A Trust Evaluation Framework in Vehicular Ad-Hoc Networks

Farhan Ahmad

College of Engineering and Technology
University of Derby
UK

This thesis is submitted for the degree of
Doctor of Philosophy

February 2019

Author's declaration

I declare that the work outlined in this dissertation was carried out in the College of Engineering and Technology, University of Derby, UK under the supervision of Dr. Asma Adnane, Dr. Virginia N. L. Franqueira and Professor Ashiq Anjum. Further, I declare that the work stated in this thesis was done by the author, and no part of the thesis has been submitted in a thesis form to any other university. No human or animal participation have been included in this research and the research presented in this thesis has been ethically approved. The author confirms that appropriate credit has been given within the thesis where reference has been made to the work of others. Parts of this thesis have previously appeared in the papers listed under list of publications.

Farhan Ahmad

University of Derby

12th April, 2018

To my beloved family

Acknowledgements

PhD is the outcome of cooperation and support of several people both at professional and personal levels. I would like to acknowledge all the people who helped me to achieve my goal.

First and foremost, I would like to thank my Director of Studies and my mentor, Dr. Asma Adnane for providing me an excellent opportunity to work under her guidance. This journey wouldn't be possible without her extensive support and encouragement. I will always feel proud to be her first PhD student. I also had a privilege to collaborate with my second supervisor, Dr. Virginia N. L. Franqueira. Her vast teaching and research experience helped me a lot in writing my PhD thesis. I will always remember the fruitful discussions with her, especially, during the second year of my PhD. Further, I will like to extend my gratitude to Prof. Ashiq Anjum for his support and motivations throughout this PhD journey.

During my stay at the University of Derby, I had an honour to meet people with some great minds. I would specifically mention Late Dr. David Evans, who was one of the best person, I had a chance to work with. Thank you, David, you will always be in my memory. I also want to thank Prof. Lu Liu for supporting my research. Further, I am highly obliged to my PhD colleague and friend, James Hardy, for providing his valuable suggestions on my work.

Living away from family is not easy. I am in debt to my friends in Derby for always making me feel at home. I thank Muhammad Kazim, Muhammad Usman Yaseen, Ali Zahir, Bilal Arshad, Sanna Aizad, Rashid Minhas and Moeez Subhani for their support in Derby.

Family is the most important part of one's life. Thank you, Dad (Prof. Nisar Ahmad) and Mom (Mrs. Nusrat Shaheen), for your unconditional love and prayers throughout my life. This journey wouldn't be possible without your continuous support and guidance. I am thankful to my sisters (Mrs. Fahiza Nisar, Mrs. Afshan Nisar, Ms. Zainab Nisar) for their love and encouragement throughout my life. I am also highly obliged to my brother (Mr. Zeeshan Ahmad) and sister-in-law (Mrs. Mehreen Zeeshan), who, were always there to support and encourage me during every phase of my life. Last, but, not the least, my deepest gratitude goes to my beloved wife (Mrs. Sana Farhan) for always being patient with me throughout my PhD.

Abstract

Vehicular Ad-Hoc Networks (VANET) is a novel cutting-edge technology which provides connectivity to millions of vehicles around the world. It is the future of Intelligent Transportation System (ITS) and plays a significant role in the success of emerging smart cities and Internet of Things (IoT). VANET provides a unique platform for vehicles to intelligently exchange critical information, such as collision avoidance or steep-curve warnings. It is, therefore, paramount that this information remains reliable and authentic, i.e., originated from a legitimate and trusted vehicle. Due to sensitive nature of the messages in VANET, a secure, attack-free and trusted network is imperative for the propagation of reliable, accurate and authentic information. In case of VANET, ensuring such network is extremely difficult due to its large-scale and open nature, making it susceptible to diverse range of attacks including man-in-the-middle (MITM), replay, jamming and eavesdropping.

Trust establishment among vehicles can increase network security by identifying dishonest vehicles and revoking messages with malicious content. For this purpose, several trust models (TMs) have been proposed but, currently, there is no effective way to compare how they would behave in practice under adversary conditions. Further, the proposed TMs are mostly context-dependent. Due to randomly distributed and highly mobile vehicles, context changes very frequently in VANET. Ideally the TMs should perform in every context of VANET. Therefore, it is important to have a common framework for the validation and evaluation of TMs.

In this thesis, we proposed a novel Trust Evaluation And Management (TEAM) framework, which serves as a unique paradigm for the design, management and evaluation of TMs in various contexts and in presence of malicious vehicles. Our framework incorporates an asset-based threat model and ISO-based risk assessment for the identification of attacks against critical risks. TEAM has been built using VEINS, an open source simulation environment which incorporates SUMO traffic simulator and OMNET++ discrete event simulator. The framework created has been tested with the implementation of three types of TM (data-oriented, entity-oriented and hybrid) under four different contexts of VANET based on the mobility of both honest and malicious vehicles. Results indicate that TEAM is effective to simulate a wide range of TMs, where the efficiency is evaluated against different Quality of Service (QoS) and security-related criteria. Such framework may be instrumental for planning smart cities and for car manufacturers.

List of Publications

Journal Papers

J1: **F. Ahmad**, A. Adnane, V. N. L. Franqueira, F. Kurugollu, L. Liu, "*Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers Strategies*", in MDPI Sensors, 2018 ; doi:10.3390/s18114040 **(IF: 2.475)**

J2: **F. Ahmad**, V. N. L. Franqueira, A. Adnane, "*TEAM: A Trust Evaluation and Management Framework in Context-enabled Vehicular Ad-Hoc Networks*", in IEEE Access, vol. 6, pp. 28643-28660, 2018. DOI: 10.1109/ACCESS.2018.2837887 **(IF: 3.244)**

J3: Y. Mehmood, **F. Ahmad**, I. Yaqoob, A. Adnane, M. Imran, S. Guizani, "*Internet-of-Things Based Smart Cities: Recent Advances and Challenges*", in IEEE Communications Magazine, vol. 55, no. 9, pp. 16-24, 2017. DOI: 10.1109/MCOM.2017.1600514 **(IF: 10.43)**

J4: **F. Ahmad**, A. Adnane, V. N. L. Franqueira "*A Systematic Approach for Cyber Security in Vehicular Networks*", in Journal of Computer and Communications, vol. 4, pp 38-62, December, 2016. DOI: 10.4236/jcc.2016.416004

Conference Papers

C1: **F. Ahmad**, A. Adnane, F. Kurugollu, R. Hussain, "*A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks*", in 11th IEEE Wireless Days, April 24 - 26, 2019, Manchester, UK *(Accepted)*

C2: **F. Ahmad**, J. Hall, A. Adnane, V. N. L. Franqueira, *"Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-hoc Network"*, in 10th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom), June 21 - 23, 2017, Exeter, UK

C3: **F. Ahmad**, A. Adnane, *"A Novel Context-based Risk Assessment Approach in Vehicular Networks"*, in 30th IEEE International Conference on Advanced Information Networking and Applications Workshops, March 23 - 25, 2016, Crans-Montana, Switzerland

C4: **F. Ahmad**, M. Kazim, A. Adnane, A. Awad, *"Vehicular Cloud Networks: Architecture, Applications and Security Issues"*, in 8th IEEE/ACM International Conference on Utility and Cloud Computing (8th UCC), December 07 - 10, 2015, Limassol, Cyprus

Book Chapters

B1: **F. Ahmad**, A. Adnane, C. A. Kerrache, V. N. L. Franqueira, F. Kurugollu, *"Trust Management in Vehicular Ad-Hoc Networks and Internet-of-Vehicles: Current Trends and Future Research Directions"*, in Global Advancements in Connected and Intelligent Mobility, IGI Global, 2018 *(Submitted)*

B2: **F. Ahmad**, M. Kazim, A. Adnane, *"Vehicular Cloud Networks: Architecture and Security Issues"*, in Guide to Security Assurance in Cloud Computing, Springer, 2015

Posters

P1: **F. Ahmad**, V. N. L. Franqueira, A. Adnane, *"A Framework for Trust Evaluation in Intelligent Transportation Systems"*, in 2^{nd} CBI East Midlands Conference on Cyber Security, October 5th, 2017, Derby, UK

P2: **F. Ahmad**, A. Adnane, *"Evaluation Platform for Trust in Vehicular Ad hoc Networks"*, in 10th European Conference on Computer Systems (EuroSys), April 18th - 21st, 2016, London, UK

P3: **F. Ahmad**, A. Adnane, *"Trust Evaluation Platform in Vehicular Ad hoc Networks"*, in University of Derby Postgraduate Research Conference (UoD-PGRC), 27th April, 2016, Derby, UK

P4: **F. Ahmad**, A. Adnane, *"Design of Trust based Context Aware Routing Protocol in Vehicular Networks"*, in 9th IFIP WG 11.11 International Conference on Trust Management (IFIPTM), May 26 - 29, 2015, Hamburg, Germany

List of Abbreviations

3G	3^{rd} Generation
4G	4^{th} Generation
5G	5^{th} Generation
AU	Application Unit
AR	Anomaly Ratio
ASIL	Automotive Safety Integrity Levels
BER	Bit Error Rate
CAN	Controller Area Network
C2C	Car-to-Car
CH	Cluster Head
CL	Confidence Level
CRW	Congestion Road Warning
DES	Discrete Event Simulation
DSRC	Dedicated Short Range Communication
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DOT	Department of Transportation
DOTM	Data-Oriented Trust Model
ECU	Electronic Control Unit
EDP	Event Detection Probability
E2E	End-to-End
EOTM	Entity-Oriented Trust Model

ERTICO	European Road Transport Telematics Implementation Co-ordination Organization
FOT	Field Operational Test
FPR	False Positive Rate
GUI	Graphical User Interface
GPS	Global Positioning System
HARA	Hazard Analysis and Risk Assessment
HTM	Hybrid Trust Model
ICT	Information and Communication Technology
ITS	Intelligent Transportation System
IoT	Internet of Things
IP	Internet Protocol
IVC	Inter-vehicular communication
LIN	Local Interconnect Network
LTE-A	Long Term Evolution Advanced
LCAW	Lane Change Assistance Warning
MANET	Mobile Ad Hoc Networks
MOST	Media Oriented Systems Transport
MOVE	Mobility Model for Vehicular Network
M2M	Machine-to-Machine
MITM	Man-in-the-middle
OBU	On-Board Unit
OMNET++	Objective Modular Network Testbed in C++
OS	Operating System
PKI	Public Key Infrastructure
PCW	Post-Crash Warning
QoS	Quality of Service
RSU	Road Side Unit
Rx	Receiver

SUMO	Simulation of Urban Mobility
SP	Service Provider
TA	Trusted Authority
TCP	Transmission Control Protocol
TEAM	Trust Evaluation and Management Framework
TEF	Trust Evaluation Framework
TL	Trust Level
TTP	Trusted Third Party
TM	Trust Model
TPR	True Positive Rate
Tx	Transmitter
TVRA	Threat Vulnerability and Risk Analysis
VANET	Vehicular Ad Hoc Networks
VEINS	Vehicles in Network Simulation
V2B	Vehicle-to-Bicycle
V2G	Vehicle-to-Grid
V2H	Vehicle-to-Home
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Anything
WAVE	Wireless Access in Vehicular Environment
WHO	World Health Organization

Contents

Acknowledgements **v**

Abstract **vi**

List of Publications **vii**

List of Abbreviations **x**

1 Introduction **1**

1.1 Motivation 1

1.2 Problem Formulation 3

1.3 Research Question 4

1.4 Dissertation Aim and Objectives 5

1.5 Dissertation Contributions 6

1.6 Organization of the Dissertation 7

2 Fundamental Concepts of Vehicular Ad-Hoc Networks **10**

2.1 Brief History of Intelligent Vehicles 10

2.2 Architecture of VANET . . . 11

2.2.1 Intelligent Vehicle . . . 11

2.2.2 Roadside Unit . . . 12

2.2.3 Communication Paradigms of VANET . . . 13

2.3 Important Applications of VANET . . . 16

2.3.1 Safety Applications . . . 16

2.3.2 Non-Safety Applications . . . 19

2.4 Challenges faced by VANET . . . 19

2.4.1 Technical Challenges . . . 19

2.4.2 Routing Challenges . . . 20

2.4.3 Security Challenges . . . 21

2.4.4 Trust Challenges . . . 22

2.5 Summary . . . 23

3 Trust Management in VANET 24

3.1 Security in VANET . . . 24

3.1.1 Privacy . . . 25

3.1.2 Security . . . 25

3.1.3 Trust . . . 27

3.2 Trust in VANET . . . 28

3.2.1 Trust Terminology . . . 28

3.2.2 Importance of Trust in VANET . . . 29

3.2.3 Why trust is preferred over traditional cryptography? 31

3.3 Trust Modelling in VANET 32

3.3.1 Entity-Oriented Trust Models 33

3.3.2 Data-Oriented Trust Models 36

3.3.3 Hybrid Trust Models 38

3.4 Evaluation Frameworks for Trust Management 43

3.5 Summary 45

4 Trust Evaluation and Management Framework 46

4.1 Proposed Trust Evaluation and Management Framework 46

4.1.1 Module 1: Threat Model 48

4.1.2 Module 2: Risk Assessment 49

4.1.3 Module 3: Identification and Categorization of Trust Models 51

4.1.3.1 Data-Oriented Trust Model (DOTM) 51

4.1.3.2 Entity-Oriented Trust Model (EOTM) 52

4.1.3.3 Hybrid Trust Model (HTM) 54

4.1.4 Module 4: Context Establishment 55

4.1.4.1 Context Identification 55

4.1.4.2 Identification of Attacker Model 56

4.1.4.3 VANET Attack Scenario 56

4.1.5 Module 5: Trust Evaluation Platform 56

4.1.5.1 Message Evaluation Module 57

4.1.5.2 Trust Computation & Updation Module 59

4.1.5.3 Trust Evaluation Module 60

4.2 Qualitative Evaluation of Trust Models 66

4.3 Summary 69

5 Research Methodology and Simulation Model 71

5.1 Research Methodology 71

5.2 Simulation Environment 74

5.2.1 Network Simulation 75

5.2.1.1 OMNET++ Simulation Environment 75

5.2.2 Traffic Simulation 76

5.2.2.1 SUMO Traffic Simulation Environment 76

5.3 VEINS Simulation Framework 77

5.3.1 Imported Maps 78

5.3.2 Traffic Modelling 78

5.3.3 Nodes Identification 79

5.3.3.1 Application Layer 80

5.3.3.2 MAC and Physical Layer 81

5.4 Summary 82

6 Context-based Risk Assessment in VANET 83

6.1 State-of-the-art: risk assessment 84

6.2 Risk Assessment Methodology . . . 87

6.2.1 Context Establishment . . . 88

6.2.1.1 Identification of VANET scenario . . . 88

6.2.1.2 Identification of attacker models . . . 89

6.2.1.3 VANET attack scenario . . . 89

6.2.2 Risk Identification . . . 90

6.2.2.1 Identification of Assets in VANET . . . 90

6.2.2.2 Classification of Assets . . . 91

6.2.2.3 Identification of Vulnerabilities in VANET . . . 92

6.2.2.4 Identification of Threats in VANET . . . 93

6.2.2.5 Identification of Attacks in VANET . . . 95

6.2.3 Risk Analysis . . . 97

6.2.4 Context-based Risk Assessment . . . 99

6.2.4.1 Risk Analysis for Attacks in Vehicles and Vehicular Users . . . 100

6.2.4.2 Risk Analysis for Attacks in Wireless Communication . . . 102

6.2.4.3 Risk Analysis for Attacks in Information . . . 104

6.2.4.4 Risk Analysis for Attacks in Infrastructure . . . 104

6.2.5 Monitor and Review . . . 106

6.2.6 Discussion . . . 106

6.3 Man-in-the-Middle Attacks . . . 108

6.3.1 MITM as Message Delayed . . . 109

6.3.2 MITM as Message Dropped . . . 110

6.3.3 MITM as Message Tempered . . . 110

6.3.4 Simulation Environment . . . 112

6.3.4.1 Simulation Setup . . . 112

6.3.4.2 Simulation Scenario Setup . . . 113

6.3.4.3 Performance Evaluation Metrics . . . 113

6.3.5 Results and Discussion . . . 115

6.3.5.1 Message Delay Attacks . . . 115

6.3.5.2 Message Drop Attacks . . . 117

6.3.5.3 Message Temper Attacks . . . 119

6.4 Summary . . . 122

7 Performance Evaluation of TEAM Framework 124

7.1 Evaluation Metrics . . . 124

7.1.1 End-to-end Delay (E2ED) . . . 125

7.1.2 Event Detection Probability (EDP) . . . 125

7.1.3 Anomaly Ratio (AR) . . . 125

7.1.4 Trusted & Untrusted Packets in the network . . . 126

7.1.5 False Positive Rate (FPR) . . . 126

7.2 Considered Adversary Model . . . 127

7.3 Evaluation of Trust Models . . . 128

7.3.1 Evaluation of trust models for general VANET . . . 128

7.3.1.1 End-to-end Delay 129

7.3.1.2 Event Detection Probability 130

7.3.1.3 Anomaly Ratio 131

7.3.1.4 False Positive Rate 132

7.3.1.5 Trusted and Untrusted Packets 133

7.3.2 Evaluation of trust models for context-enabled VANET 134

7.3.2.1 End-to-end Delay 135

7.3.2.2 Event Detection Probability 137

7.3.2.3 Anomaly Ratio 139

7.3.2.4 False Positive Rate 140

7.3.2.5 Trusted and Untrusted Packets 142

7.4 Discussion 143

7.4.1 Applicability of TEAM: 143

7.4.2 Usability of TEAM: 144

7.4.3 Scalability Analysis: 144

7.4.4 Security Analysis: 145

7.4.5 Limitation of TEAM: 145

8 Conclusion and Future Work 147

8.1 Major Contributions 147

8.2 Future Work 149

Appendix 1: Adding Attacks and Trust Models in TEAM 153

Bibliography 154

List of Tables

2.1 Communication Paradigms Properties in VANET 15

2.2 Notable Standardization Effort for Vehicular Ad-Hoc Networks 20

2.3 VANET Challenges and Possible Solutions 23

3.1 Major User Requirements, Issues and Possible Solutions 27

3.2 Trust Definitions in VANET 28

3.3 Trust Properties in VANET 31

3.4 Trust Model Comparison: Advantages and Disadvantages 42

3.5 Comparison of Trust Evaluation Frameworks 45

4.1 Risk Analysis: Scale 50

4.2 Risk Assessment for Attacks in VANET 50

4.3 VANET Attack Scenario 56

4.4 Qualitative Evaluation of Trust Models in VANET 67

4.5 Proposed Evaluation Criteria for Trust Management Compared to Previous Studies 68

6.1 Possible Attack Scenarios based on Network Mobility 90

6.2 Risk Analysis: Scale 100

6.3 Context-based Risk Analysis for Attacks in Vehicles and Vehicular Users 101

6.4 Context-based Risk Analysis for Attacks in Wireless Communication 103

6.5 Context-based Risk Analysis for Attacks in Information 105

6.6 Context-based Risk Analysis for Attacks in Infrastructure 107

6.7 Simulation Details 114

7.1 Simulation Details 129

7.2 Simulation Details for TEAM in context-enabled VANET 135

7.3 Comparison of End-to-end Delay 137

7.4 Comparison of Event Detection Probability 138

7.5 Comparison of Anomaly Ratio 140

7.6 Comparison of False Positive Rate 140

7.7 Comparison for Total Trusted Packets 142

7.8 Comparison for Total Untrusted Packets 142

List of Figures

1.1 Projection of Yearly Sales of Connected Vehicles [1] 2

1.2 Dissertation Organization 9

2.1 Illustration of VANET in the context of Smart Cities 11

2.2 Sensor locations & connectivity within Vehicle 12

2.3 In-Vehicle communication 13

2.4 Communication paradigms in VANET 15

2.5 Classification of VANET applications 18

3.1 Direct Vs Indirect Trust 29

3.2 State Transitions between Trust Levels 31

4.1 Proposed Trust Evaluation Framework 47

4.2 Asset-based approach for threat model 48

4.3 Use Cases for Message Verification and Evaluation 58

4.4 Evaluation Criteria Satisfaction in Trust Models 68

4.5 Comparison of Trust Models 69

5.1 Taxonomy of Research Methodology 73

5.2 Work-flow of VEINS simulator [2] 78

5.3 Simulated Maps of Derby (a) Urban (b) Rural 79

5.4 Node model in OMNET++ (a) Mobile Node (b) Static Node 80

6.1 Time-line of Related Risk Assessment Frameworks and Standards 86

6.2 Risk Assessment Framework 88

6.3 Assets and their classification in VANET 92

6.4 Man-in-the-Middle Attacks in VANET 108

6.5 Attacker Pattern (a) Distributed (b) Fleet 112

6.6 End-to-End Delay 116

6.7 Content Delivery Ratio 116

6.8 Compromised Messages 118

6.9 Packet Loss Ratio 118

6.10 Content Delivery Ratio 119

6.11 Dropped Messages 120

6.12 Packet Loss Ratio 120

6.13 End-to-End Delay 120

6.14 Content Delivery Ratio 120

6.15 Compromised Messages 122

6.16 Packet Loss Ratio 122

7.1 E2E Delay vs Attackers . . . 130

7.2 Event Detection Probability vs Attackers . . . 131

7.3 Anomaly Ratio vs Attackers . . . 132

7.4 False Positive Rate vs Attackers . . . 133

7.5 Trusted Packets vs Attackers . . . 134

7.6 Untrusted Packets vs Attackers . . . 134

7.7 End-to-End Delay (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM136

7.8 Event Detection Probability (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM . . . 138

7.9 Anomaly Ratio (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM . 139

7.10 False Positive Rate (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM . . . 141

7.11 Trusted packets in the network (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM . . . 141

7.12 Untrusted packets in the network (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM . . . 143

Chapter 1

Introduction

1.1 Motivation

The growing number of vehicles around the world arises various transportation issues, such as traffic accidents, congestions and air pollution. According to World Health Organization (WHO), traffic accidents are responsible for the loss of about 1.25 million human lives annually, making it the nineth leading cause of human casualties around the world [3]. Recently, a preeminent interest have been observed around the world to address the transportation issues. Many regions have initiated various pilot projects in this domain, resulting in the emergence of Intelligent Transportation System (ITS). ITS utlizes the advancements in information and communication technologies (ICT) to improve the overall transportation in terms of traffic efficiency and road safety. In United Kingdom, ITS-UK is dedicated for improving transportation in terms of traffic safety, reducing travel times, smart parking and making environment green [4]. In Europe, ERTICO is responsible for ITS development by ensuring safer, cleaner and smarter vehicle mobility [5]. In United States, Department of Transportation (DOT) is advancing the transportation technology through its strategic plan 2015-2019 [6]. This plan includes safe and enhanced traffic mobility with less impact on the environment. In Asia, Japan is leading this discipline by setting ITS standards to improve transportation [7]. In South America region, ITSB is dedicated to improve the quality of transportation in Brazil. This includes managing the high mobility demand on the existing infrastructure, reducing congestion and providing safety to the road traffic [8]. In Australia, ITS is accelerating through its strategic plan 2013 - 2018. This plan focuses on enhancing efficient and sustainable traffic mobility through the advancements in ICT sector [9]. The major aim of all of these projects is to improve the quality of life in terms of better and safer transportation.

Vehicular Ad-hoc Networks (VANET) is the state-of-the-art technology in the domain of ITS, where vehicles communicate with each other and adjacent roadside unit (RSU) to partially solve transportation issues such as reducing traffic accidents, better traffic management, minimizing traffic congestions, and providing infotainment to on-board vehicular users. These services are possible only if vehicles and RSUs are equipped with appropriate sensors, devices and Internet. In VANET, vehicles access these services via Internet, thus introducing the concept of connected vehicles [10]. VANET, being the future of ITS, is attracting massive attention from both research community and automobile manufacturing industry. According to SBD Automotive[1], about 68% of the vehicles manufactured worldwide will offer some sort of built-in connectivity by the end of 2025 [1]. Moreover, it is projected that the annual sales of connected vehicles will rise from 18.3 million to 81.2 million in just 11 years as depicted in Figure 1.1.

Removed for Copyright Purposes

Figure 1.1: Projection of Yearly Sales of Connected Vehicles [1]

[1] https://www.sbdautomotive.com/ (Accessed: 21st March, 2018)

1.2 Problem Formulation

In VANET, vehicles communicate with each other and with RSU to offer various applications, which are broadly classified into two categories: safety-related and non-safety related applications. Safety related applications are designed to ensure driver safety and to provide assistance to the vehicular users during critical situations such as steep-curves. These applications are further categorized into vehicular sensing-based applications and VANET-based safety applications. The former applications rely on different sensors (e.g., distance sensors, GPS, ultrasonic sensors, safety sensors, cameras etc.) which are embedded within the vehicles and adjacent infrastructures. These sensors have the ability to sense the event within their vicinity and inform the vehicles to take respective actions. The applications in this category include sudden lane-change warnings, slow vehicle detection warnings and pre-crash warnings etc. In contrast, VANET-based safety applications rely on collaborative communication among vehicles to ensure security within the network. Applications in this domain range from intersection collision warnings, cooperative forward collision warnings to pedestrian crossing safety warnings. On the other hand, non-safety applications provide infotainment and comfort to users during their journey, such as real-time traffic information and weather conditions etc. It is worth mentioning that safety-related applications are delay-intolerant while most of the non-safety applications are delay tolerant.

VANET mostly include safety related messages in the network. Ideally, these messages should arrive at the destination from source vehicle without any alteration to its content via intermediate vehicles. VANET is a self-organising network which lacks permanent presence of fixed infrastructure due to its highly dynamic and disperse topology, thus messages between two vehicles are exchanged in a very short span of time. Verifying the authenticity and accuracy of the received messages in such a network becomes highly challenging.

Recently, various solutions have been proposed to ensure secure message dissemination in VANET. Most of these solutions rely on traditional cryptography where vehicles utilize certificates and Public Key Infrastructure (PKI) to ensure security upto certain level within the network. However, cryptography-based solutions generate high overheads which ultimately introduce huge network delays, thus making it inappropriate for delay intolerant applications such as pre-crash or accident warnings. Moreover, these solutions secure the network from outsider attacks only. However, such solutions can be compromised by insider attacks, which results in the transmission of untrusted information throughout the network.

In order to address these shortcomings, trust has been proposed as a relevant technique to achieve network security in VANET. Trust, a concept adopted from economic science is defined as the confidence of one entity on another entity to perform specific action or set of actions. In VANET, trust is established between two vehicles based on the information exchanged regarding an event. Trust-based solutions ensure trusted data dissemination in the network with low overheads. Further, these solutions can tackle insider attacks, thus ensuring high network security.

Trust establishment in wired networks is comparatively easy as it involves a trusted third party (TTP). However, establishing trust in VANET is difficult as it is established between two vehicles in an ad-hoc manner. Due to high mobility and random distribution of vehicles in VANET, trust among the vehicles is created for a very short duration of time. Establishing and evaluating trust on the received messages in such short span of time is extremely challenging.

1.3 Research Question

Trust, as a technique to achieve security in VANET, is in its early stage of development. Trust models (TMs) are embedded within the vehicles to evaluate trustworthiness, accuracy and authenticity of received messages. TMs ensure the propagation of trusted information within the network by revoking both dishonest nodes (vehicle) and messages containing malicious content. In VANET, TMs are classified into three distinct classes, i.e., entity-oriented, data-oriented and hybrid TMs [11, 12, 13]. Entity-oriented trust models (EOTM) aims to eliminate dishonest vehicles by evaluating trustworthiness on the node. Data-oriented trust models (DOTM) evaluates trust on the received messages (data) while hybrid trust models (HTM) relies on both vehicle and data for trust establishment.

In VANET, various TMs are developed to ensure security either by eliminating dishonest vehicles or tempered messages such as [14, 15, 16, 17]. However, it is currently complicated to compare and evaluate the efficiency of these TMs due to the absence of a unified trust evaluation framework. Moreover, high mobility and random distribution of vehicles across the network result in various contexts in VANET. Therefore, it becomes significantly important to take those contexts into account for trust management. For instance, in an urban location, extensive amount of messages (trusted & untrusted) are present due to low mobility of vehicles and abundant number of RSUs. On the other hand, rural areas cannot ensure the permanent presence of RSU. Moreover, small number of messages are present in such locations due to high mobility and low number of vehicles. TMs which rely on high number of RSUs and vehicles for trust management will show poor results for a scenario involving minimum number of vehicles. As a result, both scenarios demand separate techniques to evaluate trustworthiness on transmitting node and their messages.

The TM should have the capability to perform in every context due to the sensitive nature of information involved in VANET. Evaluating the efficiency of these TMs in such a dynamic environment is an open question. In this dissertation, we fill this gap by proposing a novel framework which have the ability to evaluate TMs in various contexts of VANET.

1.4 Dissertation Aim and Objectives

This research aimed at designing and developing a novel framework to validate and evaluate trust models in VANET. To achieve this aim, following objectives will be accomplished.

- To design a comprehensive threat model for the identification of threats, vulnerabilities and attacks in different components of VANET including vehicles, network and static infrastructure. This will identify the possible attacks which can compromise the network security.

- To perform risk assessment on the attacks identified for each component of VANET and categorization of these attacks based on their severity level. Risk assessment will identify and prioritize the attacks posing critical risk on VANET.

- To propose various realistic evaluation criteria for trust management in VANET. These criteria will be used to evaluate the efficiency of the TMs in VANET.
- To design and implement a novel trust evaluation framework based on threat model, risk assessment, and evaluation criteria for the validation of TMs. This framework will provide a detailed guideline for the selection of appropriate TM in proper context of VANET.
- To implement various TMs using the proposed framework where the efficiency of the TMs are evaluated in various contexts of VANET.

1.5 Dissertation Contributions

The major contributions of this dissertation are:

- An asset-based threat model is proposed where vulnerabilities, threats and attacks are identified in different components of VANET. Moreover, attacks are identified directly by mapping threats and vulnerabilities. *(Published in: Journal of Computer and Communications, 2016)*
- A novel context-based risk assessment is proposed, where critical attacks are identified in four contexts based on the mobility of legitimate and malicious vehicles. The attacks with critical risks are integrated in the proposed framework. *(Published in: 30th IEEE International Conference on Advanced Information Networking and Applications Workshops, 2016)*
- A comprehensive set of evaluation criteria is proposed for the evaluation of TMs. It includes sixteen distinct evaluation criteria based on unique characteristics (high mobility, random distribution of vehicles and lack of infrastructure) of the network. *(Published in: 10th IEEE International Conference on Cyber, Physical and Social Computing, 2017)*

- A novel context-based trust evaluation is proposed and implemented where various TMs are evaluated in different contexts of VANET. This includes the evaluation of TMs in both various contexts and in presence of malicious vehicles. A simulation model is developed using open-source simulators (OMNET++, VEINS, SUMO) where extensive simulations are performed to evaluate the efficiency of TMs. *((Poster): in 10th European Conference on Computer Systems (EuroSys), 2016; (Journal - Published) in: IEEE Access, 2018)*

1.6 Organization of the Dissertation

The rest of the dissertation is organized as follows:

Chapter 2 provides an overview of Vehicular Ad-hoc Networks (VANET) from architecture, security and trust perspective. We start this chapter with brief history, architecture and applications of VANET. Next, we focus on the security issues of VANET, where, we discuss major security requirements and attacks violating these requirements.

Chapter 3 presents the trust management in VANET where we first reviewed the state-of-the-art literature on trust management in VANET. Further, we discussed the basic concepts of trust management in VANET. Finally, we provide an in-depth literature and related work in trust models and the trust management frameworks.

Chapter 4 presents the details of the proposed trust evaluation and management (TEAM) framework. First, we provide the basic details of TEAM framework, which is then followed by the explanation of all the involved modules. Further, this chapter provide the details of trust evaluation criteria. At the end, a qualitative evaluation of the trust models is performed using these evaluation criteria.

Chapter 5 provides the detail of the implemented simulation model for TEAM framework. First, applied research methodology is explained in detail. Further, this chapter provides the information about the network and traffic simulators in detail.

Chapter 6 is dedicated to the threat model and risk assessment in VANET. This chapter starts with the risk assessment framework where different attacks are identified and classified based on their severity levels. Next, this chapter provide details about the context-based risk assessment in VANET where the risks posed by attacks is evaluated qualitatively in different contexts of VANET. Further, Man-in-the-Middle (MITM) attacks are explained in this chapter which is implemented as a baseline attack model in TEAM framework. At the end of this chapter, a simulation model for MITM attacks is provided.

Chapter 7 is dedicated to the simulation results of TEAM framework. First, we provide the evaluation metrics which were implemented to evaluate the trust models using TEAM framework. Next, we provide the simulation results of the trust models under adversary conditions using TEAM framework. Further, simulation results of the implemented trust models in context-enabled framework is presented at the end of the chapter.

Chapter 8 summarizes the overall contributions of this dissertation. We first provide conclusions obtained from the dissertation and then we presented possible future extensions of this dissertation.

Figure 1.2 summarizes the organization of dissertation. Each preceding chapter is the input to the next chapter where it provides the basic concepts required for the chapter.

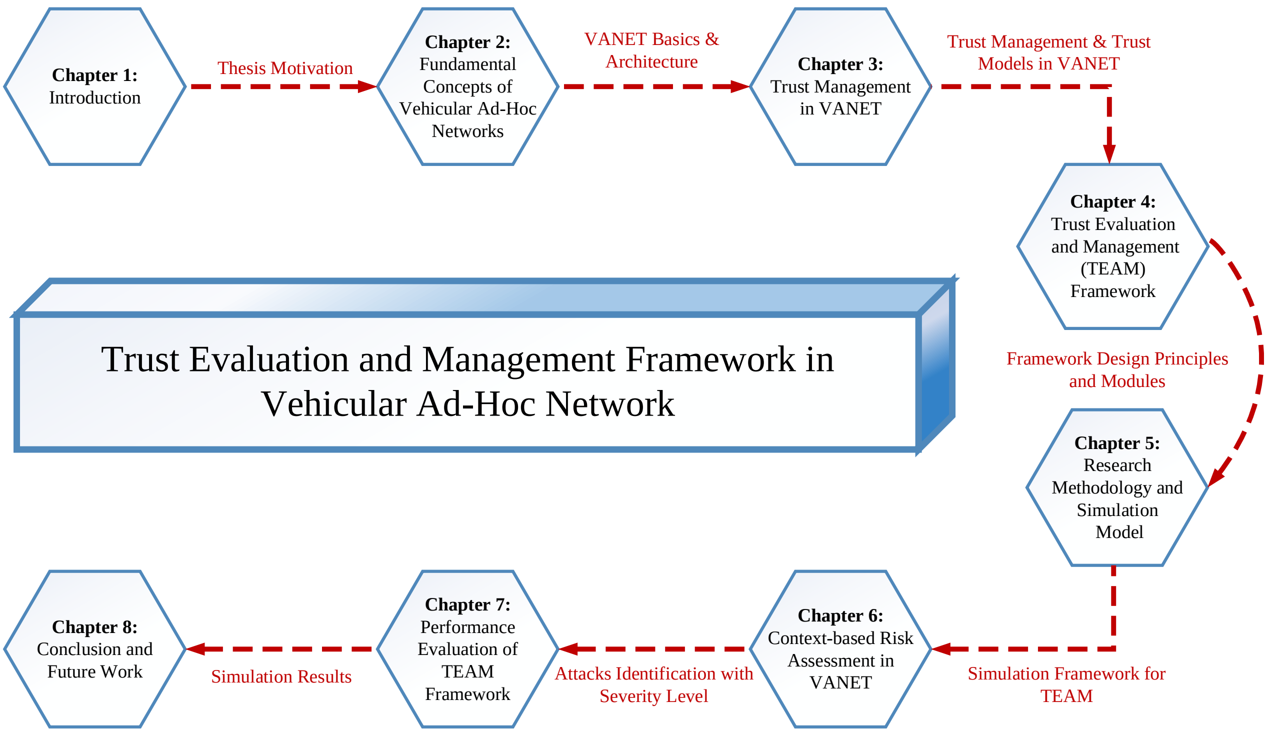

Chapter 1:
Introduction
Thesis Motivation
Chapter 2:
Fundamental Concepts of Vehicular Ad-Hoc Networks
VANET Basics & Architecture
Chapter 3:
Trust Management in VANET
Trust Management & Trust Models in VANET
Chapter 4:
Trust Evaluation and Management (TEAM) Framework
Trust Evaluation and Management Framework in Vehicular Ad-Hoc Network
Framework Design Principles and Modules
Chapter 5:
Research Methodology and Simulation Model
Simulation Framework for TEAM
Chapter 6:
Context-based Risk Assessment in VANET
Attacks Identification with Severity Level
Chapter 7:
Performance Evaluation of TEAM Framework
Simulation Results
Chapter 8:
Conclusion and Future Work

Figure 1.2: Dissertation Organization

Chapter 2

Fundamental Concepts of Vehicular Ad-Hoc Networks

2.1 Brief History of Intelligent Vehicles

The concept of intelligent vehicle was first revealed by General Motors during 1939-1940 New York Worlds Fair where the future of the transportation was exhibited as a result of extensive and large-scale development in the road related technologies [18]. However, this idea was delayed due to many reasons including World War 2. Intelligent transportation projects were re-initiated during late 1980's and early 1990's due to the advancements in information and communication technologies (ICT) such as the invention of Bluetooth, GPS and mobile communication networks. As a result of the massive break-through in ICT during post 2000s era, the concept of connected vehicles was no more a dream. Many automotive industries, such as TESLA, BMW, JAGUAR and GOOGLE, integrated ICT technologies (IEEE 802.11 and 4G mobile communicaiton networks) within the vehicles to introduce intelligent and connected vehicles. Moreover, current research work in various domains of ICT including IEEE 802.11p or 5G mobile communication networks is further extending the concept of connected vehicles towards fully autonomous or driver-less vehicles. The aim of connected and autonomous vehicles is to improve the transportation in terms of better safety and user's comfort.

2.2 Architecture of VANET

VANET is a technology which exploits the advantages of both wired and wireless technologies to provide various applications which range from safety to non-safety applications. Figure 2.1 depicts the architecture of VANET in the context of smart cities where vehicles communicate with each other and with static infrastructure via various modes of communication. VANET integrates various modules such as vehicles, Roadside Units (RSUs), communication network etc to offer a diverse range of applications. In the following section, we briefly explain these components.

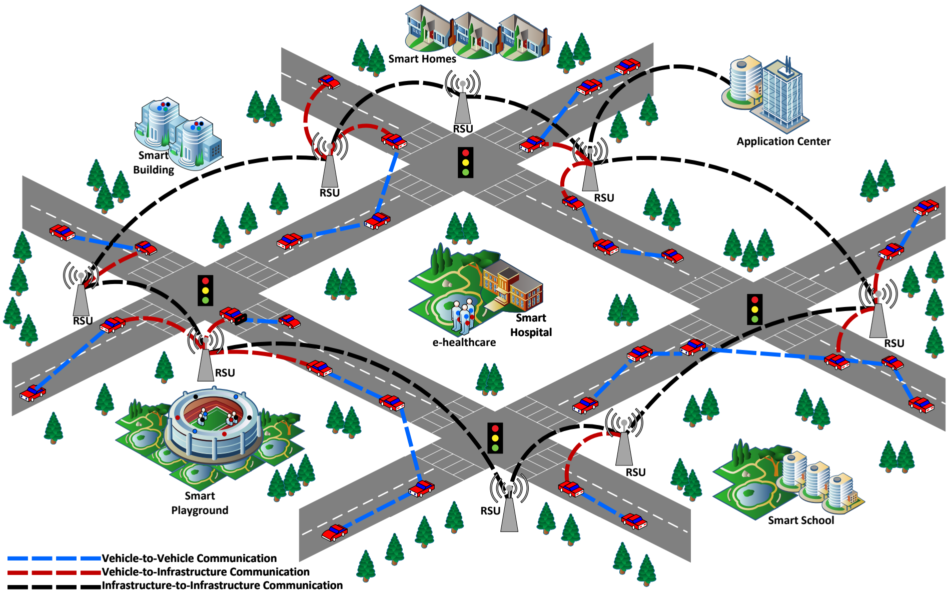


Figure 2.1: Illustration of VANET in the context of Smart Cities

2.2.1 Intelligent Vehicle

Typically, each intelligent vehicle is equipped with various modules like On-board Unit (OBU), Electronic Control Unit (ECU), Application Unit (AU), cameras and wide range of sensors such as distance sensor, GPS, RADAR, and safety sensors. All these devices are connected to each other via high speed internal buses such as Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST) and Ethernet etc as depicted in Figure 2.2 [19]. For instance, distance sensor of a vehicle detects the presence of neighbouring vehicle in its critical distance zone. This information from the vehicle is shared with neighbouring vehicle via internal buses and OBU, suggesting the vehicles to increase distance between them.

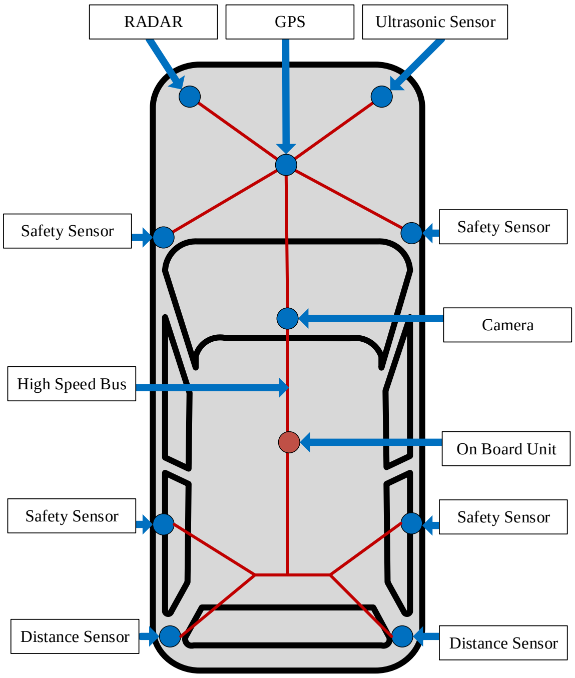


Figure 2.2: Sensor locations & connectivity within Vehicle

2.2.2 Roadside Unit

Roadside Units (RSUs) are installed at strategic locations which acts as a bridge between vehicles and infrastructure in the network. RSUs are static in nature and are deployed at specific locations such as traffic signals, lamp posts or mobile tower etc [20]. In RSU, the important components are its hardware, operating system (OS) and software residing on OS. This software communicates with vehicles on one hand and with infrastructure on the other. RSU is usually utilized and helpful for disseminating messages on the large scale within the network.

