various RSUs is reduced by computing both ETC and DTC by receiver nodes, thus assigning RSU a crucial role in handling revoke messages.

4.5.1 SCENARIO - III

Alongside propagating of traffic and safety-related messages, each vehicle is assigned to detect and disclose the malicious behavior of its neighboring vehicle. Upon detecting any malicious behavior, each vehicle sends a message to nearby RSUs to revoke the credentials of the dishonest vehicle; hence the name revoke messages. RSUs upon receiving revoke message, performs various plausibility checks such as gathering evidence about both reported vehicle (Vr) and foreclosed vehicle (Va) from trusted vehicles in the form of opinions, calculating the distance between Vr and Va, and accessing their rating information such as A and P values. Using these values, RSU

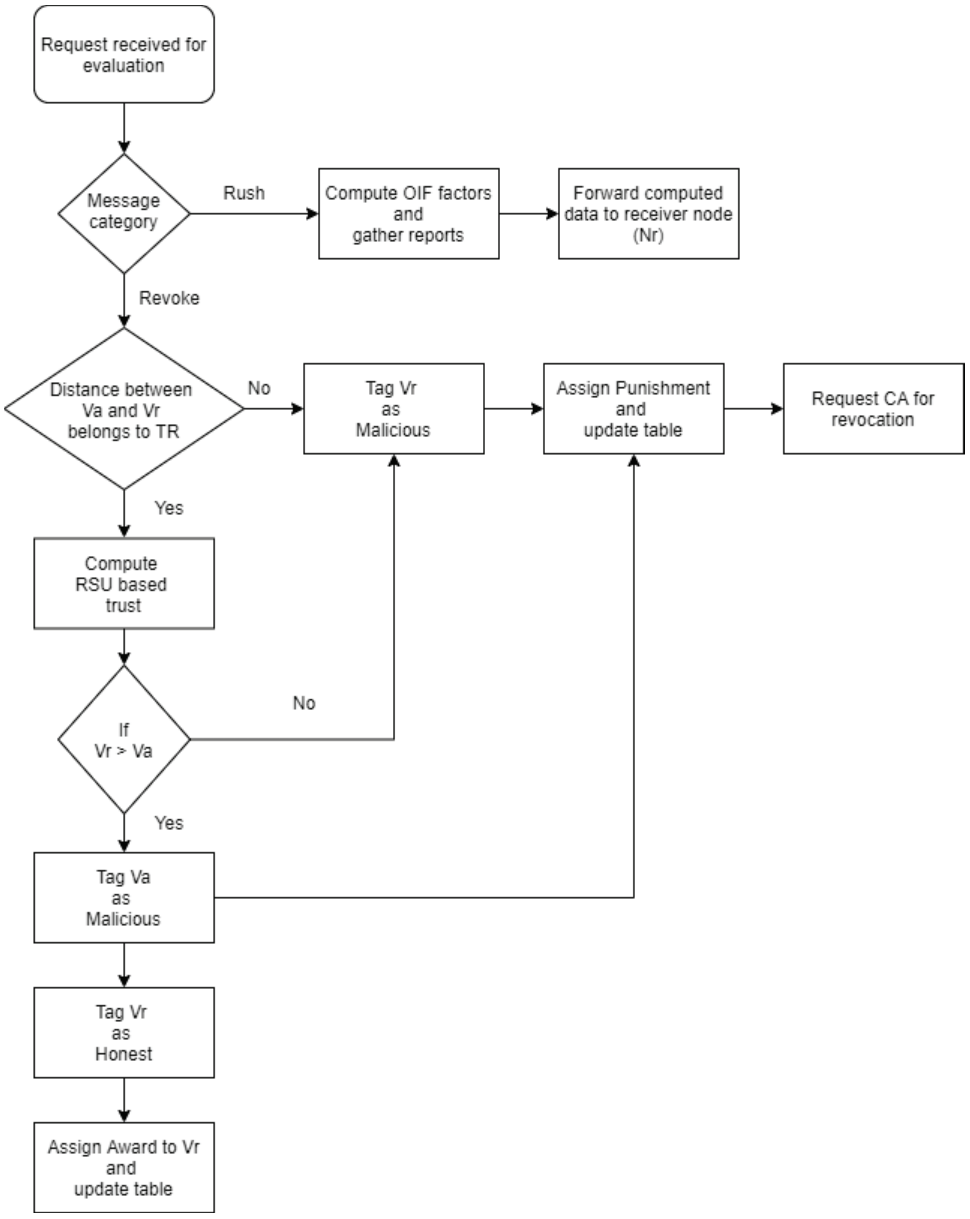

Figure 4.3: Flowchart for RSU-based trust computation

can identify the trustworthiness of both Vr and Va. If Va is identified as malicious, a penalty of P is assigned to Va, and an award of A is assigned Vr. In few cases, the reported vehicle deliberately misleads RSU by falsely foreclosing an honest node. In such cases, a penalty of P is assigned to Vr and hence revokes its credentials. Efficient trust management can be achieved by modularizing the responsibilities between RSUs and mobile nodes.

RSU initiates its computation by calculating the distance between Va and Vr in order to check whether both the vehicles belongs to same vicinity. If the distance between Va and Vr falls in the threshold range, then RSU perform infrastructure computation [9] of both the vehicles based on the positive and negative reports and rating factors such as A and P:

$$TrustVa = [(\frac{A}{A+P} \times \sum_{i=1}^{n} Pos) + (\frac{P}{A+P} \times \sum_{i=1}^{n} Neg)] \tag{4.7}$$

$$TrustVr = [(\frac{A}{A+P} \times \sum_{i=1}^{n} Pos) + (\frac{P}{A+P} \times \sum_{i=1}^{n} Neg)] \tag{4.8}$$

If TrustVr >TrustVa, then Va is tagged as a malicious vehicle, assigned a penalty, Vr is assigned an award, requested for revoking credentials, and the information is updated.

If TrustVr <TrustVa, then Vr is tagged as malicious, assigned a penalty, requested for revoking credentials, and the information is updated.

4.6 SCENARIO – IV

Theoretically, this section explains the possibilities and solutions designed in a particular scenario where a dishonest node is assigned with a positive rating or an award. As mentioned above, the proposed model works on a trust-based rating scheme where different types of evaluations are performed to calculate the trustworthiness of both the sender node and the propagated message. During these evaluations, the receiver node (Nr) has to initially assess the trustworthiness of the sender node (Ns) by accessing a lookup table. Prior information about Nr is available in the form of ratings. These ratings are calculated based on the award(A) and punishment(P) factors assigned during their previous interaction. Accuracy of the decision made by Nr, after performing a series of evaluations, is prudent because it does not rely only on one factor. Various factors such as MTR, ratings, MDR, DT, RT, RET and RSU-based trust are considered as part of evaluating the trust values and forming a final decision. Based on the final verdict, each Ns is either awarded or punished. Few malicious

Algorithm 3 RSU-centric trust computation for Scenario III

Initialize the system with inputs.
(A,P) values; positive(Pos) and Negative(Neg) reports and number of distinct vehicles(n).
procedure RTC
    Calculate the distance range between Ns and Nr.
    if ($Distance\ range \in TR$) **then**
        Compute trust for foreclosed vehicle (V_a)
        Compute trust for reported vehicle (V_r)
        Compare V_a and V_r
        if ($Vr > V_a$) **then**
            V_a is tagged as malicious and assigned punishment
            V_r is tagged as honest and assigned award
        else
            V_r is tagged as malicious and assigned punishment
            RSU request CA for revocation of V_r credentials.
        end if
    else
        Tag V_r as malicious vehicle for wrongly foreclosing V_a
        Assign punishment and request for revocation
    end if
end procedure

nodes, to maintain a good reputation in the system, behave honestly during few interactions and thus receive an award. During such scenarios, they tend to transmit proper messages and do not cause any harm to the receiver vehicles. After attaining a positive rating, they plan to attack in the form of propagating harmful messages or MiTM attack in this case.

The proposed model is designed in a way to handle such scenarios. Even though ETC of Ns is positive due to its positive rating in the lookup table, DTC employs a majority of its evaluation for calculating and identifying the occurrence of the reported event and trustworthiness of the sent data. For example, while calculating DTC, one of the metrics that has been employed is RT, where opinions and recommendations from neighboring vehicles and RSUs are considered. While calculating RT, the Award factor (A) of Ns is multiplied with Positive Opinions (Pos), and the P factor is multiplied with Negative Opinions (Neg). In such a case, even though Ns contain a good level of A factor, more negative opinions can result in negative RT. Alongside RT, RET proves to be handy in delivering an accurate opinion since these vehicles are assigned the highest priority in the system. Hence, when a malicious or dishonest node with a positive rating tries to attack the system by transmitting an improper message, the neighbors' negative opinions, RSUs, and RET helps Nr in identifying the correctness of the data.

4.7 SCENARIO - V

This section explains, theoretically, the possibilities and preventive measures applied in a scenario where an honest node is assigned with a negative rating or punishment. In scenario – IV, a situation where a dishonest node is receiving an award for behaving honestly as part of its plan to attack in the future is explained. But the proposed model effectively avoids a condition of assigning a negative rating to an honest vehicle, which has no intention of launching an attack in the future. This can be proved by the efficiency level of DTC and especially the presence of role and experience-based vehicles (RET). The RET step ensures that the information transmitted by Ns is properly validated and opinionated. Moreover, the role of such vehicles is not limited to assisting the mobile nodes. Still, they report the occurrence of any event,

periodically, to nearby RSUs such that RSUs can validate and assist mobile nodes accurately during their interaction. By precisely evaluating the trustworthiness of the information, the proposed model ensures that no honest node is assigned with a negative rating or punishment.

4.8 Summary

These five scenarios explain the occurrence of possible situations in a VANET system during V2I and V2V communication. The novelty of this dissertation lies in describing each scenario in detail, the possibility of their occurrence, designing different approaches that are suitable to each situation, and generating an efficient and effective trust management scheme for VANETs that addresses one of the major security issues, MiTM.

Chapter 5

Implementation and Results

This chapter describes the modules in the proposed work and implementation details, including simulation parameters and software requirements. Moreover, the simulation tools and their details, such as integrating various tools for simulating the VANETs scenario, are explained in detail along with respective block diagrams. Finally, the screenshots taken during the simulation are demonstrated. The proposed scenario-based security solution for VANETs is compared to the basic AODV and reference list-based trust framework. The performance of those protocols is evaluated using several routing metrics. The routing metrics are evaluated under two different scenarios, which are created by varying the number of nodes and the percentage of attackers.

5.1 Simulation and Software requirements

The VANET is simulated with various parameters, as shown in the following table. The observed behaviors of vehicles in various scenarios are demonstrated using the performance metrics. For the performance evaluation, the proposed and existing protocols are evaluated with a network density of 30 to 90 vehicles. In such a scenario, 10% of attackers are installed. Another network topology with 60 vehicles is created with 5 to 25% of attackers. The vehicles moved with speed ranging from 5 to 25 m/sec. The transmission range of vehicles is set as 250m. A road traffic scenario is created using SUMO with the traffic of a various number of vehicles. Moreover, the SUMO is integrated with network simulator - NS2. The traffic files are generated using SUMO trace exporter, and it is exported to NS2. The NS2 is a network simulator, and it is used for analyzing the VANETs performance using the proposed and existing protocols [30][4][7]. The output of the sumo simulator file is an input to the NS2 simulator.

Table 5.1: Simulation Tools and Parameters

Tools and Parameters	**Values**
Operating System	Ubuntu 16.04 LTS 64bit
Network Simulator	NS 2.35
Traffic Simulator	SUMO
Map Model	OSM
Interface Type	Phy/WirelessPhy
Queue type	Drop Tail/Priority Queue
Queue length	50 Packets
Antenna type	Omni Antenna
Propagation type	Two Ray Ground
Transport Layer Protocol	TCP
MAC Layer Protocol	IEEE 802.11
Number of Vehicles	30 to 90
Vehicle Speed	5 to 25 m/sec
Transmission Range	250 m
Propagation Model	Two ray ground, Nakagami
Data Rate	27 Mbps
Packet Size	512 bytes
Application Type	CBR

5.2 VANET Simulation Tools

To design the simulation scenario and reflect the VANETs environment, it is essential to exploit two different simulators, such as traffic and network simulator. The first one is used to generate network traffic. The latter is for simulating the network scenario. For instance, the SUMO traffic generator creates real-time road traffic, and the SUMO trace exporter generates the mobility of traffic data. It is exported to the network simulator, NS2, which is utilized as a vehicular network simulator for analyzing the performance of VANET[**?**].

5.2.1 Network Simulator and its Architecture

The network simulator is a software program where the behavior of nodes in the network is modeled. It simulates wired/wireless networks through the interaction between different network entities, such as nodes and gateway. NS2 is an object-oriented, discrete event simulator that consists of five schedulers, and each scheduler

is implemented with a different data structure as follows[30]:

1. A simple linked- list
2. Heap
3. Calendar queue (default) and
4. A special type called "real-time".

The scheduler selects the next earliest event for executing it to completion and return and execute the next event. The scheduler exploits the unit of seconds for the time factor. An appropriate handler class assists the NS2 in handling an event shown in the following figure. The most important Handler is NsObject with TclObject[30][7]. Moreover, they are called twins in the Tcl world. They offer the basic functions for making the objects interact with one another. For this purpose, the scheduler exploits the receive function group. For handling OTcl statements in C++, it provides the NsObjects. NsObject acts as the parent class for some important classes, and those classes are Classifier, the Connector, and the TraceFile class. The handler class diagram is shown in figure 5.1.

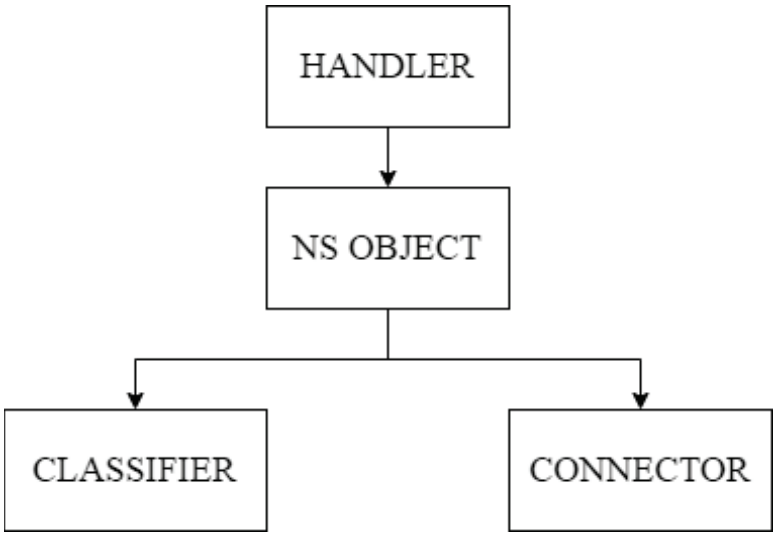

Figure 5.1: Handler Class

The TCL scripts play an important role in controlling the NS2 simulation. It is

because the TCL scripts include all necessary parameters and configurations. Additionally, the following command can be used to modify the opt parameters within the TCL script[30][4].

```
ns script.tcl -nn 100 -x 5000 -y 5000 -stop 800 \
-tr out.tr -sc mov -cp traffic
```

Figure 5.2: TCL script

The TCL script is used to denote the path of movement and connection files to be loaded. Moreover, it is used to specify the path to the trace files, i.e., a nam and a tr file, which are the simulation product. It is demonstrated in figure 5.3. The TCL file consists of several important parts:

- Specifications for the protocol
- Node creation and movement
- Node communication
- Trace, event log, and visualization setup

5.2.2 Traffic Simulator

To simulate the VANET environment, there are many traffic simulators available, such as VanetMobiSim, CanuMobiSim, SUMO/MOVE, NCTUns, and TraNs. SUMO is an open, microscopic, and continuous road traffic simulation tool, and it supports large road networks also. The SUMO traffic simulator is used for making realistic scenarios during simulation when it is combined with NS2. The NS2 starts the process by defining the basic parameters for topology, nodes, and traffic models (input files). It executes the commands of netconvert and netgenerate for generating the SUMO files. Finally, the NS2 applies additional SUMO commands and exports usable SUMO files in other formats[44]. Figure 5.4 shows the general procedure of SUMO to generate

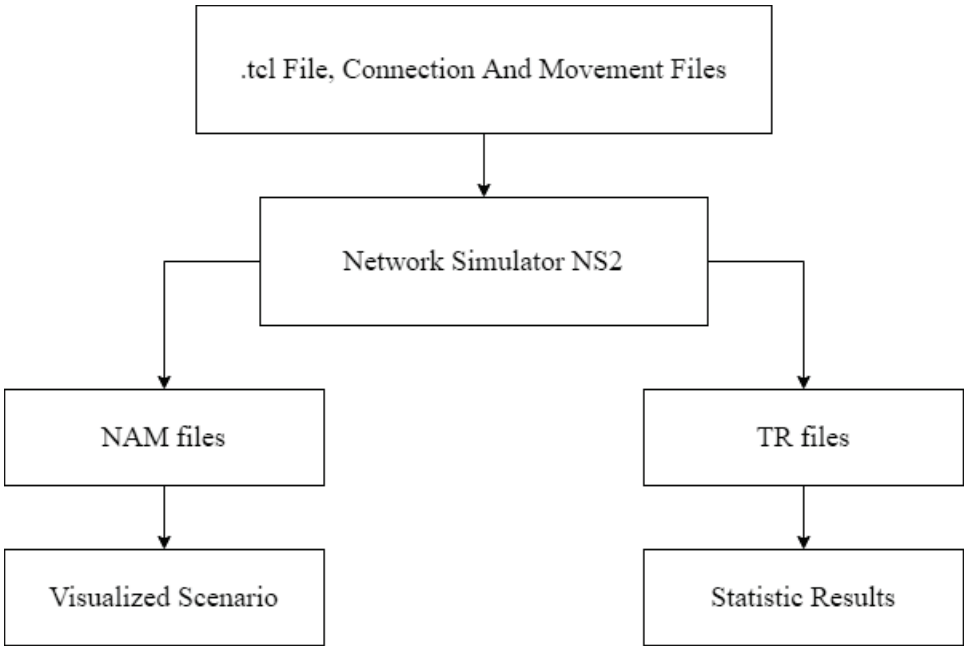

Figure 5.3: Files used in NS2

traffic networks in the VANET environment.

5.3 Simulation Tools Integration in Software Equipment

To make the VANET environment, it is essential to integrate the features of NS2 and traffic simulator, SUMO. For simulating the realistic VANET environment using NS2 and NS2, the addition of node mobility is prominent. In the following figure 5.5, the addition of mobility characteristics to the vehicles starts with creating the network topology. Moreover, it generates an output file in the format of TCL. It consists of individual data of mobility for the total number of nodes in the network over an entire simulation time in NS2. The final steps are taken in NS2 to import the mobility data and aggregate mobility within the VANET environment. The mobility scenario in VANETis created by allowing the nodes to move through the highway topology by varying their moving speed and inter-vehicle distance.

5.4 Languages and Files Used in VANET Simulation

Several languages are used in NS2 for simulating the VANET environment[4][7]. Those are listed as follows:

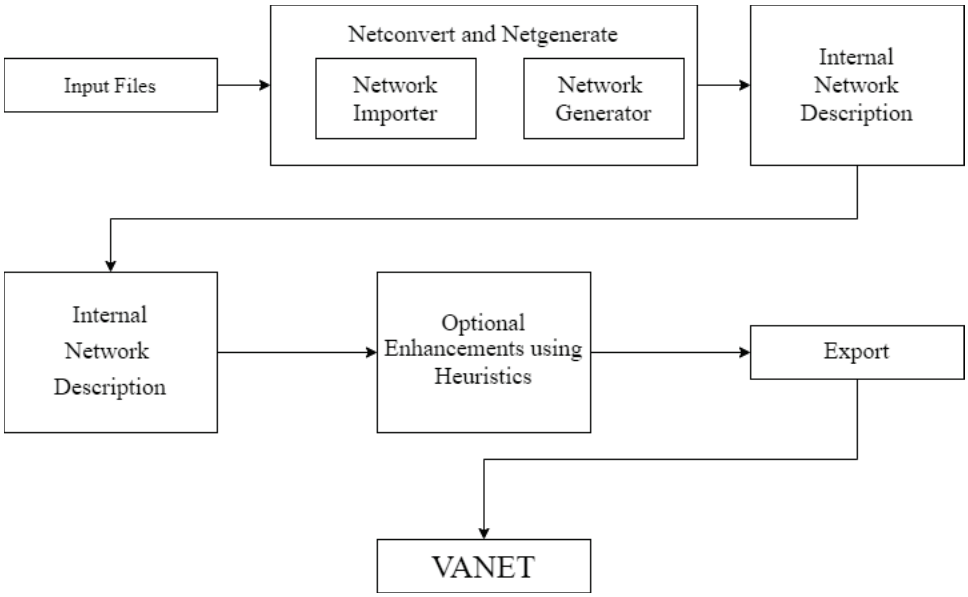

Figure 5.4: Traffic Simulator in VANET

1. Extensible Markup Language (XML) and Trace File
2. TCL Language
3. AWK Language
4. Trace and NAM File
5. X-Graph

XML and Trace File: The simulators have to simulate the VANET environment at the microscopic level, and so the NS2 exploits vehicular mobility simulation. The VanetMobiSim considers the input file in the format of an XML configuration file. The VanetMobiSim consists of several files to define the vehicular mobility model in VanetMobiSim. It is prominent in a real-time road topology environment to effectively utilize all the attributes like the vehicle's speed, traffic light, number of lanes, trip motion, and road topology in the XML file. An XML file consists of many mobility scenario launching files, and the VanetMobiSim framework with those files is necessary to produce a node mobility trace file in NS2 format. The output of the XML file is the model of network topology with proper road and vehicle setup.

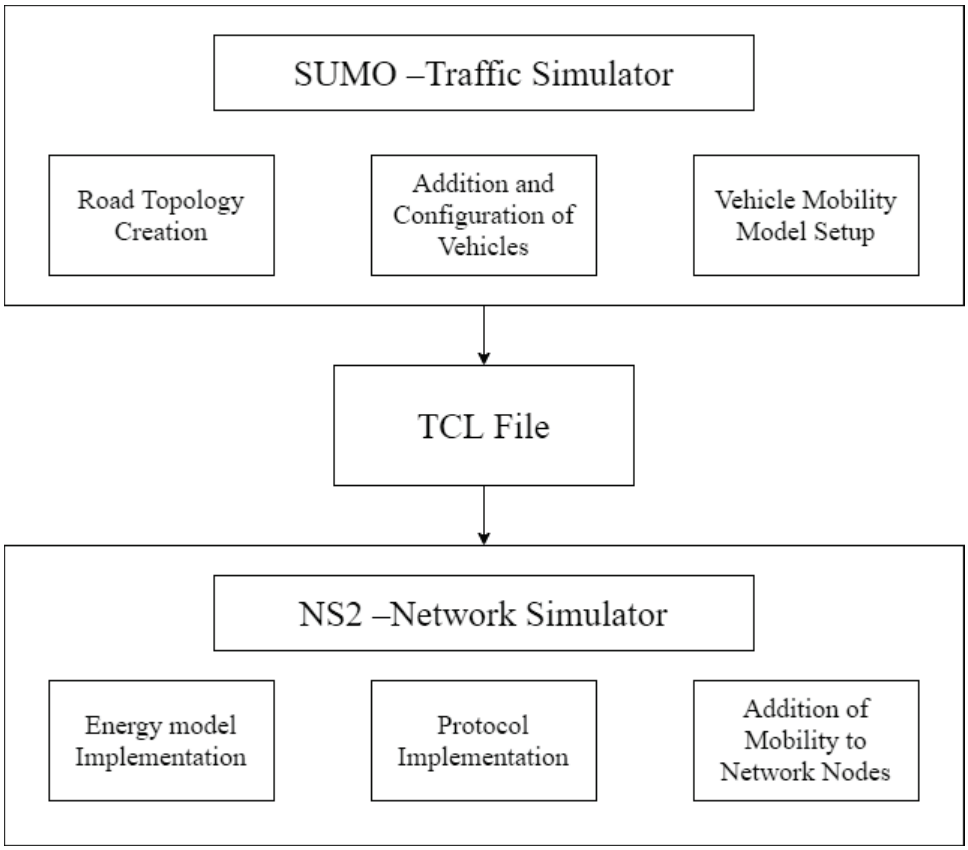

Figure 5.5: Integration of Simulation Tools

TCL Language: The TCL language is a translated script language. It assists in implementing the scripting to develop code for networking topology as per the requirement of vehicular ad-hoc network traffic flow on the road and relative movement of vehicles. Those files are scripted for making and linking applicable files. It depends on different parameters and their settings of generated means of transportation, including mobility, safety, and likewise constraints. The TCL files play an important role in simulating the network environment along with their characteristics. The on-demand routing protocols require a TCL file as input, which includes traffic and movement files for initializing the traffic pattern and simulating the network in the same manner. Finally, as a result, it generates two files—Trace files (*.tr) as the outputs and Network Animator File (*.nam).