2.2.3 Communication Paradigms of VANET

Wireless communication is a significant asset in VANET which enable the vehicles to communicate with each other via various communication protocols such as IEEE 802.11p and mobile communication technology (for instance, Long Term Evolution-Advanced (LTE-A)). Broadly, communication in VANET can be categorized into following:

1. **In-Vehicle Communication:** The scope of in-vehicle communication is limited to vehicle itself where different components of vehicle such as sensors, AU and ECU communicates with OBU via high speed buses such as CAN, LIN or MOST. This communication enable the different components of vehicle to exchange information via its OBU. The high level view of in-vehicle communication is depicted in Figure 2.3, where, OBU transmits the messages generated by the AU according to the information provided by sensors and ECU.

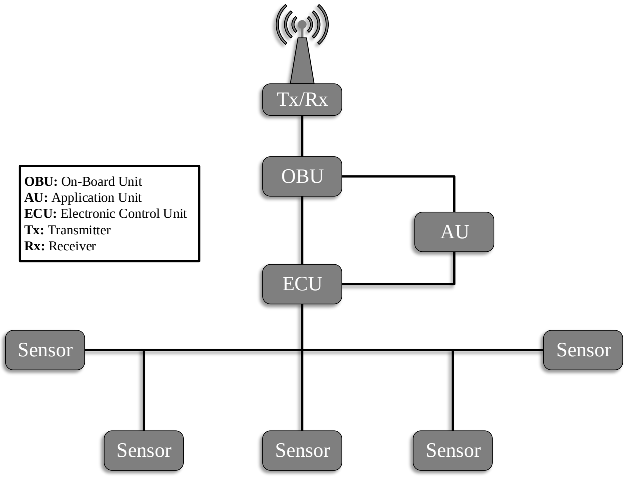


Figure 2.3: In-Vehicle communication

2. **Vehicle-to-Infrastructure Communication:** Vehicle-to-infrastructure (V2I) refers to communication between vehicles and adjacent infrastructure such as RSU. The main purpose of V2I communication is to disseminate information in a large geographical location via RSU or set of RSUs. V2I mostly uses mobile communication protocols such as LTE-A to inform drivers about the road hazards. Moreover, V2I is helpful for traffic management applications such as road warnings, traffic signal violation warnings, and weather

warnings. Additionally, V2I communication provides the platform for internet-enabled applications such as online banking, online streaming and infotainment.

3. **Vehicle-to-Vehicle Communication:** Vehicle-to-vehicle (V2V) communication refers to the communication among vehicles directly. This term is also sometimes called inter-vehicular communication (IVC) or car-to-car (C2C) communication. V2V communication uses dedicated short range communication (DSRC)[1][21] or ITS-G5 standard[2] [22, 23] in a pure ad-hoc manner to offer different applications. For instance, V2V communication is helpful in the design of safety applications to enhance driver awareness in the network such as sudden lane change warning, steep-curve warning, assistance in dense fog, intersection warning and emergency brake lights. Moreover, V2V communication can be utilized for non-safety applications as well such as roadside service discovery.

   In V2V communication, the scope of the vehicles is limited to specific geographical location as the information is exchanged among vehicles in a hop-by-hop manner via short range communication technologies, such as, DSRC or ITS-G5. These technologies correspond to set of protocols called as Wireless Access in Vehicular Environments (WAVE)[3] which operates at 5.9 GHz [24, 25].

4. **Hybrid Communication:** Hybrid communication refers to the scenario where V2V communication is used in conjunction with V2I communication for message distribution among the vehicles across the network. The main purpose of hybrid communication is to extend the coverage by providing information to those vehicles which are not in communication range of the static infrastructure.

5. **Vehicle-to-Anything Communication:** Vehicle-to-Anything (V2X) is a general terminology used for every communication among vehicles within VANET. It includes V2V, V2I, Vehicle-to-Pedestrian (V2P), Vehicle-to-Grid (V2G), Vehicle-to-Home (V2H), and Vehicle-to-Bicycle (V2B).

Figure 2.4 depicts the communication paradigms in VANET in case of steep-curve scenario

[1] DSRC is ITS standard which is deployed in USA

[2] ITS-G5 is GeoNetworking protocol standard used for ITS in Europe

[3] WAVE is built upon IEEE 802.11p standard

where messages are forwarded using V2V, V2I and hybird mode of communication. In case of V2I communication (2.4(a)), messages are shared with group of vehicles in a large geographical location. Similarly, V2V communication (2.4(b)) is useful to forward messages to vehicles close to event proximity. The illustration of hybrid communication in case of steep-curve is depicted in (2.4(c)), where vehicles exchange messages via both V2V and V2I communication. Moreover, Table 2.1 summarizes the properties of communication paradigms in terms of its coverage and communication protocols.

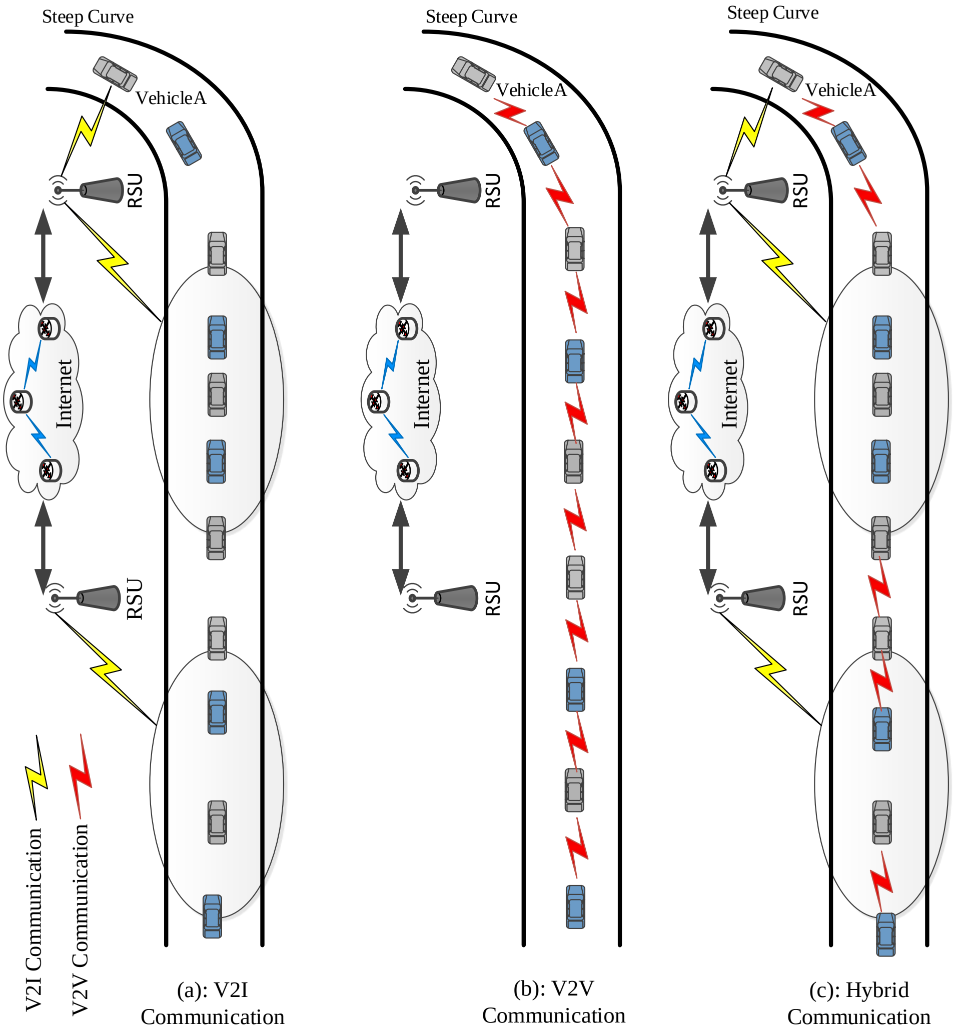


Figure 2.4: Communication paradigms in VANET

Table 2.1: Communication Paradigms Properties in VANET

	Area Coverage	**Communication Standard**	**Impact Location**
V2V	Small geographical location	DSRC, ITS-G5, WAVE	Vehicles close to event occurrence
V2I	Large geographical location	3G, LTE, LTE-A, 5G	Vehicles far from event occurrence
Hybrid	Large geographical location	DSRC, ITS-G5, WAVE, 3G, LTE-A, 5G	Vehicles close and far from event occurrence

2.3 Important Applications of VANET

The applications of VANET are on the rise as a result of massive research effort across the globe in this domain. The major focus of VANET is to ensure road safety. However, it can also be used for non-safety aspects of VANET. Main objectives of VANET include:

- Ensuring traffic safety on the road.
- Assisting drivers during critical situations including accidents and traffic congestions.
- Providing infotainment to vehicular users such as information about traffic and weather.
- Assisting the large fleet of vehicles to support logistics.

Based on the above objectives, VANET applications are broadly classified into following two categories [26].

1. Safety applications
2. Non-safety applications

2.3.1 Safety Applications

Safety applications are designed to ensure traffic safety and enhance efficiency of the network. Safety applications are further categorized into:

1. Sensing-based Safety Applications
2. VANET-based Safety Applications

1. **Sensing-based Safety Applications:** These applications rely on embedded sensors (such as GPS, distance sensors, camera, etc.) which are integrated within the vehicles. These sensors sense the event within its vicinity and generate information to inform the

vehicular user. Thus, it generates the idea of driver active safety applications where the driver can take various immediate measures in response to the received message to avoid traffic jam and clear way for ambulances and law-enforcement vehicles. The applications include the following:

(a) *Active safety applications* are designed for on-board vehicular user safety by issuing pre-crash warnings. For example, these applications ensure that the vehicular user has his seat belt fastened during the journey.

(b) *Passive safety applications* are designed to protect vehicular users after the occurrence of event such as accident. These applications cannot help to avoid an accident. Rather, these applications provide assistance to vehicular user to minimize the accident impact. For instance, air bag in vehicle are example of such applications.

(c) *Warning applications* are designed to alert the vehicular user by issuing different warnings such as post crash warnings, traffic congestion warnings, pedestrian crossing warnings etc [27].

(d) *Post-Crash Warning (PCW):* The vehicle involved in particular event such as accident usually broadcasts its location. PCW will ensure to exchange these warning messages with other vehicles with the help of V2V and V2I communication protocols. For example, swift lane change warning message should be transmitted to trailing vehicles which are very close to that particular event. The vehicles then flood these messages throughout the network. V2V mode cannot be efficient for vehicles with greater distances. In such case, V2I mode is used to disseminate messages across the network.

(e) *Lane Change Assistance Warning (LCAW):* This application assists the drivers in the event of lane change. It also informs the driver if the distance between two vehicles is very less. LCAW operates in two modes, i.e., active and passive mode. In the active mode, LCAW exchange messages with other cars if the distance between two cars is less while in passive mode, it only measures the distance between cars and keep the information to same vehicle only.

2. **Traffic Efficiency Applications:** These applications are designed to significantly increase the efficiency of vehicular traffic by issuing various warnings during hazard situations. These warning applications include Post-Crash Warnings (PCW), Congestion Road Warnings (CRW) and Lane Change Assistance Warnings (LCAW).

   (a) *Mutual cooperative driver assistance applications* where messages between vehicles are continuously transferred in a real time [28]. Thus, these applications can increase the vision of the driver regarding current traffic. For instance, vehicle A can inform vehicle B about the icy road conditions in an efficient and timely manner, so that vehicle B can take respective measures.

   (b) *Congestion Road Warning (CRW):* The main aim of this application is to assist

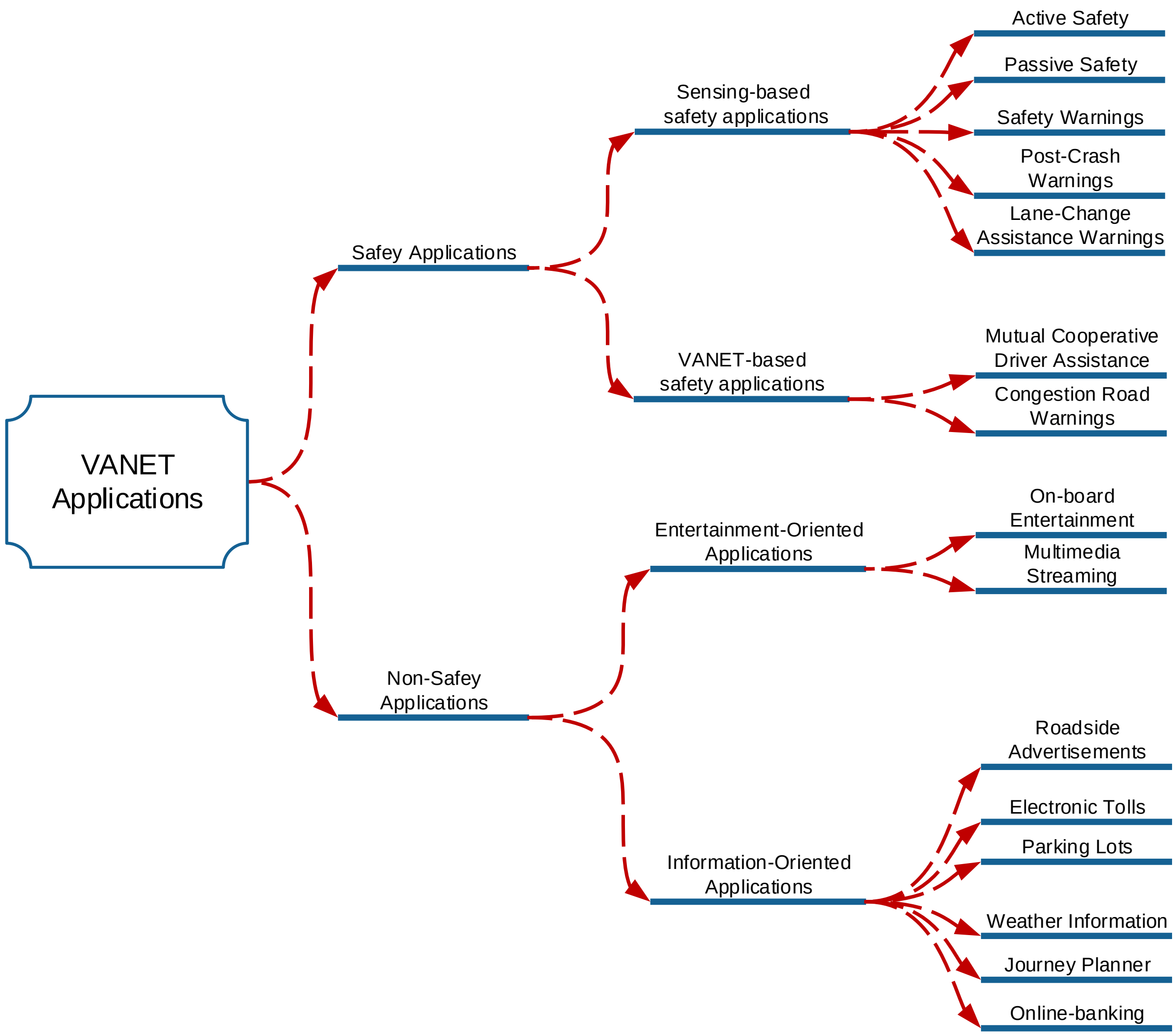


Figure 2.5: Classification of VANET applications

vehicular user in a road congestion scenario by identifying and proposing a new route for vehicles. The identification of new route is achieved with the combination of both GPS and vehicle based software such as Radio Data System-Traffic Message Channel (RDS-TMC) [29]. GPS provides the location coordinates and the updated route based on GPS information is achieved via RDS-TMC.

2.3.2 Non-Safety Applications

The requirements for non-safety applications are quite different to the safety applications. These applications provide infotainment to vehicular user ensuring quality of service (QoS). These applications includes information oriented and entertainment oriented applications such as weather warnings, roadside advertisements, electronic tolls, journey planner, online-banking and multimedia streaming. Entertainment-oriented applications are usually provided via V2I communication since multimedia is mostly bandwidth hungry. Figure 2.5 depicts the taxonomy of classification of important applications of VANET.

2.4 Challenges faced by VANET

Though, a lot of research effort is being carried out to make VANET reality, there are still various challenges which need to be tackled. This range from technical challenges to routing and further to security challenges. In this section, we particularly focus on some of the important challenges which VANET is currently facing.

2.4.1 Technical Challenges

VANET is a combination of various technologies including both wired and wireless communication technologies. Integrating all the technologies together on a singular platform is one of the huge challenge in VANET. For instance, interoperability of vehicles from different regions. Further, different continents and regions have their own communication technologies standards, such as, vehicles in Europe include ITS-G5 standard for short range wireless communication. On the other hand, DSRC is used as the base technology for short range communication in US. Therefore, the integration and interoperability of vehicles from different regions is a great challenge. In order to solve these challenges, huge standardization effort is being carried out throughout the world in order to provide connectivity to vehicles from different regions. For instance, Institute of Electrical and Electronics Engineering (IEEE) proposed a standard for V2V communication, known as IEEE 802.11p [30]. On the other hand, Institute of Standard Organization (ISO) provides the guidelines to access IEEE 802.11p protocol under ISO 21215 standard [31]. Further, Table 2.2 highlights the major organizations involved in the development of standards for VANET.

Table 2.2: Notable Standardization Effort for Vehicular Ad-Hoc Networks

Standardization Organization	**Proposed Standard**	**Publication Year**	**Standard Details**
International Organization for Standardization (ISO)	ISO 17515 [32]	2015	Details of Using Cellular technologies for ITS
	ISO 21215 [31]	2018	Technical details of using IEEE 802.11 in ITS
	ISO 26262-2 [33]	2018	Road vehicles Functional safety Part 2: Management of functional safety
	ISO 21218 [34]	2018	Technical details of utilizing access technologies in ITS
European Telecommunications Standards Institute (ETSI)	ETSI TR 102 638 [27]	2010	Basic set of applications for vehicular networks
	ETSI EN 302-636 [22]	2014	Technical details of GeoNetworking protocol for vehicular communications
	ETSI EN 302-637 [35]	2014	Message set for cooperative ITS
Institute of Electrical and Electronics Engineering (IEEE)	IEEE 802.11p [30]	2010	Technical details of IEEE 802.11p in vehicular environment
	IEEE 1609.0 [36]	2014	Reference architecture for WAVE technology
	IEEE 1609.2 [37]	2017	WAVE security services for ITS applications
	IEEE 1609.3 [38]	2016	WAVE networking for ITS
Society of Automotive Engineers (SAE)	SAE J2735 [39]	2016	DSRC Message Set Dictionary
	SAE J3061 [40]	2016	Cyber Security guidebook for cyber-physical vehicle systems

2.4.2 Routing Challenges

Efficient message transmission among vehicles in case of safety applications is foremost important. In VANET, these messages are disseminated via an underline routing protocol. However, due to volatile, robust and open-nature of VANET, several routing challenges exists such as.

- **Routing in case of broadcast storm:** Consider a city centre scenario with high number of vehicles during peak times. These vehicles broadcast an abundant number of messages in a limited geographical location. This results in a denial-of-service due to broadcast storm and message flooding, thus reducing the overall network efficiency. To deal with such situations, VANET requires an intelligent routing protocol to disseminate messages, so that every vehicle in the network receives messages in time.

- **Routing in case of obstacle shadows:** Routing messages among vehicles in case of high buildings or mountains is another open challenge. The shadows caused by such objects arise data delivery issues which prohibit the vehicles to receive messages correctly. In order to solve this issue, efficient channel modelling is required which can ensure message transmission among vehicle by minimising Bit Error Rate (BER) of the network.

- **Routing in case of channel unavailability:** In case of attacks by malicious vehicles, the channel for message routing can be compromised, resulting in a denial-of-service scenario. Routing mechanisms should be intelligent enough to exchange messages in case of channel unavailability.

- **Routing overheads:** Every vehicle add its credentials (identity, location, time) while forwarding messages to other vehicles. Therefore, overhead of the message increases for hop-by-hop message propagation. Due to delay sensitivity of the applications in VANET, overheads of the routing mechanisms should be minimised.

Due to critical and sensitive nature of VANET, a trusted environment is mandatory where the vehicles can broadcast and disseminate information in a trusted and secure way. This can be achieved by using an underline trusted routing protocol for message dissemination. Further, considering the above challenges, routing protocols must be designed efficiently, so that the vehicles can receive sensitive information (e.g., accident warning) in a timely manner.

2.4.3 Security Challenges

Security is one of the essential and foremost user requirement in VANET as it provides a secure environment for the propagation of safety messages across the network. Minimum security level must be defined in VANET for safety applications otherwise, the attacker can launch various attacks leaving huge impact on the network, e.g., alteration of steep-curve warning from attacker can put the human life in danger. VANET can succeed only if it satisfies various security requirements, i.e., confidentiality, authentication, integrity, availability, non-repudiation and real-time verification of the messages [41, 42]. Though, various security challenges exist in VANET, but we mention the following important challenges, which need to be addressed to provide secure environment for message propagation in the network.

- **Privacy:** Privacy is a major concern for vehicular users which makes it an important user requirement in VANET [43]. Most of the available solutions rely on some sort of user credentials (user identity and location) for security purposes. Therefore, privacy of the users must be respected while designing security solutions.
- **Lightweight security solutions:** Due to involvement of delay sensitive messages in VANET, the security solutions must be lightweight such that they achieve security with minimum overheads.
- **Network security:** An attack-free network is mandatory for secure propagation of messages within the network. VANET is a large-scale network which contains large number of vehicles and RSUs along with malicious nodes (any illegal and unauthorised equipment connected to VANET). The malicious nodes hinder the normal VANET operation by launching several network attacks which range from DoS to message tempering. In order to achieve network security, attacks must be mitigated within the network by identifying and revoking malicious nodes and their messages.

2.4.4 Trust Challenges

Trust is an essential pillar of security [44]. Any vehicle receiving messages from its neighbourhood must verify its authenticity. One way to achieve security is to create a trusted environment where trust is establish between vehicles to exchange messages regarding specific event. However, due to high mobility of vehicles in VANET, trust establishment is very challenging as the trust on the message has to be evaluated in a very short span of time. Cooperation of the vehicles is mandatory for trust establishment in such specific time and the honesty of the vehicles must be promoted by providing relevant incentives [45]. Moreover, trust establishment among the vehicles in presence of malicious nodes is another important challenge which must be tackled to provide trusted environment in the network. Trust is explained in detail in chapter 3.

Table 2.3 summarizes the challenges faced by VANET with some of the possible solutions.

Table 2.3: VANET Challenges and Possible Solutions

Category	**Challenge**	**Solution**
Technical	Interoperability	Centralised and flexible reference models for vehicles to integrate and communicate
	Communication standard	Open reference model and standardised solutions
Routing	Broadcast storm	Revoking duplicated messages
	Shadowing	channel modelling
	Channel unavailability	alternative communication channel
	Routing overheads	Minimising overheads for low E2E delays
Security	Privacy	Strong encryption with pseudonyms
	Lightweight security	Low overheads
	Network security	attack-free model
Trust	High mobility	Lightweight trust management proposal
	Presence of malicious vehicles	Trusted environment; revoking malicious vehicles
	Trust establishment in ad-hoc manner	Provide incentives for honest vehicles

2.5 Summary

In this chapter, we provided an insight introduction to the fundamental concepts of vehicular ad-hoc networks. This included the basic architecture of VANET along with its significant components, applications and major challenges in terms of routing and security. The next chapter will introduce trust management in VANET with the aspects of VANET security.

Chapter 3

Trust Management in VANET

The concept of sharing and broadcasting false information in the network by the adversaries for their own interests brings up manifold concerns for the legitimate users, for instance, freeing up the highway or congesting the road for other vehicles by sharing wrong information in the network. In order to solve these kind of issues, trust can be incorporated both at the network and vehicles level to identify misbehaving vehicles and revoking them from the network. Due to imperative and open nature of VANET, incorporating trust is extremely challenging due to limited communication window between two vehicles.

Securing vehicular networks is one of the open challenge and currently huge effort is being carried out by the research community in this domain. Before proceeding to trust in VANET, first we will discuss security in VANET and different security requirements.

3.1 Security in VANET

Security is one of the essential and foremost user requirement in VANET as it provides a trusted environment for message propagation. VANET mostly includes safety related messages, therefore, a secure environment is mandatory for message dissemination. Minimum security level must be defined in VANET for safety applications otherwise, the attacker can penetrate in the network to launch attacks, leaving huge impact on the network. For instance, modifying and altering the accident warning message by adversaries can result in a traffic jam scenario which decreases the overall network efficiency in terms of time and fuel wastage.

According to [43], privacy, security and trust are the main user requirements in VANET. The network must fulfil these requirements in order to provide an ideal environment for message propagation.

3.1.1 Privacy

Privacy is one of the major requirement in VANET and it must be ensured that the user related information are kept private in the network. Majority of the available security solutions in VANET are dependent on user credentials, such as [46, 47, 48, 49, 50]. In case of failure of such security solutions, there is a high probability that the attacker might identify the vehicular user or some of its credentials, such as location or identity. The users will only trust in VANET if their credentials are kept private at all the times. Moreover, a secure communication system must be guaranteed in VANET as this may contain sensitive information, such as internet banking. In order to fulfil the privacy requirement in VANET, pseudonyms based solutions can be utilized in conjunction with PKI-based schemes.

3.1.2 Security

Security in VANET is another major user requirement which provides an attack-free environment for the propagation of messages (both safety and non-safety). VANET is a large-scale network which can include high number of vehicles and infrastructure at specific location and times such as vehicles in city center during busy office times. The network may integrate malicious nodes (any illegal and unauthorized equipment connected to VANET) as well which may disturb the normal operation of VANET by launching several attacks such as man-in-the-middle (MITM), replay, jamming and eavesdropping attacks etc [51, 52, 53, 54, 55, 56, 57]. We classify these attacks into four major classes based on attack characteristic and attack location.

- **Network Monitoring Attacks:** In this type of attack, the attacker monitors and eavesdrop in the network to listen the communication among the vehicles. This communication may be of sensitive nature such as the communication between the law-enforcement vehicles or the communication between ambulances. The attacker may listen to this communication and it is highly possible that the attacker may forward this sensitive information to the beneficiaries.

- **Ethical Attacks:** These attacks are linked to moral ethics where the attacker may send inappropriate messages to other vehicles. The main purpose of these attacks is to play with the emotions of the driver. For instance, the attacker may criticize the legitimate user purposely on the highway, which may force the user to take inappropriate steps. It is highly possible that these steps taken by the user at such high speed may result in a traffic accident scenario.

- **Application Attacks:** In this specific class of attacks, the attacker changes the content of the application messages in this type of attacks, e.g., introducing bogus information into the network. The attacker mostly acts as a middle man where it first intercepts messages from the legitimate users and updates the content with malicious information and broadcasts it with neighbouring vehicles. These attacks are one of the severe attacks as tempering safety message may result in life-threating situation to the vehicular users. For instance, if the attacker changes the content of the steep-curve warning in a mountainous region during foggy conditions may put legitimate user in danger.

- **Network Attacks:** Network attacks are potentially the most destructive attacks since they can act as an entry point for the attackers where they can launch different attacks. Examples of such attacks include denial-of-service (DoS), distributed DoS, jamming, sybil and replay attacks.

The success of VANET relies in the deployment of secure environment, therefore, the network must fulfill security requirements to ensure security in VANET such as confidentiality, authentication, integrity, availability, non-repudiation and real-time verification [58, 59]. To achieve security in VANET, following techniques can be used such as [60, 61]:

- PKI-based certificates – Certificate generation from trusted central authority

- PKI-based pseudonym certificates – Using pseudonym by RSU to ensure security and privacy of users

- Group-based signatures – Anonymity and privacy preserving techniques where a group leader is responsible for communication between RSU and central authority

- Crypto-based security – Using symmetric cryptography to ensure confidentiality, integrity and security.

3.1.3 Trust

Trust is the essential pillar of security which creates a trusted environment in the network where vehicles can trust the received messages from vehicles in its vicinity [62]. When a message is received by any vehicle from the neighbourhood, trust relationship has to be established beforehand in order to ensure security. Trust in VANET is explained in detail in next section.

Table 3.1 summarizes the major user requirements, major issues and some possible solutions to meet user requirement.

Table 3.1: Major User Requirements, Issues and Possible Solutions

User Requirements	Major Issues	Possible Solutions
Privacy	Exposing user identity Revealing user location	1) Pseudonyms with PKI-based schemes 2)Time-changing pseudonyms
Security	Attackers penetration in the network Disturbing normal network operation Disclosing user credentials	1) Strong encryption techniques 2) Strong security solutions 3) Continuous risk assessment to identify, vulnerabilities, threats and attacks
Trust	Untrusted environment Propagation of compromised messages	Scalable, time efficient, decentralized and context-independent trust management

3.2 Trust in VANET

3.2.1 Trust Terminology

Trust defines the degree to which a node is capable of accepting correct information from other nodes. Trust establishment in wired networks is comparatively easy than ad-hoc networks as the wired networks are connected to central authority. On the other hand, ad-hoc network lacks this connection with central authority. However, trust establishment in VANET is extremely difficult as the communication window between the vehicles is very small. Moreover, the central entity is also not available most of the time in VANET, which makes the trust establishment extremely challenging.

In literature, there is no specific definition for trust in VANET. Different authors have developed their own specific definition of trust. Table 3.2 compiles some of these definitions.

Table 3.2: Trust Definitions in VANET

Authors	**Trust Definitions**
J. Grover et al. [63]	Confidence of an entity on other entity in VANET
Y-M. Chen et al. [64]	Relationship between entities based on past interactions
Ahmed et al. [65]	Subjective expectation that correct information will be transmitted by node in future
M. Monir et al. [66]	Trust is the foundation of building trusted vehicular environment to ensure security
N. Bismeyer et al. [67]	Trust management increases network efficiency by ensuring traffic safety

Based on above definitions, this thesis will focus on the following definition of trust which is extended from [63]. Therefore, we define trust as " *confidence of one vehicle on the other vehicle for performing certain action or set of actions*". Let '*ac*' represents the set of actions which are taken by the message sending vehicle (say vehicle B). When this message is received at destination (say vehicle A) from vehicle B, then generally trust can be expressed as:

$$Trust = A \rightarrow B \; if \; action \; = \; ac \tag{3.1}$$

However, trust has specific characteristics such as the vehicle can trust other vehicle for only one specific action and not all actions. For instance, vehicle A may trust vehicle B for safety messages (action = ac) but not for non-safety messages (action = bc). Trust in this case can be given by Equation 3.1 and distrust as:

$$Distrust = A \rightarrow B \; if \; action \;\; = \;\; bc \tag{3.2}$$

3.2.2 Importance of Trust in VANET

VANET is a large scale network and it mostly involves the propagation of safety messages in the network. In order to provide a secure environment, the identification and revocation of malicious vehicles along with their data is of great importance in VANET. When a legitimate vehicle receive any safety message, the trustworthiness and authenticity of the received message should be evaluated before accepting and forwarding it to other vehicles. In order to do so, a trust model is required which can evaluate the trustworthiness of the data received to increase the efficiency of the network by ensuring a secure environment for the propagation of trusted messages. In VANET, trust exists in following forms as depicted in Figure 3.1

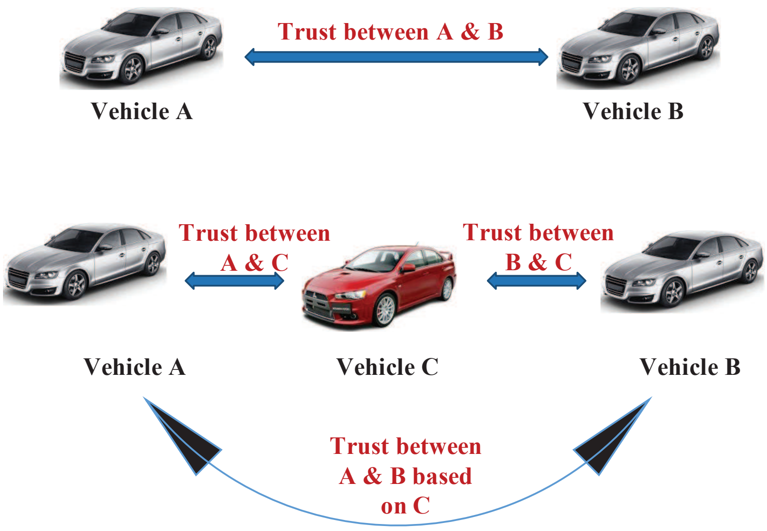


Figure 3.1: Direct Vs Indirect Trust

1. **Direct Trust:** Direct trust is the result of direct interactions between two entities. The calculation of trust in this mode depends on two factors: 1) *observation* of nodes, and 2) *experience* based on past interactions. Mathematically, it can be given as:

$$Trust = A \rightarrow B\ if\ trust\ set\ = \{observation, experience\} \tag{3.3}$$

2. **Indirect Trust:** Trust between two vehicles is calculated based on the opinion of third node in this approach. Trust establishment and evaluation in indirect trust depends on following factors: 1) *Recommendation* from neighbouring vehicles, 2) *Reputation* of the message sending vehicle, and 3) *collaboration* between clusters of vehicles. Mathematical formulation of indirect trust can be expressed as:

$$Trust = A \rightarrow B\ if\ trust\ set\ = \{recommendation, reputation, collaboration\} \tag{3.4}$$

In order to achieve a desired trust between two entities of VANET, following four trust levels exists to estimate the node's behaviour in terms of trustworthiness and data authenticity [68], i.e., 1) Conditional Distrust (DC) 2) Unconditional Distrust (DU) 3) Conditional Trust (TC) and 4) Unconditional Trust (TU).

The maximum achievable trust level is unconditional trust and the minimum is unconditional distrust as depicted in Figure 3.2. Trust is time transitive and with the passage of time, trust level changes based on the nodes' behaviour, i.e.,

1. Trust level increases towards unconditional trust if the vehicles behaves appropriately in the desired manner as depicted in Equation 3.5 , and
2. Trust level decreases towards unconditional distrust if vehicle is malicious and disseminating false information in the network as shown in Equation 3.6.

$$Trust_{A \rightarrow B} = ++\ \ if\ vehicles\ follows\ desired\ actions\ (ac) \tag{3.5}$$

$$Trust_{A \rightarrow B} = --\ \ if\ vehicles\ contradicts\ desired\ actions\ (ac) \tag{3.6}$$

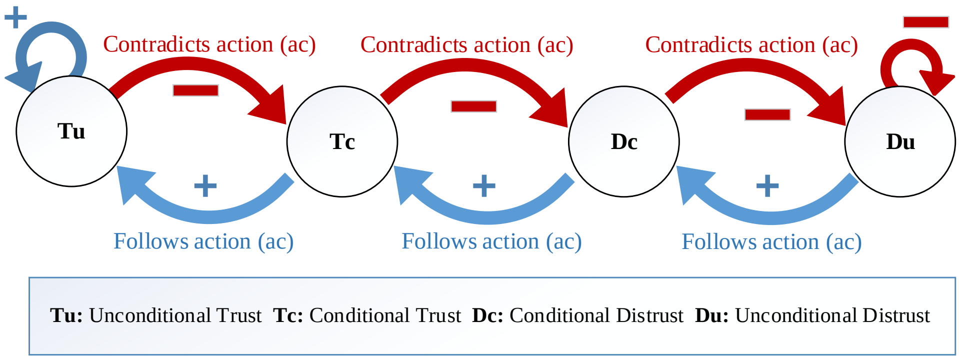


Figure 3.2: State Transitions between Trust Levels

Trust in VANET can be subjective, situational and dynamic depending on the nature of the event. Moreover, the relationship between the vehicles can either be symmetric or non-symmetric. These properties are described in Table 3.3.

Table 3.3: Trust Properties in VANET

Trust Property	**Description**
Subjective	Trust establishment based on 1) personal direction trust evaluation 2) indirect trust evaluation via neighbors, and 3) past history
Situational	Trust evaluation based on different contexts
Dynamic	Trust evaluation of similar event may be evaluated differently by two vehicles
Relationship	1) *Symmetric*: All vehicles have same trust values in the network, i.e., either 0 or 1 2) *Non-symmetric*: All vehicles have different trust values between [0, 1] based on their observations

3.2.3 Why trust is preferred over traditional cryptography?

Security in VANET is an active research area and many solutions are proposed to secure the overall network and its various aspects. Most of these solutions revolve around cryptography where vehicles utilize the concept of traditional public key infrastructure (PKI) and certificates. PKI-based solutions fail in VANET due to their dependence on adjacent centralized infrastructure which may not be available in every context of VANET. The high mobility of the vehicles further increases the complexity of PKI-based solutions to ensure network security. On the other hand, trust-based solutions are mostly decentralized in nature, where trust between the vehicles is established in a fully decentralized manner. Thus, from the network architecture perspective, trust-based solutions are more reliable than PKI-based solutions as they are mostly decentralized in nature.

Further, in PKI-based system, certificates are assigned to every node, which contain both the keys and identity of the user. Every node having a valid certificate is considered as legitimate in PKI-based system. Detecting misbehaving nodes in such networks is extremely challenging as the network considers them as authentic members due to their valid certificates, which is the major limitation of the PKI-based systems. On the other hand, trust among the nodes bring flexibility within the network as every node has the ability to make decisions based on the its own observations in the network and possible recommendations from other nodes. Thus, introducing trust can increase the efficiency of the network where the collaborative communication among the nodes can identify the insider misbehaving node along with its disseminated content.

3.3 Trust Modelling in VANET

As VANET involves highly mobile vehicles with sparse distribution, modelling real-time trust is very challenging. According to [69], two vehicles with 60 mph communicate only for 5 seconds. The trustworthiness of message should be evaluated in such short span of time in a highly dynamic environment. Similarly, VANET is a decentralised network with vehicles joining and leaving the network simultaneously and the probability of communication between these vehicles in future is very low [70]. Also, the lack of central entity in such an environment makes the trust calculation very challenging. The trust models (TM) in VANET should be able to address these issues. An ideal trust model is expected to be de-centralised, time efficient, context independent, scalable, robust and resilient against different security threats.

In VANET, main objective of a TM is to ensure secure and trusted data dissemination by identifying dishonest vehicles and revoking compromised messages from the network. Recently, various trust models have been proposed in VANET, which can be broadly classified into three categories:

1. Entity-oriented trust model (EOTM)
2. Data-oriented trust model (DOTM), and

3. Hybrid trust model (HTM)

The focus of entity-oriented trust models is the calculation of trustworthiness of a vehicle, while data-oriented trust models calculate trust of the information itself. On the other hand, hybrid trust models combine the properties of both entity-oriented and data-oriented trust models to evaluate the trust of a vehicle and the information it transmits.

3.3.1 Entity-Oriented Trust Models

Entity-oriented TMs focus on the evaluation of trustworthiness of the message transmitters. The success of these trust models heavily relies not only on how trustful neighbours of the trust evaluator node (E_V) are, but also on the message originator. The neighbours of E_V endorse the reputation of the message sender. These trust models perform well in low mobility and highly dense scenarios as more and more neighbours can transmit information about a certain event and, thus, E_V can evaluate trust based on the information provided by these neighbours. However, such TMs cannot evaluate the trustworthiness of the data content which is one of the main objects in VANET. Moreover, highly mobile vehicles fail to collect sufficient information for trust calculation and evaluation.

Several studies have been proposed in the literature which focus entirely on EOTM. For instance, Khan et al. proposed a cluster-oriented approach where the elected cluster head (CH) in the network is responsible for the calculation and evaluation of trust in the network [71]. CH employs a watchdog mechanism in its neighbourhood where legitimate vehicles provide their recommendation to CH about the presence of misbehaving vehicle in its vicinity. Once, such malicious vehicles are identified, CH informs the trusted authority (TA) about these vehicles which are then removed from the network of trusted vehicles. However, major drawback of this approach is high overhead caused due to the report, thus reducing network efficiency. Moreover, the communication details among vehicles, CH, and TA is missing in this study.

A similar TM is presented by Jesudoss et al. where trust is calculated by electing a CH in the network [72]. The CH is responsible to disseminate trusted information in the network. All the participating nodes follow a truth-telling approach to gain reputation in the network. The information is trusted only by CH if participating node gains higher weights in CH election and by continuously monitoring its neighbouring nodes and identifying malicious information. However, this solution will fail in a highly mobile and rural location where CH might not have enough neighbors and the presence of the malicious vehicles may result in a biased selection of CH.

Unlike cluster-based approaches in EOTM, Haddadou et al. adapted a different technique based on economic incentive model to exclude malicious nodes from the network [73]. In this model, all nodes in the neighbourhood are assigned with a specific credit value in a distributed manner. The increase or decrease in the credit depends on node behaviour in the network. In case of an attack, the credit is decreased. When the node has no credit left, it is assumed to be malicious and is excluded from the network. The main limitation of this TM is its inability to differentiate between direct or indirect trust.

Minhas et al., on the other hand presented a TM where trust is calculated and aggregated based on four sources, i.e., (1) sender node's experience, (2) priority, (3) role and (4) majority opinion [74]. When a message is received, E_V identifies and prioritizes vehicles (V_P) in its vicinity based on their reputation and experience, thus incorporating role and experience-based trust. The E_V then broadcast requests to V_P about the event authenticity, and waits for their response. Based on time and location closeness, V_P reply back to the E_V with their opinions. Once messages from all V_P are received, E_V applies a majority rule to identify the trustworthiness of the vehicle. If the majority of the vehicles agree about the event, E_V accepts the messages, otherwise it follows the advice of vehicle with the highest role and experience in the network. Main limitation of this TM is its reliance on PKI cryptography for the calculation of role-based trust where the presence of a central authority is required for the verification of those certificates.

Another entity-oriented trust model based on trust and reputation mechanism is presented Yang in [75], where a similarity mining approach is adapted to calculate trust in the network. Whenever a message propagates in the network, E_V identifies similarity between received messages which is calculated based on Euclidean distance and reputation weights of the participating vehicles. However, the main shortcoming of this TM is its dependence on Euclidean distance between the two vehicles as this does not provide a global information on similarity of the messages.

A centralized trust model is presented by Marmol et al. in [76] which relies on adjacent infrastructure for the evaluation of neighbour's reputation. The main aim of this scheme is to quickly identify the legitimate and malicious vehicles. When a message is received at the evaluator node (EV), a fuzzy based trust score for neighbours is calculated based on (a) recommendation provided by infrastructure (RSU), (b) recommendation provided by neighbouring vehicles, and (c) previous direct reputation of the sending vehicle. Once trust score is calculated, decision is taken based on the following three conditions:

- Drop the message if not trustworthy. (Not Trust)
- Accept the information but don't forward message (+/- Trust)
- Accept the information and forward it (Trust)

This model also classify the messages into three classes according to severity levels, i.e., high, medium and low level. High level messages are accepted only from the vehicles placed in 'Trust' group. The other groups 'Not Trust' and '+/- Trust' accepts only medium and low level messages. Due to its reliance on adjacent infrastructure for trust computation, this trust model cannot perform well in rural areas where the presence of infrastructure is not guaranteed every time.

M. Gerlach proposed a trust model which takes the sociological factors into account [77]. In this model the evaluator node (EV) calculates trust of a particular vehicular node by identifying different methods of trust i.e., situational trust: Information available about specific situation, dispositional trust: vehicular node own point of view and belief about the particular event, and system trust: depending on the system where both EV and vehicular node resides. The main drawback of this trust model is the lack of architecture where trust is calculated based on these input factors.

3.3.2 Data-Oriented Trust Models

In these TMs, data plays a central role where trustworthiness in the accuracy and authenticity of received message is computed by the node. These TMs highly depend on their previous interactions with the peers, and the opinions shared from the vehicles in its vicinity.

One of the earlier work in this direction is the TM proposed by Raya et al., where evidence on the received events is accumulated based on Bayesian inference (BI) and Dempster-Shafer Theory (DST) [78]. In this TM, evaluator node (E_V) first receive reports from vehicles in the neighbourhood, and then assign weights to every received report based on location and time closeness to the event. At the E_V, these reports along with the assigned weights are then passed to a decision logic module where trust is calculated using BI and DST. The main shortcoming of this TM is the fact that trust is calculated every time a data is received, thus making it inefficient for highly dynamic and sparse environment.

Gurung et al. proposed a complex distributed data-oriented trust model where the trustworthiness of information generated about a particular event is evaluated in real time by the vehicles themselves, without dependence on adjacent infrastructure [79]. The trust model involves two phases. (a) First, the message received from a large number of neighbours is classified into two levels using clustering algorithms. This first level includes messages with the similar content, while the second level includes messages with conflicting information. Once the messages are classified into levels, (b) the next phase evaluates the trustworthiness of the messages based on three factors, i.e., information similarity, information conflict and similarity of message routing path. This TM is very complex as it involves real time validation of the received messages, which may not be feasible in highly mobile and sparse contexts. Moreover, discussion on how this TM would behave in the presence of different attacks are not addressed.

Shaikh et al. filled this gap and proposed an intrusion-aware TM, which has the capability to identify and detect malicious messages, such as fake location [80]. In this model, the E_V calculates trust in three stages. Firstly, a confidence value of every message is calculated based on location, time closeness and verification. Secondly, trust is calculated for every message based on the confidence value. Thirdly, a fuzzy logic methodology is used to evaluate the trustworthiness of the message. A message is accepted only if its trustworthiness value achieves a certain threshold. Although this TM is very light and efficient for infotainment applications, it is not applicable for safety applications due to the delay introduced in the calculation of trust values.

Wu et al. proposed a centralised trust modelling framework for the evaluation of data by exploiting the advantages of adjacent infrastructure (RSU) [81]. Trust is calculated at RSU based on two factors: 1) observation, and 2) feedback. Vehicles detect an event and generate observations along with their confidence on the observation and shares it with RSU. The confidence of the vehicle on the observation depends on its distance from the event, its maximum message detection rate and the number of embedded sensors which detects the event. RSU updates the recently observed events list and evaluates the observation factor for the recently received event information by calculating trust on it. RSU then disseminates this information to vehicles with the updated trust. This trust model fails in a highly mobile and rural scenario as it heavily relies on adjacent infrastructure for trust calculation.

Another data-oriented trust model is developed and proposed by Sun et al. [82]. This trust model detects false data in real-time based on the angle of arrival, Doppler speed and modified Kalman filer. When a message is received, the path of message arrival is measured at the evaluator node. Once, the path is calculated, then the next step involves the measurement of message deviation. If it exceed the desired deviation, then the message is discarded and the vehicle is classified as malicious vehicle. Though, this trust model establishes trust on the fly and in real-time, but it also offers few drawbacks. For instance, one such drawback is the assumption that the evaluator node will always have an eye on the event. It is possible that the message is received at the evaluator node indirectly via intermediate vehicles. Moreover, this paper lacks its performance for urban scenario with high number of vehicles. Further, how the angle of arrival is measured in a scenario which follows a shadow-based communication due to high buildings.

In order to address the dynamics (high mobility and random distribution) of VANET, Liu et al. presented a novel lightweight trust model which operates in a fully distributed manner [83]. The proposed trust model is light weight as it only integrates trust-based and recommendation-based evaluations. To accurately determine the overall trust evaluations, three factors (number weight, time decay weight and context weight) are integrated for the trust-based evaluations. On the other hand, recommendation-based evaluations depends on maximum local trust values which are used to identify and maintain the neighbourhood by creating a trusted environment. The main shortcoming of this scheme is its failure to distinguish among the trust of node and the message. If sensor of the legitimate vehicle is faulty or impersonated by an attacker, then compromised messages will be transmitted from that vehicle.

A tier-based and analytical approach is adapted by Gazdar et al. where vehicles continuously evaluates the trustworthiness on the received data based on direct experiences in the network [15]. Such technique can detect malicious vehicles which are eavesdropping in the network and altering the messages with fake locations. In this proposed model, trust is evaluated for every participating vehicle, where the main purpose is to identify the pool of highly trusted vehicles and malicious vehicles. Each vehicle maintains a trust table for its neighbours which changes depending on the received message. Trust value increments for messages received from trusted vehicles, while it decrements for malicious vehicles. This technique is efficient in identifying the malicious vehicles as it only involves direct experiences of the participating vehicles. However, trust has to be calculated for every received message, which makes it inefficient in an urban scenario.

3.3.3 Hybrid Trust Models

Hybrid trust models (HTM) evaluate trust based on the trustworthiness of vehicles and the data they exchange. In other words, these TMs evaluate trust of data by utilizing trust of vehicles, assuming a trade-off between data authenticity and sender's reputation. Therefore, vehicles' reputation and neighbourhood opinions about a particular vehicle play a vital role in evaluating trust. These TMs involve a high level of complexity, as a significant number of control messages have to be processed in a very short span of time.

The following hybrid trust models can be found in the literature. Sedjelmaci et al. proposed a TM to evaluate the trustworthiness of a message in presence of various attacks including sybil and packet duplication attacks [84]. This TM adopts a two level approach for trust management. First level identifies CH which evaluates the message trustworthiness in a fully distributed manner. The second level relies on an adjacent Road Side Unit (RSU) to calculate trust in a global manner. Therefore, it assumes that stable clusters are always present in the surroundings of RSU which is the main limitation of this TM. Moreover, the formation of a cluster around a RSU, and the selection of CH are time-intensive processes which increase the overall complexity of the network.

In order to identify malicious nodes in the network, Dhurandher et al. adapted an event-oriented approach to achieve security in VANET by employing reputation and various plausibility checks to disseminate safety related messages in the network [85]. This approach integrates a reputation-based trust management to identify and isolate malicious nodes from the network. The E_V performs following four steps for trust management and eviction of the malicious nodes from the network: (1) neighbour discovery, (2) data dispatching once neighbours are discovered, (3) trust decision on the event message received, and (4) continuous monitoring of the neighbourhood. However, this approach has some limitations: First, the detection range as proposed by the authors in trust decision is very short, i.e., 50m. Secondly, detection relies heavily on the vehicle's sensors. If the sensors malfunction for some reason, then this approach may classify compromised messages as legitimate which result in the propagation of false information in the network.

Kerrache et al. [86] proposed a light-weight TM to efficiently relay messages towards their destination by utilising advantages of the DSRC communication protocol. In this TM, messages received via the communication module are classified into four classes, where safety messages are given higher priority. Moreover, its intrusion detection module utilises anomaly-based detection algorithms to keep statistical information of neighbouring nodes, thus, resulting in the ability to detect DoS attacks. The main issue with this approach is its assumption that malicious nodes will behave consistently throughout their journey, which is invalid in VANET.

Another hybrid trust model, which is proposed recently by Shrestha et al. [14], calculates trust on the neighbouring nodes via two methods without any dependence on infrastructure. First step of this trust model evaluates trust on node itself while the second step calculates trust on the received information. Trust on the node is achieved by clustering algorithm where legitimate and malicious vehicles are classified into two groups to identify the trustworthiness of the neighbouring nodes. Once, the category of the vehicle is identified, next step evaluates the trustworthiness on the received information based on the modified threshold random walk algorithm. The main drawback of this paper is the assumption of uniformly distributed malicious vehicles in the network, which is invalid in VANET as the distribution of the malicious vehicles is not uniform and they are randomly distributed in the network.

In order to enhance the user privacy in the network, Chen et al. [87] proposed a beacon-based trust management system which combines the characteristics of both entity-oriented and data-oriented trust models. Trust is calculated in two steps in this model. First, trust on the entity is calculated based on the received beacon messages, while, the next step calculates data trust based on various plausibility checks to identify and revoke malicious vehicles along with their content. This trust model highly depends on PKI and central authority for their trust evaluation, which make it inefficient due to the high overheads added to each forwarded messages.

Another hybrid oriented trust model is proposed by Ahmed et al. which integrates a logistic-based trust computation model to quickly identify nodes which are injecting false information in the network [88]. In this trust model, correct events are learned at the evaluator nodes via various sources which includes direct observation as well. Once, the true event is identified, this information is then used to classify the behaviour of the sender node as legitimate or malicious. Trust, in this model, is computed via weighted voting and logistic trust function. This trust model is efficient in identifying malicious nodes propagating false information in the network. However, this scheme requires many sources to learn about the authenticity of the event, which may not be feasible in rural locations.

To sum up this section, we see that various TMs are designed to ensure trust management between vehicles in VANET. However, current solutions have various issues resulting from inability to cope with attacks, performance and complexity overheads. Table 3.4 provides the comparison of the three categories of the trust models. We can see that most of the trust models are efficient in identifying the malicious nodes, but they only considers a specific context for the their proposal validation. However, VANET considers various contexts, for instance, high and low mobility of both legitimate and malicious vehicles. Therefore, the trust models should be validated for every possible contexts as they involve and propagate very sensitive and critical information. Further, according to our literature review, all of the above trust models are evaluated and validated for simulated data rather than real data.

Table 3.4: Trust Model Comparison: Advantages and Disadvantages

Trust Model	Category			Topology		Technique	Attacker Model				Advantage	Disadvantage
	Entity	Data	Hybrid	Centralized	Distributed		No Info	MITM	DoS	Sybil		
Khan et al. [71]	✓				✓	Clustering with watchdog	✓				Effective misbehaviour detection	High overheads
Jesudoss et al. [72]	✓				✓	Cluster heads with payment punishment mechanism		✓			Cooperation and active participation of nodes, thus avoiding presence of selfish behaviour	Biased CH selection in rural locations due to limited neighbours
Haddadou et al. [73]	✓				✓	Credit change based on node behaviour		✓			Evacuation of selfish nodes from the network	Inability to differentiate between direct and indirect trust
Minhas et al. [74]	✓				✓	Multi-faceted approach		✓			Scalable in dynamic environment	Robustness not addressed
Yang [75]	✓				✓	Similarity mining mechanism	✓				Help the vehicular user to decide on trusting the received data	No global information on message similarities
Marmot et al. [76]	✓			✓		Fuzzy-based trust computation		✓			Early identification of malicious vehicles due to infrastructure	Trust evaluation based on previous,history (invalid in VANET)
Gerlach [77]	✓				✓	Sociological trust evaluation model	✓				Provide security and privacy	Missing architecture to merge all trust values
Raya et al. [78]		✓		✓		Bayesian inference and Dempster-Shafer Theory based calculations		✓			Accurate event identification as trust calculation is based on time and location, closeness	Inefficient in highly dynamic environment
Gurung et al. [79]		✓			✓	Trust calculation based on information similarity, information conflict and routing path similarity		✓			Real-time validation of received messages	Complex trust model and inefficient in spare scenarios
Shaikh et al. [80]		✓			✓	Fuzzy logic for message trustworthiness		✓			Light and efficient TM for infotainment applications	Privacy of vehicular user is not,address properly
Wu et al. [81]		✓		✓		Trust calculation based on observation and feedback		✓			Up-to-date information in the network	Rely on infrastructure for trust calculation
Sun et al. [82]		✓			✓	Angle of arrival, Doppler shift and modified Kalman filter		✓			Trust calculation in real-time	Complex modelling of angle of arrival for urban scenarios
Liu et al. [83]		✓			✓	Trust-based and recommendation-based calculation		✓			Light-weight trust model which addresses dynamics of VANET	Failure to distinguish between node and message trust
Gazdar et al. [15]		✓			✓	Direct trust evaluation		✓			Identification of vehicles with fake locations	Trust calculation for every messages, Inefficient in urban scenario
Sedjelmaci et al. [84]			✓	✓		Trust calculation based on Cluster head selection				✓	Framework with intrusion detection for different attacks	Assumption of stable cluster availability
Dhurandher et al. [85]			✓		✓	Reputation-based trust calculation		✓			Intelligent eviction of the malicious nodes	Blind reliance on vehicular sensors
Kerrache et al. [86]			✓		✓	Trust calculation based on message classification and DSRC protocols			✓		Light-weight trust model to distribute messages via DSRC protocols	Assumption that malicious nodes behave constantly
Shrestha et al. [14]			✓		✓	Clustering and random walk algorithm		✓			Trustworthiness is evaluated in an infrastructure-less environment	Assumption of uniformly distributed malicious nodes
Chen et al. [87]			✓	✓		Beacon-based trust model		✓			Revokes internal attackers in privacy-enhanced network	High overheads
Ahmed et al. [88]			✓		✓	weighted voting and logistic regression		✓			Quickly identifies malicious nodes propagating false information in the network	High number of sources are required for event authentication

3.4 Evaluation Frameworks for Trust Management

In the previous section, we identified various available TMs in VANET. These TMs establish trust via different mechanisms which range from trusting the vehicle to trusting its data. However, very little work has been done for the evaluation of these TMs. In this section, we focus on such frameworks which provide some sort of evaluation of TMs.

Chen et al. proposed a trust management framework where CH is responsible to establish trust on vehicles based on neighbors' opinion aggregation mechanism in a dynamic environment [89]. In this framework, messages are disseminated only by CH after verification of its authenticity. Every member of the cluster shares its opinion with CH, where trust on the aggregated message is calculated based on its validity and correctness. CH then applies majority rule, where messages are accepted only if majority of the members agree with the authenticity of the event. This trusted message is then broadcast by CH which propagates throughout the network. The main drawbacks of this framework are: (1) This solution fails in a highly mobile and rural scenario due to low availability of the cluster members. (2) This framework can only evaluate the EOTMs, and (3) lastly, the behaviour of attackers on the TM is missing from the paper.

In order to address these issues, J. Oluoch proposed a theoretical framework incorporating RSU for trust evaluation in VANET [90]. In this framework, a threat model is designed at first place which consists of means of access of attackers in the network (either V2V communication, or updates from RSU), type of attacks launched by attackers (e.g., Sybil and Betrayal attacks) and the action (such as active or passive) of the attacker in the network. In the next step, threat model is integrated with trust establishment module, where trust is calculated by two methods, i.e., global trust establishment and local trust establishment. Global trust establishment is accomplished via RSU, where vehicles in its vicinity share their opinions about the event with available RSU. RSU performs majority rule to authorize trusted information in the network. Local trust establishment between vehicles is also computed in the absence of RSU, where information received at E_V is analysed for its authenticity. In such case, a dynamic threshold is set for trust at the E_V. Message is dropped if it falls below certain threshold, and it is accepted only if it surpasses the threshold value. This framework has several drawbacks.

First, the authors only proposed a theoretical framework for trust establishment with no mathematical foundations. Secondly, very basic threat model is considered in the framework, and the information about threats and vulnerabilities are missing in the proposed framework. Third, this is very generic framework and it does not provide any information about the evaluation of different trust models.

Recently, Ahmed et al. proposed a novel entity-based framework where true events are prioritised by identifying and filtering recommendations from malicious vehicles [91]. Particularly, to achieve its goal, this framework integrates recommendation trust, event trust and effective node trust. All these modules work together to evaluate overall trust on the node based on the shared recommendation from neighbours. Specifically, recommendation trust module evaluates the behaviour of neighbours using similarity and consistency of the received messages from the same sending vehicle. Effective node trust module, on the other hand, is responsible for trust establishment on the neighbouring nodes based on its direct experiences and neighbour recommendations. The accumulated trust is then passed to the event trust module which integrates a decision logic system. This module determines the legitimate and malicious vehicles along with the credibility of their messages. However, this proposal fails in a scenario where the evaluator node is surrounded by malicious nodes which are working together in a collaborative fashion to transmit compromised messages. Moreover, this framework only considers the entity-oriented trust modelling, and hence, it cannot evaluate data-oriented and hybrid trust modelling.

From our literature review, we realized that currently available frameworks have various limitations for trust evaluation. Therefore, we fill this gap by proposing a novel trust evaluation framework, which has the capability to evaluate different TMs (EOTM, DOTM and HTM). Moreover, our framework integrates an asset-based threat model where attacks are mapped directly from threats and vulnerabilities in assets. Further, attacks with serious impact on the network are identified and prioritized via ISO-based risk-assessment. Moreover, our framework provides a context establishment module where we identified four scenarios based on node's mobility. Once, attacks with high risks and contexts are identified, TMs are then evaluated against these attacks in different contexts using realistic trust evaluation criteria in the trust evaluation platform.

Table 3.5 provides the basic comparison of the available trust evaluation frameworks. It can be seen that less attention has been paid by the research community for the design of evaluation frameworks. Current available frameworks focused only on entity-oriented trust models, while on the other hand, our proposed framework can evaluate a wider range of trust models (entity-oriented, data-oriented and hybrid). Moreover, we evaluated the framework in presence of malicious nodes which can propagate false information in the network, i.e., by changing the message content and delaying the sensitive messages. In the next chapter, we provide the details of our proposed trust evaluation framework.

Table 3.5: Comparison of Trust Evaluation Frameworks

Trust	**Considered trust model**			**Threat**	**Risk**	**Attack**	**Evaluation Method**	
Framework	**Entity**	**Data**	**Hybrid**	**Model**	**Assessment**	**Model**	**Simulations**	**Theoratical**
Chen et al. [89]	✓					Replay attack	✓	
J. Oluoch [90]	✓			✓		1) DoS attack 2) Sybil attack		✓
Ahmed et al. [91]	✓					1) MITM - false information 2) MITM - false recommendation	✓	
Proposed framework	✓	✓	✓	✓	✓	1) MITM - false information 2) MITM - content alteration 3) MITM - message delay	✓	

3.5 Summary

In this chapter, we introduced the concept of trust management as a security mechanism in vehicular ad-hoc networks (VANET). Moreover, we explained different available trust models in VANET which are categorised into three major categories such as entity-oriented, data-oriented and hybrid trust models. We concluded that every trust model has certain advantages and disadvantages. Further, we identified available trust evaluation frameworks in VANET. In the next chapter, we will focus on the details of our proposed trust evaluation framework.

Chapter 4

Trust Evaluation and Management Framework

In the previous chapter, we identified various trust models in vehicular ad hoc networks. Trust models in VANET increases the overall efficiency by creating a trusted environment for message propagation. Therefore, the trust models should be validated in every possible context before integrating in the real network. However, there is no such framework which can validate the trust models. In this thesis, we addressed this gap by proposing a trust evaluation and management (TEAM) framework which can validate and evaluate a wide range of trust models. In this chapter, we provide the details of TEAM framework.

4.1 Proposed Trust Evaluation and Management Framework

In order to evaluate the trust models in VANET, we adopted an approach which consists of five distinct modules as depicted in Figure 4.1.

1. **Module 1:** Threat model

2. **Module 2:** Risk assessment
3. **Module 3:** Identification and categorization of trust models (EOTM, DOTM, HTM)
4. **Module 4:** Context establishment
5. **Module 5:** Trust Evaluation Platform

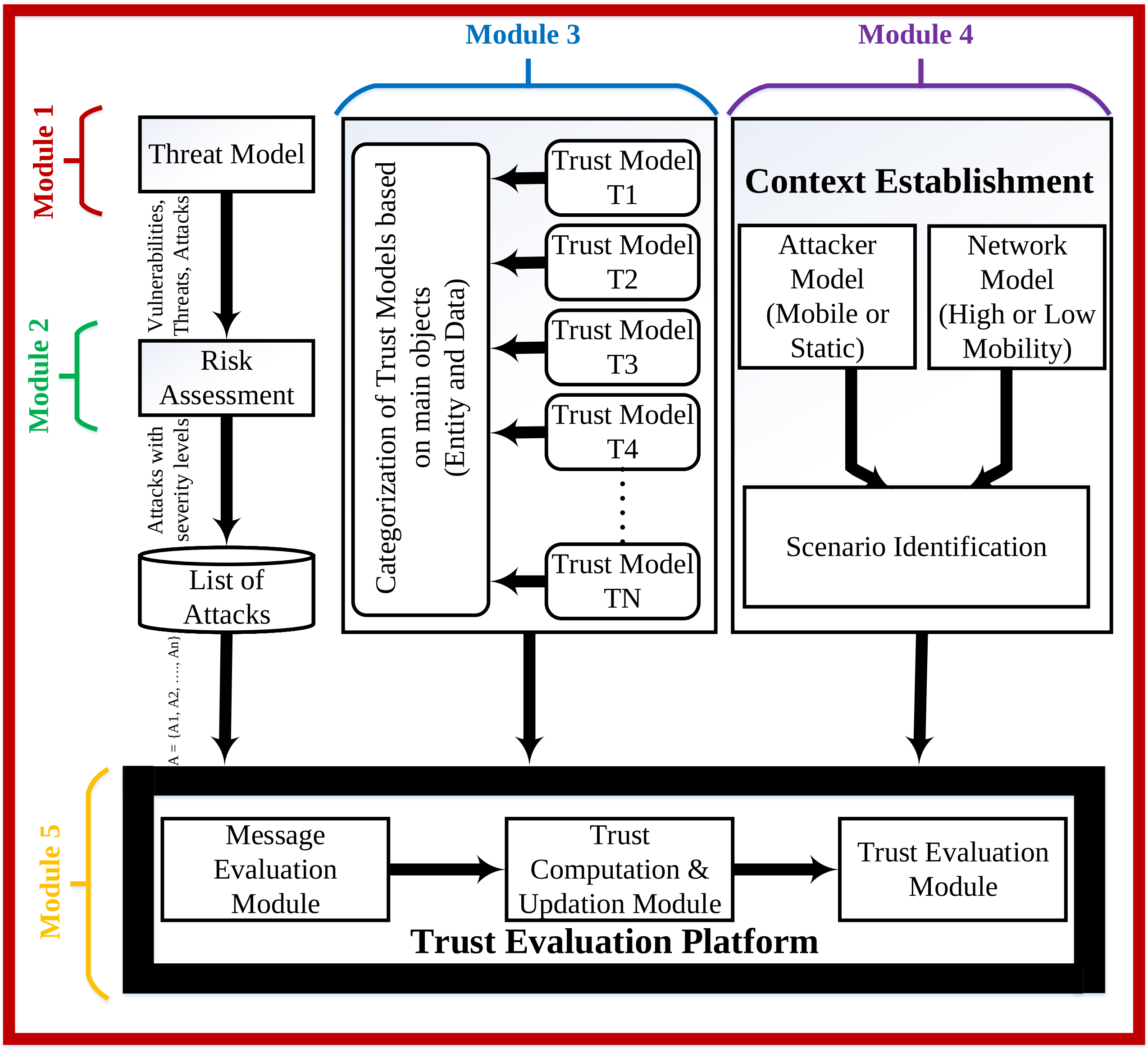

Module 3
Module 4
Module 1
Threat Model
Vulnerabilities, Threats, Attacks
Module 2
Risk Assessment
Attacks with severity levels
List of Attacks
A = {A1, A2, ..., An}
Categorization of Trust Models based on main objects (Entity and Data)
Trust Model T1
Trust Model T2
Trust Model T3
Trust Model T4
Trust Model TN
Context Establishment
Attacker Model (Mobile or Static)
Network Model (High or Low Mobility)
Scenario Identification
Module 5
Message Evaluation Module
Trust Computation & Updation Module
Trust Evaluation Module
Trust Evaluation Platform

Figure 4.1: Proposed Trust Evaluation Framework

The first two modules (threat model and risk assessment) are designed to identify various attacks in VANET. Once, attacks with critical risks are identified, then the efficiency of TMs are evaluated in various contexts and in the presence of attacks.

4.1.1 Module 1: Threat Model

The first and foremost module of our framework is the threat model. In order to design the threat model, we adopted a systematic approach for attack identification in VANET. We first identified assets in VANET and classified them into three categories based on their characteristics in the network. Next, we identified vulnerabilities and threats on the group of assets which are exploited by adversaries to launch attacks in VANET. Figure 4.2 shows the approach taken for the design of threat model. The major steps of the threat model are:

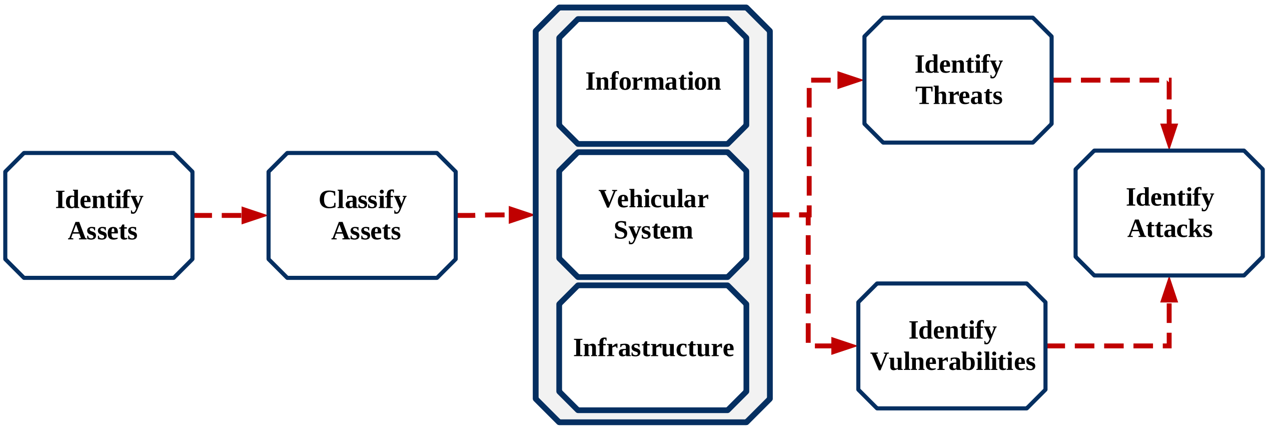


Figure 4.2: Asset-based approach for threat model

1. Identification and classification of assets into three classes based on their role, mobility and impact in VANET.
   (a) *Information:* carrying sensitive messages across different assets.
   (b) *Vehicular System:* contains vehicular user, vehicles and communication network.
   (c) *Infrastructure:* includes static entities of the network, such as RSU and CA.
2. Identification of vulnerabilities in assets of VANET.
   (a) **V1:** Insecure algorithms for exchanging user credentials.
   (b) **V2:** Software flaws such as buffer over flow, key management failure, insecure cryptographic algorithms.
   (c) **V3:** Non-availability of wireless communication channel during message transfer.

   (d) **V4:** Hardware malfunction and error.

3. Identification of threats in VANET, such as

   (a) **T1:** Message transmission with weak encryption tools.

   (b) **T2:** Exposing sensitive information such as confidential communication between law enforcement vehicles.

   (c) **T3:** Message interception by adversaries.

   (d) **T4:** Hardware damage due to natural disasters.

4. Identification of attacks in VANET. For instance,

   (a) **A1:** Social engineering attack dealing with moral ethics of VANET users.

   (b) **A2:** Man-in-the-Middle (MITM) attacks to intercept and modify messages.

   (c) **A3:** Replay attacks by injecting obsolete messages in the network.

   (d) **A4:** Jamming attacks by launching denial of service attacks.

   (e) **A5:** Bogus information addition attacks by introducing false information in the networks

4.1.2 Module 2: Risk Assessment

Once, attacks in various components of VANET are identified, the next phase involves risk assessment to identify risks caused by attacks in VANET. Risk is directly related to the vulnerability identified in assets which are exploited by threats in form of attacks, causing damage to the whole network. In order to identify attacks with severe risk, we performed risk assessment according to ISO 27005 [92]. Risk is a measurable quantity which depends on “likelihood of attack occurrence”, and “impact of an attack on network assets”. Likelihood and impact can be mapped into three categories. The resulting risk can be given as:

$$Risk = function\ (Likelihood\ ,\ Impact) \tag{4.1}$$

Corresponding risk is also categorized into three classes, i.e., *Minor, Major* and *Critical.* Risks identified as major and critical need urgent attention from the user. Table 4.1 shows the corresponding risk levels based on the likelihood and the impact values.

Table 4.1: Risk Analysis: Scale

Likelihood (L)	**Impact (I)**	**Risk (R) = L * I**
L1 = 1 (Unlikely)	I1 = 1 (Low)	R1 = 1, 2, 3 (Minor)
L2 = 2 (Possible)	I2 = 2 (Medium)	R2 = 4 (Major)
L3 = 3 (Likely)	I3 = 3 (High)	R3 = 6, 9 (Critical)

Table 4.2 performs the risk assessment for attacks identified in module 1. It can be seen that MITM and DoS attacks have high risk values in VANET. This is due to the fact that both jamming and modifying the sensitive message can have catastrophic results in the network.

Table 4.2: Risk Assessment for Attacks in VANET

Attacks (A)	**Likelihood (L)**	**Impact (I)**	**Risk (R)**
A1	Possible:2	High:3	Critical:6
A2	Likely:3	High:3	Critical:9
A3	Possible:2	Low:1	Minor:2
A4	Likely:3	High:3	Critical:9
A5	Possible:2	High:3	Critical:6

Module 1 (threat model) and module 2 (risk assessment) represents the preliminary study of the framework and is responsible for the identification of the attacker models in VANET. Let $A = \{A_1, A_2, A_3, ..., A_N\}$ are such attacks with critical and major risks in VANET. This list of attacks is provided to the framework as an input where the efficiency of the TMs has to be evaluated in presence of malicious nodes. These two modules are described in detail in chapter 6.

4.1.3 Module 3: Identification and Categorization of Trust Models

This module has two major responsibilities: (1) Firstly, it identifies the desired trust model (TM) and, (2) secondly, it categorize TMs into their respective class, i.e., data-oriented trust model (DOTM), entity-oriented trust model (EOTM), and hybrid trust model (HTM). Let $T = \{T_1, T_2, T_3, ..., T_N\}$ are 'N' TMs in VANET. However, In order to identify respective TM, these TMs are categorized into three classes according to their trust evaluation mechanism. TEAM is a flexible framework which has the ability to integrate any trust model. In order to demonstrate the framework, we have implemented one TM from each category. For the implementation purposes, we considered following two basic criteria. 1) the TM should be accepted by the research community which can be highlighted from its high number of citations, or 2) the TM should be proposed within ten years. The TMs, which are implemented for the framework demonstration and validation purposes satisfy these criteria. The details of these TMs are as follows:

4.1.3.1 Data-Oriented Trust Model (DOTM)

As mentioned earlier, these TMs rely on data for trust establishment. In this work, we implemented a data-oriented TM proposed by Kerrache et al., where, trustworthiness on the data is calculated [93]. In this model, trust is established among vehicles based on two methods: direct trust and indirect trust. Direct trust is calculated among the vehicles where vehicles evaluate each other based on the quality of the messages they provide. On the other hand, indirect trust establishment is calculated based on the broadcast/drop ratio from the sender. Let V_a is the vehicle which received message from V_b, the trust is computed as follows:

$$Trust(a, b) = \sqrt{Trust(a, b) \times \sqrt{Trust_{ind} \times Trust_{dir}}} \tag{4.2}$$

$Trust_{dir}$ depends on the received message quality where it is updated with a factor of α if the message quality is above certain trust threshold. $Trust_{dir}$ is decreased with factor β if message quality falls below threshold value. $Trust_{ind}$, on the other hand, and is calculated as:

$$Trust_{ind}(a,b) = \frac{B(a,b)}{B(a,b) + D(a,b)} \tag{4.3}$$

where, $B(a,b)$ and $D(a,b)$ are the number of broadcast and drop packets by the vehicle.

Whenever a message is received by V_a, it computes trust on the received information based on two values, i.e., (1) Quality of Information ($infoQ$), and (2) Belief Degree (BD). $InfoQ$ depends on the quality of the message received, where, $infoQ \in (0,1)$. This factors takes into account the distance between the nodes and reporting time. If reporting nodes are away from the event location and the reporting time is old, then it assigns the lowest $infoQ$ value, while messages with closest reporting location and time are assigned with the highest values [35]. On the other hand, based on BD, the report is either classified as true or false. BD is computed as follows:

$$BD(a,b) = \sqrt{Trust(a,b) \times \sqrt{BD(a,b) \times infoQ}} \tag{4.4}$$

4.1.3.2 Entity-Oriented Trust Model (EOTM)

For the demonstration of our framework, we implemented an entity-oriented TM proposed by Minhas et al. [74]. This model incorporates a multifaceted approach for trust modelling where trust on the entity is established based on experience, priority, role and majority opinion based trust. When evaluator node (E_V) received a message from other vehicles, it identifies vehicles with highest role and highest experience in the network. Messages received from these vehicles are assigned with higher weights in the network. If E_V receive messages from other vehicles in its vicinity, then it generates a report based on time closeness and location closeness. Based on these reports, E_V performs a majority opinion for its trust calculation. If majority of the vehicles agree on the message validity, then the message is accepted, otherwise, E_V follows the advise of vehicles with the highest roles.

Let $T_{V2V}(i)$ denote the vehicle-to-vehicle trust of vehicle i, then

$$T_{V2V}(i) = \begin{cases} T_{role(i)} & \text{if } vehicle\ i\ has\ a\ role \\ T_{exp(i)} & \text{else} \end{cases} \tag{4.5}$$

Role based trust (RBT) is significantly important in this TM, as these represent highly trusted vehicles which are approved from higher authorities. Thus, messages transmitted from these vehicles are mostly trusted. These vehicles include (1) law-enforcement authorities such as police vehicles, (2) public transport such as buses and taxis, and (3) professional vehicles with higher experience of driving. We computed RBT via equation 4.6.

$$Trust_{RBT} = \begin{cases} 1 & \text{if } veh = HA \\ 0.9 & \text{if } veh = PT \\ 0.8 & \text{if } veh = P \end{cases} \tag{4.6}$$

For vehicles with no roles, experience based trust (EBT) is calculated. EBT integrates a forgetting factor (λ), which ensures that old interactions with vehicles gets less weight as the behaviour of vehicles may change over time. If a trusted message is shared from the vehicle, then the overall trust of the vehicle is increased by:

$$T_{exp(i)} = \begin{cases} (\lambda)^{t}(1-\alpha)T_{exp(i)} + \alpha & \text{if } T_{exp(i)} \geq T_{Thr} \\ (\lambda)^{-t}(1-\alpha)T_{exp(i)} + \alpha & \text{if } T_{exp(i)} < T_{Thr} \end{cases} \tag{4.7}$$

In case of tempered and compromised messages by the attackers, E_V decreases trust of the sender by:

$$T_{exp(i)} = \begin{cases} (\lambda)^{t}(1-\beta)T_{exp(i)} + \beta & \text{if } T_{exp(i)} \geq T_{Thr} \\ (\lambda)^{-t}(1-\beta)T_{exp(i)} + \beta & \text{if } T_{exp(i)} < T_{Thr} \end{cases} \tag{4.8}$$

In equations 4.7 & 4.8, α is the honesty reward for providing correct information and the value is $(0 < \alpha < 1)$, while, β is the dishonesty penalty for the malicious information. Value of β is in range $(0 < \beta < 1)$. Moreover, $\lambda \in (0, 1)$. In above equations, t is the time closeness factor. Let t_{event} is the time of occurrence of event, $t_{current}$ represents the current time, t_{max} is the maximum forgetting time of EBT, time closeness factor (t) is modeled as follows:

$$t = \begin{cases} \frac{t_{current} - t_{event}}{t_{max}} & \text{if } (t_{current} - t_{event}) < t_{max} \\ 1 & \text{if } else \end{cases} \tag{4.9}$$

Once, trust and distrust on the received message is calculated, then majority opinion is performed by E_V to decide the trustworthiness of the message. If majority of vehicles agree to the event occurrence, then E_V accepts the information, otherwise, it follows advise from the vehicles with the highest roles in the network.

4.1.3.3 Hybrid Trust Model (HTM)

As stated earlier, these TMs rely on both node and data for the evaluation of trust. An event-oriented HTM, known as VSRP (Vehicular Security through Reputation and Plausibility checks) is considered in this thesis [85, 94]. VSRP integrates a reputation-based trust model to quickly identify and isolate adversaries from the network. In this TM, every node is equipped with two tables: (1) neighbouring table and (2) trust table. Whenever, E_V encounters any neighbour, it stores its ID and reputation in the neighbouring table and its trust value in the corresponding trust table.

E_V performs following four steps for trust management and eviction of the malicious nodes from the network:

1) **Neighbour discovery:** This phase identifies neighbours by broadcasting a *neighbourreq* packets. Neighbours in the vicinity respond back to this message via *neighbourrep*. Once, neighbour is identified, then initial check is performed on the message from that node by checking the trust table. If entry for the specific node is present with trust value other than 0, then message is accepted, otherwise, message is discarded from such node.

2) **Data dispatching:** In this phase, data is dispatched to the identified neighbours.

3) **Trust decision:** This step calculates trust on the received information based on the threshold range and detection range of the node. If the message is received from a node which lies beyond the threshold range, the message is discarded by the fact that node lies very far from the E_V. If the message is received from the node inside threshold range, then second check on the detection range is performed on the message. If E_V receives a message from within the detection range, then it calculates trust on the message. Since, E_V has direct information about the event within the detection range, then if the message received from the transmitting vehicle contradicts the point of view of E_V, then the message is assumed to be compromised and is discarded. However, if the received message is correct, then E_V increments the trust of the message sender with an honesty factor. In the next step, if E_V node lies outside the detection range of the message, then it collects responses from its neighbours. If total received responses exceeds the defined threshold, then information is accepted and trust is increases, otherwise, the message is classified as malicious and trust is decreased.

4) **Neighbour monitoring:** E_V relies heavily on its neighbourhood for information collection in VSRP, therefore, every vehicle monitors its neighbours continuously. Based on the shared information from neighbours, E_V can decide whether the node is transmitting correct message or compromised message.

4.1.4 Module 4: Context Establishment

4.1.4.1 Context Identification

In this section, we present the contexts where efficiency of the TMs are to be evaluated. In our work, we have identified two contexts based on the mobility of the vehicles in the network.

CON1: Vehicles with high mobility

CON2: Vehicles with low mobility

4.1.4.2 Identification of Attacker Model

In order to evaluate the efficiency of different TMs in presence of adversaries, we considered attacker model (AM) which is altering and delaying legitimate messages with the factor of "*d*". The following two AMs were considered in this work:

AM1: Attackers are static in the network

AM2: Attackers are mobile in the network

4.1.4.3 VANET Attack Scenario

With the identification of the context and AMs in VANET, following four combinational scenarios are possible as shown in Table 6.1. Scenario 1 represents a network with highly mobile legitimate vehicles and attackers which are statically present in the network. In scenario 2, both legitimate vehicles and attackers are mobile. Scenario 3 is composed of network where vehicles have low mobility and attackers are static in the network, while in scenario 4, legitimate vehicles have low mobility, but attackers are also mobile in the network.

Table 4.3: VANET Attack Scenario

Scenario	**Context**	**Attacker Model**
Scenario 1 (S1)	High Mobility (CON1)	Static Attacker (AM1)
Scenario 2 (S2)	High Mobility (CON1)	Mobile Attacker (AM2)
Scenario 3 (S3)	Low Mobility (CON2)	Static Attacker (AM1)
Scenario 4 (S4)	Low Mobility (CON2)	Mobile Attacker (AM2)

4.1.5 Module 5: Trust Evaluation Platform

Trust Evaluation Platform (TEP) represents the most significant module of the trust evaluation framework where TMs are evaluated according to several proposed criteria. The message received at E_V is acceptable only when it is verified in terms of its authenticity and integrity. According to Figure 4.1, TEAM framework has three inputs, i.e., (1) list of attacks, (2) trust models, and (3) identified contexts. TEAM has following three modules for the evaluation of TMs:

1. Message Evaluation Module
2. Trust Computation & Updation Module
3. Trust Evaluation Module

4.1.5.1 Message Evaluation Module

This module is responsible for the early identification of false events in the network by performing initial checks on the messages. The messages generated about specific event is verified and evaluated for its authenticity and accuracy. In our framework, the received message (M) is composed of two sub-messages:

$$M = M_O + M_T \tag{4.10}$$

where M_O represents original message containing information regarding location and time of event generation, while M_T is the trust message incorporating confidence of sender about the event. Once M is received at E_V, it is verified in the following two dimensions:

- **Message Validity (M_V):** Every M have respective validity depending upon the event. For instance, the information related to route closure due to construction should be valid for about 60-120 minutes while temporary road blockage due to minor accident should be valid for 30-40 minutes in that specific region. This information regarding the message validity can be verified by time stamps of M.
- **Message Relevancy (M_R):** ensures accurate information dissemination to the vehicular users. For example, if E_V is located at Kedleston Road in Derby, UK, and the received

messages contains information about road accident in Birmingham, UK, then this information is irrelevant for E_V. M_R can be achieved with GPS coordinates of the message sender.

Based on M_V and M_R, following four cases arises. Figure 4.3 shows that E_V computes trust on received M only if it provides both valid and relevant messages. Distrust is computed by E_V in all other cases if M violates these early checks on the messages. Once, M is evaluated in terms of its validity and relevancy, then in the next step, trust on M is computed.