AWK Language: It is a tool used to extract the data and send a report. It exploits the data-driven scripting language. The main aim of using this language is

to generate formatted reports. In other words, the AWK is used as a filter and acts as a file for the text processor. This kind of file is used to record a sequence, and each line is recorded by default. Every line is divided into a sequence of fields. The first field is referred to as the first word; the second field is denoted as the second word. The AWK reads the input line by line manner over a particular time. Moreover, according to the AWK pattern in a program, each line is scanned, and for every matching pattern, it executes the related action. It is easy to use AWKs and highly feasible compared to any other usual programming languages. It is also named the pseudo-C interpreter. It is because it performs the arithmetic operators, as written in C language. In AWK functions, string manipulation can be performed, using these functions, particular strings can be searched, and the output gets modified.

Trace and Network Animator (NAM) File: The trace file consists of the number of forwarded, dropped, and received packets, and the sequence number, type, and packet size. This file is created in the text format, and it is named as simulation's log file. It consists of all information in the format of the logs in the column. The NAM file includes all the operations performed at the time of simulation, positioning information, graphical information, and information about the defined parameters. Using the built-in nam command, the execution of the NAM file is also performed using the NS file's Operation component call.

5.5 Screenshots

There are several screenshots of the processes involved in both the proposed and existing works. Those are taken by varying the number of nodes and the percentage of attackers inVANET. This section explains the implementation of all three scenarios in the form of screenshots and sample values used while running the simulation. It also provides details about MiTM attack detection and prevention mechanism using trust evaluation and message dissemination in VANET. Each screenshot represents the working of the proposed trust management scheme, which is executed on NS2.

5.5.1 Screenshots of the Proposed Work in Scenario 1:

The network is created with 90 nodes. Among them, nodes 26,27,28 and 29 are RSUs, as shown in figure 5.6

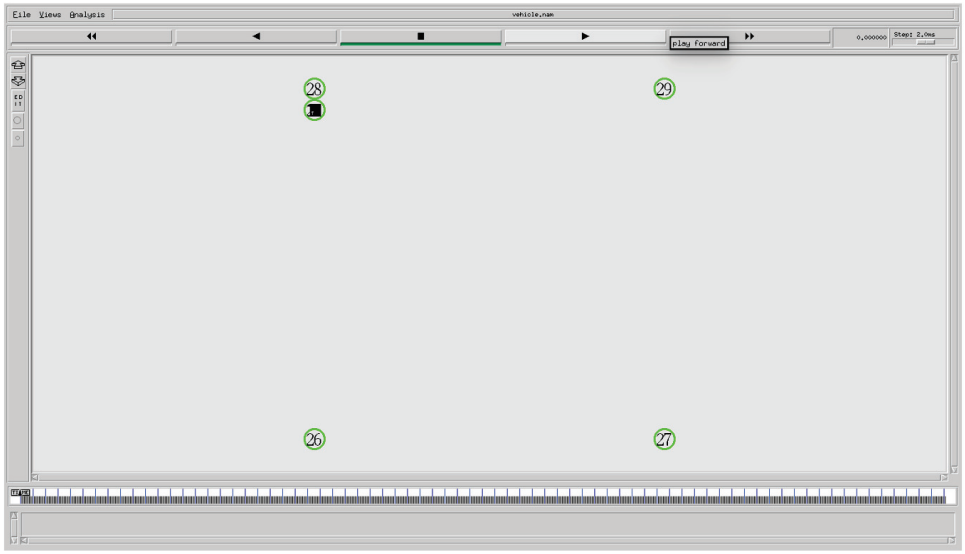

Figure 5.6: Network model

RSUs are responsible for monitoring all the nodes in the network and updating all the information. When any network nodes found an emergency event, it sends the Rush messages to the nodes in its vicinity. It is demonstrated in figure 5.7.

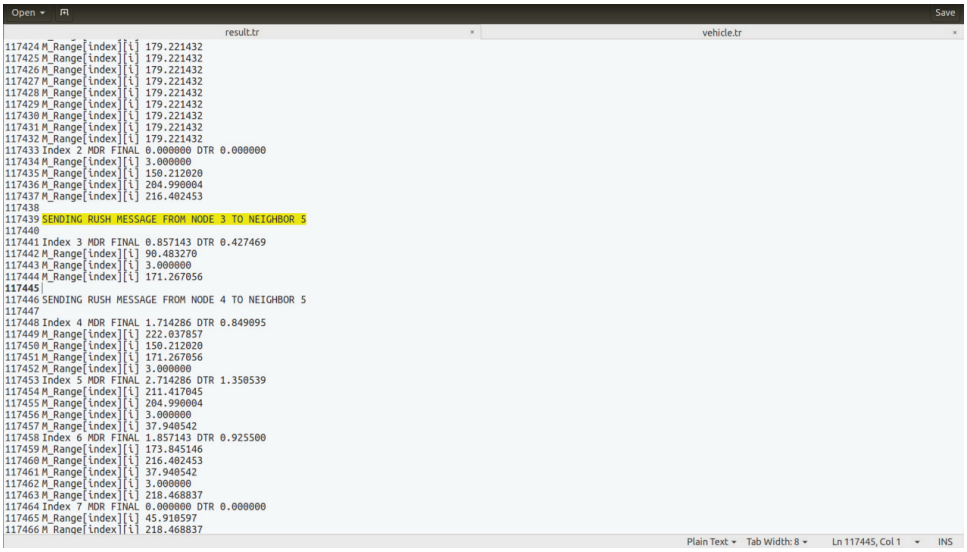

Figure 5.7: Rush message dissemination

For instance, consider nodes 0,3, and 4 are sending rush messages to node 5. The packet id of the data is 14 cbr, and it can be shown in figure 5.8. Node 5 receives the same alert message of packet id 14 cbr.

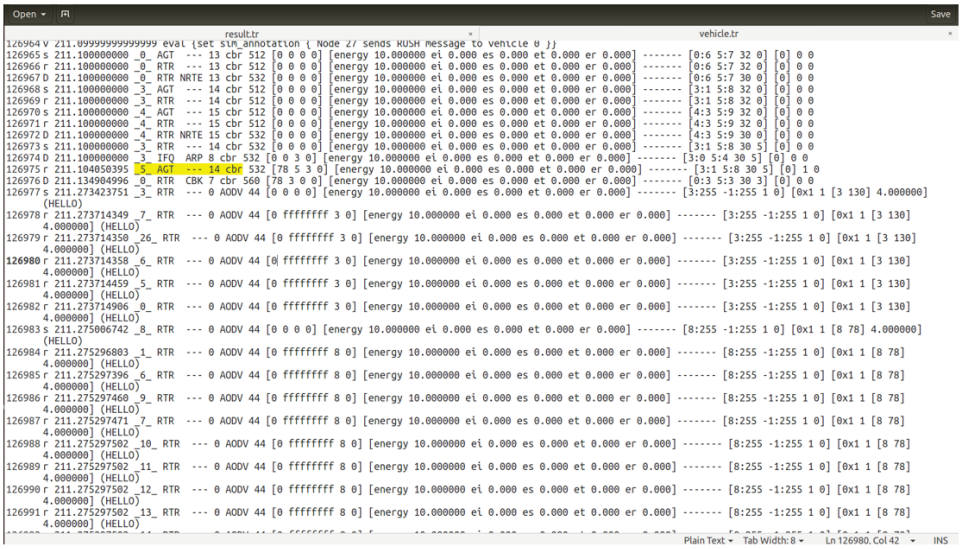

Figure 5.8: Confirmation of Packet ID

Now, the receiver node computes entity-centric trust by checking the lookup table. In this case, node 5 identifies node 3 as a previously interacted vehicle and obtains trust information. The receiver nodes in the network first calculate the trust of the sender nodes as shown in the figure 5.9

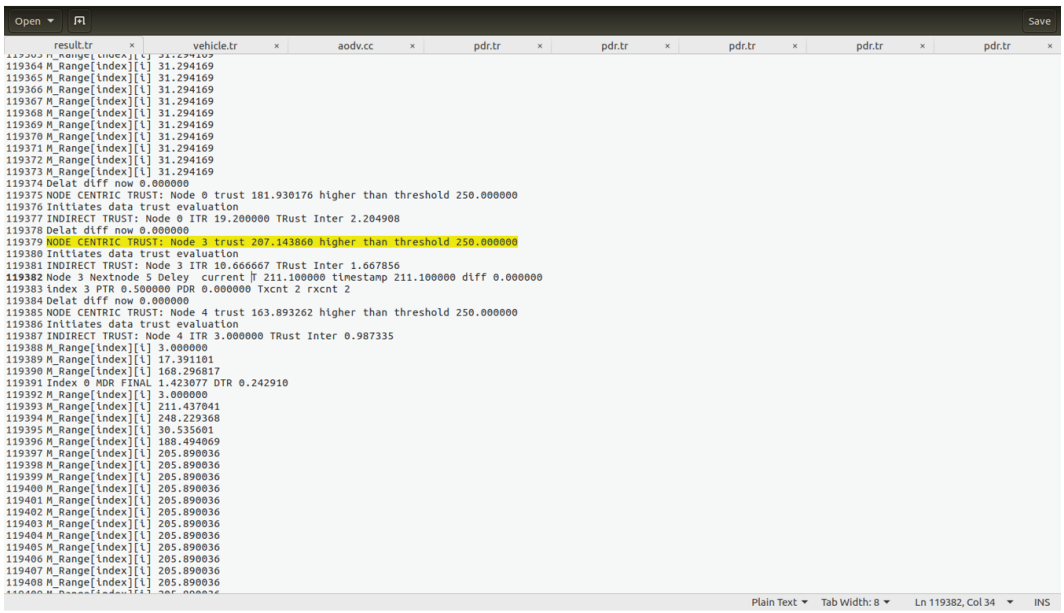

Figure 5.9: Entity-centric Trust Computation

Here node 5 is calculating the node trust based on distance and antenna heights. Entity-centric trust for Node 3 is computed as 207.143860, which is higher than the predefined threshold of 250.000000. Hence, Then node 5 forwards node 3 for data-centric trust calculation.

Figure 5.10: Data-centric Trust Computations

Upon successfully computing ETC, node 5 performs Data-centric trust computation (DTC) for node 3 based on two trust metrics, such as Direct trust(DT) and Recommendation trust(RT). RT is also termed as indirect trust due to the fact that in this case trust computation is performed based on opinions and recommendations of neighboring vehicles and there is no direct communication with the sender vehicle. The initiation of data trust estimation is shown in figure 5.10.