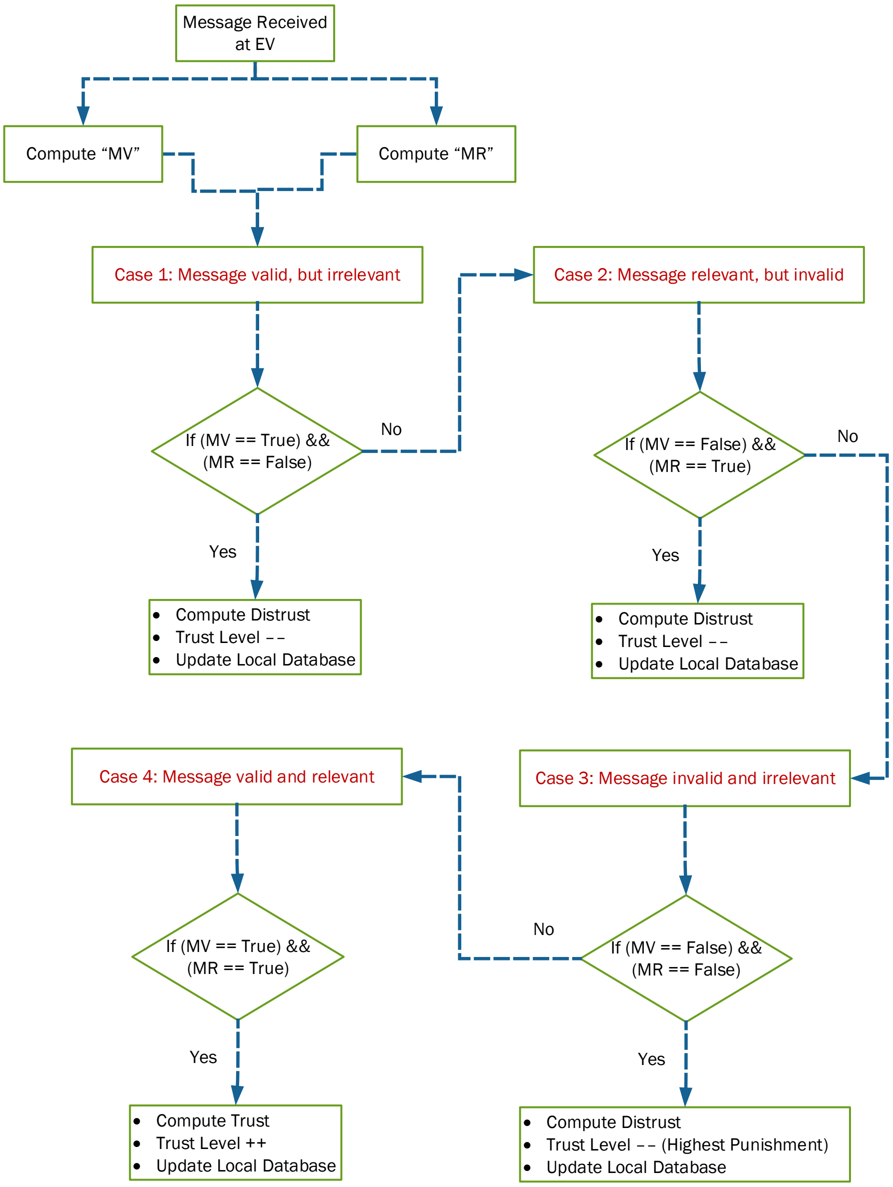

Message Received at EV
Compute "MV"
Compute "MR"
Case 1: Message valid, but irrelevant
If (MV == True) && (MR == False)
No
Yes
Compute Distrust
Trust Level – –
Update Local Database
Case 2: Message relevant, but invalid
If (MV == False) && (MR == True)
No
Yes
Compute Distrust
Trust Level – –
Update Local Database
Case 4: Message valid and relevant
If (MV == True) && (MR == True)
Yes
Compute Trust
Trust Level ++
Update Local Database
Case 3: Message invalid and irrelevant
If (MV == False) && (MR == False)
No
Yes
Compute Distrust
Trust Level – – (Highest Punishment)
Update Local Database

Figure 4.3: Use Cases for Message Verification and Evaluation

4.1.5.2 Trust Computation & Updation Module

This module is responsible for trust computation on the received message. Particularly, following two steps are involved in this module: (1) Identification of initial trust computations, and (2) Trust up-gradation of vehicle in a given time span at the E_V.

The trust computation module is further categorized into two submodules: (1) trust computation on vehicle, and (2) trust computation on data.

Trust Computation on the Vehicle

Whenever a message is received at E_V, trust is either computed on vehicle or its data based on the above two submodules. This module integrates two basic trust computation methods: 1) Role-based trust (RBT), and 2) Experienced-based trust (EBT). RBT incorporates trust from those vehicles which are highly trusted in the network. For instance, law-enforcement vehicles or ambulances etc. In our framework, we have defined four types of vehicles (veh) in the network. (1) Higher authority (HA) vehicles (such as law-enforcement, and ambulances) – the messages from such vehicles are highly trusted. (2) Public transport (PT) vehicles – highly trusted as they are authorized by the central authority, (3) Professional (P) vehicles – drivers with higher travel experience, (4) Ordinary (O) Cars – cars with no travel history. Therefore, we can model RBT via equation 4.6.

As stated earlier, VANET is a large scale, therefore, we assume that the network will have majority of ordinary vehicles and a minority of role-based vehicles. In our model, messages received from first three types of vehicles are highly trusted as shown in equation 4.6. However, if message is received from ordinary vehicles, then EBT is computed to check the authenticity and accuracy of the message. As explained earlier, EBT incorporates location and time closeness factor into account to calculate trustworthiness on the received message. If vehicle transmitted correct message (M), then E_V increase trust level of the message sender vehicle by an honesty factor. However, trust of the transmitting vehicle is decreased by a punishment factor if shared M is malicious as described by equation 4.11.

$$Trust_{EBT} = \begin{cases} Honesty & \text{if } M = Trusted \\ Punishment & \text{if } M = Untrusted \end{cases} \quad (4.11)$$

Trust Computation on the Data

Whenever sender vehicle transmits a message, it also integrates its confidence level (C_L) on the message. C_L plays a significant role in trust computation, where it ensures that the sender vehicle is confident enough on the authenticity and accuracy of the transmitted message. C_L depends on two aspects: (1) high C_L values are desirable if vehicle has direct link to the event, (2) C_L varies from high to low for indirect interaction of vehicle with the event. Thus, trust computation on the message depends on the link between the sender and the E_V. For direct message, trust is calculated based on the quality of message which depends on C_L and the information quality ($infoQ$). Vehicles residing close to event have high C_L and ($infoQ$), thus messages received from such vehicles are trusted. On the other hand, trust from vehicles decreases with its increasing distance from the event. In case of trust evaluation for indirect messages, a broadcast/drop ratio is employed according to Equation 4.3. High trust is assigned to vehicles if this ratio is high and vice versa.

4.1.5.3 Trust Evaluation Module

Once, trust on the node and data is computed, next step is to evaluate the trust via trust evaluation module. In order to do so, we proposed and implemented sixteen distinct evaluation criteria in our framework based on the network topology, data generation and time duration [95]. The details of the evaluation criteria are as follows:

C1: Ability of TM to be decentralised

TMs should be able to manage trust effectively in a fully distributed, decentralised manner. Therefore, it should be able to operate without any reliance on a centralised entity. Furthermore, given the likely lack of available infrastructure, specially for high mobility vehicles, any fully centralised schemes utilising traditional PKI methods would not be as effective. It would be more beneficial to develop decentralised schemes as they can be easily deployed, such as dynamic distributed key-management approaches for trust establishment. This, however, does not mean that trust management frameworks should not take advantage from RSUs and other fixed infrastructure for resources, information dissemination, broadcasts, message Quality of Service (QoS) purposes, or any other aids.

C2: Ability of TM to calculate trust with minimum information

The success of VANET relies on the transmission of information in a secure and trusted way. Therefore, TMs need to be as realistic as possible such that they can be implemented in a real world environment. This places importance on modelling granular simulations across every conceivable context scenario, and employing realistic mobility models to achieve more realistic datasets. This will likely to improve their applicability to test-beds for real-world testing. Equally important are assumptions made when designing or testing the trust modes. For example, assuming that there will always be a cluster head or an event witness available; that there will always be sufficient event reports; that probing packets will gather sufficient neighbours information; that there will always be complete information available for a global view of VANET; that there will never be over 70% malicious nodes; and that there will be a certain degree of information available regarding the environment.

C3: Ability of TM to be scalable

VANET is a large-scale network formed by vehicles distributed randomly. The number of vehicles which enter and exit such network is not directly linked to each other. Vehicles mobility and density increase the overall network complexity and results in a very crucial requirement in VANET – scalability. Trust management solutions should be scalable, independently of network size, vehicles mobility and their density within an environment. As abundant information (messages) propagates in such highly dense network, TMs both dependent on centralised or distributed solutions should perform their tasks well. Moreover, solutions which highly depend on RSU for trust management may not cope in a network with high mobility and low density due to the lack of these static infrastructure.

C4: Ability of TM to be privacy-aware

From a vehicular users' perspective, the privacy of their information (such as identity and location) is of foremost importance when they want to remain anonymous and not traceable. The messages transmitted by vehicles usually contain their identity which relate to users. Based on these identity containing messages, trust is established between vehicles using authentication mechanisms (which may be distributed or centralised); such mechanisms evaluate and confirm the origin of a message. Moreover, traditional PKI-based authentication mechanisms create message logs containing user details for communication with every vehicle, thus, violating the privacy requirement of users who can be exposed by traversing these logs. For instance, the message log may contain users' name, their home address and journey records. Privacy of the user is very sensitive, therefore, TMs should respect their privacy. One such method was proposed in [96] [97] where time varying PKI based pseudonyms were used to preserve the identity of the vehicular user.

C5: Ability of TM to be configurable to range to parameters

TMs should be capable of being configured according to a range of parameters to maximise efficiency in a given environment. Example configurations are communication range, number of nodes within trusted zones, number of reports needed, and thresholds for both data-centric and entity-centric information. Making use of context information (e.g., traffic density and road conditions) also helps to increase the certainty and assurances of an event happening. Nevertheless, when parameters and variables are configurable, it would be worth documenting any additional overheads generated to allow benchmarking and comparisons to be made on the effects they have on operations throughout the network.

C6: Ability of TM to cope with varying levels of density

TMs need to be able to cope with sparseness and varying levels of vehicles, infrastructure and available information, in the sense that they should be able to just as effectively (a) establish trust relationships with nodes with whom they have no prior knowledge of, and (b) establish trust relationships in situations where no secondary nodes are available to advocate another. This could pose an issue to schemes that are purely concerned with entity centric information;

hence, the requirement for minimal information to make a decision should be enforced across all schemes. Further mechanisms could be used in order to accommodate for potential trust relationship issues in areas with sparse node populations; they are: efficient technology switching, extension of communication range, and dynamic communication mechanisms such as additional message fields/tags. Hybrid schemes may be able to accommodate better for sparseness being concerned with information about data as well as information regarding individual users.

C7: Ability of TM to ensure event certainty

When vehicles receive event-driven messages, there is a need for a degree of certainty to be established regarding whether the event in question has actually happened (event plausibility). Also, a vehicle should be aware of all relevant events to be able to take action, taking into account data that has been directly observed. In light of the importance of communication exchange, there should also be a degree of certainty that the received messages are from a legitimate user, with feedback information during the data trustworthiness evaluation process. Measures should be in place to identify whether a node treated as legitimate has not been influenced by another node or multiple nodes and started sending falsified information. Collusion/collision resistance measures should be implemented to mitigate bogus and altered messages, in the same sense that information cascading and oversampling issues need to be addressed; this falls in-line with model robustness.

C8: Ability of TM to calculate trust in real-time environment

Given the nature of message content and the potential of safety-critical applications available for use in VANET environments, data exchange requirements should be met in real-time, with quality of service assurance for higher priority information (such as event-driven messages). This needs to be achieved whilst ensuring low overheads, low bit error rate, and correct packet reception; any other potentially relevant performance variables should be taken into consideration as well to maximise the potential of the TM. Real-time trust management should ensure that trust relationships are formed as quickly and as efficiently as possible. Reputation recalculation is required and importance should be given to the pivotal role trust plays in the network. This also counts for information dissemination (which should be easily distinguishable) and processing in the sense that the quicker the response is to the information presented, more likely it is that the environment will be secure.

C9: Ability of TM to be robust against attacks

It is highly important for TMs to resist against attacks (e.g., Blackhole, Sybil, bad-mouthing attacks) which target the establishment of trust between nodes such as collusion attacks. Protection against these commonly known and sophisticated attacks should be guaranteed, so that legitimate users of the network are protected. Entities like RSU can be compromised easily due to their static nature, potentially populating the whole network with malicious data. TMs depending on RSU may also be compromised during attacks, providing an opportunity for attackers to be part of the network. Therefore, TMs should be robust enough so that they can perform properly against the majority of attacks. Unfortunately, most of the TMs do not address robustness, which remains one core evaluation criteria for trust management in VANET.

C10: Ability of TM to be adaptable to network dynamics

Well developed TMs should be able to cope with the dynamics of the network and to adapt to rapid changes, given that any potential number of nodes can both join and leave at any time, so the number of nodes within a domain changes frequently. As a result of this, trust management should consider short term associations between nodes efficiently – both asymmetric or symmetric associations. Furthermore, given the volatile nature of VANET, it would not be feasible to maintain a too large number of historical trust relations between nodes, i.e., a trust relationships table or historical transactions within a group. Authors in [76] raised a key point that trust models should be independent of vehicles mobility. Therefore, TMs should not be bound to mobility which is likely to change in different VANET contexts.

C11: Ability of TM to detect false positive and false negative

The realization that VANET is subject to attacks and misbehaviour raises the importance of detection in real-time. Therefore, there has to be measures in place to manage false positive/false negative values, with respect to trust management, which could potentially have adverse effects on nodes' trust value or status within the network. This could lead to genuine next best forwarding nodes being excluded and having an incorrect cost assigned to it, or not being able to form trust relationships with other nodes in the vicinity based on incorrect message trustworthiness. Raya et al. proposed the LEAVE protocol within their scheme in order to reduce the number of false positives [78]. However, one major drawback of this scheme is its failure to cope with false positive detection when most vehicles are malicious. Moreover, their solution also fails if there are not enough vehicles to provide feedback. A method to detect false positives and false negatives within trust models would improve accuracies of the assessment and evaluation results.

C12: Ability of TM to promote node trustworthiness

Honest and intelligent inter-vehicle communication is one of the most fundamental aspects of VANET. As such, TMs should provide mechanisms to promote honesty and discourage dishonesty/misbehaviour when communicating amongst others, and to produce feedback for accurate maintenance of those relationships. In addition, confidence of node trustworthiness should be maintained to ensure accuracy up to the most recent point in time. This will help to maintain the accuracy of assessments, re-evaluations and overall outcomes, which is of importance given the requirements of safety applications and data-delivery.

C13: Ability of TM to manage end-to-end delays

It is important that the approach to establishing trust between vehicles impose minimal overhead and delays on other operations in the network. This should be achieved without compromising the safety of the network or creating any windows of vulnerability during the process. Although the use of trust mechanisms can enhance security and produce lower overheads, compared to cryptography-based approaches, it is still important to consider all potential vulnerabilities that could impact the network performance and undermine its purpose that stem from end-to-end delays and cost, during establishment and maintenance of relationships between nodes (minimum amount of data exchanged between neighbours).

C14: Ability of TM to operate in presence of malicious vehicles

Though a number of the reviewed schemes are capable of operating as effectively in the presence of malicious nodes to an extent, it is important that these measures, and others following suit, are further improved to increase the efficiency of trust models. One such TM is designed by

Shaikh et al. which operate effectively in the presence of malicious vehicles [80]. In context-enabled VANET, TMs should be designed in a way that legitimate vehicles identify and revoke information from malicious vehicles, within its communication range.

C15: Ability of TM to operate in various contexts

Given some of the potential issues noted with the use of subjective information within TMs, it would be worth considering drawing benefit from context information. This would reduce the likelihood that the received information has been influenced or tampered with based on traffic information. In conjunction to this, context-based information could be of use to better identify whether a node is broadcasting falsified information for its own benefit, such as to free up congestion which could be correlated with information from RSUs. Subjective information is more likely to be susceptible to bias.

C16: Availability of TM to benchmark against other models

It is highly important, when designing and testing TMs, to be able to compare it with other schemes that have already/recently been proposed. This promotes reasoning in relation to whether the approach for establishing trust in one scheme has benefits compared to others, in which circumstances it works or not, which are its limitations. Thus far, only a few of the proposed TMs go to such an extent where they fully benchmark themselves against existing ones. Thus, this criteria regards the availability of such results.

4.2 Qualitative Evaluation of Trust Models

A qualitative comparison of TMs is presented in Table 4.4 using the above criteria. This table shows result of the evaluation of 4 TMs from each of the 3 classes, therefore, a total of 12 TMs, published between 2006 and 2016, were analyzed for this purpose. The TMs were selected based on the popularity and acceptability by the researchers which is indicated by their high number of citations. A check mark (✓) in Table 4.4 means that a certain criterion is met by the TM in question. For example, a (✓) in C1 for TMs by Haddadou et al. [73] and Minhas et al. [74] indicates that these TMs fulfill the first criterion for trust management, i.e., they have the ability to calculate trust in a decentralised manner.

Table 4.4: Qualitative Evaluation of Trust Models in VANET

Trust Models		**Evaluation Criteria for Trust Management**															
		C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**	**C12**	**C13**	**C14**	**C15**	**C16**
Entity-Oriented	Khan et al. [71]						✓		✓	✓		✓	✓	✓	✓		
	Jesudoss et al. [72]		✓			✓				✓		✓	✓	✓			
	Haddadou et al. [73]	✓				✓						✓	✓	✓	✓		
	Minhas et al. [74]	✓		✓	✓			✓	✓		✓		✓				
Data-Oriented	Raya et al. [78]	✓		✓		✓		✓	✓	✓	✓		✓		✓		
	Shaikh et al. [80]	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓		✓		✓
	Wu et al. [81]			✓		✓	✓		✓	✓	✓	✓					
	Patwardhan et al. [98]	✓					✓			✓	✓	✓					
Hybrid	Kerrache et al. [99]	✓	✓	✓		✓		✓		✓	✓	✓	✓	✓	✓		✓
	Gazdar et al. [100]	✓		✓		✓	✓	✓	✓	✓		✓	✓	✓	✓		
	Sedjelmaci et al. [101]			✓		✓		✓			✓		✓				
	Li et al. [17]	✓	✓	✓		✓			✓	✓	✓		✓		✓		✓

We can see from Table 4.4 that the majority of TMs do not meet the complete evaluation criteria. Since TMs ensure the routing of trusted information in VANET, all of these criteria should be satisfied and validated. Thus, a TM should only be implemented in a real network, once it meets the evaluation criteria.

Table 4.5 provides a comparison of different studies where evaluation criteria for trust models in VANET were identified. Our work provides a comprehensive set of evaluation criteria (C1 - C16) for trust management, some of which were neglected in previous studies. For instance, we defined criteria C11 and C12, as they play a significant role during trust establishment, i.e., they ensure that the legitimate vehicle providing accurate information gets incentive for their honesty. Moreover, the ability of TM to detect false positive and false negative values increases network efficiency by eliminating malicious information. Introducing context information (C15) for trust establishment is another important neglected criterion. The use of context-based information can provide additional information for TMs in the network, thus providing an extended window of opportunity for vehicles to establish trust.

Figure 4.4 illustrates the extent to which TMs, belonging to a certain class, meet the evaluation criteria; this is achieved by means of a satisfaction ratio. This ratio is calculated based on how many evaluation criteria are taken into account by TMs analyzed within a class. It can be seen that every class of TM only partly satisfies the evaluation criteria for VANET. Therefore,

Table 4.5: Proposed Evaluation Criteria for Trust Management Compared to Previous Studies

Evaluation Criteria for Trust Management	J Zhang [13]	Marmol et al. [76]	Shaikh et al. [80]	Alriyami et al. [102]	Proposed Evaluation Criteria (Current Study) [95]
C1	✓		✓	✓	✓
C2				✓	✓
C3	✓	✓	✓	✓	✓
C4	✓	✓	✓	✓	✓
C5		✓			✓
C6	✓				✓
C7			✓		✓
C8		✓	✓	✓	✓
C9	✓	✓		✓	✓
C10	✓		✓	✓	✓
C11					✓
C12					✓
C13		✓		✓	✓
C14	✓	✓			✓
C15					✓
C16				✓	✓

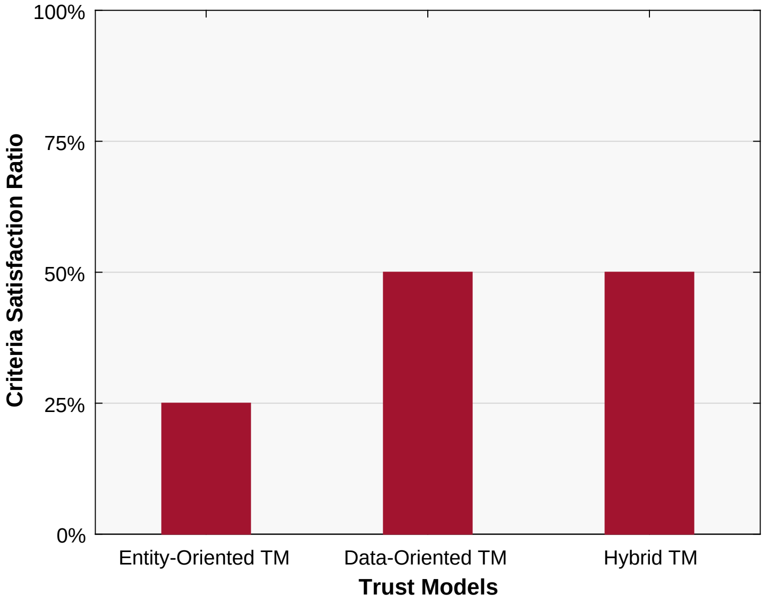


Figure 4.4: Evaluation Criteria Satisfaction in Trust Models

entity-oriented TMs satisfy only 25% of the criteria, while data-oriented TMs and hybrid TMs, both, satisfy 50% of the criteria. These statistics indicate that further research is required in trust management.

Figure 4.5, on the other hand, provides a comparison of the TMs on every considered criterion, per class. Entity-oriented TMs only satisfy criterion C12, i.e., it only promotes trustworthiness among the nodes. On the other hand, data-oriented TMs operate well in a dynamic and robust environment, thus satisfying criteria C9 and C10, respectively. Hybrid TMs are more scalable (criterion C3) to various ranges of parameter (criterion C5) to promote trustworthiness (criterion C12) in the network. Further, Figure 4.5 also depicts that none of the TM (entity-

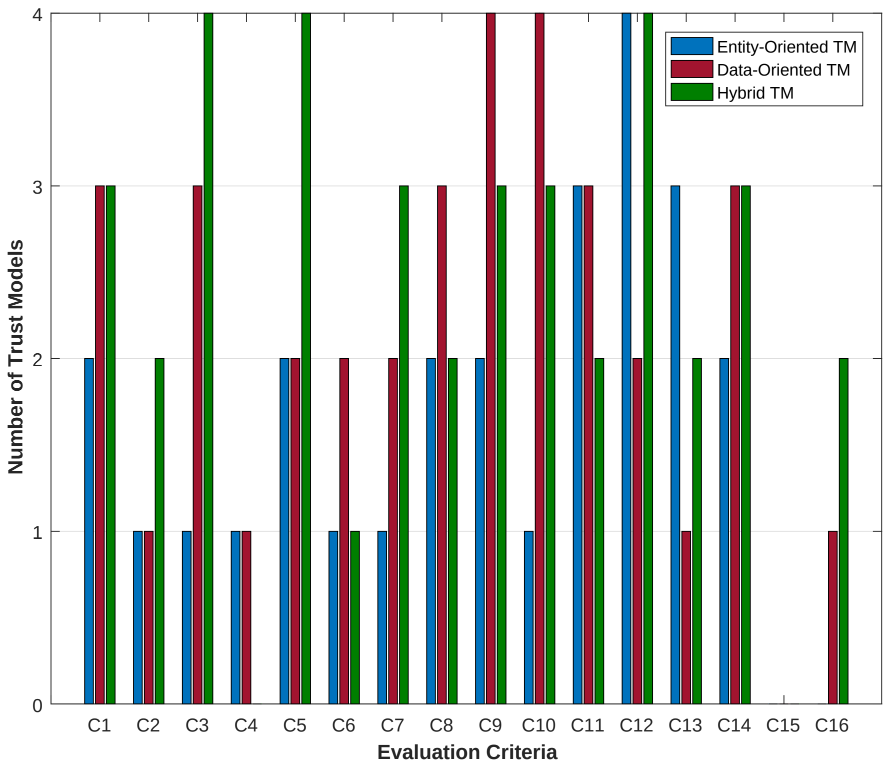


Figure 4.5: Comparison of Trust Models

oriented, data-oriented and hybrid) satisfy criterion C15 as context-establishment is neglected for trust evaluation. From this analysis, it becomes evident that the majority of the criteria are neglected by TMs, especially, the aspects of privacy and context.

4.3 Summary

In this chapter, we introduced the trust evaluation and management framework in vehicular ad-hoc network, where different involved modules are explained in detail. In particular, we focused on the details related to trust models and their evaluation. First we briefly introduced threat model and risk assessment, which then followed by details about context establishment and implemented trust models. To evaluate these trust models, we explicitly identified sixteen trust evaluation criteria. At the end, we provide the qualitative analysis of the trust models based on the proposed evaluation criteria. In the next chapter, we will explain the risk assessment along with threat model in detail which forms the foundation of this trust evaluation and management framework by identifying and quantifying the risk of different attacks in VANET. It is worth mentioning here that the proposed framework is flexible as it can easily integrate new attacks and TMs. The details of implementing new attacks and TMs are provided in Appendix 1.

Chapter 5

Research Methodology and Simulation Model

In the previous chapters, we identified a trust evaluation and management (TEAM) framework for vehicular ad-hoc networks. The main purpose of this chapter is to provide the implementation details of the simulation model which is developed to evaluate the performance of TEAM framework. TEAM framework is built on different open-source frameworks such as OMNET++ simulation environment, VEINS framework and SUMO traffic model. SUMO is used specifically for the mobility patterns of the vehicles while OMNET++ for the modelling of the vehicles. This chapter starts with the discussion about research methodology which is then followed by the detailed description of simulation environment. At the end, we will discuss the implemented TEAM framework using OMNET++, VEINS and SUMO simulators.

5.1 Research Methodology

Research is a systematic approach to investigate a particular problem through various procedures and studies often known as research methods. In general, various research methods exists to solve a particular problem e.g, lab experiments, case studies etc. However, to understand and solve the research problem in a systematic manner, a detailed research methodology is required which provides a work plan to achieve a particular aim [103]. Research methodology can be broadly categorized into following three classes. 1) *Qualitative approach* first identifies various criteria through comparative study, systematic literature review, case study, simulations etc. and then analyse and evaluates the performance of the system based on the these criteria. 2) *Quantitative approach* on the other hand, uses statistical means for the evaluation of the system. This approach includes experiments with raw and structured data, and test beds etc. 3) *Hybrid approach* uses both (qualitative and quantitative) approaches for the system validation and evaluation.

Vehicular network is an emerging technology where major research and manufacturing effort is being carried out for safer overall transportation. This research results in the development of revolutionary technologies which are quite complex in nature. Integration of these technologies into vehicular network is a challenge for the industry as the performance of these technologies have to be performed beforehand.

In order to perform and validate the research, several methods can be utilized, including mathematical analytical modelling, field operational tests (testbeds) and simulations. *Mathematical analytical modelling* are more robust than simulations where problem can be solve at a much faster rate than simulations. However, there are certain drawbacks of mathematical analytical modelling. For instance, they can only be used for modelling a particular small section of the network such as one-hop communication between two vehicles. However, this modelling gets extremely difficult for the overall network which contains high number of nodes. The complexity level increases further if the participating nodes have high mobility. Moreover, for modelling a complex network like VANET, mathematical modelling can include various assumptions on parameters which limits the actual implementation of the network in the real environment. Therefore, these assumptions and approximations result in a network where accuracy is sacrificed.

Field Operational Tests (FOTs) are the second type of modelling method which provides a testbed implementation of the proposed algorithm on the employed hardware. Though FOTs provide a real testbed for experimentation, but it also offers some disadvantages. First, FOTs deployed for small scale cannot guaranteed same results for full deployment of VANET. Second, a very high cost is involved in FOTs due to the involved hardware and lastly, FOTs have to massively deal with the real world difficulties for large scale network in order to obtain the accurate results.

Due to the major issues highlighted above, most of the research on VANET is carried out via *simulations*. Simulations can be used to model the whole VANET by adjusting the parameters very close to reality, so that the results produced via simulations are accurate and close to the reality. Moreover, once, the performance of the proposed algorithm is validated via simulations, this can be integrated in the real network as the results produced as accurate and satisfies the real world criteria. Figure 5.1 shows the detailed taxonomy of the research methodology. The proposed research methodology is highlighted in green. The next section will focus on the details of the simulations environment in VANET.

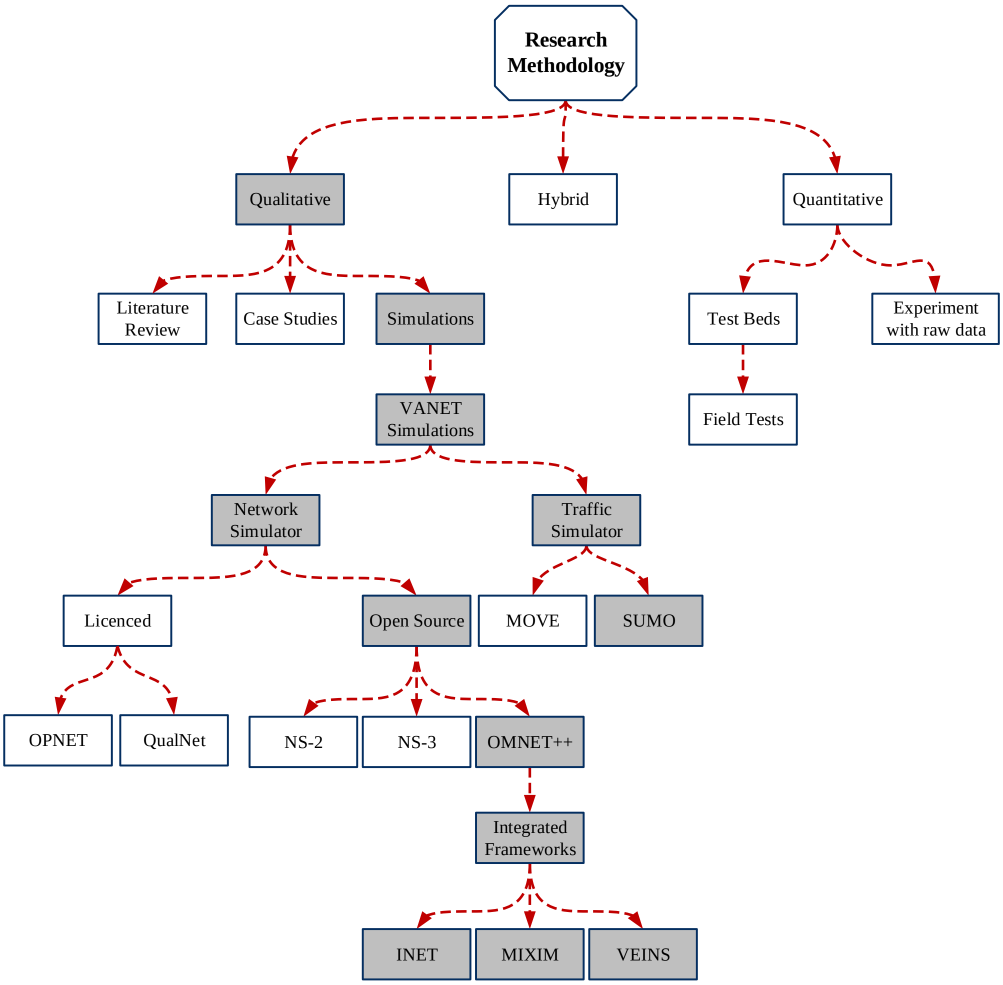


Figure 5.1: Taxonomy of Research Methodology

5.2 Simulation Environment

Simulations are widely used beforehand to optimize and modify the existing system, thus reducing the chances of failures [104, 105]. Simulations offer several benefits such as (1) the results produced by simulations are mostly close to reality which can be mapped to real network after extensive validation, and (2) simulations are cost effective comparing to test beds. Simulations are usually categorized as:

1. **Link Level Simulations:** are used for the performance evaluation at the link level, i.e., a radio link between the sender and receiver node. These simulations are mostly focusing on the lower layer (physical layer) of vehicles and roadside units to maximize the link capability which can ensure the efficient distribution of messages [106]. For instance, modulation and demodulation algorithms to increase efficiency of channel spectrum [107].

2. **System Level Simulations:** on the other hand, system level simulations consider a broad view of the network for modelling different components such as vehicles, RSUs, and backhand infrastructure. Link level simulations are usually the input for the system level simulations. Main focus of this thesis is system level simulation where different nodes (vehicles and RSUs) communicate with each other via V2V and V2I communication.

Various simulation tools are available which can simulate VANET including both mobile (vehicles) and static (RSUs) nodes in the network. In order to implement VANET having characteristics close to reality, modelling should be done for a network having realistic network traces. Therefore, VANET simulation mostly relies on more than one simulation environments for real world scenarios. VANET simulations are a combination of following two kinds of simulation.

1. Network simulation

2. Traffic simulation

5.2.1 Network Simulation

Network simulations are widely used for the implementation and performance evaluation of the network before their actual deployment in the real world. Moreover, network simulations are very helpful for the validation of newly proposed network protocols [108].

Several network simulation frameworks are currently available which use discrete event simulations (DES) to analyse the network and network protocols. These simulation frameworks are mostly open-source such as 'Network Simulator-2 (NS-2)' [109], 'Network Simulator-3 (NS-3)' [110], 'OMNET++' [111], 'JIST/SWANS' [112], and licensed such as 'Riverbed Modeler' [113] and 'Qualnet' [114].

In this thesis, OMNET++ is used as a base DES simulation framework as it includes a rich library of various simulation models such as LTE and LTE-Advanced mobile communication (SimuLTE) [115], peer-to-peer networks (OverSim) [116, 117], mobile ad-hoc networks (INET-MANET) [118] and vehicular networks (VEINS) [2, 119].

5.2.1.1 OMNET++ Simulation Environment

OMNET++[1] is an open-source simulation environment which is primarily used for research and development of both wired and wireless networks and their different components. Key features which OMNET++ provide are:

- Rich model library including source code of different protocols such as TCP/IP, UDP, IEEE 802.11 etc
- Discrete event and hybrid simulation frameworks
- Graphical User Interface (GUI) based tool for debugging and analysis
- Modular architecture for models which are programmed in C++
- Compatibility with wide range of platforms such as Windows, Linux, Mac OS etc.

[1] OMNET++ stands for "**O**bjective **M**odular **N**etwork **T**estbed in C++"

- Integration of different simulation frameworks such as:
  - INET framework - provides internet protocol stack for communication networks [118]
  - VEINS framework - for VANET simulations [2, 119]
  - NETA framework - for network attacks [120]

5.2.2 Traffic Simulation

Traffic simulators deploy and simulate road behaviour by providing realistic traffic traces which contain node's location [121]. These traces are used as input to the network simulator. Examples of traffic simulators are Simulation in Urban Mobility (SUMO) [122, 123], VANETMobiSim [124, 125], Mobility model for vehicular network (MOVE) [126] and PAMRAMICS [127].

In the context of this thesis, we have used SUMO as a traffic simulator due to the fact that it can be integrated with OMNET++.

5.2.2.1 SUMO Traffic Simulation Environment

SUMO[2] is an open-source traffic simulator which supports simulation of vehicles at a large scale network. The main features of SUMO are:

- Ability to model vehicle at the micro-level having specific characteristics such as vehicle type, vehicle length, vehicle maximum speed, acceleration and deceleration.
- Ability to use various car following models including $Krau\beta$ model [128] etc.
- Ability to import real traffic traces from OpenStreetMap.
- Ability to integrate with network simulator such as OMNET++.

Based on our literature survey, we selected OMNET++ as network simulator and SUMO as traffic simulator as they were ideal for our case to implement our trust evaluation framework.

[2] SUMO stands for "**S**imulation in **U**rban **MO**bility"

OMNET++ provides various modules ranging from physical to application layer of both mobile and static nodes of the network. Moreover, SUMO on the other hand can import real maps from OpenStreetMap. As the prime objective of this thesis is the evaluation of trust models in VANET, simulations must be performed on the real maps which is provided by SUMO and OpenStreetMap. Further, to simulate VANET, we used VEINS framework which is used widely by the research community to model vehicular networks [2, 119].

5.3 VEINS Simulation Framework

Facilitating and modelling inter-vehicular communication close to reality via simulations require traffic mapping on the real world map. VEINS[3] framework provides such kind of environment where vehicular traffic pattern on the real map is provided by SUMO, while OMNET++ provides provides various modules (application layer, DSRC and physical layer) to ensure realistic network behavior. A small patch "Traffic Control Interface (TraCI)" is used for communication between OMNET++ and SUMO [129]. Whenever, an event (accident information) is triggered in OMNET++, TraCI enables the vehicles in SUMO to change their route by sending out respective commands. This enables the two simulators to operate in the real-time. Figure 5.2 depicts the work-flow of VEINS. It can be seen that VEINS is bidirectionally coupled simulator, providing connectivity between two simulators via a TCP connection which is achieved using TraCI standard.

In order to implement our trust evaluation framework, we extended the veins framework mostly at the application layer where every vehicle is equipped with the trust model. Whenever, a vehicle from SUMO enters into OMNET++ environment, vehicles communicate with each other through the modules which are defined at the PHY and MAC layer. At the application layer, vehicles are using the trust model which evaluates the trustworthiness of the messages received. In the next section, we explain the simulation flow in more detail.

[3] VEINS stands for "**VE**hicles **I**n **N**etwork **S**imulation"

Removed for Copyright Purposes

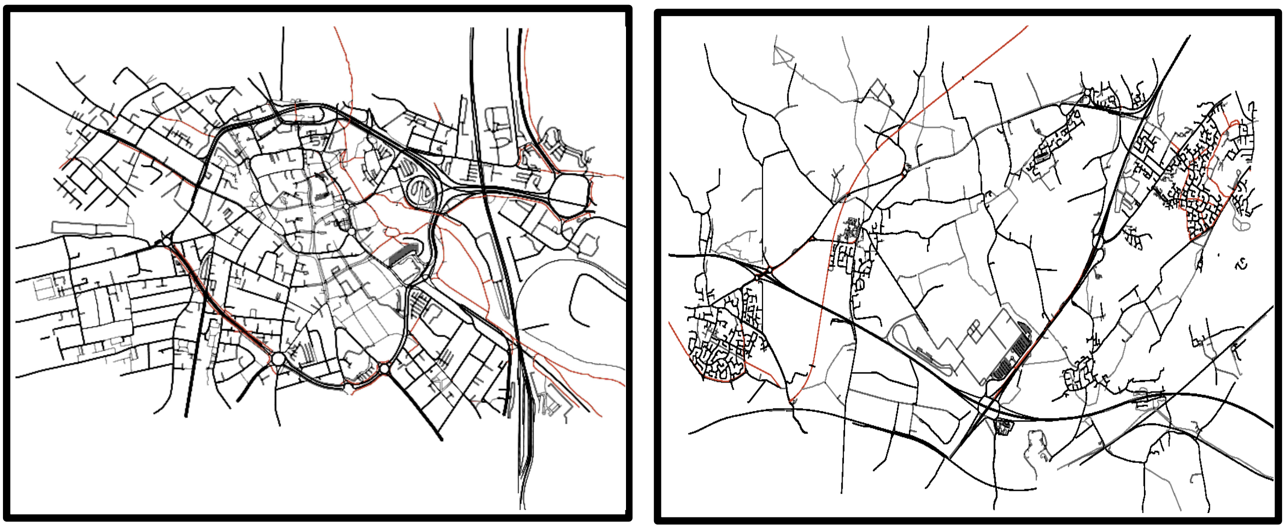
Figure 5.2: Work-flow of VEINS simulator [2]

5.3.1 Imported Maps

As the core objective of this thesis is the evaluation of trust models under adversaries condition in different contexts. Therefore, to model and evaluate the trust models in such environment, we imported two real maps from from the city of Derby, United Kingdom using OpenStreetMap [130, 131]. Figure 5.3a shows the city center scenario while figure 5.3b depicts the rural area of Derby. The considered area for the urban map is $4km \times 2.5km$ while for rural location, we considered a map having dimensions $10km \times 8km$. The vehicles in the city center have low mobility while rural area contain vehicles with high mobility.

5.3.2 Traffic Modelling

Once, the respective maps are identified via OpenStreetMap, the next step is the identification of the traffic on these maps. This is achieved via SUMO where the traffic is deployed. Since, the vehicles are usually spread randomly throughout the city, therefore, we deployed vehicles which penetrates into the map at random rate. Moreover, every vehicle enters into the considered map after sometime to ensure realistic behaviour. For simulations, we kept this entrance rate to be 1 second, meaning that the vehicles enters into the simulations after every 1 second at a random location.



(a) (b)

Figure 5.3: Simulated Maps of Derby (a) Urban (b) Rural

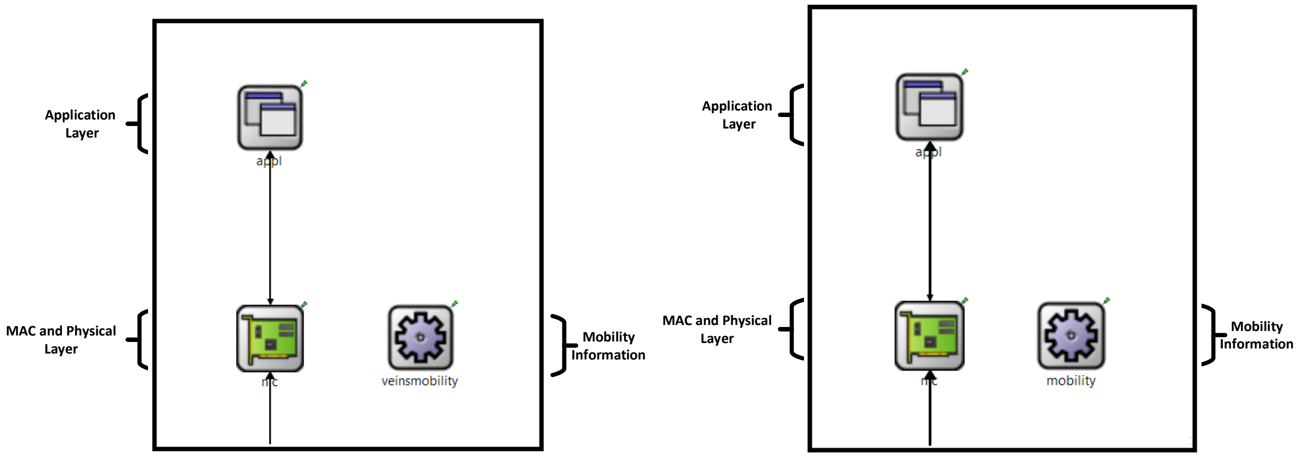
5.3.3 Nodes Identification

VANET is an environment which includes both mobile nodes (vehicles) and static nodes (RSU) in the network. Therefore, in our considered simulation model, we deployed both vehicles and RSUs. Further, to achieve our aim of trust modelling under adversaries condition, we particularly identified attacker models in the simulations. These attacker models are identified via risk assessment where we identified attacks based on their severity levels. As a result, our framework has following four nodes:

- **Legitimate vehicle:** This node represents those mobile vehicles which are transmitting legitimate and honest information throughout the network. In our simulations, we have both vehicles with low and high mobility. Vehicles are defined according to the protocol stack and all the vehicles are equipped with application, MAC and physical layer. Moreover, vehicles also includes the mobility module which contains the mobility related information of the vehicles.

- **Mobile Attacker:** This node represents the attacker having mobility. These attackers are launching attacks in the network while on the move. Mobile attackers are also equipped with standard protocol stack, however, their behaviour is modified accordingly based on their role in the network.

- **Roadside Unit:** RSUs, on the other hand, are the static entities of the network which are deployed at the intelligent locations on the map. Thus, RSUs have no mobility modules. RSUs are also equipped with protocol stack which is similar to vehicle.
- **Static Attacker:** Static attackers are also present in our simulator, where, these nodes are placed at random locations with the capability to launch an attack in the network. These nodes also contains full protocol stack, however with zero mobility.



(a) (b)

Figure 5.4: Node model in OMNET++ (a) Mobile Node (b) Static Node

Figure 5.4 shows the node model implemented in OMNET++ and veins. In our simulation model, mobile nodes refers to 'legitimate vehicles' and 'mobile attackers'. Similarly, static nodes represents 'RSU' and 'static attackers'. Further, we can see that both nodes are based on the protocol stack and contains two major layers, i.e., application layer and mac and physical layer.

5.3.3.1 Application Layer

This layer operates at the top of the protocol stack, where it generates and receive safety related message. In our platform, three different application are running at the nodes. They are:

- Application used by legitimate vehicles

- Application utilized by RSUs
- Application used by attackers (mobile and static)

As the simulation major focus is the identification and revocation of malicious messages from the network, therefore, legitimate vehicles are equipped with trust model. This enables the vehicles to identify the trustworthiness of the received message. Whenever a message is received at the application layer of the legitimate vehicles, message is evaluated for trustworthiness based on the considered trust model which may be either data-oriented or entity-oriented or hybrid.

Next, at the RSU, messages are broadcast when they are received at the application layer. This application is used to share the messages with vehicles in the large geographical location. In our simulations, we have used RSU to facilitate V2I communication where the messages generated at the application layer is shared with vehicles in its vicinity.

Further, for attacker nodes, we designed different attacker models which are used at the application layer of the attacker nodes (both mobile and static). In our simulations, we considered man-in-the-middle (MITM) attacker. MITM attacks are explained in detailed in section 6.3. Specifically, we considered following MITM attack models which are integrated in our framework.

1. Attack Model 1: MITM delaying message
2. Attack Model 2: MITM suppressing message
3. Attack Model 3: MITM tempering message
4. Attack Model 4: MITM tempering and delaying message

These attack models will be discussed in detail in chapter 6 and chapter 7.

5.3.3.2 MAC and Physical Layer

Every node in veins simulator is fully equipped with WAVE protocols and vehicular network version of IEEE 802.11 protocol, i.e., IEEE 802.11p which operates at the MAC layer. This layer combines the functionality of both MAC and physical layer where communication protocols are implemented at the MAC layer. Further, physical layer functionalities, such as, channel model, interference model and propagation model are also integrated in this layer.

Moreover, every node in veins simulator contains mobility module which contains mobility related information. For mobile nodes, it contains mobility models while for static nodes, these mobility models have zero mobility.

5.4 Summary

In this chapter, we explained the simulation model of VANET which is implemented using veins simulation framework. Veins is implemented further on two simulators, i.e., OMNET++ and SUMO. Further, in the context of this thesis, we identified several attacker models which are used for the evaluation of the trust models in VANET. In the next chapter, we will focus on the performance evaluation of the trust evaluation framework where we implemented three trust models at the application layer of the vehicles.

Chapter 6

Context-based Risk Assessment in VANET

In the previous chapters, we proposed and explained our trust evaluation and management framework which is designed specifically for the efficiency evaluation of trust models under adversary conditions in various contexts of VANET. The trust models must be evaluated under adversary conditions in order to satisfy security requirement in VANET. Therefore, we dedicate this chapter to the details of threat model and risk assessment which are the core modules of our TEAM framework, designed specifically for the identification of major attacks in VANET. The attacks with critical severity are implemented in our framework and we evaluated the efficiency of these trust models in the presence of these attacker models.

This chapter is categorized as follows. The chapter starts with the state-of-the-art in risk assessment. Next section focuses on the risk assessment framework where risk of the identified attacks are evaluated. Further, context-based risk assessment is also presented in this chapter where the risk caused by an attack in different context is evaluated. At last, we explain the identified critical attack (man-in-the-middle) in VANET, where we implemented it for general VANET scenario.

6.1 State-of-the-art: risk assessment

As discussed previously, VANET is a very sensitive network, as it disseminates critical information among the network entities such as safety information. Further, it also directly involves human lives, which are always at stake in such networks. A small human or sensor error can result in loss of a human live. Moreover, VANET includes both legitimate and misbehaving vehicles that can compromise the normal operation of VANET by launching different attacks. In order to identify the severity of the attacks by these malicious vehicles, risk assessment should be performed as a preliminary study before designing security solutions. Risk assessment is a vital component of cyber security and currently huge standardization effort is being carried by notable organizations such as ISO and SAE. In the domain of VANET, we identify following three related standards that can be utilized to tackle both system safety and system cyber security.

- **ISO 27005:** ISO 27005 provides a general framework for risk assessment, which can be applied within every context and network. ISO 27005 adopted an iterative approach to perform risk assessment in order to increase the capability of the user to deal with the identified risk. The important components of this framework are context establishment, risk assessment, risk treatment, monitor, and review. Once, context is identified, risk assessment is performed on the context where risk is identified, analysed and evaluated by identifying likelihood of attack occurrence and its overall impact. Countermeasures for the severe attacks can be designed via risk treatment in order to mitigate the effect of the attack. ISO 27005 provides a flexible framework where risk assessment can be performed for every context. Since VANET is a large-scale network, which involves various assets including communication, vehicular components and sensors, adjacent infrastructure, therefore, ISO 27005 is an ideal candidate that provides flexibility of applying risk assessment by establishing context.
- **ISO 26262:** ISO 26262 is specifically proposed for electrical and electronic systems within the vehicles to achieve automotive safety. This standard integrates a safety life cycle

including development, production, operation, service and decommissioning. Further, this standard defines Automotive Safety Integrity Levels (ASIL) for the evaluation of risk, which can be calculated using three parameters [132]. (1) Severity, (2) Exposure, and (3) Controllability. For the evaluation of ASIL, ISO 26262 suggests a risk assessment technique known as "Hazard Analysis and Risk Assessment (HARA)". Though, ISO is defined for automotive domain, but its scope is very limited as it targets only components having electrical and electronics. As VANET includes devices from a wide range, thus, ISO 26262 has very limited scope within VANET.

- **SAE J3061:** SAE recently proposed J3061 standard that provides a basic guideline to achieve cyber security specifically for vehicular cyber physical systems [40]. J3061 is built upon ISO 26262, where, it extends the scope from system safety to system cyber security. From risk assessment point of view, J3061 includes threat analysis and risk assessment in its concept phase where the main objective is to identify threats (attacks) having high risks. Though, J3061 suggested various mechanisms to perform risk assessment including attack trees [133], fault tree analysis [134], HARA [135] and TVRA [136], but it left the choice to the organization to decide a mechanism for risk assessment [137, 138].

Figure 6.1 shows the time-line of the introduction of notable standards and techniques to perform risk assessment. Further, we can see that these standards are constantly revised and modified. As an illustration, ISO 27005 was first introduced in 2008, which is then revised in 2011. This standard is recently updated in 2018 based on the increasing landscape of cyber-attacks.

Risk assessment is one of major concerns in VANET and as a result, it was part of various notable research projects around the globe. For instance, VANET risk analysis was proposed in EVITA project [139] which identified various vulnerabilities and threats in vehicles and categorized them into three levels, i.e., critical, major and minor. Similarly, the risk analysis considering security and privacy for vehicles and vehicular users were performed for VANET in various research projects such as SeVeCom [140], OVERSEE [141], SafeTRIP [142] and PRESERVE [143].

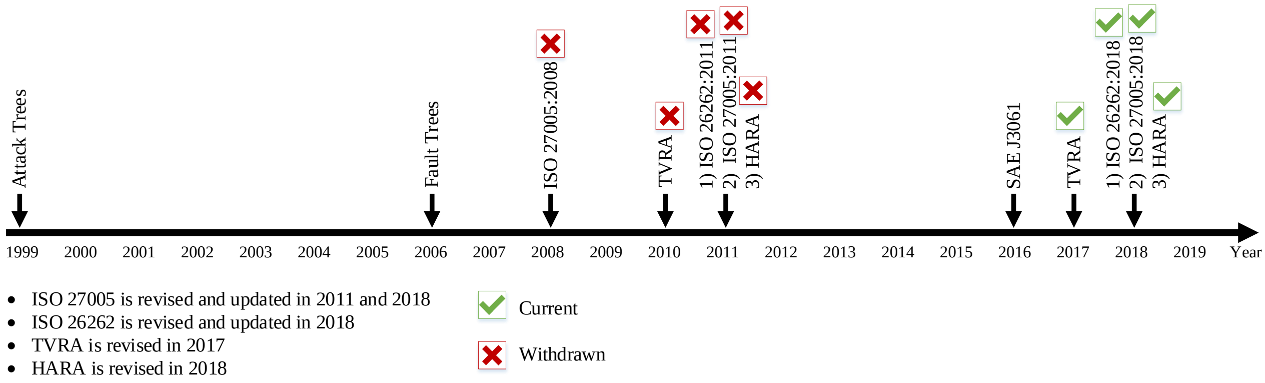


Figure 6.1: Time-line of Related Risk Assessment Frameworks and Standards

Different researchers also studied risk assessment in VANET. For instance, Tim et al. provided a risk assessment study where different attacks were identified in VANET. The authors concluded that road-side attackers with messaging forging capabilities posed highest risk in VANET [144]. Laurendeau et al. focused specifically on the risk analysis of DSRC wireless communication medium in VANET [145]. Moalla et al. provided a study where different threats to the communication protocols of VANET are identified, however, the authors were unable to provide risk analysis for the overall VANET architecture [146]. The threats for the back-end wired communication channel were identified by Bhattarai et al. in [147]. A tree based risk assessment approach was introduced by Ren et al., where, the authors focused more on the privacy issues in VANET [148]. Further, Bayad et al. presented a risk assessment framework using ISO framework [149]. However, the authors performed risk assessment for basic attacks in VANET.

To sum up, the risk analysis was conducted based on the security requirements of VANET and was limited to general network threats and attacks assessment. Indeed, VANET operates in different contexts related to the density and the mobility of the network, where the attack vector and the threats impact vary.

In fact, VANET is a large scale network where vehicles are distributed randomly and messages propagates between them throughout the network. These networks can include both high and low speed vehicles. Similarly, some locations in VANET can experience high number of vehicles while some locations have limited vehicles with variable acceleration and speed. In the same fashion, presence of an attacker in the network can vary. The attackers can be either mobile or static throughout the network. The attacks can have different impact on the network depending on the context and the attackers interest. For example, risks associated with particular attack in urban area and rural area can be entirely different which depends on various factors. In our point of view, the facilitation of context was neglected for the risk analysis in VANET. In our work, we identify VANET contexts where different attacks were classified by identifying assets in VANET. The main aim of our risk assessment is twofold: 1) First, we identified vulnerabilities, threats and attacks on cluster of assets in VANET, and 2) secondly, we proposed a context-based risk analysis by taking the mobility of vehicles into account.

6.2 Risk Assessment Methodology

VANET is an emerging technology whose main aim is to improve the overall transportation on the roads. However, VANET is prone to various attackers as they have the ability to launch a wide range of attacks due to its large-scale and open nature. To identify the risks caused by these attacks, we performed risk assessment in VANET using ISO 27005, due to the flexibility it can provide to identify vulnerabilities, threats and attacks throughout this large-scale network. Further, our risk assessment also relies on ISO 26262 and ETSI TVRA mechanism which are specifically used for identification of assets and vulnerabilities in the network. The detailed risk assessment framework is depicted in Fig. 6.2, consisting of following four modules:

1. ***Context Establishment:*** Identification of scenario for risk analysis.
2. ***Risk Identification:*** Identification of risks for attacks associated with assets in VANET.
3. ***Risk Analysis:*** Categorization and evaluation of risks according to their severity levels.
4. ***Monitor and Review:*** Monitoring and review of identified risks in order to take countermeasures at early stages.

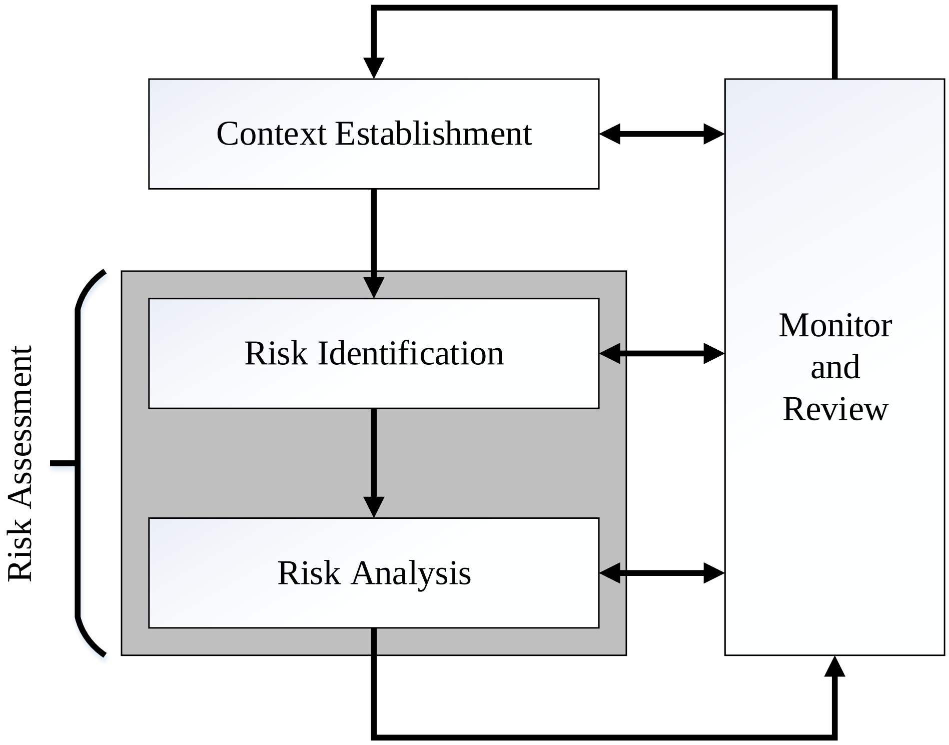


Figure 6.2: Risk Assessment Framework

6.2.1 Context Establishment

6.2.1.1 Identification of VANET scenario

In this phase, we present the scenario where the risk evaluation will be different in VANET. In our work, we have identified two scenario based on the status and the distribution of nodes across the network, i.e. the mobility patterns.

C1: Vehicles with high mobility

C2: Vehicles with low mobility

For example, contexts such as urban and rural areas, or areas with or without traffic jam will present different security threats, and require different security measures.

Indeed, VANET have unique characteristics such as high dynamic topology and predictable mobility. In fact, VANET mobility models have been a subject of various research works [150], and any VANET application design should be using adequate mobility models. Hence a detailed risk analysis methodology in VANET is required based on the characteristic of the network.

6.2.1.2 Identification of attacker models

Attack is an attempt by the attacker to gain illegal and unauthorized access into the system by exploiting its vulnerabilities [151]. The attack is not a sudden process but is the result of proper planning from an attacker to gain benefits for his/her own interest [152]. Therefore, identification and classification of attacker models are necessary as they play an important role during risk analysis. The attacker models identify the attacker strength, weakness, capacities and capabilities [153]. Several attacker models have been identified in previous works [154] [155], for example: insider or outsider, active or passive, and dependant or independent attackers. In this thesis, we define the attacker models from mobility perspectives. The following two attacker models were considered:

At1: The attacker is static in the network

At2: The attacker is mobile in the network

A static attacker could be an attacker in a vehicle parked in a car park or near a RSU.

6.2.1.3 VANET attack scenario

With the identification of the context and attacker models in VANET, following four combinational scenarios are possible:

Scenario 1: Network with high mobility (C1) and Static Attacker (At1)

Scenario 2: Network with high mobility (C1) and Moving Attacker (At2)

Scenario 3: Network with low mobility (C2) and Static Attacker (At1)

Scenario 4: Network with low mobility (C2) and Moving Attacker (At2)

Scenario 1 represents a network having highly mobile legitimate vehicles and static attackers. In scenario 2, both legitimate vehicles and attackers are mobile within the network. Scenario 3 is composed of network where vehicles have low mobility and attackers are static in the network, while in scenario 4, legitimate vehicles have low mobility, but attackers are also mobile in the network. Table 6.1 summarizes the VANET attack scenarios. In this thesis, we focused on these four scenarios for risk assessment and evaluation of the trust models.

Table 6.1: Possible Attack Scenarios based on Network Mobility

Scenario	**Context**	**Attacker Model**
Scenario 1 (S1)	High Mobility (C1)	Static Attacker (At1)
Scenario 2 (S2)	High Mobility (C1)	Mobile Attacker (At2)
Scenario 3 (S3)	Low Mobility (C2)	Static Attacker (At1)
Scenario 4 (S4)	Low Mobility (C2)	Mobile Attacker (At2)

6.2.2 Risk Identification

Risk identification module is responsible for the identification of attacks in VANET for risk analysis. In order to do so, we followed a very systemic approach which consist of following steps:

1. Identification of assets in VANET,
2. Classification of assets into groups,
3. Identification of vulnerabilities in group of assets,
4. Identification of threats related to the assets, and
5. Identification of possible attacks based on the threats and identified vulnerabilities

6.2.2.1 Identification of Assets in VANET

Assets are the valuable components of the network whose failure or misuse will cause damage to the entire network and its users [156]. A vulnerable asset is a threat to the network and creates possible attacks if the vulnerabilities are identified and used by malicious users. Thus, the process of identifying and securing the assets[1], and controlling the access of every user is a crucial step in VANET security. From a security point of view, the following are considered as assets in VANET because they have values for stack-holders:

[1] In ISO 26262, this step is referred to as “item definition” in its concept phase

AS1: Vehicles,

AS2: Vehicular users,

AS3: Wireless communication protocols,

AS4: In-vehicle communication,

AS5: Exchanged Information between vehicles and RSU,

AS6: Adjacent Infrastructure (RSU),

AS7: Wired back-end communication channel, and

AS8: Central Entity

6.2.2.2 Classification of Assets

Asset classification is the key to various security measures that need to be implemented for asset optimization. In most security assessments reports, assets are divided in four categories: 1) Information, 2) Software, 3) Physical, and 4) Services [45]. In our point of view, this classification doesn't reflect the VANET operations and security requirements. For example, the vehicle and the central entity are both physical assets, but they use different communication protocols (vehicle is a mobile node using wireless communication protocols, and the central entity is static and part of the wired network), and they require different security implementations (the security of the wireless ad-hoc network is different compared to the wired network).

In this thesis, we have classified the assets into three broad classes according to their role, mobility and impact on the VANET. The purpose of this classification is to facilitate the security assessment and the threat analysis. Since, in VANET, the assets are distributed in different domains, therefore, we classify these assets into three classes as depicted in Figure 6.3. These are:

b) Vehicular System: This contains vehicular user, vehicles and the communication network.

a) Information: This cluster represents the information carrying important messages across different assets in the network.

c) Infrastructure: It includes static entities in VANET, such as RSU and central entity.

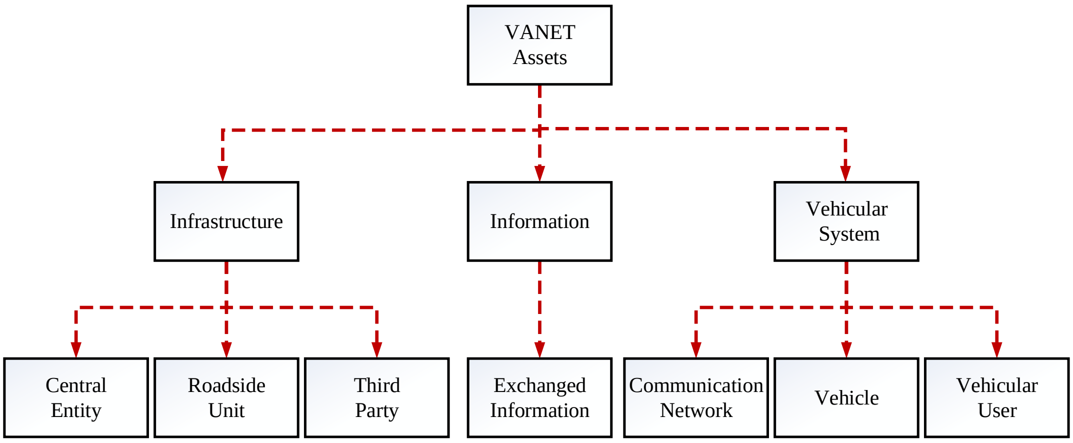


Figure 6.3: Assets and their classification in VANET

6.2.2.3 Identification of Vulnerabilities in VANET

According to ETSI, vulnerability represents a weakness, which can be exploited by malicious users in the form of attacks for their own benefits [136]. In the following, the vulnerabilities of the VANET will be presented according to asset categories.

1. **Vehicular Systems:** The major vulnerabilities in vehicular system are:

   V1: Vehicle wireless communication, which is used to transmit, relay and receive message containing significant information.

   V2: Software flaws including buffer over flow, insecure cryptographic algorithms and key management failure.

   V3: Insecure algorithms for exchanging significant information such as user information and credentials via wireless communication channel.

   V4: Physical access to vehicle or infrastructure.

   V5: Absence of time-stamp in the wireless communication protocol.

   V6: Non-availability of wireless communication channel during message transfer between two vehicles.

2. **Information:** The messages carrying the important information in VANET possess the following vulnerabilities.

   V7: No or weak integrity checks in the exchanged messages (data and routing messages).

V8: No or weak encryption protocols of sensitive data.

V9: Non-availability of messages with wrong routing table containing fake routing information.

V10: Non reliability of the exchanged protocol over wireless communication, making some messages unavailable (data and routing messages).

V11: Using expired or revoked cryptographic keys and certificates in the network.

V12: Encryption keys and tools lost.

3. **Infrastructure:** The infrastructure vulnerabilities are as follow:

   V13: Hardware malfunction and error.

   V14: No or weak encryption between RSU and central entity, and

   V15: Software and operating system (OS) vulnerabilities.

6.2.2.4 Identification of Threats in VANET

In this step, we identified threats to the cluster of assets, i.e., threats to information, vehicular system and infrastructure.

1. **Threats to Vehicular System:** Vehicles and its users represent the most important entities of VANET. Since, VANET is designed to provide comfort and traffic guidance to vehicles and its users, security in terms of confidentiality, integrity and authentication must be ensured. Following threats exist for vehicles and vehicular users.

   T1: Transmission of messages with no or weak passwords or encryption tools.

   T2: Unauthorized manipulation of routing tables containing sensitive information such as vehicular user identity.

   T3: Illegal software updates including security updates at vehicle.

   T4: Sensor malfunctions in vehicles, compromising the whole network with wrong information.

   T5: Sabotaging the vehicle physically and compromising its security.

   T6: Natural Disasters such as earthquakes, tsunami.

T7: VANET users lack of education and awareness about security.

Wireless communication is another important component in vehicular system domain with high significance as it is responsible to circulate important messages among vehicles and RSU. Following threats lies to wireless communication:

T8: Exposing sensitive information such as confidential communication between law enforcement vehicles.
T9: Revelation of user private credentials and information.
T10: Message alterations en-route to other vehicles and RSU by adding bogus information.
T11: Denial of service making users messages unavailable (data and routing messages).
T12: Messages intercepted and copied by malicious users.
T13: Unencrypted in-vehicle message transfer.

2. **Threats to Information:** VANET messages contain important information about a particular event, which is usually exchanged among the vehicles and RSUs during V2V and V2I communication. Threats to information always exist where the main interest of the attacker is to compromise its availability, confidentiality, integrity and authenticity. The threats to information can be exploited as:

T14: Natural disasters such as earthquake, tsunami can compromise the VANET by damaging its infrastructure. The transmission of any message via the infrastructure gets difficult.
T15: Hardware damage such as unexpected fire in OBU of vehicle, heated servers, and sudden power loss at the infrastructure etc.
T16: Password guessing to recover authentic user credentials.
T17: Cracking the encrypted message with its signature, and
T18: Non-verification of the encrypted and/or signed messages.

3. **Threats to Infrastructure:** The VANET Infrastructure being static in nature is more vulnerable to threats where attacker can launch an attack by exploiting the respective vulnerability. Following threats exists to the infrastructure:

T19: Privacy leakage of sensitive vehicular data on back-end wired channel.

T20: Introduction of Rogue RSU by an attacker to manipulate the communication between vehicles and RSU.

T21: Message alterations en-route to other vehicles via RSU and central entity.

T22: Malicious data forwarding to vehicles via central entity and RSU.

T23: Introduction of malware at central entity and RSU.

T24: Compromised security misconfiguration at central entity and RSU.

T25: Hardware damage to infrastructure due to natural disasters.

T26: Denial of service due to malfunctioning and unavailability of server.

6.2.2.5 Identification of Attacks in VANET

In this section we identify major attacks in VANET, i.e.,

A1: Social engineering attack dealing with the moral ethics of the VANET users (vehicles and infrastructure users).

A2: Malware integration to vehicles and its assets remotely.

A3: Jamming attacks at vehicle level to jam the communication between internal components of vehicle.

A4: Sensor impersonation attacks [157].

A5: Bogus information addition attack by introducing spam content to the authentic messages at one of the following asset.

a) *In-Vehicle:* Adds bogus information to the messages propagated inside vehicular components,

b) *Wireless Communication:* Intercept messages in transit to neighbouring vehicles and adds bogus information to original message, and

c) *Wired Infrastructure:* Modify messages between RSU and central entity.

A6: Replay attacks by injecting old messages in the network to bypass the infrastructure protection [158].

A7: Illegal remote firmware updates containing especially security updates provided by service providers. This process can take upto an hour [159].

A8: Physical damage (e.g. car accident or vandalism), compromising the vehicle security and its assets.

A9: Eavesdropping of sensitive information, i.e., vehicular user private credentials or communication between two police vehicles while chasing the criminal.

A10: Jamming attacks to block the communication channel which stops the propagation of messages in the network. Jamming attacks can be launched at following venues in the communication network: a) *Wireless Communication:* Jams the communication channel between two vehicles and neighbouring RSU, and b) *Wired Communication:* Jams the communication between RSU and central entity.

A11: Impersonation attacks to deceive the law enforcement agencies by using the identity of valid vehicular user.

A12: Network attacks exploiting the insecure wireless communication channel to launch illegal monitoring of the network containing important messages such as traffic accident. The attacker can launch following attacks in the network.

a)DoS attacks, leaving a severe impact on the network by preventing vehicles receive sensitive information such as road accident warnings [160]. Two techniques are used to perform DoS attacks in VANET [161]. 1) transmits random signal in a given frequency range of message transmission, and 2) generate messages in huge quantity at physical layer of VANET to take down the communication channel.

b) Sybil attacks involving the generation of multiple identities by a malicious attacker [162], and

c) Worm hole attacks which involves tunnelling of packets between two nodes located at remote locations [163].

A13: Man-in-the-Middle (MITM) attacks to intercept and modify the messages en-route from

RSU to vehicles and vice versa by exploiting the non- encrypted nature of messages or spoof the messages on the insecure wireless communication channel.

A14: Spoofing attack where the attacker steals the identity of a legitimate vehicle to become part of the network.

A15: Arbitrary and malicious code injection in VANET to gain information about the legitimate users by injecting malware, Trojans and virus in the network to compromise the vehicle and infrastructure. Mostly, arbitrary codes are specifically injected in two components of VANET.

1. Arbitrary code injection in vehicle containing AU to disrupt the vehicle, and
2. Malicious code injection to the database of central entity to identify particular user information.

Once, the node or certain component of node such as application unit is compromised, the attacker can launch different attacks such as message modifications or identify different users and their locations.

A16: Message flooding attacks by flooding the network with bogus messages.

The main consequences of threats and attacks in VANET are: (1) Sensitive information loss via wireless communication, (2) Vehicular user private credentials revelation and exposure, (3) Unavailability of important messages, (4) Communication loss between internal components of vehicles and with neighbouring vehicles and RSU, and (5) Damages to the device containing cryptographic tools in vehicles and central entity. In the next sections, risk analysis will be performed for the attacks identified in different assets of VANET.

6.2.3 Risk Analysis

Risk is directly related with the vulnerability identified in assets which are exploited by threats in the form of attacks, causing harm to the overall network [164]. Risk is a measurable quantity and it depends on following two factors:

1. Likelihood of occurrence of an attack, and
2. Impact of an attack on the network assets

The *'likelihood'* is used to define and measure the probability of carrying attacks on VANET assets, and how often the attack can occur. The Likelihood that an attacker will launch a successful attack depends on several factors [165], including motivation, technical expertise, knowledge about target network, available hardware component to the attacker, and an opportunity to pursue an attack in timely manner. The likelihood of an attack is mapped into three categories with corresponding values ranging from 1 to 3.

1. **Unlikely (=1):** The likelihood of carrying out an attack is very low in this case as the strong motivation of an attacker is required with strong expertise to find vulnerabilities in the network.
2. **Possible (=2):** The likelihood of an attack is possible here as the attacker needs less technical expertise and moderate motivation to launch an attack.
3. **Likely (=3):** The likelihood of an attack is likely as the attacker's motivation is high enough and basic technical knowledge is required here.

The *'impact'* on the network is fully dependant on the likelihood and the intensity of an attack. The overall impact on the network assets is different due to the fact that each attack has unique likelihood and intensity on a particular component of the network. It is the attack impact on the network that motivates the risk analysis process on VANET. The following three values are mapped for the impact parameter.

1. **Low (=1):** The damage caused to the network is minor.
2. **Medium (=2):** The damage caused to the network is short term but serious.
3. **High (=3):** Permanent and long term damage to the network.

Based on the definition of the attack likelihood and its resulting impact, the overall risk is now defined mathematically as the function of likelihood and resulting impact:

$$Risk = function(Likelihood, Impact) \tag{6.1}$$

6.2.4 Context-based Risk Assessment

This section is dedicated for the risk analysis in VANET by taking the mobility context into account. The main advantage of performing such risk analysis is that it identifies risk caused by a particular attack on target assets in different contexts. Once the attack risk is identified, the corresponding countermeasures can be applied to reduce or eliminate the possibility of an attack. VANET involves various context where the same attack can present different likelihood and/or impact (different risks). Therefore, we define the risk in the context of VANET as follows.

$$Risk = function(Likelihood, Impact, Context) \tag{6.2}$$

This definition leads to the following equation which is used in this work for the evaluation of attacks in several VANET context.

$$Risk_{context} = Likelihood_{context} \times Impact_{context} \tag{6.3}$$

The corresponding context-based risks are categorized into three classes, i.e., *Minor, Major and Critical.*

1. **Minor (=1, 2, 3):** The attacks have short term consequences and no urgent attention is required for these attacks.

2. **Major (=4):** These attacks have short term consequences but need attention with suitable countermeasures.

3. **Critical (=6, 9):** These attacks leave severe impact on the network and need urgent attention, countermeasures should be applied without any delay.

The risks identified as major and critical need urgent attention from the user. Table 6.2 shows the corresponding risk levels based on the likelihood and the impact values.

Table 6.2: Risk Analysis: Scale

Likelihood (L)	Impact (I)	Risk (R) = L * I
L1 = 1 (Unlikely)	I1 = 1 (Low)	R1 = 1, 2, 3 (Minor)
L2 = 2 (Possible)	I2 = 2 (Medium)	R2 = 4 (Major)
L3 = 3 (Likely)	I3 = 3 (High)	R3 = 6, 9 (Critical)

6.2.4.1 Risk Analysis for Attacks in Vehicles and Vehicular Users

In this section, the critical comparison of attacks on vehicles and vehicular users are discussed for the four different VANET contexts presented in section 6.2.1.3 and are compared with overall risk analysis of VANET.

In the Table 6.3, an attack has different likelihood and impact in each context of the network which results in different risks. E.g., the risk by bogus information addition attack (A5) varies in various context. The vehicles and attackers with similar mobility patterns in scenario 2 and 3 can have critical impact on the network as the messages generated by the vehicle will be updated with false information by the attacker, resulting in the propagation of wrong messages in the network. The risk posed by these scenarios is critical as the data integrity is not ensured. However, for the context with different mobility patterns (scenario 1 and 4), the risk changes to major due to short communication time frame where the message is updated with false information.

The impact of attacks like malware integration (A2) to vehicles also varies in different context. In scenario 2 and 3, the attacker and the target will have the same mobility pattern, the attack will spread more quickly, which will have a high impact on the network as it will be flooded with malware and more vehicles might be targeted. The corresponding risk will be critical in

Table 6.3: Context-based Risk Analysis for Attacks in Vehicles and Vehicular Users

Context	Attacks (A)	Likelihood (L)	Impact (I)	Risk (R)
General	A1	Possible:2	High:3	Critical:6
Scenario 1	A1	Possible:2	Medium:2	Major:4
Scenario 2	A1	Possible:2	High:3	Critical:6
Scenario 3	A1	Possible:2	High:3	Critical:6
Scenario 4	A1	Unlikely:1	Low:1	Minor:1
General	A2	Possible:2	High:3	Critical:6
Scenario 1	A2	Unlikely:1	High:3	Minor:3
Scenario 2	A2	Possible:2	High:3	Critical:6
Scenario 3	A2	Likely:3	High:3	Critical:9
Scenario 4	A2	Unlikely:1	Medium:2	Minor:2
General	A3	Likely:3	High:3	Critical:9
Scenario 1	A3	Likely:3	High:3	Critical:9
Scenario 2	A3	Likely:3	High:3	Critical:9
Scenario 3	A3	Possible:2	Medium:2	Major:4
Scenario 4	A3	Possible:2	Low:1	Minor:2
General	A4	Possible:2	Medium:2	Major:4
Scenario 1	A4	Unlikely:1	Medium:2	Minor:2
Scenario 2	A4	Possible:2	Medium:2	Major:4
Scenario 3	A4	Possible:2	Medium:2	Major:4
Scenario 4	A4	Unlikely:1	Medium:2	Minor:2
General	A5	Possible:2	High:3	Critical:6
Scenario 1	A5	Possible:2	Medium:2	Major:4
Scenario 2	A5	Likely:3	High:3	Critical:9
Scenario 3	A5	Likely:3	Medium:2	Critical:6
Scenario 4	A5	Possible:2	Medium:2	Major:4
General	A6	Possible:2	Low:1	Minor:2
Scenario 1	A6	Possible:2	Low:1	Minor:2
Scenario 2	A6	Possible:2	Medium:2	Major:4
Scenario 3	A6	Likely:3	Low:1	Minor:3
Scenario 4	A6	Likely:3	Low:1	Minor:3
General	A7	Possible:2	High:3	Critical:6
Scenario 1	A7	Unlikely:1	High:3	Minor:3
Scenario 2	A7	Possible:2	High:3	Critical:6
Scenario 3	A7	Likely:3	High:3	Critical:9
Scenario 4	A7	Possible:2	Medium:2	Major:4
General	A8	Likely:3	High:3	Critical:9
Scenario 1	A8	Unlikely:1	Low:1	Minor:1
Scenario 2	A8	Unlikely:1	Medium:2	Minor:2
Scenario 3	A8	Possible:2	High:3	Critical:6
Scenario 4	A8	Unlikely:1	Low:1	Minor:1

this scenario. However, the risk changes to minor in scenario 1 and 4 as both attackers and vehicles will communicate for a very short time. In general, the risk caused by the attack is critical as the integration of malware will result in the propagation of infected messages with virus and Trojans. Table 6.3 provides the risk analysis for attacks in vehicles and vehicular users in all four contexts.

6.2.4.2 Risk Analysis for Attacks in Wireless Communication

This section is dedicated to the critical analysis of the attacks on wireless communication in VANET in different context. For instance, Denial of Service (DoS) attack (A12) is one of the significant attack in wireless communication in VANET [166, 56]. In scenario 1, the static attacker performing DoS is located at a particular location in the network for example targeting a RSU. In this context, all the critical messages managed by the targeted RSU are lost, and critical VANET applications will be affected. The risk encountered is major in this scenario as the attack is going to affect only the geographical location of the targeted RSU, but as the vehicles are mobile, they might send/receive lost messages from other RSU. However, DoS attack can leave severe impact on the network if both the vehicles and attackers are mobile in the network and are propagating in same direction, thus preventing the legitimate vehicle from transmitting and receiving important messages. The consequence on VANET gets more drastic if many mobile attackers block the network over a large geographical location. The critical comparison of attacks in wireless communication under various contexts are described in Table 6.4.

In general, all the attacks have critical risks in second scenario, where both the attacker and target are mobile. In fact, when the mobility is high, the target vehicle might not have the time and the possibility to check the integrity and validity of certain content. For example, no central entity is available in the wireless range and attacker identity and messages will not be verified.

Table 6.4: Context-based Risk Analysis for Attacks in Wireless Communication

Context	Attacks (A)	Likelihood (L)	Impact (I)	Risk (R)
General	A5	Possible:2	High:3	Critical:6
Scenario 1	A5	Possible:2	Medium:2	Major:4
Scenario 2	A5	Likely:3	High:3	Critical:9
Scenario 3	A5	Likely:3	Medium:2	Critical:6
Scenario 4	A5	Possible:2	Low:1	Minor:2
General	A6	Possible:2	Low:1	Minor:2
Scenario 1	A6	Possible:2	Low:1	Minor:2
Scenario 2	A6	Possible:2	Medium:2	Major:4
Scenario 3	A6	Likely:3	Low:1	Minor:3
Scenario 4	A6	Likely:3	Low:1	Minor:3
General	A9	Possible:2	Medium:2	Major:4
Scenario 1	A9	Possible:2	Medium:2	Major:4
Scenario 2	A9	Likely:3	Medium:2	Critical:6
Scenario 3	A9	Possible:2	Medium:2	Major:4
Scenario 4	A9	Unlikely:1	Medium:2	Minor:2
General	A10	Likely:3	High:3	Critical:9
Scenario 1	A10	Possible:2	Medium:2	Major:4
Scenario 2	A10	Likely:3	High:3	Critical:9
Scenario 3	A10	Possible:2	Low:1	Minor:2
Scenario 4	A10	Possible:2	Low:1	Minor:2
General	A11	Possible:2	High:3	Critical:6
Scenario 1	A11	Unlikely:1	Medium:2	Minor:2
Scenario 2	A11	Possible:2	High:3	Critical:6
Scenario 3	A11	Possible:2	Medium:2	Major:4
Scenario 4	A11	Unlikely:1	Low:1	Minor:1
General	A12 (a)	Likely:3	Medium:2	Critical:6
Scenario 1	A12 (a)	Possible:2	Medium:2	Major:4
Scenario 2	A12 (a)	Likely:3	High:3	Critical:9
Scenario 3	A12 (a)	Possible:2	Medium:2	Major:4
Scenario 4	A12 (a)	Possible:2	Low:1	Minor:2
General	A12 (b)	Possible:2	Medium:2	Major:4
Scenario 1	A12 (b)	Unlikely:1	Medium:2	Minor:2
Scenario 2	A12 (b)	Possible:2	Medium:2	Major:4
Scenario 3	A12 (b)	Likely:3	Medium:2	Critical:6
Scenario 4	A12 (b)	Possible:2	Low:1	Minor:2
General	A12 (c)	Possible:2	Medium:2	Major:4
Scenario 1	A12 (c)	Unlikely:1	Low:1	Minor:1
Scenario 2	A12 (c)	Possible:2	Medium:2	Major:4
Scenario 3	A12 (c)	Possible:2	Medium:2	Major:4
Scenario 4	A12 (c)	Possible:2	Low:1	Minor:2

6.2.4.3 Risk Analysis for Attacks in Information

This sections describes the analysis of attacks performed on information in VANET in various contexts. As an illustration, MITM attacks (A13) are very common in VANET where information is exchanged between legitimate vehicles via intermediate nodes [167]. The risks associated with A13 varies in different contexts. MITM attacks are critical in scenario 2 and 3 where legitimate vehicles and attackers have same mobility patterns, providing enough time for the attacker to elaborate and launch an attack. However in scenario 1 and 4, the point of contact between legitimate vehicles and attackers is small and they communicate for a very short interval of time, the attacker is still able to intercept the communication but do not have enough time to elaborate an attack targeting specific vehicles. For example, the attacker can create a rogue RSU to communicate with legitimate vehicles. However, the quantity of intercepted messages is different for highly mobile vehicles and for vehicles with low mobility. The resulting risk is critical and major in these scenario as the vehicle may transmit sensitive information related to the vehicle identity or location during that time interval. Context-based risk analysis for attacks on information is depicted in Table 6.5.