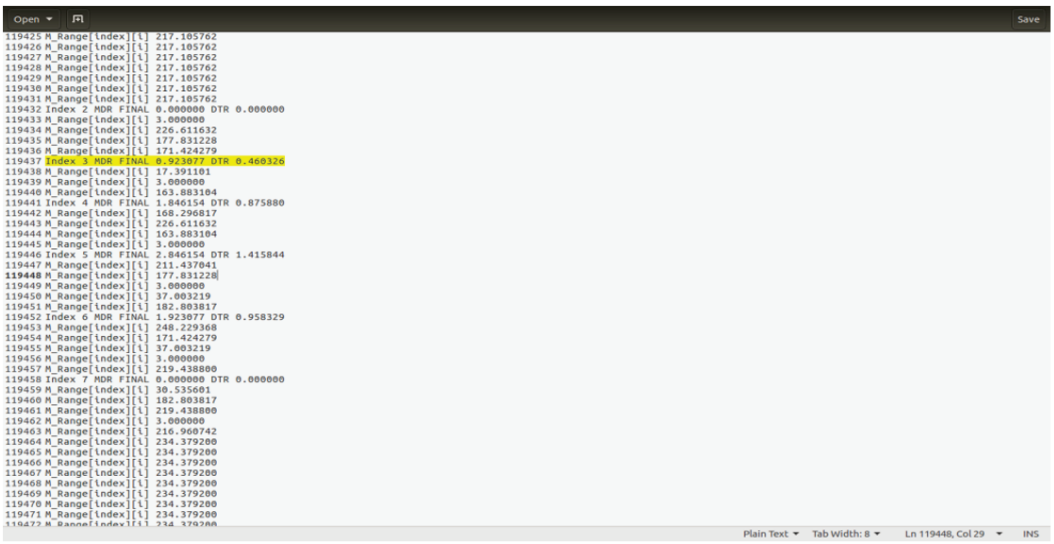

Figure 5.11: Direct trust computation based on MDR and distance

Direct trust is calculated based on the message dissemination ratio and the distance between the source and destination. A node 3 values for Message Dissemination Ratio and Direct Trust Ratio are as follows and shown in figure 5.11. MDR = 0.923077 & Direct Trust (DT) = 0.460326

Recommendation trust or Indirect trust is calculated based on the positive and negative responses from the neighboring nodes and award and punishment factors as shown in the figure 5.12. Based on computed DT and RT, DTC for node 3 is calculated as 1.667856.

Figure 5.13 illustrates the man in the middle attacker, which will either drop or

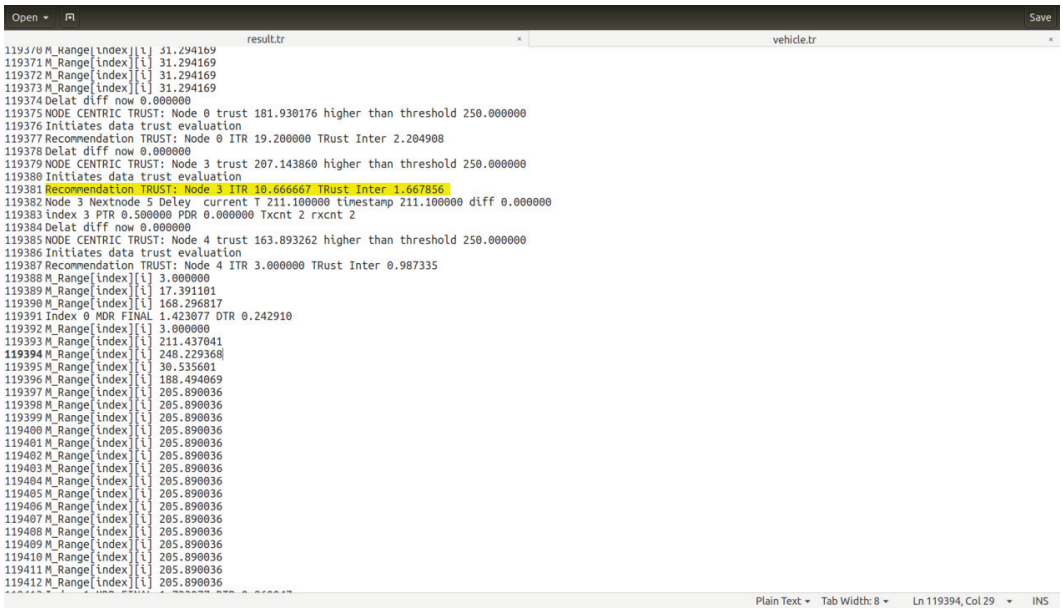

Figure 5.12: Recommendation trust computation based on the opinions from neighboring vehicles

delay the data packets. 10% attacker is considered for the scenario I, and hence three attackers are available in the network.

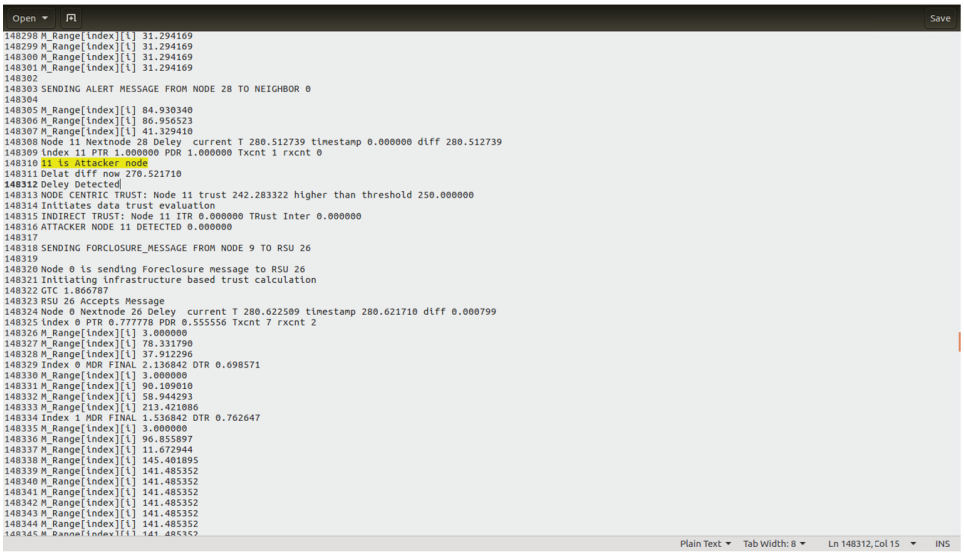

Figure 5.13: Attacker Node detection

Here since node 11 is identified as an attacker as shown in the figure 5.14 and it launches MiTM attack in the form of dropping the packet. Once any of the nodes detect misbehaving nodes in its vicinity, it reports to RSU by sending a revoke or

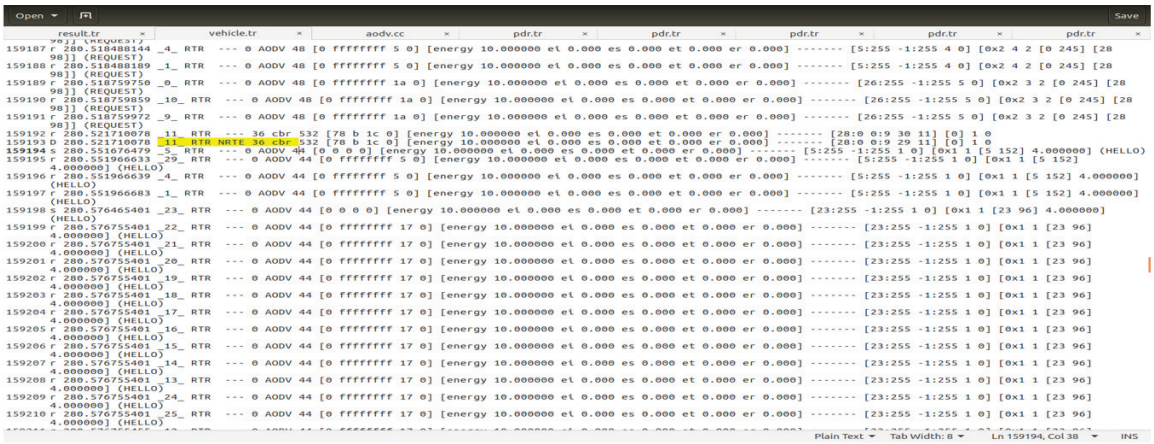

Figure 5.14: Packet dropping behavior

foreclosure message. Here node 9 is sending a revoke message to RSU 26 as shown in the figure 5.15. Then RSU performs the infrastructure trust based on two factors. Firstly it verifies the neighborhood confirmation of both the vehicles and proceeds for RSU-based trust computation as shown in the figure 5.16. Node 9 sends a revoke message to RSU 26 about node 11, where node 9 is considered as reporting vehicle and node 11 is considered as an foreclosed vehicle.

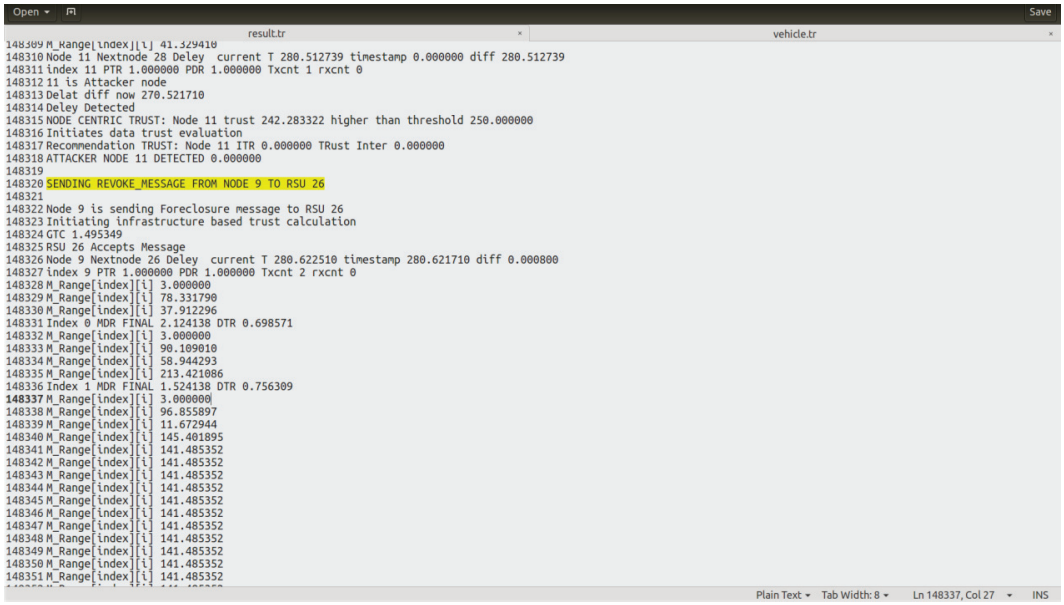

Figure 5.15: Revoke message dissemination

Figure 5.16: RSU-based trust computation

5.5.2 Screenshots of the Proposed Work in Scenario 2

This section describes the scenario in which the trust computation of a newly interacted vehicle is considered. A VANET is created by varying the nodes from 30 to 90. Nodes 56, 57, 58, and 59 are considered as RSUs, responsible for monitoring the network and message Dissemination. Moreover, they have to update all the information related to the characteristics of vehicles. When any network node found an emergency event, it sends the alert messages to the nodes in its vicinity. The receiver node confirms its lookup table for any previous interaction. Here, node 13 is propagating a rush message to node 14 as shown in the figure 5.17.

The packet id of the data is 10 cbr. It is demonstrated that node 14 receives the same rush message of packet id 10 cbr. If any nodes in the network start communication for the first time or do not have any node history in its database, it initiates an offline infrastructure factor, which is in figure 5.18.

Node 14 initiates Entity-centric trust calculation for node 13 based on received offline factors from nearby RSU and distance factor related antenna heights as mentioned in the figure 5.19.

Figure 5.17: Newly interacted vehicle message dissemination

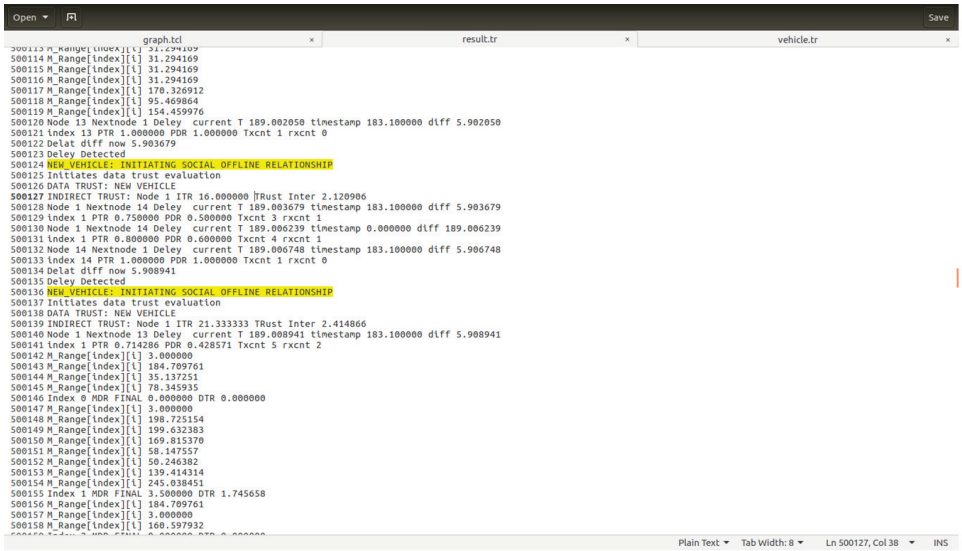

Figure 5.18: OIF

Node 14 calculates the entity trust based on distance and antenna heights, and it is computed as 200.247373, which is higher than the threshold of 250.000000. Then the node 14 forwards node 13 to data-centric trust calculation.