6.2.4.4 Risk Analysis for Attacks in Infrastructure

In this section, we describe the context-based risk analysis for static entities in VANET, i.e., infrastructure. For example, static attackers have more chances of launching malicious code injection attack (A15) to the server applications in the central entity as compared to mobile attackers. In scenario 1 and 3, the attackers with no mobility are located at favourable location in the network where they can inject malicious codes to the central entity easily. Since the target is static in the network, the time frame to execute the attack is large. If the attacker succeeds to launch A15, the impact on the overall network is high due to the fact that the central entity is responsible to transmit critical information via RSU to vehicles over a large geographical location. If malicious codes are injected in the central entity, the network will experience the propagation of messages with malicious content leaving severe impact on the network. Therefore, the risk is critically high. However, for mobile attackers in scenario 2 and

Table 6.5: Context-based Risk Analysis for Attacks in Information

Context	Attacks (A)	Likelihood (L)	Impact (I)	Risk (R)
General	A9	Possible:2	Medium:2	Major:4
Scenario 1	A9	Possible:2	Medium:2	Major:4
Scenario 2	A9	Likely:3	Medium:2	Critical:6
Scenario 3	A9	Possible:2	Medium:2	Major:4
Scenario 4	A9	Unlikely:1	Medium:2	Minor:2
General	A10	Likely:3	High:3	Critical:9
Scenario 1	A10	Possible:2	Medium:2	Major:4
Scenario 2	A10	Likely:3	High:3	Critical:9
Scenario 3	A10	Possible:2	Low:1	Minor:2
Scenario 4	A10	Possible:2	Low:1	Minor:2
General	A11	Possible:2	High:3	Critical:6
Scenario 1	A11	Unlikely:1	Medium:2	Minor:2
Scenario 2	A11	Possible:2	High:3	Critical:6
Scenario 3	A11	Possible:2	Medium:2	Major:4
Scenario 4	A11	Unlikely:1	Low:1	Minor:1
General	A12 (a)	Likely:3	Medium:2	Critical:6
Scenario 1	A12 (a)	Possible:2	Medium:2	Major:4
Scenario 2	A12 (a)	Likely:3	High:3	Critical:9
Scenario 3	A12 (a)	Possible:2	Medium:2	Major:4
Scenario 4	A12 (a)	Possible:2	Low:1	Minor:2
General	A12 (b)	Possible:2	Medium:2	Major:4
Scenario 1	A12 (b)	Unlikely:1	Medium:2	Minor:2
Scenario 2	A12 (b)	Possible:2	Medium:2	Major:4
Scenario 3	A12 (b)	Likely:3	Medium:2	Critical:6
Scenario 4	A12 (b)	Possible:2	Low:1	Minor:2
General	A12 (c)	Possible:2	Medium:2	Major:4
Scenario 1	A12 (c)	Unlikely:1	Low:1	Minor:1
Scenario 2	A12 (c)	Possible:2	Medium:2	Major:4
Scenario 3	A12 (c)	Possible:2	Medium:2	Major:4
Scenario 4	A12 (c)	Possible:2	Low:1	Minor:2
General	A13	Possible:2	Medium:2	Major:4
Scenario 1	A13	Possible:2	Medium:2	Major:4
Scenario 2	A13	Likely:3	High:3	Critical:9
Scenario 3	A13	Possible:2	High:3	Critical:6
Scenario 4	A13	Unlikely:1	Medium:2	Minor:2
General	A14	Unlikely:1	High:3	Minor:3
Scenario 1	A14	Unlikely:1	Medium:2	Minor:2
Scenario 2	A14	Unlikely:1	Medium:2	Minor:2
Scenario 3	A14	Possible:2	Low:1	Minor:2
Scenario 4	A14	Unlikely:1	Low:1	Minor:1
General	A16	Possible:2	Medium:2	Major:4
Scenario 1	A16	Likely:3	Low:1	Minor:3
Scenario 2	A16	Likely:3	Medium:2	Critical:6
Scenario 3	A16	Likely:3	Medium:2	Critical:6
Scenario 4	A16	Possible:2	Low:1	Minor:2

4, launching the attack A15 is very difficult and as a result, associated risk is at minimum level. The rest of risk analysis of attacks in the infrastructure is given in details in Table 6.6.

6.2.5 Monitor and Review

This module plays a significant role in the risk assessment framework. We concluded from above risk assessment that the risk of an attack is not constant due to different likelihood and its impact, therefore, it changes for every context of VANET. The main objective of this module is the continuous monitoring of the network to reduce the overall risk of an attack. Further, the likelihood and impact of an attack can change abruptly based on the highest motivation, upgraded equipment etc of an attacker. Thus the risk values of the attacks may change over the time. Therefore, this module is helpful in reviewing the current risk and updated risk of an attack.

6.2.6 Discussion

In this chapter, we performed risk assessment in various contexts to identify attacks with critical risk. Our context-based risk assessment showed that the same attack can have different risks in different context and scenarios.

In order to evaluate our trust models under adversary conditions, different attacks can be integrated in TEAM framework. In order to do so, we implemented man-in-the-middle (MITM) attacks in TEAM framework as a baseline attack due to its major and critical risk evaluation in most of the contexts in VANET. Further, Table 3.5 also suggests that most of the current trust models are evaluated under different forms of MITM attacks. In the next section, we focus on the details of man-in-the-middle attacks where the network efficiency is evaluated in presence of such attackers.

Table 6.6: Context-based Risk Analysis for Attacks in Infrastructure

Context	Attacks (A)	Likelihood (L)	Impact (I)	Risk (R)
General	A8	Unlikely:1	High:3	Minor:3
Scenario 1	A8	Unlikely:1	Low:1	Minor:1
Scenario 2	A8	Unlikely:1	Medium:2	Minor:2
Scenario 3	A8	Possible:2	High:3	Critical:6
Scenario 4	A8	Unlikely:1	Low:1	Minor:1
General	A9	Possible:2	Medium:2	Major:4
Scenario 1	A9	Possible:2	Medium:2	Major:4
Scenario 2	A9	Likely:3	Medium:2	Critical:6
Scenario 3	A9	Possible:2	Medium:2	Major:4
Scenario 4	A9	Unlikely:1	Medium:2	Minor:2
General	A10	Likely:3	High:3	Critical:9
Scenario 1	A10	Possible:2	Medium:2	Major:4
Scenario 2	A10	Likely:3	High:3	Critical:9
Scenario 3	A10	Possible:2	Low:1	Minor:2
Scenario 4	A10	Possible:2	Low:1	Minor:2
General	A11	Possible:2	High:3	Critical:6
Scenario 1	A11	Unlikely:1	Medium:2	Minor:2
Scenario 2	A11	Possible:2	High:3	Critical:6
Scenario 3	A11	Possible:2	Medium:2	Major:4
Scenario 4	A11	Unlikely:1	Low:1	Minor:1
General	A12 (a)	Likely:3	Medium:2	Critical:6
Scenario 1	A12 (a)	Possible:2	Medium:2	Major:4
Scenario 2	A12 (a)	Likely:3	High:3	Critical:9
Scenario 3	A12 (a)	Possible:2	Medium:2	Major:4
Scenario 4	A12 (a)	Possible:2	Low:1	Minor:2
General	A13	Possible:2	Medium:2	Major:4
Scenario 1	A13	Possible:2	Medium:2	Major:4
Scenario 2	A13	Likely:3	High:3	Critical:9
Scenario 3	A13	Possible:2	High:3	Critical:6
Scenario 4	A13	Unlikely:1	Medium:2	Minor:2
General	A14	Unlikely:1	High:3	Minor:3
Scenario 1	A14	Unlikely:1	Medium:2	Minor:2
Scenario 2	A14	Unlikely:1	Medium:2	Minor:2
Scenario 3	A14	Possible:2	Low:1	Minor:2
Scenario 4	A14	Unlikely:1	Low:1	Minor:1
General	A15	Possible:2	Medium:2	Major:4
Scenario 1	A15	Likely:3	Medium:2	Critical:6
Scenario 2	A15	Unlikely:1	Low:1	Minor:1
Scenario 3	A15	Possible:2	High:3	Critical:6
Scenario 4	A15	Unlikely:1	Low:1	Minor:1
General	A16	Possible:2	Medium:2	Major:4
Scenario 1	A16	Likely:3	Low:1	Minor:3
Scenario 2	A16	Likely:3	Medium:2	Critical:6
Scenario 3	A16	Likely:3	Medium:2	Critical:6
Scenario 4	A16	Possible:2	Low:1	Minor:2

6.3 Man-in-the-Middle Attacks

The term "*Man-in-the-Middle*" has been derived from basketball scenario where a player in the middle tries to intercept the ball while other two players try to pass it [168]. The same concept is derived in VANET, where MITM attacker jeopardize communication and modify messages among legitimate vehicles. Such attacks leave severe consequences on the network, especially, if the content of message contains safety related information. In VANET, the attacker must satisfy following two conditions in order to implement MITM attack, i.e., (1) Firstly, the message containing significant information must be received by the attacker node, and (2) Secondly, the attacker must be able to interpret the content of message. MITM attacks in VANET can be launched under following two modes as depicted in Figure 6.4.

1. *Passive Mode:* Passively, the attacker can eavesdrop on the communication channel between legitimate vehicles, e.g., law-enforcement vehicles.

2. *Active Mode:* Actively, the attacker can drop, delay or change the content of received information in the network.

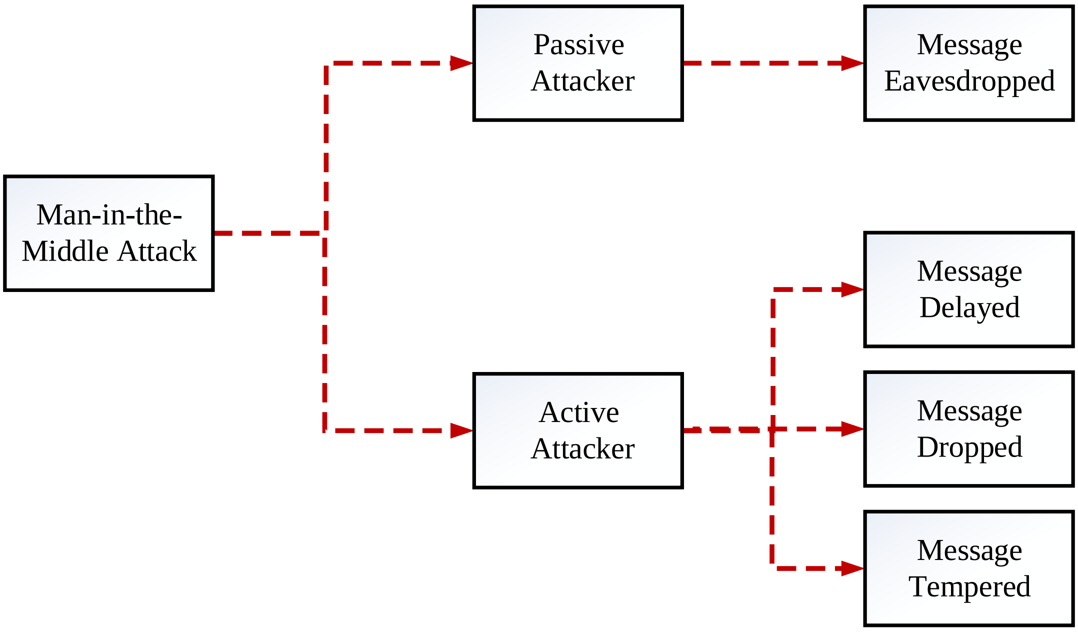


Figure 6.4: Man-in-the-Middle Attacks in VANET

When an event occurs in VANET, the transmitted packet from message generated vehicle contains two important information, i.e., (1) data regarding the event and (2) the time of the event occurrence. Actively, attacker can launch MITM in following three manners:

1. Delay the legitimate message

2. Drop the legitimate message

3. Temper the legitimate message

6.3.1 MITM as Message Delayed

The success of VANET relies on the successful transmission of messages to every legitimate vehicle. In this attack model, the malicious nodes deliberately delays the messages it receive, i.e., the messages are forwarded to neighbour nodes with a factor of 'delay'. Due to sensitive nature of the messages in VANET, delaying such messages can create disaster in the network. For instance, consider a scenario where legitimate vehicles are sharing information about steep-curve during night. Delaying such message by malicious node can result in extreme situation, where, the legitimate vehicles are unable to receive this messages on time. Therefore, such vehicles have to take step in real-time to avoid an accident scenario. Further, this situation can also put the human life in danger. High level pseudo code of MITM attack as message delaying is shown in Algorithm 1. It shows that malicious attacker always introduces a delay in transmitting the messages towards legitimate vehicles.

Algorithm 1 Message Delay Attack

```
Input: Legitimate Message $M_G$
Output: Attacked Message $M_A$
if ($Received\ Message == M_G$) then
    Check 'content' of $M_G$
    if ($content ==$ "$data''$") then
        Introduce delay ($d$) in $M_G$
    end if
    Transmit $M_G$ at time ($t_{send} + d$)
end if
```

6.3.2 MITM as Message Dropped

This type of attack also refers to “black hole” attacks in VANET, where attacker intentionally drops the received legitimate message (M_G), thus suppressing the further propagation of M_G [169]. Hence, this action of the attacker prohibits the legitimate vehicles to receive any kind of message (safety and non-safety) as the messages never reaches to their destination. Dropping the safety-related messages can have significant impact on the network as it contains sensitive information such as collision avoidance. As an illustration, consider a scenario where legitimate vehicles are broadcasting the messages regarding black-ice on the road. Dropping such information can put the life of vehicular users in danger as they are prohibited from receiving sensitive information by the attacker. Pseudo code of message dropping action of MITM is given in Algorithm 2. It shows that whenever a message is received at the malicious node, it is always lost as the messages are dropped by the attacker.

Algorithm 2 MITM as Message Drop

```
Input: Legitimate Message $M_G$
Output: Attacked Message $M_A$
if ($Received\ Message == M_G$) then
    Check ‘content’ of $M_G$
    if ($content ==$ “$data''$”) then
        drop $M_G$
    end if
end if
```

6.3.3 MITM as Message Tempered

In this attack, the attacker particularly targets the content of the received message. Whenever a message is received at the malicious node, attacker changes the content of the message. This form of attack has severe impact on the network as the content may contain sensitive information. For instance, legitimate vehicle broadcast a message during heavy rain that “there is steep-curve ahead, slow down”. The message is received at the attacker node, where the content is intentionally altered to “there is no steep-curve, speed up”. This message is misleading for the legitimate vehicles and it can create disaster (such as accident occurrence) in the network.

Further, every transmitted message in VANET contains three important information, i,e, (1) data, (2) time, and (3) location. In this attack, the attacker have the ability to change "data", "transmission time" or "transmission location". Each of this alteration have different impact on the network. Algorithm 3 summarizes the pseudo code for message alteration attack. It shows that attacker can change,

- "data" into misleading "compromised data"
- "transmission time" into compromised transmission time by changing it with garbage time t_g
- coordinates of sender location ($loc(x, y, z)$) into unknown location ($loc(x_a, x_b, x_c)$)

Algorithm 3 Message Alteration Attack

```
Input: Legitimate Message $M_G$
Output: Attacked Message $M_A$
if ($Received\ Message == M_G$) then
    Check 'content' of $M_G$
    if ($content ==$ "$data''$) then
        change "data" to "garbagedata"
    end if
    if ($transmission\ time ==$ "$t_s''$) then
        change "$t_s''$ to "$(t_s + t_g)''$
    end if
    if ($sender\ location ==$ "$loc(x, y, z)''$) then
        change "$loc(x, y, z)''$ to "$loc(x_a, x_b, x_c)''$
    end if
    Transmit $M_A$ at time ($t_{send}$)
end if
```

In this thesis, we implemented the above three versions (message delay, message drop, message alter) of the MITM attack. It is worth mentioning that MITM nodes can violate integrity, authentication, confidentiality and availability security requirement for VANET. Further, to evaluate the impact caused by these attacks, we considered two different strategies of attackers performing MITM.

1. First, the attackers are distributed randomly across the network

2. Second, the attackers exist in fleet structure where the attacks are launched in a collaborative manner.

Figure 6.5 highlights the difference of attacker pattern in the network. In the next section, we describe the simulation environment for these MITM attacks in VANET.

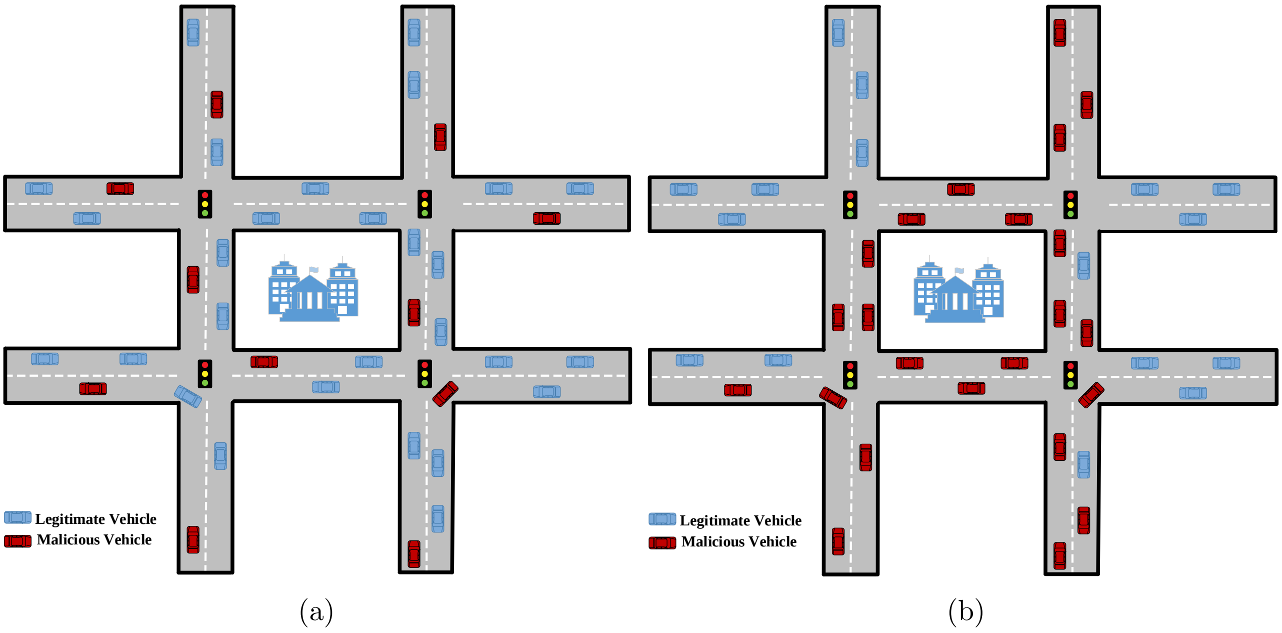


Figure 6.5: Attacker Pattern (a) Distributed (b) Fleet

6.3.4 Simulation Environment

6.3.4.1 Simulation Setup

The core objective of our simulation is to study performance of the vehicular networks in presence of malicious nodes performing MITM attacks. To facilitate our simulations, we used Veins [2, 119]. Veins is an open source framework which is used widely for simulations of vehicular networks. Veins is built on top of two popular simulators: SUMO (traffic simulator) [122] and OMNET++ (discrete event simulator) [111]. SUMO provides traffic patterns for specific realistic map while OMNET++ provides various modules (application layer, DSRC and PHY layer) to ensure realistic network behavior. A small patch TraCI is used for communication between OMNET++ and SUMO [129]. Whenever, an event (accident information) is triggered in OMNET++, TraCI enables the vehicles in SUMO to change their route by sending out respective commands.

6.3.4.2 Simulation Scenario Setup

To evaluate MITM attacks in VANET, we used the default map in Veins. Further, we introduced 100 vehicles in the network which are enough for many urban scenarios [170]. We then injected 10%, 20%, 30%, 40% and 50% malicious nodes in the network respectively to study the impact caused by such attackers. Different parameters to perform simulations is described in Table 7.1. To study the attacker pattern, we created two scenarios:

1. **Scenario 1:** Attackers are distributed randomly across the network, and
2. **Scenario 2:** Attackers are present together in a fleet structure.

In scenario 2, we polluted network with 'N' malicious nodes in such a way that they obliged specific pattern in the network, i.e., $N/3$ MITM nodes exist near the event occurrence, $N/3$ in the center of the network, while the rest of the MITM nodes ($N/3$) are located at the end of the network.

6.3.4.3 Performance Evaluation Metrics

In order to evaluate the performance of VANET in presence of attackers, we implemented following evaluation criteria which can evaluate the MITM attacks in VANEET. These are:

- **End-to-End Delay:** This metric is related to QoS of the network, indicating the delay caused to packet generated by legitimate node to be shared with neighbouring nodes. E2ED is the difference of packet generation time (T_G) and packet reception time (T_R) which is calculated as follows:

$$E2ED = T_R - T_G \tag{6.4}$$

Table 6.7: Simulation Details

Parameter		**Value**
Simulation Framework	Network Simulator	OMNET++ 5.0
	Traffic Simulator	SUMO 0.25.0
	V2X Simulator	VEINS 4.4
Simulation Details	No. of Vehicles	100
	No. of RSUs	5
	No. of Malicious Nodes	10%, 20%, 30%, 40%, 50%
	Simulation Time	1000 sec
	Accident Start time	75 sec
	Accident Duration	50 sec
	Communication Range	250 m
	Vehicle Maximum Speed	13.9 km/h
	Total Simulation Runs	25 times
Protocols	MAC Protocol	IEEE 802.11p
	Network Protocol	IEEE 1609.4 (WAVE)
	Radio Propagation Model	Simple Path Loss
	Data Size	1024 bits
	Header Size	256 bits

- **Content Delivery Ratio (CDR):** Content delivery ratio shows the amount of messages which are received successfully by the legitimate vehicles [171]. Let M_R are the number of received messages and M_{PRE} are the number of messages which are expected to be received within the network, then CDR is given as:

$$CDR = \frac{M_R}{M_{PRE}} \tag{6.5}$$

Let 'N' is the total number of vehicles which are transmitting 'M_{TRANS}' messages, then M_{PRE} is calculated as:

$$M_{PRE} = N \times M_{TRANS} \tag{6.6}$$

- **Packet Loss Ratio (PLR):** Packet loss ratio shows the amount of the messages which are lost due to MITM nodes. Let M_T are the total number of messages, out of which M_L messages are lost, then PLR is given as:

$$PLR = \frac{M_L}{M_T} \tag{6.7}$$

M_T includes messages which are received at both legitimate and malicious nodes. Let M_R is the number of received messages at legitimate nodes and M_L is the amount of messages lost at the MITM nodes, then M_T is given as:

$$M_T = M_R + M_L \tag{6.8}$$

- **Number of Compromised Messages:** This metric indicates the number of messages compromised (either tempered or delayed) from the malicious node.
- **Number of Dropped Messages:** This metric is defined for MITM which is dropping the messages received from legitimate nodes. This metric shows the amount of messages dropped by the attackers in the network.

6.3.5 Results and Discussion

This section is dedicated to discuss the results of MITM attacks in VANET. We simulated MITM attackers according to above two scenarios (distributed attackers and fleet of attackers) and evaluated network efficiency based on the evaluation metrics listed in section 6.3.4.3.

Further, each simulation scenario is carried out twenty-five times with random seed value to ensure unique initial vehicle assignment within the network every time. Moreover, the simulation results presented below are the average of twenty-five runs for each simulation scenario.

6.3.5.1 Message Delay Attacks

Figure 6.6 shows end-to-end (E2E) delay in the presence of MITM which are delaying the packets by 2 seconds. It can be seen that the E2E delay increases when the network is introduced with such malicious nodes which are delaying the legitimate messages. Ideally, the legitimate vehicles should receive such legitimate messages with minimum delay, however, MITM attackers with message delaying capability prohibits the legitimate nodes to receive the messages in time. Further, this figure also depicts that E2E delay increases when the attackers are distributed throughout the network. Since, a wide portion of the network is affected due to distributed attackers, therefore, the overall E2E delay increases in the network. On the other hand, attackers in fleet are only delaying the packets at certain locations. As a result, network experience low E2E delays in presence of attackers in fleet structure. Further, it can also be seen that for 10% malicious nodes, the network with distributed attackers achieve about 47.94% high E2E delays than the network containing fleet malicious nodes. This delay further increases to 73.44% when the network is injected with 50% malicious nodes.

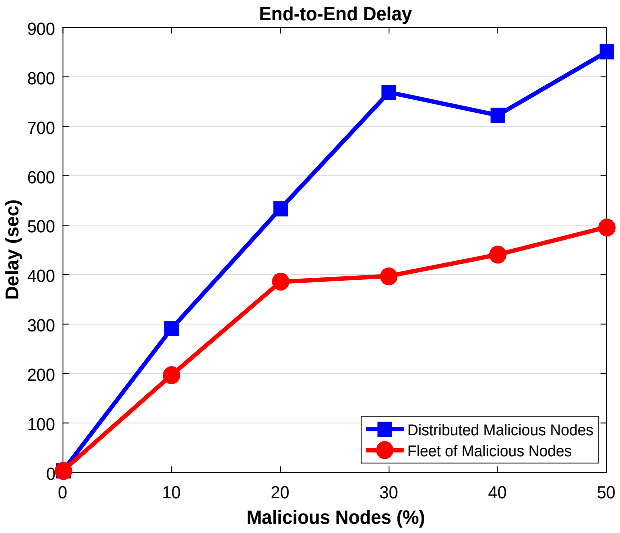


Figure 6.6: End-to-End Delay

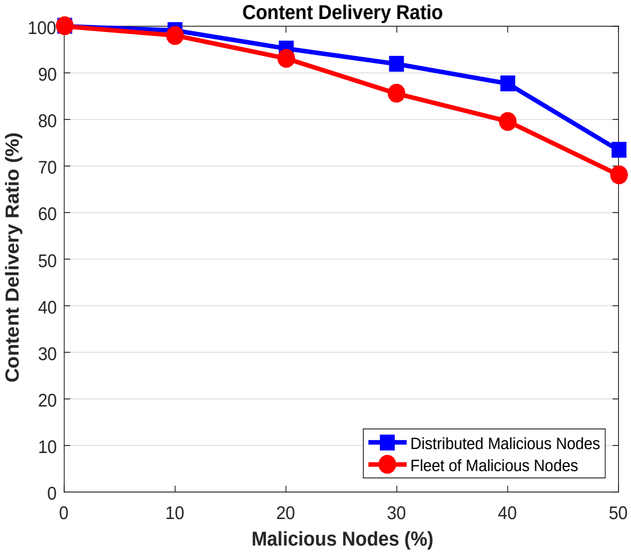


Figure 6.7: Content Delivery Ratio

Next, the amount of content delivered in the network is depicted in Figure 6.7, showing that content can be delivered to the legitimate vehicles in presence of MITM attackers with delaying capabilities. This metric indicates that the messages arrived at the legitimate nodes but with certain delay. Further, high CDR is achieved in the network in presence of distributed malicious nodes, while, the network with fleet of malicious nodes attains low CDR. This is due to the fact that fleet of malicious vehicles are delaying the packets together, thus, high number of packets are delayed in such locations and as a result, the legitimate vehicles receives the content but not in time.

Figure 6.7 also suggests that for 10% malicious nodes, the network containing distributed malicious nodes achieve about 1.1% high CDR as compared to the network with attackers in fleet pattern. Moreover, the network with distributed malicious nodes achieves about 7.8%

high CDR than the network with fleet attackers. Thus, fleet vehicles affect the network more by delivering less amount of content.

Further to the above discussion, the number of compromised messages generated by the malicious nodes is depicted in Figure 6.8. It can be seen that the number of compromised messages increases with the increase in malicious nodes in the network. However, high number of messages are compromised by the fleet malicious nodes than distributed malicious nodes. The attackers in fleet are working together to delay the messages, thus, higher number of messages are delayed and compromised. For instance, for a network containing 10% attackers, fleet malicious nodes compromises about 4.43% messages than distributed attackers. The compromised messages increases to 12.23% when the network is polluted with 50% attackers. This shows that high number of messages are compromised in presence of attackers in fleet structure as the attackers are compromising the messages in a collaborative manner.

Packet Loss Ratio (PLR) in presence of malicious nodes in depicted in Figure 6.9. It shows that PLR increases with the increase in the malicious nodes in the network. However, the presence of fleet attackers deteriorates the network more as high number of packets are lost by such attackers. This is due to the fact that fleet attackers compromises high number of messages, therefore, the resulting network experience high packet loss. On the other hand, presence of distributed malicious nodes also results in packets loss, but, the resulting packet loss is less than the fleet attackers. For instance, when the network is flooded with 50% malicious nodes, about 23.75% more packets are lost in presence of fleet attackers as compared to distributed attackers.

6.3.5.2 Message Drop Attacks

Content delivery ratio in case of message drop attacks is presented in Figure 6.10, depicting that CDR decreases with the introduction of malicious nodes in the network. Further, the network assures high number of content when it is polluted with fleet of malicious attackers. Since, the attack vector of such attacker is limited to specific location, therefore, content is lost only in that location. The nodes may be able to receive messages from other legitimate nodes

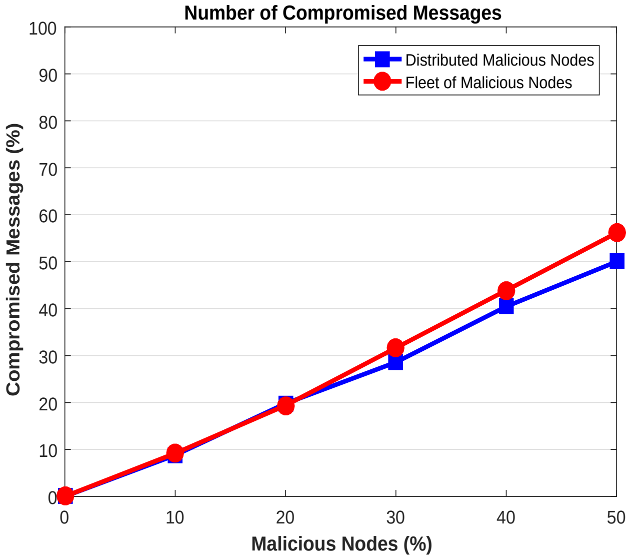


Figure 6.8: Compromised Messages

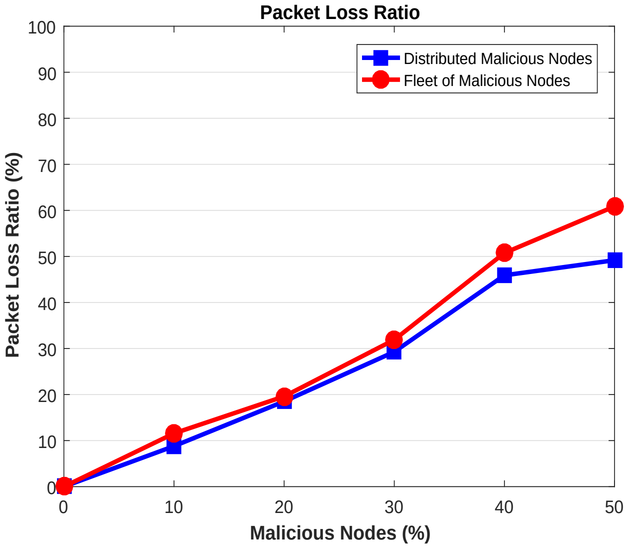


Figure 6.9: Packet Loss Ratio

within its neighbourhood. On the other hand, the scope of distributed malicious attackers is not limited to specific location, hence, low CDR is achieved in this scenario.

Further, as mentioned earlier, CDR decreases when the malicious nodes are introduced in the network. Specifically, low CDR is achieved in presence of distributed malicious nodes with the capability to drop legitimate packets. For instance, when the network contains 10% attackers, the network with fleet malicious nodes attain about 12.44% higher CDR than the network with distributed malicious nodes. However, by increasing the ratio of malicious nodes to 50%, network with fleet attackers achieves 44.89% high CDR than the distributed malicious nodes. This is due to the fact that significant amount of messages are dropped by distributed malicious vehicles as they are spread throughout the network. Therefore, content is always lost the vicinity of such attackers. On the other hand, in case of fleet attackers, content is only dropped in specific locations of the network, while, the network where attackers not present can share messages with their neighbouring vehicles.

Next, the number of dropped messages by malicious nodes is shown in Figure 6.11, suggesting that high number of messages are dropped when the ratio of malicious nodes is increased in the network. Both attacker patterns (distributed and fleet) have high impact on the network in terms of the amount of messages dropped in the network, i.e., both distributed and fleet attackers drops almost similar number of messages. However, the network with fleet attackers

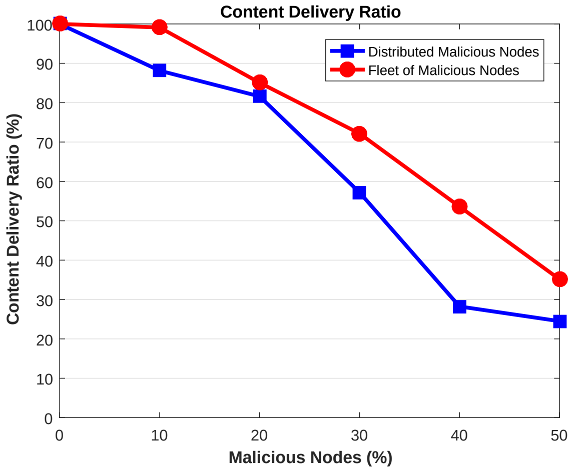


Figure 6.10: Content Delivery Ratio

achieve a little higher packet drop rate than distributed attackers due to their collaborative nature of attack launching. Increasing such attackers increases the drop rate of the messages in the network. For example, for 50% attackers in the network, fleet attackers drop 4.60% more packets than distributed attackers.

Though, almost both fleet and distributed attackers results in dropping the packets in the network, its impact can be elaborated more via packet loss ratio in Figure 6.12. This shows that the network with distributed malicious nodes results in high number of lost packets. As the attack-vector of the distributed malicious nodes is exposed to wide area of the network, therefore, increasing such malicious nodes results in high PLR. For instance, for a network with 10% malicious nodes, network with distributed attackers experience about 11.31% high PLR than fleet attackers. This ratio increases to 44.67% when the network is flooded with 50% malicious nodes.

6.3.5.3 Message Temper Attacks

As described above, the malicious node can either alter data, time or location of the legitimate message. In this particular attack, we focused on the data of the message. Thus, whenever an attacker received a message, the content is tempered by this malicious nodes into garbage data which is then shared with the neighbouring vehicles.

Figure 6.13 shows the end-to-end delay of the network in presence of the malicious nodes which

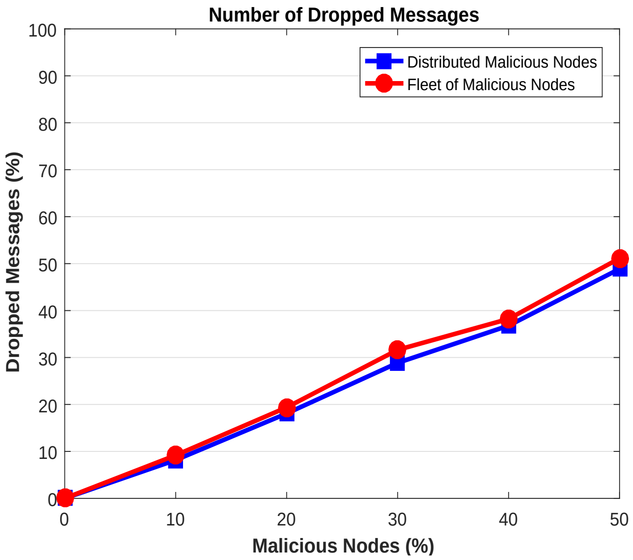


Figure 6.11: Dropped Messages

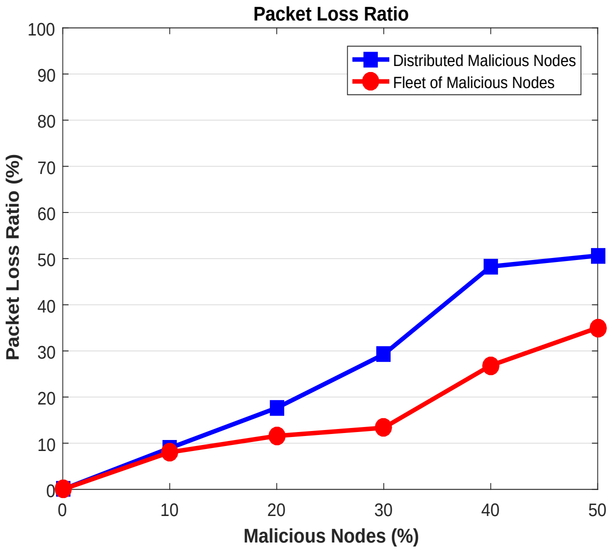


Figure 6.12: Packet Loss Ratio

are changing the content of the messages. First, it can be seen concluded that E2E delay of the network increases with the increase in malicious nodes. Second, high E2E delay is achieved by the network in presence of distributed malicious nodes due to their wide spread attack scope. On the other hand, fleet of malicious nodes are launching attacks which are limited to specific location, therefore, the low E2E delay is achieved as legitimate messages are shared in a large section of the network. As an illustration, for a network with 50% malicious nodes, network containing distributed attackers achieves 69.91% high E2E delays than fleet attackers.

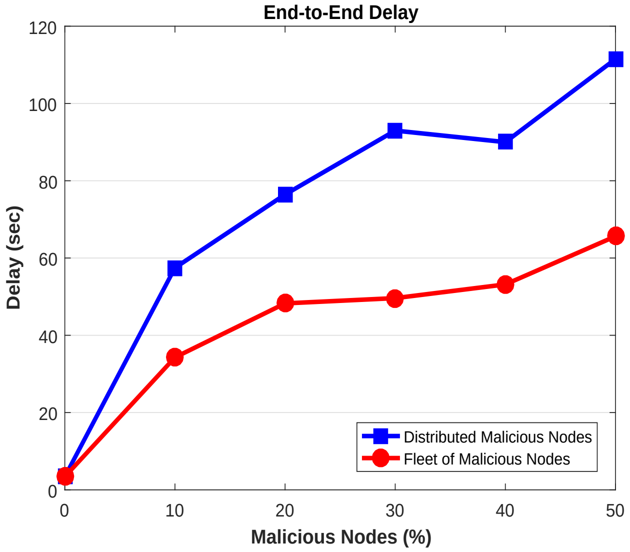


Figure 6.13: End-to-End Delay

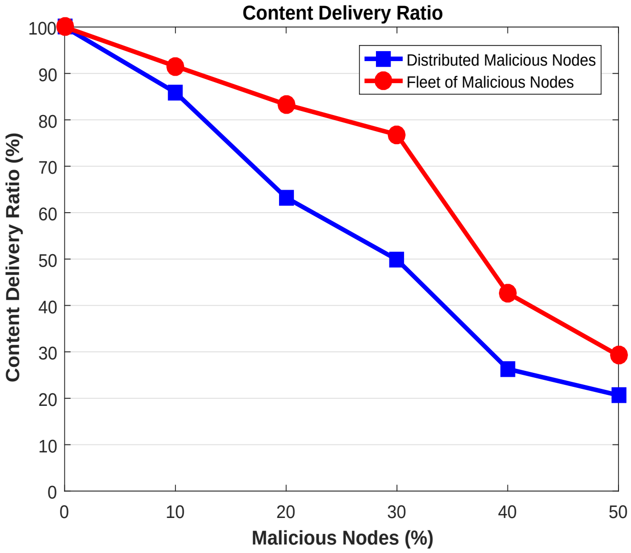


Figure 6.14: Content Delivery Ratio

The ability of the network to transmit legitimate messages within the network via CDR is depicted Figure 6.14. It shows that CDR decreases when the number of malicious nodes increases within the network. As the malicious nodes are changing the content of the legitimate messages, therefore increasing such malicious nodes results in low values of CDR as the ratio of garbage data increases within the network. Further, the attack pattern also affects CDR. It can be seen that when the network contains attackers in fleet, high CDR is achieved as compared to distributed malicious nodes. This is due to the fact that fleet of attackers are located in particular section of the network, thus, only a portion of the network is affected by these attacks. In the meantime, legitimate messages are transmitted between the nodes in large section of the network, thus high CDR is achieved. On the other hand, due to wide-spread attack vector of the distributed malicious nodes, large section of the network is affected. As a result the network achieve low CDR values. Further, figure also depicts that for 50% malicious nodes, the network with fleet attackers achieves about 41.48% high CDR as compared to distributed attackers.

Next, the number of compromised messages is shown in Figure 6.15. It can be seen that the high number of messages are tempered and compromised in presence of high number of malicious nodes. Further, high number of messages in the network are in compromised state in presence of fleet of malicious nodes. As the attackers are launching attack together, therefore, network is affected more in presence of such attackers. For 50% malicious attackers, the network with fleet vehicles are compromising about 12.23% more packets than distributed attackers.

The impact of the attackers on the network in terms of lost packets in depicted in Figure 6.16. Ideally, small value of PLR is desired. Figure shows that network is affected more when malicious nodes are increased within the network. Moreover, the attack pattern of the malicious nodes also results in different PLR. The distributed malicious nodes affect the network more as high PLR is achieved in the network. As mentioned earlier, these attacker have high impact on the network due to their wide-range of attack vector. As a result, high number of legitimate packets are lost within the network. On the other hand, fleet of attacker are only targeting at the specific portion of the network, thus, packets are lost in such location only. For 50% distributed attackers, the network experience about 6.89% more lost as compared to the network containing fleet attackers.