Figure 5.20 illustrates data-centric trust computation for node 13 based on three factors, unlike in scenario 1. The third factor, role and experience-based trust (RET) is computed only in the case of newly interacted vehicles. For the new vehicle, the

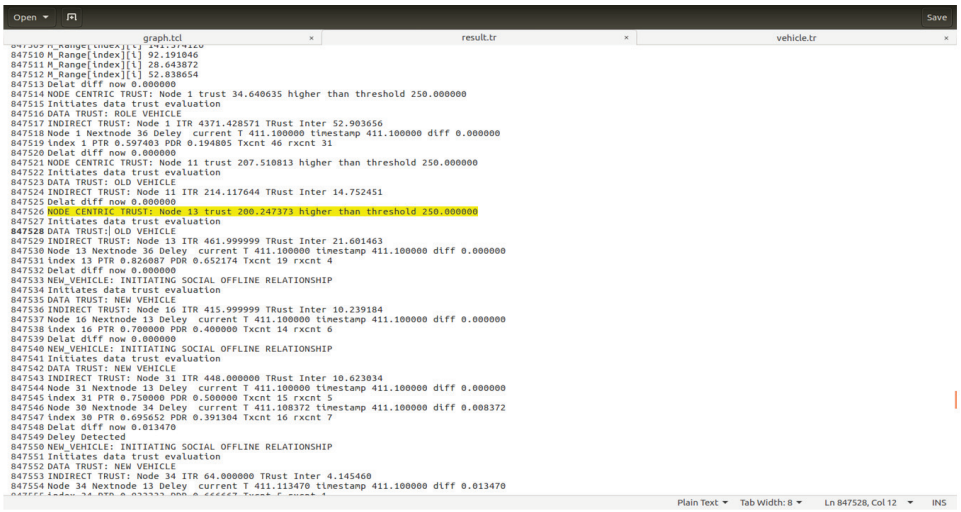

Figure 5.19: Entity-centric Trust Computation of newly interacting node

data trust is evaluated based on direct trust, recommendation trust, and RET as shown in the figure.

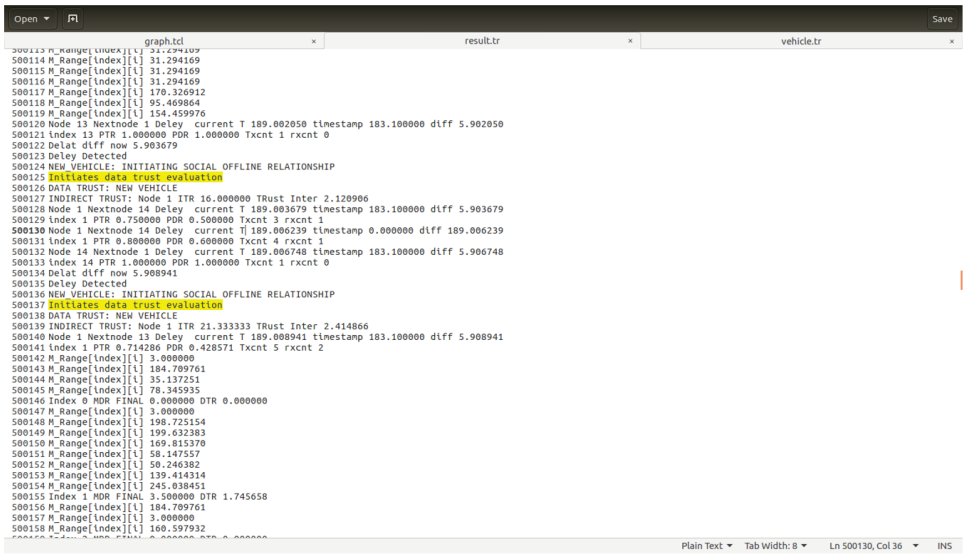

Figure 5.20: Data-centric Trust Computation of newly interacting node

In the case of evaluating data trust for role vehicle, the Ro is considered as 0.8, and for experience vehicle, E0 is considered as 0.5 as shown in the figure 5.21. Node 13 values for Message Dissemination Ratio and Direct Trust Ratio are as follows. MDR = 1.750000 RT = 0.871749. Indirect trust is calculated based on the positive and negative responses from the neighboring nodes and award and punishment factors.

The recommendation trust values for node 13 is as follows. Recommendation trust for Node 13 = 370.909092. Based on DT and RT, final DTC is calculated as 9.691423 as shown in the figure 5.22

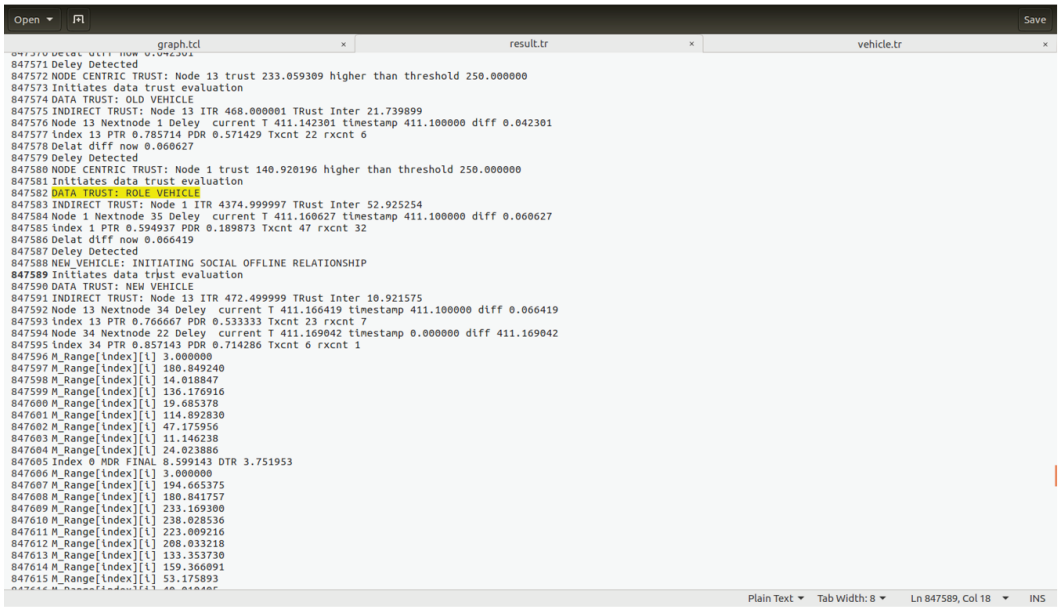

Figure 5.21: Role and Experience based Trust Computation of newly interacting node

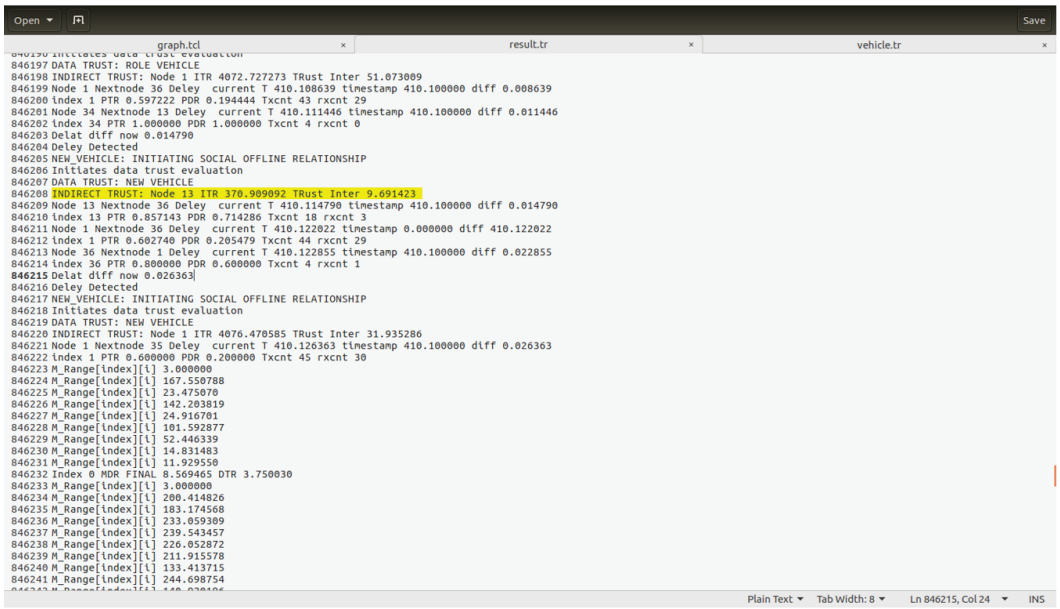

Figure 5.22: Data-centric Trust Computation of newly interacting node

Chapter 6

Performance Evaluation

This chapter demonstrates scenario-based secure routing and existing protocols, such as AODV routing protocol, and reference list-based secure routing, such as the theoretical framework for trust management. The performance of these protocols is evaluated using various metrics. The selected routing metrics are evaluated under various scenarios for the proposed work. The main aim of the proposed model is to disseminate trust information and enable reliable communication within the network in the presence of malicious nodes. The proposed model addresses two key security aspects, namely routing efficiency and trust management. Routing efficiency is obtained by implementing a modified version of AODV protocol that ensures accurate dissemination of messages in the network, thereby achieving a high packet delivery ratio and throughput. Trust management can be achieved by enabling the mobile nodes to accurately detect dishonest nodes and malicious content, thereby reducing delays and reliable propagation of trust information.

6.1 Performance Metrics

Four metrics are used to evaluate the proposed and existing works, including packet delivery ratio, throughput, delay, and detection accuracy.

Packet Delivery Ratio: The ratio between successfully delivered packets to the receiver from the sender vehicle and the generated packets at the sender vehicle. In other words, it can be defined as proportion of number of packets delivered against the number of packets sent[1].

$$\textit{Packet Delivery Ratio (PDR)} = \sum \frac{\text{Number of packets received}}{\text{Number of packets sent}} \tag{6.1}$$

Throughput: In short, throughput is the total number of delivered bits to the receiver vehicle. In other words, throughput can be defined as the amount of data transferred from a source to a destination at any given time in the network. It is the rate (in bits per sec (bps) or packets per second (PPS)) at which packets or bits are successfully delivered over a network channel. So, we can sum the packets received by all nodes to calculate the value for a small network or network segment[50].

Delay: Delay can be defined as the time taken by a data packet to reach the receiver from the sender vehicle and is measured in seconds. Delays are caused mainly due to the dynamic mobility characteristics of VANETs and sparse distribution of vehicles in the system. Delay is broadly categorized into processing, queuing, transmission, and propagation delays[6]. Various factors influence the cause of delays in a VANET system, such as message delivery distance and density of vehicles, to name a few[45].

Detection Accuracy: It is defined as the ratio of malicious nodes detected accurately to the total number of malicious nodes in VANET. To validate the performance and working of a system accurately, it is required to introduce a certain level of malicious nodes into the network. The resultant percentage of detection accuracy depicts the performance of the proposed system in terms of detecting malicious activities and nodes residing in the network.

6.2 Simulation Results

In order to validate the performance of the proposed model, two scenarios are considered. In the first scenario, the proposed model is tested with the basic AODV routing protocol to validate the efficiency of STAR in terms of its working with respect to routing. AODV is a reactive routing protocol, which is designed without any security features. The primary aim of AODV protocol is to determine routes on demand by flooding the route with Route Request (RREQ) packets [15]. However, ad-hoc routing protocols are significantly different from traditional routing protocols, so a set of security features must be introduced to support the routing protocol. To show the

impact of malicious activities and the proposed scheme on the performance metrics, the proposed model is tested with the basic AODV protocol. The scenario is created by varying the number of nodes in the system from 30 to 90. It is carried out with seven simulation runs by increasing the number of nodes by ten units in each run. The second scenario is intended to validate the performance of STAR with respect to the level of efficiency in its trust management scheme. In this scenario, the comparison is made with the existing trust model, namely the reference list-based trust framework. However, to validate the proposed scheme to the maximum extent, the number of nodes is set to be constant while the number of attackers varies. A total of 5 simulation runs are performed with an increase of 5% attackers in each run. The following section illustrates both scenarios with respective graphs built on xgraph.