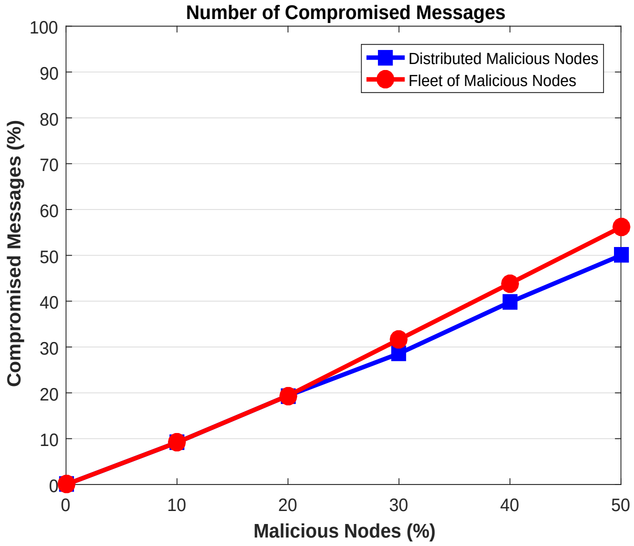


Figure 6.15: Compromised Messages

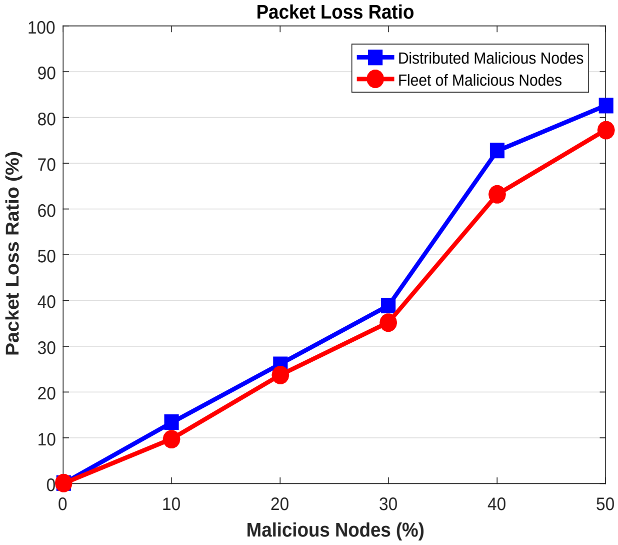


Figure 6.16: Packet Loss Ratio

From above results, we can conclude that the network efficiency decreases when attackers are introduced within the network. We implemented three flavours of MITM attacks in VANET to study the impact caused by these attackers. Results suggest that these attacks have massive impact on the network in terms of low content delivery, high end-to-end delay, compromised messages and packet loses.

The success of VANET relies on message transmission in safe and trusted environment. In the context of trust evaluation and management framework, Man-in-the-middle attacks are suitable for the evaluation of trust models as these attack can delay or drop or alter the messages. Since, trust models rely highly on the received messages from neighbouring vehicles, therefore, these attack models can be used as the baseline attacks in TEAM framework.

6.4 Summary

In this chapter, we proposed and performed the context-based risk assessment where we identified and categorized the attacks according to their severity levels. Further, we chose MITM attacks as the baseline attack for the evaluation of TEAM framework due to their high severity in the network. Therefore, we implemented different MITM attacks in VANET, where we evaluated the network in presence of malicious nodes based on two attack patterns. This chapter refers to module 1 and module 2 of the TEAM framework. In the next chapter, we explained the simulation model of VANET and TEAM framework which is implemented using veins simulation framework. Veins is implemented further on two simulators, i.e., OMNET++ and SUMO. Further, in the context of this thesis, we identified several attacker models which are used for the evaluation of the trust models in VANET.

Chapter 7

Performance Evaluation of TEAM Framework

Chapter 5 explained the simulation model developed for the implementation of trust evaluation and management framework. The aim of this chapter is to present the results of TEAM framework which are generated via simulation model. Results are presented in two modes. First, the results of the three trust models are presented for a general scenario. Second, we present the results for context-based VANET, where the performance of the trust models are evaluated for four scenarios based on the mobility.

This chapter is organized as follows. First, we provide the details of the evaluation metrics which are used to evaluate the performance of trust models. Then, the details of the considered attacker model is presented. Last, we present our results for both general and context-enabled VANET.

7.1 Evaluation Metrics

In order to evaluate trust models quantitatively, we defined following metrics which focuses particularly on the security and QoS of the trust models.

7.1.1 End-to-end Delay (E2ED)

This metric is related to QoS of the trust model, which depicts the delay caused to packet, generated by legitimate node to be shared with neighbouring nodes. E2ED is the difference of packet generation time (T_G) and packet reception time (T_R) which is calculated as follows:

$$E2ED = T_R - T_G \tag{7.1}$$

7.1.2 Event Detection Probability (EDP)

This metric is defined to identify true events in the network. In case of VANET containing sensitive information, identifying correct event (messages) are of extreme importance. EDP is defined to identify such events. Trust models should have capability to detect true events efficiently. Let E_{Tot} represents total events generated, out of which E_T and E_M are true and malicious events respectively, then probability of detecting true event (EDP) can be represented by:

$$EDP = \frac{\sum(E_{Tot} - E_M)}{E_{Tot}} \tag{7.2}$$

7.1.3 Anomaly Ratio (AR)

This ratio is defined to identify anomalies and malicious activity in the network. Based on the information provided by the sender, the evaluator node can identify the behavior of transmitting node. Upon detection of malicious activity in the network, the evaluator node shares this information with its neighbouring nodes. Higher the AR ratio, higher the node have ability to detect malicious node in the network [172]. AR is defined as the ratio of malicious packets to the total generated messages. Let sender S generates total $M_T(S)$ messages, $M_M(S)$ represents those packets which are tempered and compromised by the sender, then, AR ($\eta(S)$) can be represented as follows.

$$\eta(S) = \frac{M_M(S)}{M_T(S)} \tag{7.3}$$

7.1.4 Trusted & Untrusted Packets in the network

These statistics show the amount of trusted and untrusted packets generated within the network. Let N_{Total} is the total number of packets generated by the nodes in the network. Out of N_{Total} packets, $N_{Trusted}$ are the trusted packets and $N_{Untrusted}$ are the untrusted packets. Then we calculate trusted and untrusted packets as follows in equation 7.4 & 7.5:

$$N_{Trusted} = \sum(N_{Total} - N_{Untrusted}) \tag{7.4}$$

$$N_{Untrusted} = \sum(N_{Total} - N_{Trusted}) \tag{7.5}$$

7.1.5 False Positive Rate (FPR)

FPR represents the capability of trust model to identify those malicious messages which are incorrectly identified as legitimate nodes. The trust models should have less FPR values. Let $P_{M|L}$ represents the probability of detecting node as malicious, given the node is legitimate, and $P_{L|L}$ is the probability of detecting node as legitimate, given the node is legitimate, then FPR is mathematically written as:

$$False\ Positive\ Rate = \frac{P_{M|L}}{P_{L|L} + P_{M|L}} \tag{7.6}$$

7.2 Considered Adversary Model

In order to evaluate performance of TMs in presence of attackers, we considered man-in-the-middle attacks (MITM) as an adversary model for TEAM framework which is identified via threat model (module 1) and risk assessment (module 2) of the framework. According to risk assessment, MITM poses critical risk in VANET, therefore, we considered MITM attack with the ability to alter and delay sensitive (i.e., accident) information by a factor of “d” seconds. Since, very sensitive information (such as collision avoidance) is shared among vehicles in VANET, therefore, tempering such data can have severe impact on the network. Further, delaying such sensitive data prohibits the legitimate vehicles to receive information on-time. The designed adversary model is equipped with both of these capabilities. In order to demonstrate TEAM framework, three trust models are evaluated in presence of such MITM attackers.The high level pseudo code of considered adversary model is depicted in Algorithm 4. It can be seen that whenever message arrives at the MITM attacker, the attacker first creates an attacked message M_A, where the content is first altered using specific alteration function. In the next phase, delay is calculated at the attacker node which is then appended to the altered message. At this stage, the attacker broadcast the message which is then received by the legitimate vehicles in its vicinity.

Algorithm 4 Message Alteration and Delay Attack (A_{MAD})

```
Input: Legitimate Message $M_G$
Output: Attacked Message $M_A$
if ($Received\ Message == M_G$) then
    Check ‘content’ of $M_G$
    if ($content ==$ “$data''$) then
        change “data” to “garbagedata”
        Introduce delay ($d$) in $M_G$
    end if
    Transmit $M_A$ at time ($t_{send} + d$)
end if
```

7.3 Evaluation of Trust Models

This section is dedicated to the simulation results of the trust models which are implemented in TEAM framework. The trust models are evaluated in two modes.

1. Evaluation of trust models for general VANET
2. Evaluation of trust models for context-enabled VANET

The simulation results described in this chapter are the mean values of twenty-five simulation runs for every scenario.

7.3.1 Evaluation of trust models for general VANET

In this section, we evaluated the performance of TEAM framework by implementing three different trust models, i.e., entity-oriented trust model (EOTM), data-oriented trust model (DOTM) and hybrid trust model (HTM). The trust models are evaluated under adversary conditions based on the above evaluation metrics. In order to do so, we considered a scenario where we continuously inject malicious nodes in the network and their presence is increased from 10% to 80%. Further, the attackers are mobile and they are continuously changing their location in the network.

Table 7.1 provide the details of various parameters used for the evaluation of TMs. We used a condition that ($\beta = 10 \times \alpha$) based on logic that trust cannot be established easily, i.e, trust is very rare and easy to break. In our simulations, we also kept the initial trust value to 0.5 to avoid the cold start problem [173, 174].

As VANET is a large-scale and open network, it is possible to have an attack which involves high number of malicious nodes, e.g., distributed denial-of-service (DDoS) or worm-hole attack. Therefore, we evaluated the efficiency of TMs in presence of different number of malicious nodes. We first evaluated TMs for 10% malicious nodes, and we then increased the quantity of malicious nodes to 80% with a step of 10%.

Table 7.1: Simulation Details

Parameter		Value
Simulation Framework	Network Simulator	OMNET++ 5.0
	Traffic Simulator	SUMO 0.25.0
	V2X Simulator	VEINS 4.4
Simulation Details	Simulation Area (km × km)	2.5 × 2.5
	No. of RSU	5
	Simulation Time	1000 sec
	Accident Start Time	75 sec
	Accident Duration	50 sec
	Communication Range	250 m
	Total Simulation Runs	25 times
	No. of Legitimate Vehicles	100
	No. of Malicious Vehicles (%)	10, 20, 30, 40, 50, 60, 70, 80
Protocols	MAC Protocol	IEEE 802.11p
	Network Protocol	IEEE 1609.4 (WAVE)
	Radio Propagation Model	Simple Path Loss
	Data Size	1024 bits
	Header Size	256 bits
Trust Model	Initial Trust	0.5
	Trust Threshold	0.5
	Honesty Factor (α)	0.01
	Dishonesty Factor (β)	0.1
Attacker Model	Actions	1) Content Alteration 2) Content Delay
	Delay (d)	2 secs

7.3.1.1 End-to-end Delay

Figure 7.1 depicts E2E delay of three TMs in presence of malicious nodes. It can be seen that among three considered TMs, network achieves high E2E delay for HTM, while, EOTM experience lowest E2E delays. There are two main reasons for this behaviour. First, EOTM integrates role-based and experienced-based trust management schemes which can detect and eliminate malicious vehicles from the network. Second, DOTM and HTM relies on the data for trust evaluation which is continuously delayed by the malicious nodes. This behaviour of attackers prohibits the vehicles to receive messages in-time, thus, leaving a strong impact on the network in terms of high E2E delays.

Next, Figure also suggests that the E2E delay of the network increases when the network is polluted with malicious nodes. Since, one of the characteristics of the considered attacker

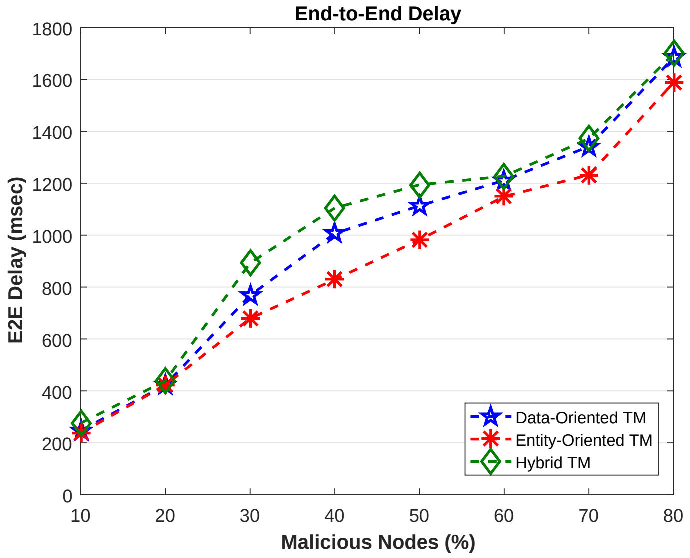


Figure 7.1: E2E Delay vs Attackers

model is to delay the messages by ‘d’ factor, as a result, network experience high E2E delays. This delay further increases when the quantity of malicious nodes are increased in the network. E2ED for EOTM is increased from 237.513 msec to 1587.18 msec, DOTM from 246.82 msec to 1682.74 msec, and 276.072 msec to 1699.35 msec for HTM, when malicious nodes are increased from 10% to 80%. Figure also depicts that nodes utilizing EOTM achieves low E2ED than DOTM and HTM. For instance, when network contains 50% malicious nodes, then EOTM achieves 21.58% less E2ED, while EOTM achives 7.26% than HTM.

7.3.1.2 Event Detection Probability

The ability of the trust models to identify true events in the network can be expressed by determining Event Detection probability (EDP). Since, two types of messages propagates in the network, i,e, (1) legitimate messages which are generated by honest vehicles, and (2) compromised messages which are generated by attackers. Therefore, this metric is helpful in determining the performance of the trust models to detect true events. The capability of three TMs to detect true event is depicted by Figure 7.2. It suggests that EOTM can detect high number of true events than DOTM and HTM. Since, EOTM integrates a role-based trust model, therefore, there is high probability that these nodes provides correct information, resulting in higher detection rates. The presence of such trusted nodes increases the scope of vehicles to detect true events in the network in presence of malicious nodes. For instance, EOTM and DOTM detects 24.36% and 9.82% more events correctly than HTM, if the network contains 50% malicious nodes.

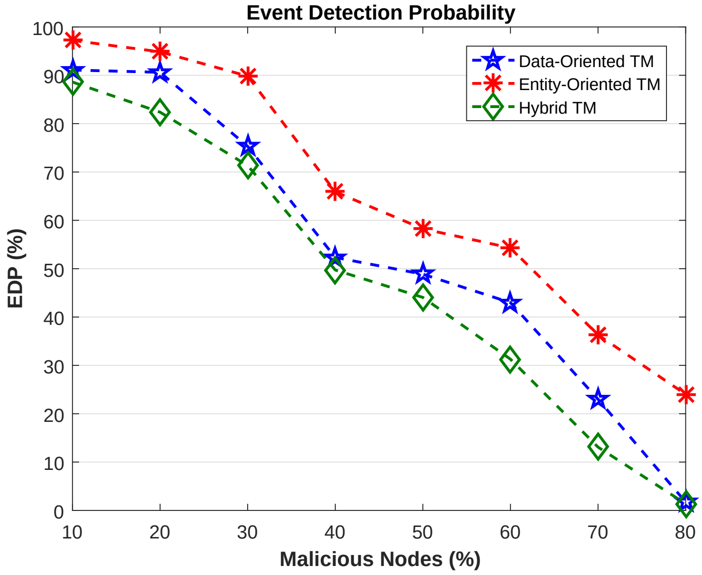


Figure 7.2: Event Detection Probability vs Attackers

Further, figure also depicts that EDP of the network decreases when malicious nodes are introduced in the network. Since, the considered attacker model is changing the content of the legitimate messages. Thus, as the attack vector of malicious nodes increases in the network, the ability of the trust model to identify true messages decreases. For instance, when the adversaries are increased in the network from 10% to 80% in the network, EDP for EOTM decreases from 97.21% to 24.02%, for DOTM, it decreases from 91.09% to 1.722 %, while for HTM, EDP declines from 88.60% to 1.38%.

7.3.1.3 Anomaly Ratio

The ability of trust models to detect anomalies in the network can be expressed via Anomaly Ratio (AR). Figure 7.3 depicts the AR of the three trust models, which suggests two important observations. (1) First, DOTM provides worst result than EOTM and HTM in terms of identifying anomalies in the network. Since, trust establishment in DOTM relies entirely on the received data, which, can be tempered by the malicious nodes. This results in poor performance of DOTM in identifying network anomalies. On the other hand, EOTM relies on highly trusted nodes, i.e., role-based vehicles, which have the ability to identify and revoke malicious entities from the network. Similarly, direct trust evaluation mechanism in HTM also increases the capability of legitimate nodes to identify malicious nodes. For a network with 80% attackers, both EOTM amd HTM performs about 19.2% better than DOTM. (2) Second, Figure 7.3 also depicts that the ability of trust model to detect anomalies in the network decreases when it is flooded with attackers. Less amount of anomalies will be detected by the legitimate nodes in presence of significant number of malicious nodes in the network. As an illustration, when the quantity of attackers are increased from 10% to 80% in the network, then AR for HTM and EOTM is decreased from 90% to 21%. For DOTM, AR decreases from 90% to 16.84%, indicating the poor performance of DOTM than EOTM and HTM.

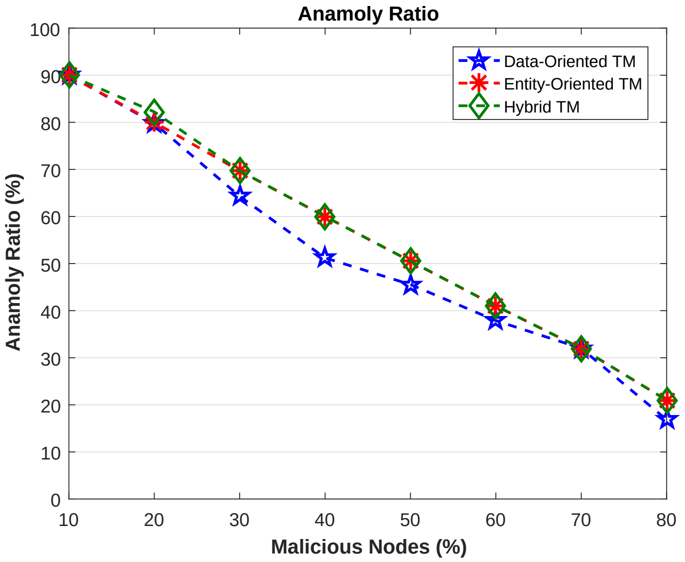


Figure 7.3: Anomaly Ratio vs Attackers

7.3.1.4 False Positive Rate

False positive rate (FPR) illustrate the error margin of the TM where malicious node and its content is incorrectly identified as legitimate. As mentioned earlier, low FPR is desired for a good trust model due to the sensitive nature of the messages. Lower the FPR values, better the trust model is. FPR for the TMs is depicted in Figure 7.4. It can be seen that with the introduction of malicious nodes in the network, FPR increases. Since, attacker is altering and delaying the legitimate messages, therefore, the probability of error margin increases. The attackers provide a limited window of opportunity for legitimate vehicles to communicate with each other. Increasing such attackers in the network increases the probability of incorrectly labelling valid data as malicious. For a network where malicious nodes are increased from 10% to 80%, FPR of EOTM increases from 0.004% to 1.73%, while DOTM and HTM increases from 0.024% to 3.75% and 0.61% to 4.01% respectively. This shows that all implemented TMs achieve low FPR values (less than 4.5%), however, EOTM outperforms HTM and DOTM in terms of FPR, where EOTM achieves lower values than others. As an illustration, for a network with 50% malicious nodes, EOTM and DOTM achieves about 58% and 12% better FPR values than HTM. This is due to the fact that EOTM and HTM includes role-based and direct trust evaluation mechanism respectively, thus reducing the probability to incorrectly detect malicious nodes.

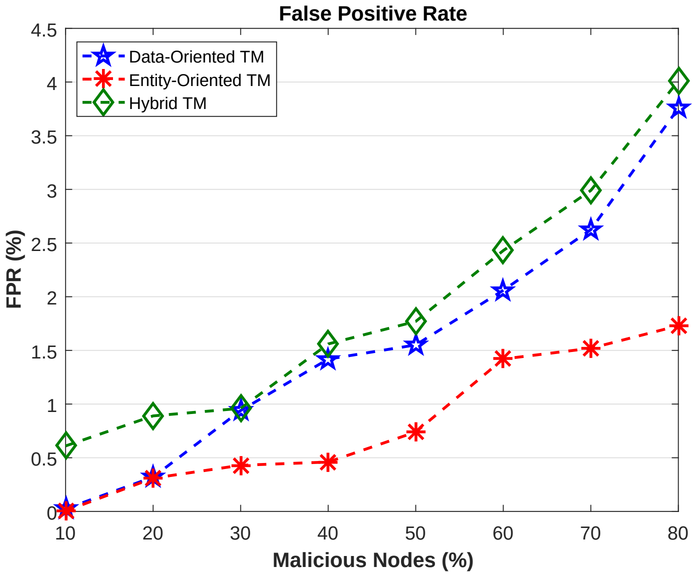


Figure 7.4: False Positive Rate vs Attackers

7.3.1.5 Trusted and Untrusted Packets

It can be seen from Figure 7.5 that when number of malicious entities are increased in the network, trust decreases. In other words, the amount of trusted packets decreases while untrusted packets increases in the network as depicted in Figures (7.5 & 7.6) respectively. Since the attacker model in our simulator is changing the content of the packet before broadcasting, thus resulting in the generation of untrusted information in the network. Thus, the amount of trusted information decreases and untrusted information increases. For instance, the number of trusted packets decreases from 90% to about 20% and the amount of untrusted information increases from 10% to about 80%, when the quantity of malicious nodes are increased from 10% to 80%.

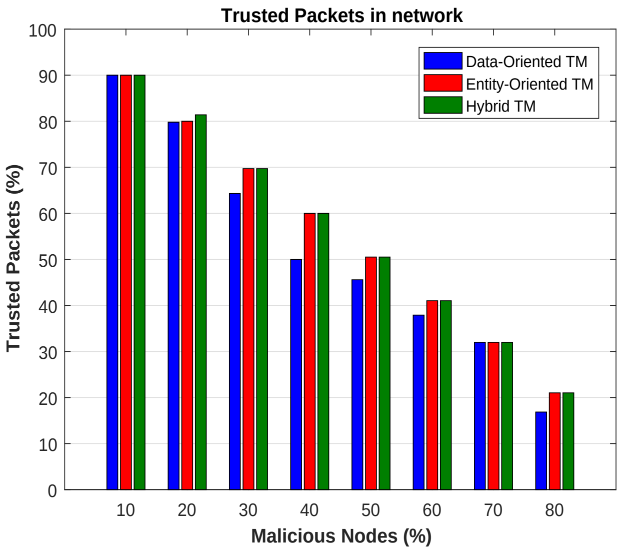


Figure 7.5: Trusted Packets vs Attackers

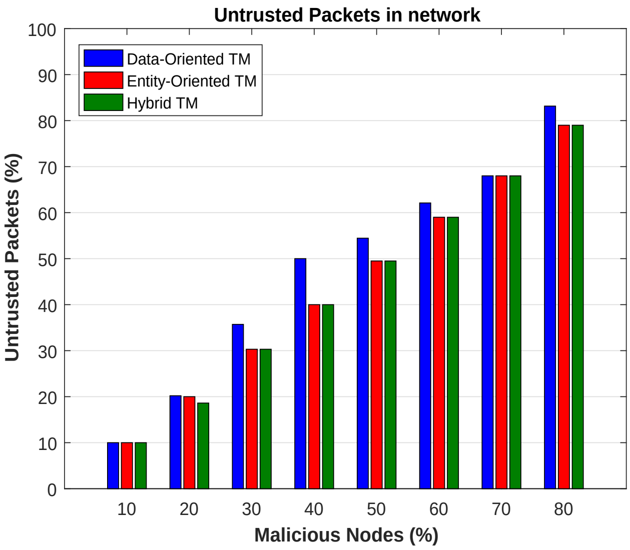


Figure 7.6: Untrusted Packets vs Attackers

Moreover, it is also depicted from Figure 7.5, that the network containing EOTM and HTM ensures more trusted packet than DOTM. Similarly, Figure 7.6 depicts that the network with DOTM contains high number of untrusted packets. Since, DOTM highly relies on the data trustworthiness, which can be tempered by malicious nodes. This results in the loss of trusted packets in the network which is replaced by untrusted packets due to alteration by the attackers. On the other hand, presence of role-based vehicles and direct trust evaluation mechanism of HTM ensures high trust packets.

7.3.2 Evaluation of trust models for context-enabled VANET

We evaluated the performance of TMs using different evaluation criteria which mainly focused on security and QoS of the network as mentioned in section 7.1. Results explained below depict that malicious vehicles deteriorate the performance of TMs in terms of high end-to-end delays, false positive rates and high number of untrusted packets in the network. Moreover, the presence of adversaries also reduces the probability to detect true events, anomalies and generation of trusted packets in the network.

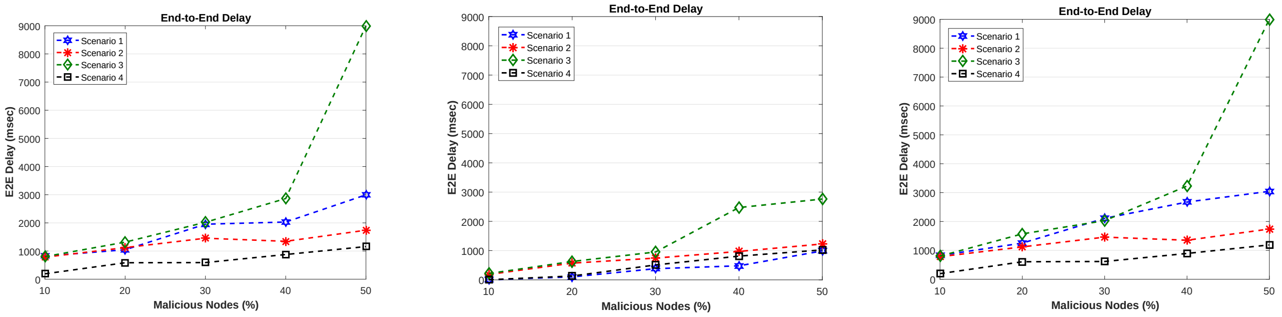
Table 7.2 provide the details of various parameters used for the evaluation of TMs. We used a condition that ($\beta = 10 \times \alpha$) based on logic that trust cannot be established easily, i.e, trust is very rare and easy to break. In our simulations, we also kept the initial trust value to 0.5 to avoid the cold start problem [173, 174].

Table 7.2: Simulation Details for TEAM in context-enabled VANET

Parameter		**Value**
Simulation Framework	Network Simulator	OMNET++ 5.0
	Traffic Simulator	SUMO 0.25.0
	V2X Simulator	VEINS 4.4
Simulation Details	Simulation Area (Urban)	4 km × 2.5 km
	Simulation Area (Rural)	10 km × 8 km
	Simulation Time	1000 secs
	Event Start Time	75 sec
	Event Duration	50 secs
	No. of Legitimate Vehicles	100
	No. of Malicious Vehicles (%)	10, 20, 30, 40, 50
	Total Simulation Runs	25
Protocols	MAC Protocol	IEEE 802.11p
	Network Protocol	IEEE 1609.4
	Radio Propagation Model	Simple Path Loss
	Data Size	1024 bits
	Header Size	256 bits
Trust Model Details	Initial Trust	0.5
	Trust Threshold	0.5
	Honesty Factor (α)	0.01
	Dishonesty Factor (β)	0.1
Attacker Model	Actions	1) Content Alter 2) Content Delay
	Delay (d)	2 secs

7.3.2.1 End-to-end Delay

Figure 7.7a shows E2ED of data-oriented trust model in four scenarios. It can be seen that scenario 4 outperforms other scenarios by achieving lowest end-to-end delay (E2ED). Moreover, static attackers affect the network more rather than mobile attackers. As the impact created by static attackers is limited to a specific geographical location, therefore, increasing such malicious vehicles results in delaying more packets in the network, ultimately increasing the overall E2ED. On the other hand, the scope of attack by mobile attacker is not limited to specific location due to their constant mobility. It is quite possible that legitimate vehicles might receive messages from neighborhood in that specific location. Comparing all scenarios for DOTM, for a network with 50% malicious vehicles, we observed that scenario 1, 2 & 3 attains 61.33%, 96.47% & 98.92% high E2EDs respectively as compared to scenario 4.



(a) (b) (c)

Figure 7.7: End-to-End Delay (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM

Figure 7.7b highlights E2ED for entity-oriented trust model, where network with low mobility is affected significantly by static malicious entries. These malicious vehicles introduce massive delay in the attack-prone area which prohibits the legitimate vehicles to receive messages on time. Increasing static attackers in the network increases the attack vector which results in higher message delay. On the other hand, mobile attackers have high influence on the network with high mobility. Attack vector of such attackers continuously change due to their mobility, thus the impact caused by mobile malicious vehicles is different from static malicious vehicles. From Figure 7.7b, we observe that when a network contains 50% malicious vehicles, scenario 1 performs 19.31%, 64.16% and 3.3% better than scenario 2, 3 and 4 respectively by achieving low E2E delays.

Figure 7.7c represents the E2E delay of the network utilizing hybrid trust model. The performance of HTM is similar to DOTM, where, network achieves highest end-to-end delays in scenario 3 and lowest in scenario 4. HTM integrates both sender reputation and data correctness, thus the evaluator node requires more time to calculate and evaluate trust as these are time intensive processes. From Figure 7.7c, scenario 4 performs 31.6%, 60.9% and 86.7% better than scenario 2, 1 and 3 respectively by achieving lower E2ED.

Table 7.3 highlights end-to-end delay of all trust models, which depicts that EOTM achieves better results than DOTM and HTM by ensuring overall lower E2E delay in the network. This is due to the presence of role-based and highly experienced vehicles which can detect and eliminate dishonest vehicles from the network. On the other hand, DOTM and HTM depends on data for trust evaluation, which is continuously delayed by malicious vehicles. As a result, legitimate vehicles are unable to receive messages in-time, thus leaving a strong impact on the network in terms of high E2E delay.

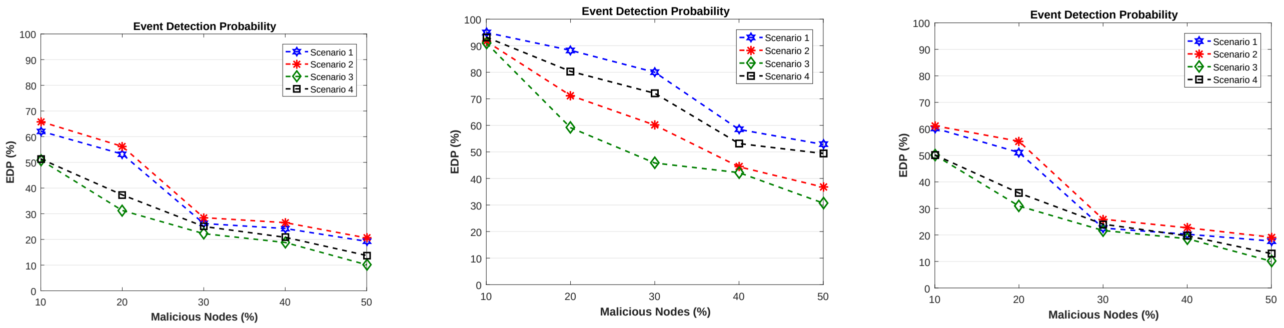
Table 7.3: Comparison of End-to-end Delay

Malicious Nodes (%)	**Scenarios**												**Best Model**
	Scenario 1			**Scenario 2**			**Scenario 3**			**Scenario 4**			
	DOTM	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	
10	820.1	2.67	824.2	781.977	185.41	782.301	801.49	216.66	803.3	190.347	3.04	195.051	**EOTM**
20	1045.63	102.32	1252.9	1120.82	571.72	1121.12	1315.556	628.46	1571.85	583.61	131.52	606.185	
30	1952.54	382.67	2110.82	1454.8	744	1459.2	2021.13	952.26	2029.72	590.166	510.11	615.60	
40	2029.823	480.04	2673.37	1345.29	971.871	1351.4	2864.5	2472.36	3229.59	876.115	811.44	894.27	
50	2995.97	989.9	3045.61	1739.76	1226.83	1740.3	8998.84	2762.6	8999.41	1158.31	1023.89	1189.24	

7.3.2.2 Event Detection Probability

Figure 7.8a depicts the probability of data-oriented trust model to detect true events in four scenarios. It can be seen that highest EDP is achieved when the network contains mobile attackers. The attack vector of the mobile attacker constantly changes. As a result, probability of vehicles to detect true event increases as they might receive true events from other honest vehicles in its vicinity. On the other hand, static attackers decreases the ability of legitimate vehicles to detect true events due to constant attack-vector in geographical location. For a network with 20% malicious nodes, scenario 2 achieves 5.3%, 44.3% & 33.5% high EDP than scenario 1, 3 & 4 respectively.

Event detection probability of entity-oriented TM is shown in Figure 7.8b, highlighting that high mobility networks are affected to a greater extent with mobile attackers, where the detection of true events decreases massively in the network. Static attackers, on the other hand, create high impact on the network with low mobility (such as city center), where increasing such vehicles increases the generation of compromised messages in the network. This limits the scope of the



(a)

(b)

(c)

Figure 7.8: Event Detection Probability (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM

legitimate vehicles to correctly detect true events in the network. Among all the considered scenarios, highest EDP is achieved in scenario 1 and lowest EDP in scenario 3. When the network is injected with 20% malicious nodes, scenario 1 achieves 8.9%, 19.2% & 32.9% better EDP than scenario 4, 2 & 3 respectively.

Figure 7.8c shows the true event detection probability of hybrid trust model in four scenarios. HTM performs similar to DOTM where highest EDP is achieved in scenario 2 and lowest in scenario 3. The vehicles incorporating HTM integrates trust evaluation on the received data, which may be tempered by malicious vehicles. Increasing such vehicles which disseminates compromised data will limit the vehicles to correctly identify true events, thus decreasing network efficiency. For a network having 20% malicious vehicles, scenario 2 achieves 7.5%, 44.1% & 35.2% high EDP than scenario 1, 3 & 4 respectively.

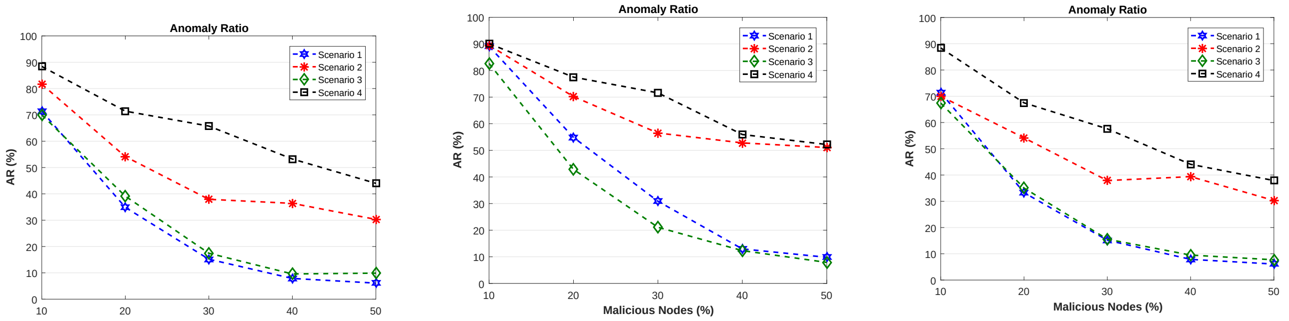
Table 7.4 depicts that the event detection probability of entity-oriented trust model is better than other trust models. EOTM integrates role-based trust mechanism which propagates correct events in the network. As a result, the scope of vehicles to detect true events increases in the network in presence of malicious vehicles.

Table 7.4: Comparison of Event Detection Probability

Malicious Nodes (%)	**Scenarios**												**Best Model**
	Scenario 1			**Scenario 2**			**Scenario 3**			**Scenario 4**			
	DOTM	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	
10	62.14	94.97	60.24	65.87	91.65	61.18	50.89	91.02	50.11	51.32	93.21	50.20	**EOTM**
20	53.22	88.25	51.1	56.21	71.244	55.31	31.265	59.13	30.9	37.34	80.33	35.81	
30	26.18	80	22.58	28.47	60.1	25.93	22.24	45.81	21.67	25.027	72.08	24.06	
40	24.24	58.46	20.27	26.54	44.4	22.7	18.8	42.2	18.58	20.82	53.14	19.68	
50	19.24	52.81	17.7	20.562	36.73	19.14	10.12	30.713	10.08	13.73	49.4	12.96	

7.3.2.3 Anomaly Ratio

Figure 7.9a depicts the capability of data-oriented trust model to detect anomalies in the network. It shows that scenario 4 outperforms other scenarios by detecting maximum number of anomalies. This is due to the fact that mobile attackers affect the high number of vehicles as a consequence of their low mobility. On the other hand, less anomalies are detected in scenario 1, as the vehicles communicate for a very short span of time for highly mobile legitimate vehicles and static attackers. For 50% malicious vehicles, scenario 4 can detect 31.1%, 77.5% & 86.13% better anomalies than scenario 2, 3 & 1 respectively.



(a) (b) (c)

Figure 7.9: Anomaly Ratio (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM

Figure 7.9b shows the anomaly ratio of the network incorporating entity-oriented trust model, highlighting that scenario 4 can detect high number of anomalies in the network as in DOTM. The low mobility and high number of legitimate vehicles (e.g., city center) can detect malicious activity in the network. When the network contains 50% malicious vehicles, scenario 4 detects 81.1%, 2.16% and 84.88% more anomalies than scenario 1, 2 and 3 respectively.

The ability of hybrid trust model to detect anomalies is shown in Figure 7.9c. HTM behaves similar to DOTM where low mobility of legitimate vehicles detects high number of anomalies in the network in the presence of mobile malicious attackers. These attackers provide an opportunity of window to the vehicles to communicate and detect anomalies in the network. For a network injected with 50 % malicious vehicles, scenario 4 provides 83.9%, 20% and 79.6% better results than scenario 1, 2 and 3 respectively by detecting more anomalies.

In short, Table 7.5 clearly depicts that entity-oriented trust model can detect high number of anomalies than data-oriented and hybrid trust model. EOTM relies on trusted and experienced vehicles which are classified as trusted members of the network by the higher authorities, thus, the ability of the vehicles to detect malicious activity in the network increases.

Table 7.5: Comparison of Anomaly Ratio

Malicious Nodes (%)	**Scenarios**												**Best Model**
	Scenario 1			**Scenario 2**			**Scenario 3**			**Scenario 4**			
	DOTM	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	
10	71.42	89.09	71.42	81.64	89.47	70	70	82.65	67.41	88.4	90.1	88.4	**EOTM**
20	34.88	54.87	33.3	54.16	70.21	54.16	39.13	42.85	35.06	71.42	77.52	67.5	
30	15.18	30.89	15.18	37.931	56.52	37.9	17.45	21.1	15.56	65.75	71.6	57.6	
40	7.87	12.96	7.87	36.39	52.8	39.39	9.58	12.32	9.51	53.24	55.95	44.08	
50	6.1	9.82	6.1	30.3	51.06	30.3	9.89	7.894	7.71	44	52.19	37.9	

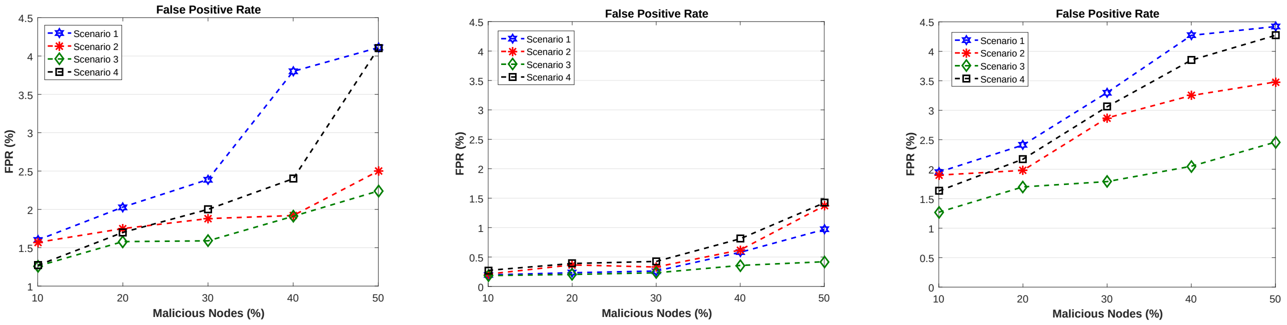
7.3.2.4 False Positive Rate

False positive rate illustrate the error margin of the TM where malicious entity and its content is incorrectly identified as legitimate. FPR of the data-oriented and hybrid trust models is shown in Figures 7.10a & 7.10c, emphasizing that network attains high FPR in scenario 1 & 4 where it increases almost exponentially as compared to scenario 2 & 3. Moreover, DOTM & HTM achieves high FPR for a network containing high mobility and static attackers. These attackers provide limited window of opportunity for legitimate vehicles to communicate with each other. Increasing such malicious vehicles in the network increases the probability of incorrectly labeling valid data as malicious. DOTM and HTM achieves low FPR in urban scenario where high density of legitimate vehicles can correctly identify valid messages. For a network incorporating DOTM and containing 30% malicious vehicles, scenario 3 achieves 50.3%, 18.23% and 25.78% low FPR than scenario 1, 2 and 4 respectively. In case of HTM, scenario 3 achieves 45.7%, 37.6% and 41.5% low FPR than scenario 1, 2 and 4 respectively.