6.2.1 Scenario Based Trust Management Vs. AODV

The performance of the proposed attack detection mechanism using trust evaluation and message dissemination in VANET is compared with the AODV in vehicular ad-hoc networks. In the simulation, the number of nodes is varied from 30 to 90, and the percentage of attackers is fixed as 10%.

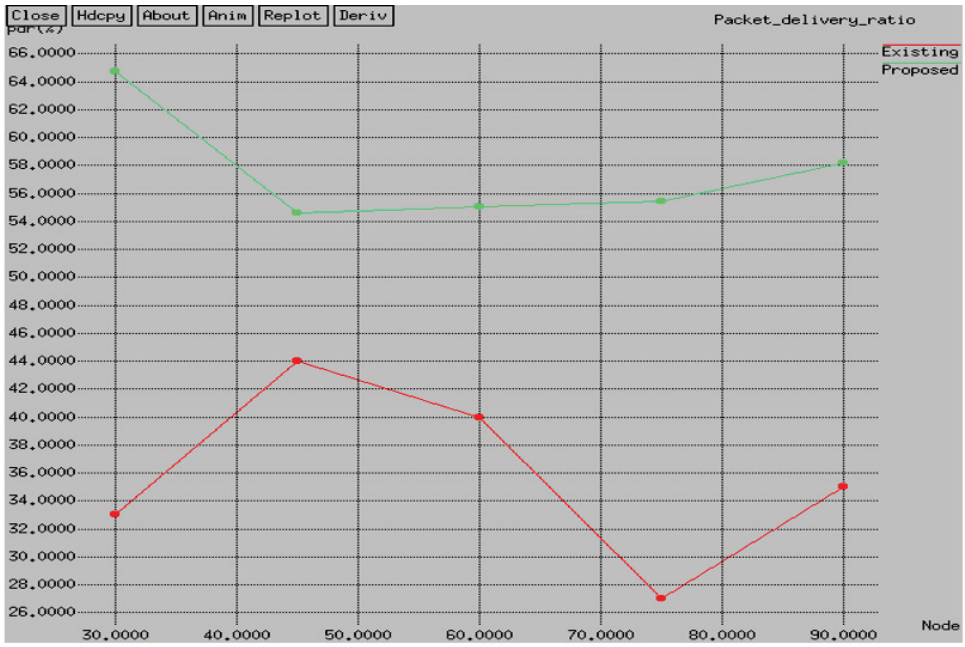

Figure 6.1: Number of Nodes Vs. Packet Delivery Ratio

Packet Delivery Ratio

Figure 6.1 shows the simulation results of both proposed and AODV routing protocols and demonstrates that the proposed work outperforms the existing AODV under various numbers of vehicles. The reason is that the proposed work employs a scenario-based secure routing decision-making algorithm for efficient attack detection. The AODV is not aware of the attacker nodes, so it tends to have high packet loss and poor packet delivery ratio. For example, the high PDR value of both proposed and AODV is 64.5% and 44%, respectively. Compared to AODV, the proposed scenario-based secure routing is resilient against attacks. Thus, it improves the routing efficiency of VANET significantly. Incorporating the previous interaction for the award and penalty measurement during the initiation of communication between vehicles tends to accurate attack detection in VANET. If the communicating devices interact with each other for the first time, the ability of message propagation and distance between the devices is taken into account for trust estimation. It is the reason for the high PDR in the proposed scenario-based secure VANET routing. Moreover, the offline infrastructure factors in trust estimation also provide a space to identify the attackers correctly in the network. This process improves the accuracy of attack detection and results in better PDR. The proposed protocol attains 58% of packet delivery ratio, whereas the AODV protocol attains 35% of packet delivery ratio only under 90 node topology. The standard deviation for both the models fall at a range of 3.5-4.0 which indicates that the data is less spread out from the mean and consistent.

Throughput

The comparative results of the throughput of both the proposed work and existing AODV are illustrated in figure 6.2. The throughput is the data bits delivered to the receiver vehicle per second in the VANET. Compared to AODV, the proposed work detects the malicious nodes successfully and promotes reliable data delivery due to scenario-based secure routing. As the proposed work is more effective in various scenarios of VANET, it detects attackers and delivers most of the data packets to the receiver vehicle successfully. Compared with AODV, the throughput of the proposed work is improved drastically. The throughput in the network is highly related

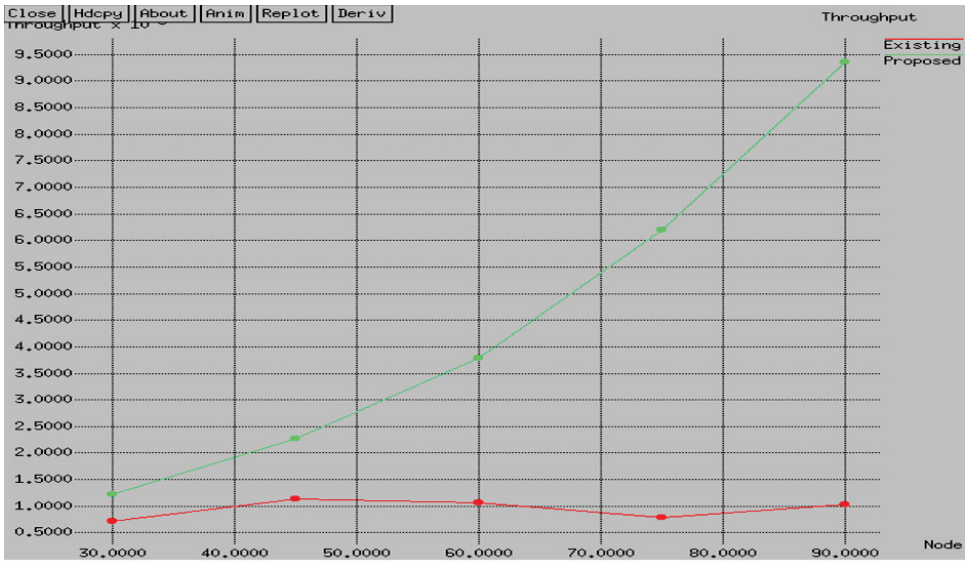

Figure 6.2: Number of Nodes Vs. Throughput

to the accurate detection capability of attackers in the network. The incorporation of recommendation trust, measured using the recommendations and opinions from the neighboring vehicles on the current event, improves the reliable packet delivery in VANETs. Each vehicle involves in the process of validating an event as soon as identifying it or acquiring it from their neighbors. For instance, the proposed work delivers most of the data packets and increases the throughput by 84% more than that in the AODV under a dense network scenario or 90 node topology.

Delay

Figure 6.3 illustrates the delay of proposed and existing AODV routing protocols. From Figure 6.3, the proposed work shows a delay less than AODV, comparatively. The fact is that the AODV considers all the nodes in VANET are trusted. The selected attacker nodes for VANET routing increases the packet loss and packet delivery delay. As per the proposed scenario-based routing, most of the attacker nodes are detected. A common security solution to all the scenarios may tend to inaccurate attack detection and poor routing performance. The scenario-specific attack detection methods in VANET improve the detection accuracy and routing performance.

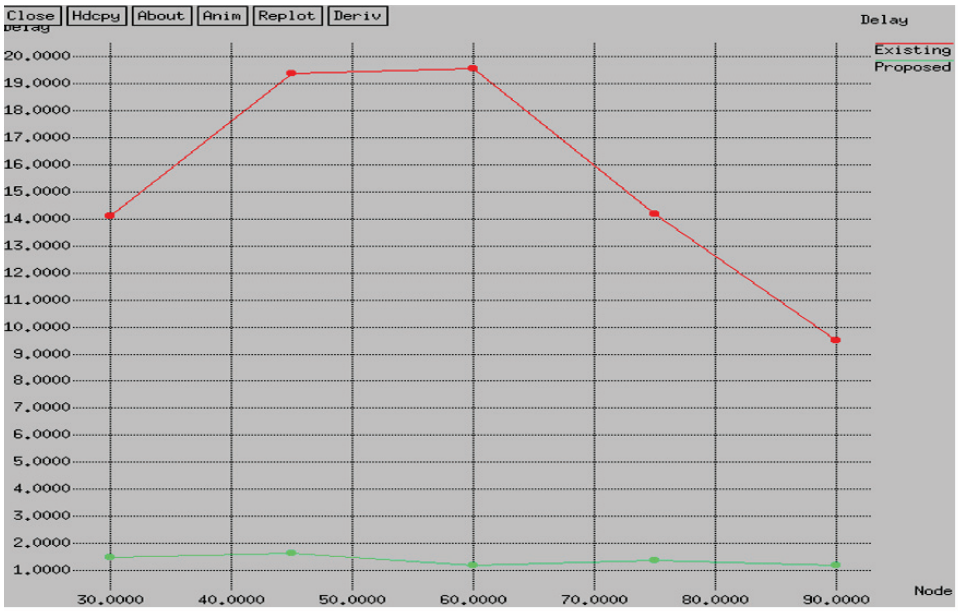

Figure 6.3: Number of Nodes Vs. Delay

The delay of the proposed work does not show a considerable difference when increasing the number of nodes from 30 to 90. It clears that the proposed work is suitable for sparse to dense networks. Moreover, the delay of AODV is increased with the number of nodes. With the sparse network, the possibility of malicious behavior is high. Thus, the AODV attains a high delay from 30 to 60 nodes. The delay of scenario-based secure routing is decreased from 1.5 seconds to 1 second when increasing the number of nodes from 30 to 90, and the percentage of attackers is 10%. In the same scenario, the delay of the proposed work is increased from 1.76 to 3.150 seconds. Under the same scenario, the delay of AODV is decreased from 14 to 9.5 seconds.

Detection Accuracy

From the simulation results, the detection accuracy is observed and plotted in figure 6.4 for the scenario-based secure routing under various node densities. Compared to the network with a low-density scenario or with the 30 node topology, the detection accuracy of the proposed work is decreased under a high dense network. The attackers are correctly identified in the proposed work when sufficient numbers of interactions are performed in the network. With the increase in the number of nodes and network

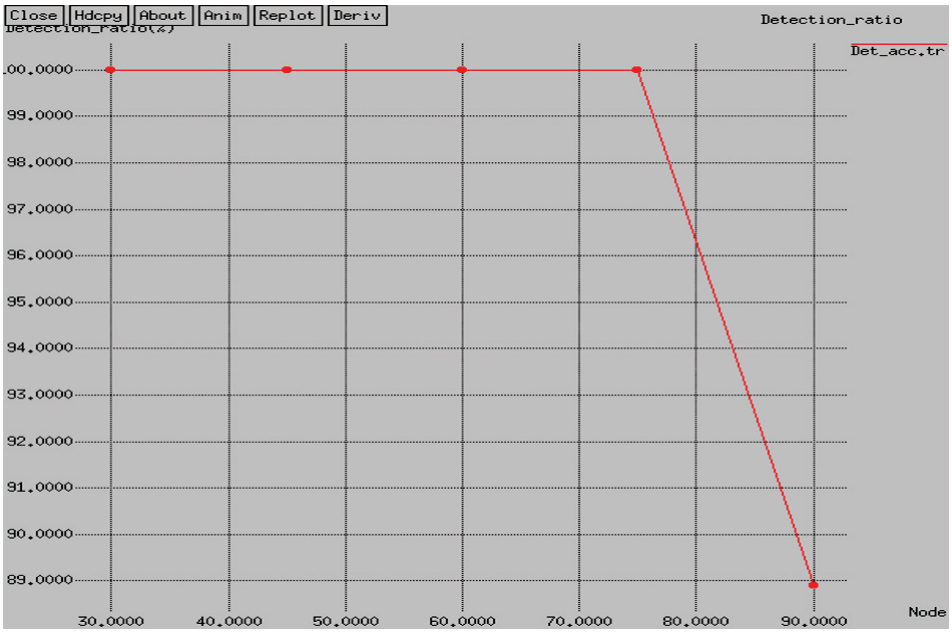

Figure 6.4: Number of Nodes Vs. Detection Accuracy

traffic, the proposed work accurately identifies the attackers. It is the main reason behind the decrement in attack detection when increasing the number of nodes from 30 to 90. In other words, the distributed network traffic affects the performance of proposed secure routing in VANETs. To avoid the impact of various scenarios on detection accuracy, the proposed work decides on security as per the observed scenario. It improves the performance of proposed work in VANETs. For instance, the attack detection accuracy of the proposed work is 100% under the 75 node topology scenario, whereas the attack detection accuracy is reduced to 89% when the number of nodes is 90 in VANETs.

6.2.2 Scenario Based Trust Management Vs. Theoretical Framework For Trust Management

The performance of the proposed attack detection mechanism using trust evaluation and message dissemination in VANET is compared with the theoretical framework for trust management in vehicular ad-hoc networks. In the simulation, the number of nodes is fixed to 60, and the percentage of attackers is varied from 5 to 25%.

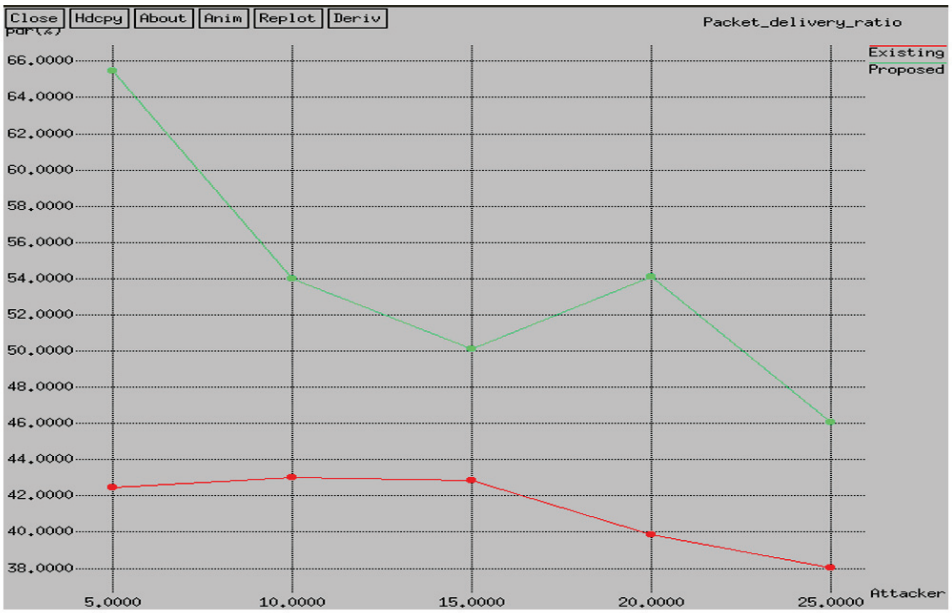

Figure 6.5: Attacker Vs. Packet Delivery Ratio

Packet Delivery Ratio

To analyze the performance of proposed secure routing, the percentage of attackers varies from 5 to 25. Figure 6.5 illustrates the performance of both the proposed and theoretical framework for trust management scheme by varying the attackers under 60 node topology. Figure 6.5 shows that the packet delivery ratio decreases with the increase in the number of attackers over the same network topology. When an RSU has a sufficient number of the previous history of a vehicle node, the possibility of detecting the attacker is higher, resulting in less packet loss and a high packet delivery ratio. When attackers' presence is high on the network, it significantly impacts the routing in existing work. It is because it does not perform well when the communicating devices meet for the first time, and the RSU has no previous interactions of such vehicles in the database. However, the proposed work solves such a problem by considering the scenario on the trust estimation method. For instance, the packet delivery ratio difference in the proposed work is 19% when varying the percentage of attackers from 5 to 25 under the network with 60 nodes. Compared to the proposed work, the performance of existing work decreases since it does not consider the different network scenarios to detect the attacker nodes in VANETs. For instance, the packet delivery difference between proposed and existing work is nearly 20% when the number of

nodes is 60, and the percentage of attackers is 5%. Hence the results indicate that the packet delivery ratio of the proposed work is improved when compared with the existing trust framework. However, the proposed model's packet delivery ratio shows a zig-zag pattern where the performance has been decreased when the percentage of attackers is 15%. In contrast, there has been an improvement when the attacker's percentage increases. In the final run, when the number of attackers increases to 25%, there is a fall in the performance. The packet delivery ratio of the proposed work is dependent on the network area and node density. During the simulation, the addition of various network situations such as high node density, packet dropping behavior, and multiple traffic events may tend to higher collision and packet loss. The attacker model designed for the comparison is intended to drop the packets at random times, which stands as the primary reason for the zig-zag pattern in the packet delivery ratio.

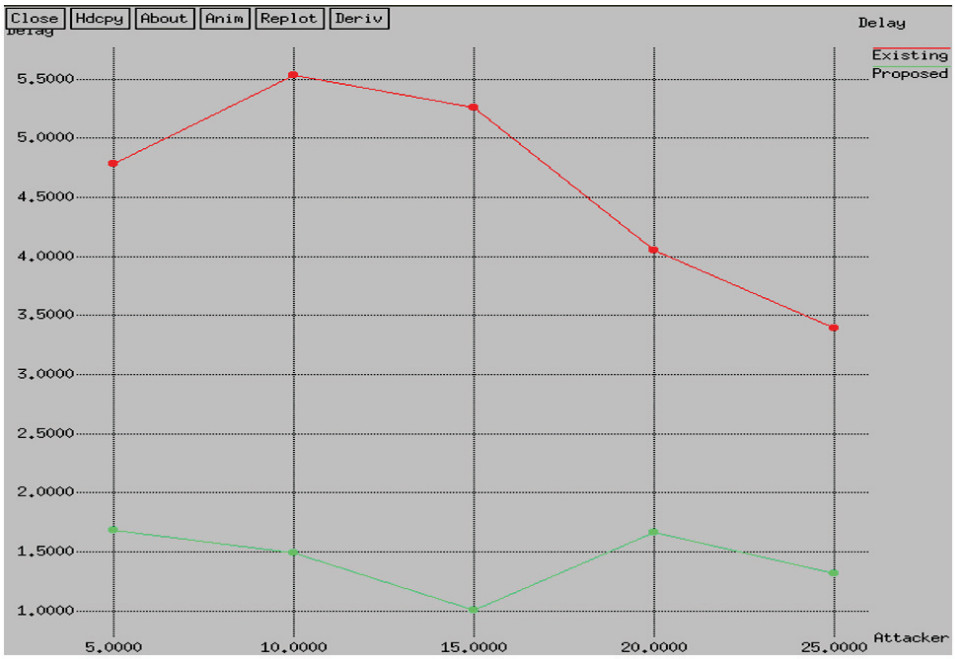

Figure 6.6: Attacker Vs. Delay

Delay

Figure 6.6 demonstrates the delay for both the scenario-based secure routing and theoretical framework for trust estimation. The network with high numbers of attackers

results in less delay, whereas the network with many trusted nodes corresponds to a high delay. In such scenarios, the main reason behind the delay difference is reliable packet delivery. With vast numbers of attackers, only fewer packets can be delivered, resulting in less delay. Using the proposed work, more packets are transmitted through trusted routers. It increases the packet delivery ratio and decreases the delay of the nodes. In the proposed work, the network throughput is increased by deciding on the trust estimation method based on the network scenario. Without considering the network scenario, the existing work shows less performance than the proposed work. Compared to existing work, the proposed work always attains better results in terms of delay. For instance, the delay of the proposed work is 1.7 seconds when the network has 5% of attackers. In the same scenario, the delay of existing work is 4.8 seconds.

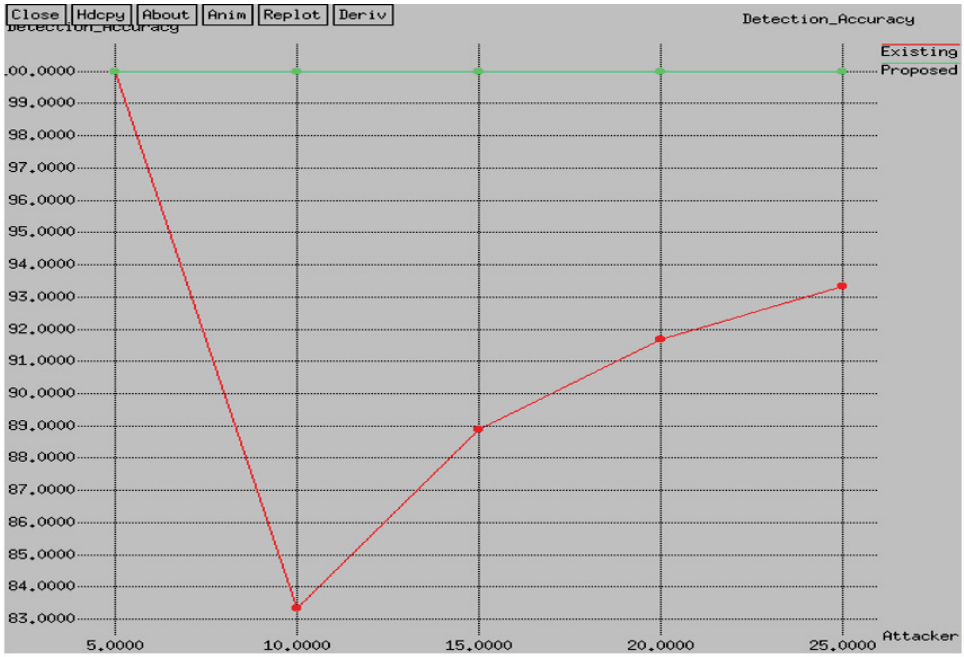

Figure 6.7: Attacker Vs. Detection Accuracy

Detection Accuracy

From the simulation results, the detection accuracy is observed and plotted in figure 6.7 for both the scenario-based secure routing and existing work. The proposed

work can accurately identify the attackers when sufficient numbers of interactions are performed between the network's communicating devices. In the same scenario, the existing work also performs well since it utilizes the advantages of the reference list in attack detection. However, in the case of newly communicating devices, the proposed work takes the knowledge from network scenarios to identify the attackers accurately. It is the main reason behind the increment/decrement in attack detection of proposed and existing secure routing. To avoid the impact of various scenarios on detection accuracy, the proposed work takes MDR, penalty, and award in trust estimation. Moreover, the proper disclosure of the malicious node's identity to the RSUs improves routing performance in VANET. For instance, the attack detection accuracy of the proposed work is 100% under the topology of having 10% of attackers. In contrast, the attack detection accuracy of existing work is 83.5% under the same scenario.

Chapter 7

Conclusion

The growth and demand of various traffic-related safety applications led to the emergence of VANETs in vehicular communications and has become an integral part of ITS. Alongside dispensing a profuse set of applications and services, VANETs are also susceptible to potential privacy and security risks, which need to be dealt with utmost priority. Numerous solutions have been implemented over the years. However, the contradictory nature of security and privacy in VANETs has been a dire challenge. Trust models based on reputation management made their existence significant in terms of progress and enhancement. This dissertation introduces a scenario-based trust management scheme (STAR) for secure routing of mobile nodes in a VANET environment.

The proposed model, STAR, aims to fill the research gap related to the illustration of various trust management scenarios. The primary objective of the proposed model is to elucidate the shortcomings of state-of-the-art trust models, where the emphasis is kept only on enhancing the technique and metrics used to build a trust management scheme. STAR focuses on implementing a scenario-based trust management scheme, which includes an illustration of 5 main scenarios that would provide insights into intricate details involved in computing trust. The proposed model also has a new feature, the classification of messages, namely rush, revoke and refresh, to distribute responsibilities among the mobile nodes, RSU and other infrastructure to reduce computational overheads. STAR also introduces a dynamic concept called Offline Infrastructure Factor (OIF) that can influence future development. This concept plays a vital role in implementing scenario II, which has not been addressed in previous works. To handle the security issues, Man-in-the-middle (MiTM) attacker model has been designed such that the efficiency and accuracy of the proposed model are validated.

Implementation of the proposed model is carried out on a network simulator called NS2. NS2 facilitates the required network simulation with the integration of SUMO for simulating traffic environment. The collaboration of NS2 and SUMO enables the implementation of traffic-related scenarios. The tools included in NS2 such as NAM and xgraph are used to visualize the simulations and graphical representation of performances, respectively. The working and performance of the proposed model are validated and compared with two existing models - AODV routing protocol, for verifying the efficiency in the routing capabilities, and reference-list based trust framework for ensuring the functioning of scenario-based trust scheme in the presence of malicious nodes.

Comparisons are performed based on two scenarios. The first scenario tests the spatial characteristic of VANETs by varying the number of nodes from 30 to 90, but the percentage of attackers has been set constant. The second scenario depicts the proposed model's threshold capacity in the presence of malicious nodes, which increase by 5% on every simulation run. The final results illustrate that the proposed model has an improvement over the existing models based on four performance metrics such as packet delivery ratio, delay, throughput, and detection accuracy. The improvement in the performance is due to the employment of specific and suitable solutions to each scenario rather than employing a standard solution, enhancing the decision-making abilities of a node. The trust metrics such as lookup table trust, direct and recommendation trust, offline infrastructure factors, and role-experience trust help each vehicular node understand different scenarios and handle them accordingly.

Bibliography

[1] What is packet delivery ratio — igi global. https://www.igi-global.com/dictionary/packet-delivery-ratio/21749. [Online; accessed Jan-2021].

[2] Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. *European Telecommunications Standards Institute*, 2019.

[3] Autonomous Driving. `https://www.autocrypt.io/autonomous-driving?gclid=CjwKCAiA2O39BRBjEiwApB2IkiqsqD4sKvm0MwE55cu9\-6KoA69YaoSKJqHWw7FsMs6VQakFduB0fRoCO88QAvD\_BwE`, 2021. [Online; accessed Jan-2021].

[4] Introduction of mobile ad hoc network (manet). `https://www.tutorialsweb.com/ns2/NS2-1.htm`, 2021. [Online; accessed Jan-2021].

[5] Master thesis on vehicular ad-hoc network (vanet). https://www.slideshare.net/profansari/master-thesis-on-vehicular-adhoc-network-vanet, 2021. [Online; accessed Jan-2021].

[6] Network delay. https://en.wikipedia.org/wiki/Network_delay, 2021. [Online; accessed Jan-2021].

[7] The network simulator - ns-2. `https://www.isi.edu/nsnam/ns/`, 2021. [Online; accessed Jan-2021].

[8] F. Ahmad, A. Adnane, Chaker Abdelaziz Kerrache, V. N. L. Franqueira, and F. Kurugollu. Trust management in vehicular ad-hoc networks and internet-of-vehicles: Current trends and future research directions. 2020.

[9] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain. Marine: Man-in-the-middle attack resistant trust model in connected vehicles. *IEEE Internet of Things Journal*, 7(4):3310–3322, 2020.

[10] S. Ahmed and K. Tepe. Using logistic trust for event learning and misbehaviour detection. In *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pages 1–5, 2016.

[11] Saneeha Ahmed. *Trust Establishment and Management in Adhoc Networks*. PhD thesis, University of Windsor, 2016.

[12] Hanin Almutairi, Samia Chelloug, Hanan Alqarni, Raghda Aljaber, Alyah Alshehri, and Dima Alotaish. A new black hole detection scheme for vanets. *MEDES 2014 - 6th International Conference on Management of Emergent Digital EcoSystems, Proceedings*, pages 133–138, 09 2014.

[13] Jakob Breu, Achim Brakemeier, and Michael Menth. A quantitative study of cooperative awareness messages in production vanets. *EURASIP Journal on Wireless Communications and Networking*, 2014:98, 06 2014.

[14] Evellyn S. Cavalcante, André L.L. Aquino, Gisele L. Pappa, and Antonio A.F. Loureiro. Roadside unit deployment for information dissemination in a vanet: An evolutionary approach. In *Proceedings of the 14th Annual Conference Companion on Genetic and Evolutionary Computation*, GECCO '12, page 27–34, New York, NY, USA, 2012. Association for Computing Machinery.

[15] I. D. Chakeres and E. M. Belding-Royer. Aodv routing protocol implementation design. In *24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings.*, pages 698–703, 2004.

[16] J. Chen, T. Li, and J. Panneerselvam. Tmec: A trust management based on evidence combination on attack-resistant and collaborative internet of vehicles. *IEEE Access*, 7:148913–148922, 2019.

[17] Y. Chen and Y. Wei. A beacon-based trust management system for enhancing user centric location privacy in vanets. *Journal of Communications and Networks*, 15(2):153–163, 2013.

[18] Ameneh Daeinabi and Akbar Ghaffarpour Rahbar. Detection of malicious vehicles (dmv) through monitoring in vehicular ad-hoc networks. *Multimedia tools and applications*, 66(2):325–338, 2013.

[19] Deeksha, A. Kumar, and M. Bansal. A review on vanet security attacks and their countermeasure. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pages 580–585, 2017.

[20] Manjusha Deshmukh and Divya Dinesh. Challenges in vehicle ad hoc network (vanet). 12 2014.

[21] D. Eckhoff, A. Brummer, and C. Sommer. On the impact of antenna patterns on vanet simulation. In *2016 IEEE Vehicular Networking Conference (VNC)*, pages 1–4, 2016.

[22] S. Ercan, M. Ayaida, and N. Messai. How mobile rsus can enhance communications in vanets? In *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pages 1–5, 2018.

[23] Michaela Fritiofsson and Patrik Olsson. Trust models in vehicular ad-hoc networks: Towards an evaluation and comparison. 2017.

[24] Diego Gambetta. Can we trust trust? diego gambetta. 08 2000.

[25] M. Gillani, A. Ullah, and H. A. Niaz. Trust management schemes for secure routing in vanets — a survey. In *2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, pages 1–6, 2018.

[26] Felix Gomez Marmol and Gregorio Martinez Perez. Trip: A trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, 35:934–941, 01 2011.

[27] Jyoti Grover, Manoj Singh Gaur, and Vijay Laxmi. *Trust Establishment Techniques in VANET*, pages 273–301. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[28] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane. A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 09 2014.

[29] Rasheed Hussain, Waqas Nawaz, JooYoung Lee, Junggab Son, and Jung Taek Seo. A hybrid trust management framework for vehicular social networks. volume 9795, pages 214–225, 08 2016.

[30] Teerawat Issariyakul and Ekram Hossain. *Introduction to Network Simulator 2 (NS2)*, pages 21–40. Springer US, Boston, MA, 2012.

[31] Auxeeliya Jesudoss, Kasmir S, v, and Ashraph Sulaiman. Stimulating truth-telling and cooperation among nodes in vanets through payment and punishment scheme. *Ad Hoc Networks*, 24, 01 2014.

[32] S. Kaul, K. Ramachandran, P. Shankar, S. Oh, M. Gruteser, I. Seskar, and T. Nadeem. Effect of antenna placement and diversity on vehicular network communications. In *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pages 112–121, 2007.

[33] Rajdeep Kaur, Tejinder Singh, and Vinayak Khajuria. Security issues in vehicular ad-hoc network(vanet). pages 884–889, 05 2018.

[34] John Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99:1162 – 1182, 08 2011.

[35] M. A. Khan, A. Safi, I. M. Qureshi, and I. U. Khan. Flying ad-hoc networks (fanets): A review of communication architectures, and routing protocols. In *2017 First International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT)*, pages 1–9, 2017.

[36] Usman Ali Khan and Sang Sun Lee. Multi-layer problems and solutions in vanets: A review. *Electronics (Switzerland)*, 8(2), February 2019. Publisher Copyright: © 2019 by the authors. Licensee MDPI, Basel, Switzerland. Copyright: Copyright 2019 Elsevier B.V., All rights reserved.

[37] Uzma Khan, Shikha Agrawal, and Sanjay Silakari. Detection of malicious nodes (dmn) in vehicular ad-hoc networks. *Procedia Computer Science*, 46:965–972, 12 2015.

[38] Anushka Khattr. Introduction of mobile ad hoc network (manet). `https://www.geeksforgeeks.org/introduction-of-mobile-ad-hoc-network-manet/`, 2021. [Online; accessed Jan-2021].

[39] A. Kothari, P. Shukla, and R. Pandey. Trusit centric approach based on similarity in vanet. In *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, pages 1923–1926, 2016.

[40] W. Li and H. Song. Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 17(4):960–969, 2016.

[41] X. Li, J. Liu, X. Li, and W. Sun. Rgte: A reputation-based global trust establishment in vanets. In *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, pages 210–214, 2013.

[42] Zhengming Li. Security, privacy and applications in vehicular ad hoc networks. 2012.

[43] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Yunchuan Sun, and Rongfang Bie. Vehicular ad hoc networks: Architectures, research issues, challenges and trends. In Zhipeng Cai, Chaokun Wang, Siyao Cheng, Hongzhi Wang, and Hong Gao, editors, *Wireless Algorithms, Systems, and Applications*, pages 102–113, Cham, 2014. Springer International Publishing.

[44] K. G. Lim, C. H. Lee, R. K. Y. Chin, K. Beng Yeo, and K. T. K. Teo. Sumo enhancement for vehicular ad hoc network (vanet) simulation. In *2017 IEEE 2nd International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, pages 86–91, 2017.

[45] Yazhi Liu, Jianwei Niu, Jian Ma, Lei Shu, Takahiro Hara, and Wendong Wang. The insights of message delivery delay in vanets with a bidirectional traffic model. *Journal of Network and Computer Applications*, 36(5):1287 – 1294, 2013.

[46] Nai-Wei Lo and Hsiao-Chien Tsai. A reputation system or traffic safety event on vehicular ad hoc networks. *EURASIP J. Wireless Comm. and Networking*, 2009, 02 2009.

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

[48] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui. A hybrid trust management heuristic for vanets. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 748–752, 2019.

[49] R. Mishra, A. Singh, and R. Kumar. Vanet security: Issues, challenges and solutions. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pages 1050–1055, 2016.

[50] A. Mu'azu, L. T. Jung, Ibrahim A. Lawal, and P. A. Shah. Throughput measurement for the guaranteed qos real-time traffic flows in vanets. *Procedia - Social and Behavioral Sciences*, 129:297–304, 2014.

[51] Qingzi Liu, Qiwu Wu, and Li Yong. A hierarchical security architecture of vanet. In *International Conference on Cyberspace Technology (CCT 2013)*, pages 6–10, 2013.

[52] F. Qu, Z. Wu, F. Wang, and W. Cho. A security and privacy review of vanets. *IEEE Transactions on Intelligent Transportation Systems*, 16(6):2985–2996, 2015.

[53] Danda B Rawat, Gongjun Yan, Bhed Bista, and Michele Weigle. Trust on the security of wireless vehicular ad-hoc networking. *Ad Hoc Sensor Wireless Networks*, 24:283–305, 01 2015.

[54] Maxim Raya and Jean-Pierre Hubaux. The security of vehicular ad hoc networks. 11 2005.

[55] Jetzabel Serna-Olvera. A trust-driven privacy architecture for vehicular ad-hoc networks. 2013.

[56] Riaz Shaikh and Ahmed Alzahrani. Intrusion-aware trust model for vehicular ad hoc networks. *Security and Communication Networks*, 7, 11 2014.

[57] S. S. Tangade and S. S. Manvi. A survey on attacks, security and trust management solutions in vanets. In *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pages 1–6, 2013.

[58] Yasser Toor, Paul Muhlethaler, Anis Laouiti, and Arnaud de La Fortelle. Vehicle ad hoc networks: Applications and related technical issues. ieee communications surveys tutorials, 10(3), 74-88. *Communications Surveys Tutorials, IEEE*, 10:74 – 88, 10 2008.

[59] G. Wang and Y. Wu. Bibrm: A bayesian inference based road message trust model in vehicular ad hoc networks. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 481–486, 2014.

[60] Yu-Chih Wei and Yi-Ming Chen. Reliability and efficiency improvement for trust management model in vanets. In James J. (Jong Hyuk) Park, Qun Jin, Martin Sang-soo Yeo, and Bin Hu, editors, *Human Centric Technology and Service in Smart Space*, pages 105–112, Dordrecht, 2012. Springer Netherlands.

[61] Y. Wu, F. Meng, G. Wang, and P. Yi. A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–7, 2015.

[62] Zhongyuan Jiang Hui Zhu Yinbin Miao Zhiquan Liu, Jianfeng Ma. Lsot: A lightweight self-organized trust model in vanets. *Mobile Information Systems*, 2016:1–15, 2016.