Table 7.6: Comparison of False Positive Rate

Malicious Nodes (%)	**Scenarios**												**Best Model**
	Scenario 1			**Scenario 2**			**Scenario 3**			**Scenario 4**			
	DOTM	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	
10	1.6	0.196	1.95	1.57	0.2099	1.90	1.26	0.184	1.27	1.27	0.273	1.63	**EOTM**
20	2.03	0.233	2.41	1.75	0.366	1.98	1.58	0.204	1.7	1.7	0.39	2.17	
30	2.39	0.262	3.3	1.88	0.33	2.87	1.59	0.232	1.79	2	0.425	3.06	
40	3.8	0.58	4.27	1.92	0.62	3.25	1.91	0.357	2.05	2.4	0.81	3.85	
50	4.11	0.968	4.42	2.5	1.37	3.48	2.24	0.42	2.46	4.1	1.42	4.27	

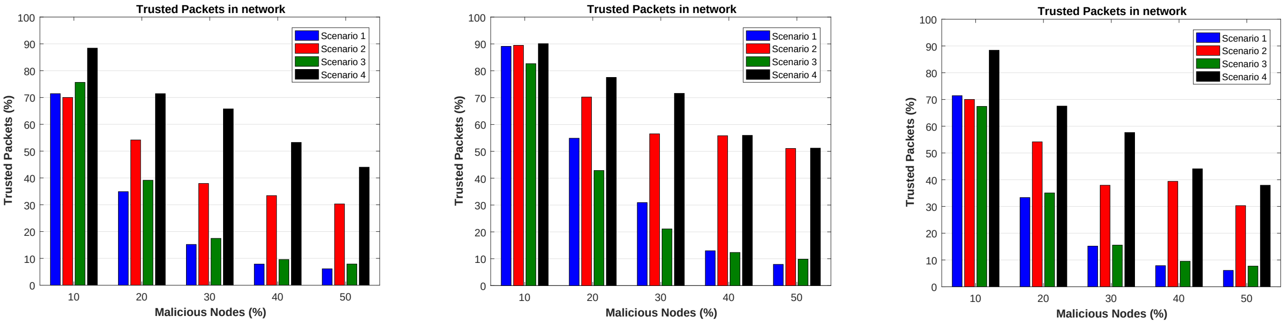
FPR for entity-oriented trust model is highlighted in Figure 7.10b, demonstrating that efficiency of the network decreases in terms of FPR when it is flooded with mobile attackers. The



(a) (b) (c)

Figure 7.10: False Positive Rate (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM

attack-vector of such attacker changes continuously which increase the probability of incorrectly classifying malicious message as valid. Among 4 scenarios, EOTM performs better in scenario 3, where low FPR is achieved. The low mobility and high density of vehicles produce a massive amount of messages, which provide an extended window to legitimate vehicles to identify true and malicious events in the network. When a network is flooded with 30% malicious nodes, scenario 3 performs 11.4%, 29.6% and 45.4% better than scenario 1, 2 and 4 respectively by achieving low FPR. Table 7.6 shows that EOTM performs better than DOTM and HTM in terms of FPR. This is due to the presence of role-based vehicles in EOTM which decreases the probability of error-margin in the network.



(a) (b) (c)

Figure 7.11: Trusted packets in the network (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM

7.3.2.5 Trusted and Untrusted Packets

Figures 7.11 & 7.12 show the number of trusted and untrusted packets generated by a network incorporating DOTM, EOTM and HTM respectively, demonstrating that scenario 4 outperforms other scenarios by propagating high number of trusted messages in VANET. This is due to the fact that low mobility of vehicles provide enough time for legitimate vehicles to validate trust on the sender. Moreover, network is affected when it is polluted with static attackers. These attackers have a constant attack-vector in a attack-prone location, thus it is highly unlikely that vehicles receive trusted messages from legitimate vehicles in presence of these attackers. On the contrary, vehicles have the possibility to receive trusted messages in presence of mobile attackers as the attack-vector changes continuously due to their mobility.

Table 7.7: Comparison for Total Trusted Packets

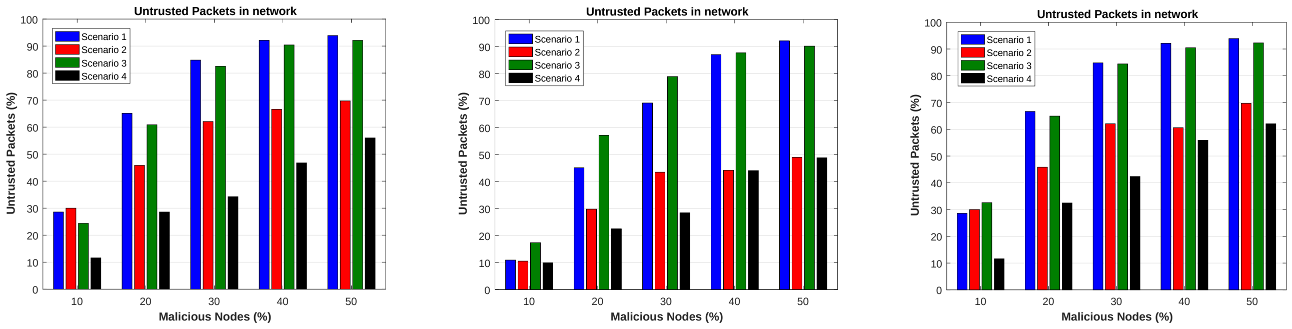
Malicious Nodes (%)	**Scenarios**												**Best Model**
	Scenario 1			**Scenario 2**			**Scenario 3**			**Scenario 4**			
	DOTM	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	
10	71.42	89.09	71.42	70	89.47	70	75.64	82.65	67.41	88.40	90.10	88.40	**EOTM**
20	34.88	54.87	33.33	54.16	70.21	54.16	39.13	42.85	35.06	71.42	77.52	67.53	
30	15.18	30.89	15.18	37.93	56.52	37.93	17.45	21.10	15.56	65.75	71.59	57.64	
40	7.87	12.96	7.87	33.93	55.81	39.39	9.58	12.32	9.51	53.24	55.95	44.08	
50	6.10	7.89	6.10	30.30	51.06	30.30	7.89	9.82	7.71	44	51.19	37.93	

When a network integrates DOTM and is flooded with 50% malicious vehicles, scenario 4 generates 86.12%, 31.12% and 82% more trusted packets and 67.66%, 24.45% and 64.46% less untrusted packets generated for scenario 1, 2 and 3 respectively. In case of the network with EOTM, scenario 4 generates 84.5%, 0.25% and 80.8% more trusted and 47%, 0.26%, 45.87% less untrusted packets than scenario 1, 2, and 3 respectively. Moreover, for a network incorporating HTM, scenario 4 produces 83.9%, 20.1% and 79.6% more trusted and 33.9%, 10.94%, 32.68% less untrusted packets than scenario 1, 2, and 3 respectively.

Table 7.8: Comparison for Total Untrusted Packets

Malicious Nodes (%)	**Scenarios**												**Best Model**
	Scenario 1			**Scenario 2**			**Scenario 3**			**Scenario 4**			
	DOTM	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	**DOTM**	**EOTM**	**HTM**	
10	28.58	10.91	28.58	30	10.53	30	24.36	17.35	32.58	11.6	9.9	11.6	**EOTM**
20	65.12	45.13	66.66	45.84	29.79	45.84	60.87	57.15	64.93	28.58	22.48	32.46	
30	84.82	69.11	84.82	62.07	43.48	62.07	82.87	78.9	84.43	34.25	28.41	42.35	
40	92.13	87.04	92.13	66.61	44.19	60.60	90.42	87.68	90.48	46.76	44.05	55.9	
50	93.9	92.11	93.9	69.7	48.94	69.69	92.11	90.18	92.28	56	48.81	62.06	

Table 7.7 & 7.8 depicts that EOTM outperforms both DOTM and HTM as high number of trusted packets are ensured in the network. Similarly, less number untrusted messages are



(a) (b) (c)

Figure 7.12: Untrusted packets in the network (a) Data-Oriented TM (b) Entity-Oriented TM (c) Hybrid TM

generated in the network containing EOTM. This is due to the presence of highly trusted entities (such as law-enforcement, ambulances etc.) in the network which assures a trusted environment where trusted information can propagate in the network.

7.4 Discussion

In this section, we focus on the discussion of TEAM framework performance in terms of its applicability, usability, scalability, security assurance and limitation.

7.4.1 Applicability of TEAM:

TEAM provides a base framework for smart city planners and automotive manufacturers to design, test and validate TMs in different contexts and attacker models before integrating them within the vehicles and network. Moreover, TEAM provides various TMs for benchmarking purposes. Further, TEAM can be used by the researchers to validate their newly designed TM. Thus, a wide range of users (automotive manufacturers, researchers and smart city planners) can evaluate the efficiency of the designed TM by comparing it against benchmarked TM using an extensive set of realistic trust evaluation criteria.

7.4.2 Usability of TEAM:

TEAM is designed using three widely used open-source platforms, i.e., OMNET++, VEINS and SUMO. OMNET++ supports the graphical user interface, therefore, TEAM can provide the graphical representation of the network where the user can visualize the behavior of the TM. Thus, the smart city planners or users with knowledge about these standardized platforms can validate newly designed and available TMs using TEAM. However, a small effort is required to understand the implementation and integration of various components of TM within the framework. TEAM is available to researchers upon request for research purposes.

7.4.3 Scalability Analysis:

Scalability is one of the crucial requirement in VANET as the rate of entering and exiting vehicles in the network is not constant. Thus, the TMs should be scalable and independent of network size and vehicles mobility. TEAM is a scalable framework as it integrates scalable simulation tools such as OMNET++ [175], SUMO [176] and VEINS [177].

We tested our framework by evaluating TMs in four contexts with random vehicular mobility. However, more contexts can easily be integrated in TEAM. For example, contexts based on vehicles concentration and dispersion across the network is not considered in current framework.

Moreover, in the context of smart city, TEAM can support high number of vehicles to better understand the behaviour of TMs for validation purposes. TEAM framework integrates realistic maps, imported directly from OpenStreetMap. Traffic is generated on these maps via SUMO which includes both mobile and static vehicles (attackers) in the network. However, identifying the ideal location on the map for placing static vehicles is a time intensive process as the user has to first identify the favorable place on the map and then align the vehicle in that location to utilize its capabilities. This complexity increases when the user has to place a high number of static vehicles in the network. For instance, placing 80% static attackers for a network with 1000 vehicles is challenging as the user has to identify ideal locations for implementing such high number of attackers on the map.

7.4.4 Security Analysis:

It is eminently important for TMs to be robust against attacks which reduces the network performance by transmitting untrusted and compromised messages in the network such as MITM attacks. Threat model and risk assessment modules of TEAM identified various attacker models (AMs) with critical and high risk in the network. Our framework has the ability to provide the security perspective for the evaluation of TMs in the network as AMs with critical risks are integrated within TEAM. We tested the performance of TMs using TEAM in presence of attackers. Simulation results indicate that DOTM and HTM are more prone to attacks than EOTM, where, security is achieved by evaluating trustworthiness on the node. Moreover, EOTM ensures the presence and dissemination of more trusted information in the network due to role-based trust.

7.4.5 Limitation of TEAM:

Simulation results showed the applicability of TEAM to accurately evaluate TMs in VANET. However, there are certain limitations in current framework.

- Modeling human factor (driver's honesty and selfishness) accurately for trust management is a challenging task in VANET. Recently, some TMs are proposed which relies on social networks for trust management such as [170, 178]. Currently, TEAM can only evaluate TMs for VANET and it cannot evaluate social-network based TMs as it is not integrated in our framework yet.

- Recently, some effort is done in adopting Content-Centric Networking (CCN) and Named Data Networking (NDN) into VANET [179, 180]. Currently, TEAM is limited to host-based communication paradigm only, and hence, it cannot evaluate TMs which are developed purely on CCN and NDN-based VANET.

- Similarly, different computing paradigms such as cloud computing and fog computing is integrated in VANET to provide wide range of applications [181, 182]. TEAM currently focused on trust modelling for pure VANET, and hence, it cannot evaluate trust models in VANET which relies on cloud or fog computing.

- We have tested the performance of our framework with up-to 300 vehicles which were generated in SUMO. Theoretically, TEAM is scalable and can support higher number of vehicles. Only complexity is placing higher number of static nodes at the micro-level on the realistic map.

Chapter 8

Conclusion and Future Work

This chapter concludes this thesis and it consists of two sections. In the first section of this chapter, we derived conclusions from this research and briefly outlined the major contributions achieved in this thesis. The last section of this chapter identifies different future research directions of this study.

8.1 Major Contributions

A secure and attack-free environment is a prerequisite in VANET for trusted message dissemination among vehicles and infrastructure. However, the random mobility (high and low) of both legitimate and malicious vehicles results in various contexts in VANET. Creating a trusted environment and maintain a trust relation among the vehicles in every context of VANET is an extremely challenging task as the attackers might penetrate the network and pollute it with bogus information. Therefore, the trust models (TMs) should be validated in different context of VANET before integrating and implementing them in the real environment. Further, there should be a way to compare different proposed TMs in VANET. In light of this discussion, we proposed a novel framework that has the capability to validate, evaluate and compare a wide range of TMs in VANET.

In order to achieve our aim and objectives, we started our thesis with providing details about vehicular networks and trust management in Chapter 2 and Chapter 3. These chapters build the foundation of this thesis where we identified various research gaps in this domain. Chapter 2 focused entirely on the fundamental basics of vehicular networks where we explained the architecture of VANET in detail and identified various research challenges faced by this intermittent technology. The next chapter elaborated the trust management issues within VANET where, we carried out an extensive literature survey on trust management and their evaluation in VANET. First, we identified a wide range of TMs in VANET and categorized them into three distinct classes, i.e., Entity-oriented TMs (EOTM), Data-oriented TMs (DOTM) and Hybrid TMs (HTM). Next, we focused on the evaluation frameworks within VANET. According to our extensive literature survey, the currently available TMs have limitations in their scope, as they only evaluate a particular class of TMs. Further, we concluded that there is no such comprehensive methodology and framework, which can compare a wide range of TMs.

Therefore, to fill this gap, we proposed, presented and implemented a novel framework in VANET that have the ability to evaluate, validate and compare different TMs under various contexts and adversary conditions. To this end, we provided the details of our trust evaluation and management (TEAM) framework in Chapter 4, which consisted of five distinct modules, i.e., threat model, risk assessment, TM categorization, context-establishment and trust evaluation platform. Further, we also carried a qualitative evaluation of various TMs in VANET in this chapter, where, we specifically evaluated 12 TMs based on sixteen trust evaluation criteria. This study showed that none of the TM in VANET satisfy all the trust evaluation criteria.

Chapter 5 is dedicated to the implementation details of this thesis, which provides the details of the proposed research methodology and the implemented simulation environment in order to design TEAM framework. Further, we also introduced VEINS simulation platform in detail as TEAM is developed on top of this simulator. Specifically, we explained various involved components of VEINS and the implementation details of TEAM framework in this chapter.

We dedicated Chapter 6 to provide extensive details of threat model and risk assessment, which are vital components of of TEAM framework. First, we explained the design of our proposed threat model that follows an asset-based approach to identify vulnerabilities, threats and attacks across different assets of VANET. Next, we performed risk assessment in VANET to identify attacks with critical impact on the network. Specifically, a context-based risk assessment model is proposed where the impact of same attack in four different contexts of VANET is evaluated based on the mobility of the nodes. We concluded from this context-based risk assessment approach that the same attack in VANET has different impact in different scenarios of VANET.

In order to demonstrate our framework, we implemented three different TMs, i.e., entity-oriented, data-oriented and hybrid trust model in Chapter 7. We conducted an extensive set of simulations to study the behaviour of TMs in presence of adversary conditions for four different contexts in VANET. Further, TMs are evaluated using realistic trust evaluation criteria proposed in Chapter 4. TEAM revealed an interesting result that changes the general perception that HTMs perform better in VANET due to their imperative nature of evaluating trust on both vehicle and data. However, according to our framework, EOTM outperforms both DOTM and HTM. This is due to the presence of highly trusted and experienced vehicles in the network ensuring the dissemination of trusted messages.

8.2 Future Work

Our proposed TEAM framework can be beneficial to the wide range of users. First, it can be instrumental and helpful for researchers in this domain to validate their newly designed TMs. As the framework integrates different TMs, thus, it provides an excellent opportunity to the researchers to compare the efficiency of their designed TMs against the benchmarked TMs. Next, TEAM framework can be used by smart city planners and vehicle manufacturers to model, evaluate and validate TMs in different contexts of VANET. Currently, TEAM framework supports four contexts in VANET which are designed based on the nodes mobility. Thus, it provides a universal platform to these users to validate TM in different contexts of VANET. Further, various realistic trust evaluation criteria are integrated within TEAM, thus, these users can validate the efficiency of TMs before integrating and implementing them within the vehicles in a real-environment.

This thesis forms the foundation for evaluating different TMs in VANET. However, this thesis can be extended in various directions such as:

- Context establishment in this thesis is based on the nodes mobility only. The accuracy of the evaluation of trust models via TEAM can be enhanced by integrating more contexts such as nodes dispersion throughout the network.
- The framework can be extended to VANET based on alternative architecture such as Named Data Networking (NDN). This extension to the TEAM framework can evaluate the performance of trust models implemented for NDN-based VANETs.
- This thesis can also be extended by integrating social networks into the framework, so that it can evaluate the trust models which considers social networks into account.
- This thesis considered only three trust models for the evaluation of TEAM framework. This work can be extended further by implementing more trust models within the framework.
- We considered man-in-the-middle attacks in VANET to evaluate the TEAM framework. The performance of TEAM framework can be extended by implementing other attacks having severe risk in VANET and evaluating the TEAM framework under such attacks.

Appendix 1: Adding Attacks and Trust Models in TEAM

This appendix provide details of adding new attacks and trust models in the TEAM framework.

Adding a New Attack

Let‘s assume that the new attack that is going to be implemented in TEAM framework is “Wormhole”. Following steps must be followed to add a new attack at the application layer.

1. Create a new folder at location “/src/attacks/wormhole”
2. In this folder, create the associated network description file (.ned), source file (.cc), and respective header file (.h)
   (a) wormhole.ned //ned file
   (b) wormhole.h //header file
   (c) wormhole.cc //source file
3. In the network description file, inherit the attack module in the following way:
   (a) Simple wormhole extends BaseWaveApplLayer
   (b) Create the class tag: @class(wormhole)
4. In the header file, inherit the class from existing attacks and add respective parameters

   (a) Class wormhole: public BaseWaveApplLayer

5. Once, .ned and .h files are defined, the next step is to implement a source file (.cc)

   (a) Include the created header file (wormhole.h)

   (b) Include the following macro (Define_Module(wormhole)) in the source file to register the implemented class with OMNET++.

   (c) Initialize the parameters in the initialize function.

   (d) Implement the attack scenario when the message is received by defining "received" function.

   (e) Define a "send" function about the attack behaviour to be transmitted in the network.

6. To execute and run the simulations, modify the "omnetpp.ini" file by adding and specifying the attackers.

   (a) *.node[1].appType = "wormhole" //Node 1 is an attack node performing wormhole attack

   (b) *.node[*].appType = Application //All other nodes are legitimate

Adding a New Trust Model

Following steps must be ensured to integrate a new trust model (TM1) within TEAM framework.

1. 1) Create a new folder at location "/src/trustmodels/TM1"

2. Create the respective network description file (.ned), source file (.cc), and respective header file (.h) at the above location.

   (a) TM1.ned //ned file

   (b) TM1.h //header file

   (c) TM1.cc //source file

3. In the network description file, inherit the trust model module via:

   (a) Simple TM1 extends BaseWaveApplLayer

   (b) Create the class tag: @class(TM1)

4. In the header file, inherit the class from existing trust models and add respective parameters

   (a) Class TM1: public BaseWaveApplLayer

5. The next step is to implement a source file (.cc) after defining .ned and .h files

   (a) Include the created header file (TM1.h)

   (b) Include the following macro (Define_Module(TM1)) in the source file to register the implemented class with OMNET++.

   (c) Initialize the parameters in the initialize function.

   (d) Implement the the trust function for a received messaged by defining "received" function.

   (e) Define a "send" function to transmit trusted messages in the network.

6. To execute and run the simulations, modify the "omnetpp.ini" file by adding and specifying the attackers.

   (a) *.node[1].appType = "TM1" //Node 1 is using trust model TM1

   (b) *.node[*].appType = Application //All other nodes are using default application (Without trust calculations)

Bibliography

[1] SBD, "Connected Car Global Forecast," tech. rep., SBD, 2015.

[2] VEINS, "Vehicles in Network Simulation, The Open Source Vehicular Simulation Framework." Available online: http://veins.car2x.org (Accessed: March 09, 2018).

[3] WHO, "Global Status Report on Road Safety," tech. rep., World Health Organization, 2015. ISBN: 978-92-4-156506-6.

[4] ITS-UK, "United Kingdom: Better Transport Through Technology." Available at: http://its-uk.org.uk/. (Accessed March 20, 2018).

[5] ERTICO, "ERTICO ITS Europe." Available at: http://ertico.com/. (Accessed November 27, 2017).

[6] J. Barbaresso, G. Cordahi, *et al.*, "Intelligent Transportation Systems (ITS) Strategic Plan 2015-2019," tech. rep., US Department of Transportation (USDOT), December 2014.

[7] ITS, "ITS Japan." Available at: http://www.its-jp.org/english/. (Accessed November 27, 2017).

[8] ITSB, "Intelligent Transportation System Brazil." Available at: https://www.itsb.org.br/. (Accessed March 21, 2018).

[9] ITS-Australia, "ITS Australia Strategic Plan 2013 - 2018." Available at: https://www.its-australia.com.au/wp-content/uploads/ITSA_Australia-Strategy4pp2015OUTweb.pdf. (Accessed March 20, 2018).

[10] R. Coppola and M. Morisio, “Connected Car: Technologies, Issues, Future Trends,” *ACM Computing Surveys*, vol. 49, pp. 46:1–46:36, Oct. 2016.

[11] C. A. Kerrache, C. T. Calafate, J. C. Cano, N. Lagraa, and P. Manzoni, “Trust Management for Vehicular Networks: An Adversary-Oriented Overview,” *IEEE Access*, vol. 4, pp. 9293–9307, 2016. doi:10.1109/ACCESS.2016.2645452.

[12] S. S. Tangade and S. S. Manvi, “A Survey on Attacks, Security and Trust Management Solutions in VANETs,” in *Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1–6, July 2013.

[13] J. Zhang, “Trust Management for VANETs: Challenges, Desired Properties and Future Directions,” *International Journal of Distributed Systems and Technologies*, vol. 3, pp. 48–62, Jan. 2012.

[14] R. Shrestha and S. Y. Nam, “Trustworthy Event-Information Dissemination in Vehicular Ad Hoc Networks,” *Mobile Information Systems*, p. 16 pages, November 2017. doi:10.1155/2017/9050787.

[15] T. Gazdar, A. Belghith, and H. Abutair, “An Enhanced Distributed Trust Computing Protocol for VANETs,” *IEEE Access*, vol. 6, pp. 380–392, October 2017. doi:10.1109/ACCESS.2017.2765303.

[16] T. Biswas, A. Sanzgiri, and S. Upadhyaya, “Building Long Term Trust in Vehicular Networks,” in *IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, May 2016.

[17] W. Li and H. Song, “ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, pp. 960–969, April 2016.

[18] A. Auer, S. Feese, and S. Lockwood, “History of Intelligent Transportation Systems,” tech. rep., U.S. Department of Transportation, May 2016.

[19] E. Christmann, “Data Communication in the Autormobile Part 1: Architecture, Tasks, and Advantages of Serial Bus Systems,” tech. rep., VECTOR, 2007.

[20] H. Tan, M. Ma, H. Labiod, A. Boudguiga, J. Zhang, and P. H. J. Chong, “A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks,” *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 9570–9584, Dec 2016.

[21] US-DOT, “Dedicated Short-Range Communications (DSRC): The future of safer driving,” tech. rep., US - Department of Transportation, 2014. Available at: https://www.its.dot.gov/factsheets/pdf/JPO-034_DSRC.pdf (Accessed March 26, 2018).

[22] ETSI, “ETSI EN 302 636-1 V1.2.1: Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements,” tech. rep., European Telecommunications Standards Institute, 2014.

[23] ETSI, “ETSI EN 302 663 V1.2.0: Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band,” tech. rep., European Telecommunications Standards Institute, 2012.

[24] P. Papadimitratos, A. D. L. Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, “Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation,” *IEEE Communications Magazine*, vol. 47, pp. 84–95, November 2009.

[25] Y. J. Li., “An Overview of the DSRC/WAVE Technology,” in *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, pp. 544–558, November 2010.

[26] E. C. Eze, S.-J. Zhang, E.-J. Liu, and J. C. Eze, “Advances in Vehicular Ad-Hoc Networks (VANETs): Challenges and Road-map for Future Development,” *International Journal of Automation and Computing*, vol. 13, pp. 1–18, Feb 2016.

[27] ETSI, “ETSI TR 102 638 V1.1.1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions (2009-06),” tech. rep., European Telecommunications Standards Institute, 2010.

[28] J. Jakubiak and Y. Koucheryavy, "State of the Art and Research Challenges for VANETs," in *5th IEEE Consumer Communications and Networking Conference (CCNC 2008)*, pp. 912–916, Jan 2008.

[29] A. M. Vegni, M. Biagi, and R. Cusani, *Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks*, ch. Vehicular Technologies - Deployment and Applications. InTech, 2013. ISBN: 978-953-51-0992-1.

[30] IEEE, "IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)," tech. rep., Institute of Electrical and Electronics Engineering, July 2010. doi:10.1109/IEEESTD.2010.5514475.

[31] ISO, "ISO 21215:2018 - Intelligent transport systems – Localized communications – ITS-M5," tech. rep., ISO, June 2018.

[32] ISO, "ISO 15717-1:2015 - Intelligent transport systems – Communications access for land mobiles (CALM) – Evolved universal terrestrial radio access network (E-UTRAN) – Part 1: General usage," tech. rep., ISO, September 2015.

[33] ISO, "ISO 26262-2:2018 - Road vehicles – Functional safety – Part 2: Management of functional safety ," tech. rep., ISO, December 2018.

[34] ISO, "ISO 21218:2018 - Intelligent transport systems – Hybrid communications – Access technology support," tech. rep., ISO, June 2018.

[35] ETSI EN 302 637-3 v1.2.1, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service (2014-09)," tech. rep., ETSI, 2014.

[36] IEEE, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," tech. rep., Institute of Electrical and Electronics Engineering, March 2014. doi:10.1109/IEEESTD.2014.6755433.

[37] IEEE, "1609.2a-2017 - IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages - Amendment 1," tech. rep., Institute of Electrical and Electronics Engineering, October 2017. doi:10.1109/IEEESTD.2017.8065169.

[38] IEEE, "1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services," tech. rep., Institute of Electrical and Electronics Engineering, April 2016. doi:10.1109/IEEESTD.2016.7458115.

[39] SAE, "J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary," tech. rep., Society of Automotive Engineers, March 2016.

[40] SAE, "J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," tech. rep., Society of Automotive Engineers, January 2016.

[41] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet Security Challenges and Solutions: A Survey," *Vehicular Communications*, vol. 7, no. Supplement C, pp. 7 – 20, 2017.

[42] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, vol. 9, no. Supplement C, pp. 19 – 30, 2017.

[43] I. A. Soomro, H. Hasbullah, and J. l. bin Ab Manan, "User Requirements Model for Vehicular Ad Hoc Network Applications," in *International Symposium on Information Technology*, vol. 2, pp. 800–804, June 2010.

[44] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, pp. 39–68, Jan. 2007.

[45] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Intelligent Agents in Mobile Vehicular Ad-Hoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty," in *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, vol. 2, pp. 243–247, Aug 2010.

[46] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, “LESPP: Lightweight and Efficient Strong Privacy Preserving Authentication Scheme for Secure VANET Communication,” *Springer Computing*, vol. 98, pp. 685–708, Jul 2016.

[47] X. Lin, X. Sun, P. H. Ho, and X. Shen, “GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications,” *IEEE Transactions on Vehicular Technology*, vol. 56, pp. 3442–3456, Nov 2007.

[48] X. Zhu, S. Jiang, L. Wang, and H. Li, “Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks,” *IEEE Transactions on Vehicular Technology*, vol. 63, pp. 907–919, Feb 2014.

[49] K. Emara, W. Woerndl, and J. Schlichter, “On Evaluation of Location Privacy Preserving Schemes for VANET Safety Applications,” *Computer Communications*, vol. 63, pp. 11 – 23, 2015.

[50] A. Boualouache, S.-M. Senouci, and S. Moussaoui, “HPDM: A Hybrid Pseudonym Distribution Method for Vehicular Ad-hoc Networks,” in *The 7th International Conference on Ambient Systems, Networks and Technologies*, vol. 83, pp. 377 – 384, 2016.

[51] K. Fysarakis, I. Askoxylakis, V. Katos, S. Ioannidis, and L. Marinos, *Intrusion Detection and Prevention for Mobile Ecosystems*, ch. Security Concerns in Co-operative Intelligent Transportation Systems. CRC Press, 2017. ISBN: 9781138033573.

[52] F. Sakiz and S. Sen, “A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV,” *Ad Hoc Networks*, vol. 61, pp. 33 – 50, 2017.

[53] M. Al-kahtani, “Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs),” in *6th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–9, December 2012.

[54] I. A. Sumra, I. Ahmad, H. Hasbullah, and J. l. bin Ab Manan, “Classes of Attacks in VANET,” in *Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, pp. 1–5, April 2011.

[55] F. Ahmad, M. Kazim, and A. Adnane, *Vehicular Cloud Networks: Architecture and Security*, ch. Guide to Security Assurance for Cloud Computing, pp. 211–226. Springer International Publishing, 2015.

[56] F. Ahmad, M. Kazim, A. Adnane, and A. Awad, "Vehicular Cloud Networks: Architecture, Applications and Security Issues," in *IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, pp. 571–576, Dec 2015.

[57] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security Attacks and Solutions for Vehicular Ad Hoc Networks," *IET Communications*, vol. 4, pp. 894–903, April 2010.

[58] I. A. Sumra, I. Ahmad, H. Hasbullah, and J. l. bin Ab Manan, "Behavior of Attacker and Some New Possible Attacks in Vehicular Ad hoc Network (VANET)," in *3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 1–8, Oct 2011.

[59] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53 – 66, 2014.

[60] N.-W. Wang, Y.-M. Huang, and W.-M. Chen, "A Novel Secure Communication Scheme in Vehicular Ad Hoc Networks," *Computer Communications*, vol. 31, no. 12, pp. 2827 – 2837, 2008.

[61] S. Gillani, F. Shahzad, A. Qayyum, and R. Mehmood, "A Survey on Security in Vehicular Ad Hoc Networks," in *5th International Workshop on Communication Technologies for Vehicles*, pp. 59–74, Springer, 2013.

[62] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[63] J. Grover, M. S. Gaur, and V. Laxmi, "Trust Establishment Techniques in VANET," *Springer, Wireless Networks and Security, Signal and Communication Technology*, pp. 273–301, 2013.

[64] Y. M. Chen and Y. C. Wei, "A Beacon-based Trust Management System for Enhancing User Centric Location Privacy in VANETs," *Journal of Communications and Networks*, vol. 15, pp. 153–163, April 2013.

[65] S. Ahmed and K. Tepe, "Misbehaviour Detection in Vehicular Networks using Logistic Trust," in *IEEE Wireless Communications and Networking Conference*, pp. 1–6, 2016.

[66] M. Monir, A. Abdel-Hamid, and M. A. E. Aziz, "A Categorized Trust-Based Message Reporting Scheme for VANETs," in *International Conference on Advances in Security of Information and Communication Networks, (SecNet)*, pp. 59–74, Springer, September 2013.

[67] N. Bismeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of Node Trustworthiness in VANETs using Data Plausibility Checks with Particle filters," in *IEEE Vehicular Networking Conference (VNC)*, pp. 78–85, Nov 2012.

[68] C. M. Jonker and J. Treur, "Formal Analysis of Models for the Dynamics of Trust based on Experiences," in *9th European Workshop on Modelling Autonomous Agents in a Multi-Agent World*, pp. 221–231, Springer, July 1999.

[69] F. Li and Y. Wang, "Routing in Vehicular Ad Hoc Networks: A Survey," *IEEE Vehicular Technology Magazine*, vol. 2, pp. 12–22, June 2007.

[70] S. Eichler, C. Schroth, and J. Eberspächer, "Car-to-Car Communication," *VDE-Kongress*, 2006.

[71] U. Khan, S. Agrawal, and S. Silakari, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks," in *International Conference on Information and Communication Technologies (ICICT)*, pp. 965 – 972, Elsevier, December 2014.

[72] A. Jesudoss, S. K. Raja, and A. Sulaiman, "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme," *Ad Hoc Networks*, vol. 24, Part A, pp. 250 – 263, 2015.

[73] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, “Trust and Exclusion in Vehicular Ad Hoc Networks: An Economic Incentive Model based Approach,” in *Computing, Communications and IT Applications Conference (ComComAp)*, pp. 13–18, IEEE, April 2013.

[74] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, “A Multifaceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad Hoc Vehicular Networks,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, pp. 407–420, May 2011.

[75] N. Yang, “A Similarity based Trust and Reputation Management Framework for VANETs,” *International Journal of Future Generation Communication and Networking*, vol. 6, no. 2, pp. 25–34, 2013.

[76] F. G. Mrmol and G. M. Prez, “TRIP, a Trust and Reputation Infrastructure-based Proposal for Vehicular Ad Hoc Networks,” *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934 – 941, 2012. doi:10.1016/j.jnca.2011.03.028.

[77] M. Gerlach, “Trust for Vehicular Applications,” in *Eighth International Symposium on Autonomous Decentralized Systems*, pp. 295–304, March 2007.

[78] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, “On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks,” in *IEEE 27th Conference on Computer Communications (INFOCOM)*, pp. 39–68, IEEE, April 2008.

[79] S. Gurung, D. Lin, A. C. Squicciarini, and E. Bertino, “Information-Oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks.,” in *7th International Conference on Network and System Security (NSS)*, pp. 94–108, Springer, June 2013.

[80] R. A. Shaikh and A. S. Alzahrani, “Intrusion-aware Trust Model for Vehicular Ad-hoc Networks,” *Security and Communication Networks*, vol. 7, no. 11, pp. 1652–1669, 2014.

[81] A. Wu, J. Ma, and S. Zhang, “RATE: A RSU-Aided Scheme for Data-Centric Trust Establishment in VANETs,” in *7th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–6, Sept 2011.

[82] M. Sun, M. Li, and R. Gerdes, "A Data Trust Framework for VANETs Enabling False Data Detection and Secure Vehicle Tracking," in *IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, Oct 2017.

[83] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and YinbinMiao, "LSOT: A Lightweight Self-Organized Trust Model in VANETs," *Mobile Information Systems*, p. 15 pages, November 2016. doi:10.1155/2016/7628231.

[84] H. Sedjelmaci and S. M. Senouci, "An Accurate and Efficient Collaborative Intrusion Detection Framework to Secure Vehicular Networks," *Computer and Electrical Engineering*, vol. 43, pp. 33–47, April 2015.

[85] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Securing Vehicular Networks: A Reputation and Plausibility Checks-based Approach," in *IEEE Globecom Workshop on Web and Pervasive Security*, pp. 1550–1554, Dec 2010.

[86] K. C. Abdelaziz, N. Lagraa, and A. Lakas, "Trust Model with Delayed Verification for Message Relay in VANETs," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 700–705, IEEE, Aug 2014.

[87] Y. M. Chen and Y. C. Wei, "A Beacon-based Trust Management System for Enhancing User Centric Location Privacy in VANETs," *Journal of Communications and Networks*, vol. 15, pp. 153–163, April 2013. doi:10.1109/JCN.2013.000028.

[88] S. Ahmed and K. Tepe, "Using Logistic Trust for Event Learning and Misbehaviour Detection," in *IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, Sept 2016.

[89] C. Chen, J. Zhang, R. Cohen, and P. H. Ho, "A Trust Modeling Framework for Message Propagation and Evaluation in VANETs," in *2nd International Conference on Information Technology Convergence and Services*, pp. 1–8, Aug 2010.

[90] J. Oluoch, "A Theoretical Framework for Trust Management in Vehicular Ad hoc Networks," *International Journal of Trust Management in Computing and Communications*, vol. 3, no. 2, pp. 147–167, 2015.

[91] S. Ahmed, S. Al-Rubeaai, and K. Tepe, "Novel Trust Framework for Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 9498–9511, Oct 2017. doi:10.1109/TVT.2017.2710124.

[92] ISO, "BS ISO/IEC 27005:2018, Information Technology - Security Techniques - Information Security Risk Management," tech. rep., BSI Standard Publication, July 2018.

[93] C. A. Kerrache, C. T. Calafate, N. Lagraa, J. C. Cano, and P. Manzoni, "Trust-Aware Opportunistic Dissemination Scheme for VANET Safety Applications," in *International IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, pp. 153–160, July 2016.

[94] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular Security Through Reputation and Plausibility Checks," *IEEE Systems Journal*, vol. 8, pp. 384–394, June 2014. doi:10.1109/JSYST.2013.2245971.

[95] F. Ahmad, J. Hall, A. Adnane, and V. N. L. Franqueira, "Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-hoc Network," in *Proceeding of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 44–52, June 2017.

[96] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '07, pp. 19–28, ACM, 2007.

[97] P. T. N. Diep and C. K. Yeo, "A Trust-Privacy Framework in Vehicular Ad Hoc Networks (VANET)," in *2016 Wireless Telecommunications Symposium (WTS)*, pp. 1–7, April 2016.

[98] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, “A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks,” in *3rd Annual International Conference on Mobile and Ubiquitous Systems Workshops*, pp. 1–8, July 2006.

[99] K. C. Abdelaziz, N. Lagraa, and A. Lakas, “Trust Model with Delayed Verification for Message Relay in VANETs,” in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 700–705, IEEE, Aug 2014.

[100] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, “A Distributed Advanced Analytical Trust Model for VANETs,” in *IEEE Global Communications Conference (GLOBECOM)*, pp. 201–206, IEEE, Dec 2012.

[101] H. Sedjelmaci, T. Bouali, and S. M. Senouci, “Detection and Prevention from Misbehaving Intruders in Vehicular Networks,” in *2014 IEEE Global Communications Conference*, pp. 39–44, Dec 2014.

[102] Q. Alriyami, A. Adnane, and A. Kim Smith, “Evaluation Criterias for Trust Management in Vehicular Ad-hoc Networks (VANETs),” in *The 3rd International Conference on Connected Vehicles & Expo (ICCVE 2014)*, IEEE, 2014.

[103] S. Rajasekar and P. Philominathan and V. Chinnathambi, “Research Methodology.” Available at: http://arxiv.org/pdf/physics/0601009.pdf, 2013. (Accessed March 05, 2018).

[104] J. S. Carson, “Introduction to Modeling and Simulation,” in *Proceedings of the Winter Simulation Conference*, IEEE, Dec 2005.

[105] A. Maria, “Introduction to Modeling and Simulation,” in *Proceedings of the 29th conference on Winter simulation*, pp. 7–13, IEEE, 1997.

[106] J. Hu, S. Chen, L. Zhao, Y. Li, J. Fang, B. Li, and Y. Shi, “Link Level Performance Comparison between LTE V2X and DSRC,” *Journal of Communications and Information Networks*, vol. 2, pp. 101–112, Jun 2017.

[107] C. Christopher and R. M. Noory, "Wireless Channel Optimization in VANET by using Adaptive Modulation," in *12th International Conference on ITS Telecommunications*, pp. 295–299, IEEE, Nov 2012.

[108] J. Heidemann, N. Bulusu, J. Elson, C. Intanagonwiwat, K.-c. Lan, Y. Xu, W. Ye, D. Estrin, and R. Govindan, "Effects of Detail in Wireless Network Simulation," in *Proceedings of the SCS Multiconference on Distributed Simulation*, pp. 3–11, 2001.

[109] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang, S. McCanne, K. Varadhan, Y. Xu, and H. Yu, "Advances in Network Simulation," *Computer*, vol. 33, pp. 59–67, May 2000.

[110] Network Simulator 3 (NS-3). Available at: https://www.nsnam.org/. (Accessed March 08, 2018).

[111] A. Varga and R. Hornig, "An Overview of the OMNeT++ Simulation Environment," in *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, Simutools '08, pp. 60:1–60:10, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[112] R. Barr, Z. J. Haas, and R. Van Renesse, "JiST: Embedding Simulation Time into a Virtual Machine," in *EuroSim congress on modelling and simulation*, 2004.

[113] Riverbed Modeler. Available at: https://www.riverbed.com/gb/products/steelcentral/opnet.html. (Accessed March 08, 2018).

[114] QualNet Network Simulator. Available at: http://web.scalable-networks.com/qualnet-network-simulator-software. (Accessed March 08, 2018).

[115] A. Virdis, G. Stea, and G. Nardini, "SimuLTE - A Modular System-Level Simulator for LTE/LTE-A Networks based on OMNeT++," in *4th International Conference On Simulation And Modeling Methodologies, Technologies And Applications (SIMULTECH)*, pp. 59–70, Aug 2014.

[116] OverSim, "OverSim - The Overlay Simulation Framework." Available at: http://www.oversim.org/. (Accessed November 27, 2017).

[117] I. Baumgart, B. Heep, and S. Krause, "OverSim: A flexible overlay network simulation framework," in *Proceedings of 10th IEEE Global Internet Symposium (GI '07) in conjunction with IEEE INFOCOM 2007, Anchorage, AK, USA*, pp. 79–84, May 2007.

[118] INET, "INET Framework: Communication Network Simulation Package for OMNET++." Available at: https://inet.omnetpp.org/. (Accessed March 08, 2018).

[119] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, pp. 3–15, January 2011.

[120] G. M. Fernandez and others, "NETA: NETwork Attacks Framework for OMNeT++." Available at: http://nesg.ugr.es. (Accessed March 08, 2018).

[121] S. A. Hussain and A. Saeed, "An Analysis of Simulators for Vehicular Ad Hoc Networks," *World Applied Sciences Journal*, vol. 23, no. 8, pp. 1044–1048, 2013.

[122] SUMO, "Simulation of Urban MObility." Available online: http://sumo.dlr.de/wiki/Simulation_of_Urban_MObility (Accessed: 2nd April, 2017).

[123] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO-Simulation of Urban Mobility: An Overview," in *Proceedings of the Third International Conference on Advances in System Simulation*, 2011.

[124] VanetMobiSim. Available online: http://sumo.dlr.de/wiki/Simulation_of_Urban_MObility (Accessed: March 08, 2018).

[125] J. Härri, M. Fiore, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation with VanetMobiSim," *Simulation*, vol. 87, no. 4, pp. 275–300, 2011.

[126] F. K. Karnadi, Z. H. Mo, and K. c. Lan, "Rapid Generation of Realistic Mobility Models for VANET," in *IEEE Wireless Communications and Networking Conference*, pp. 2506–2511, March 2007.

[127] Paramics, "Paramics - Microscopic Traffic Simulation." Available online: http://www.paramics-online.com/paramics-library.php (Accessed March 08, 2018).

[128] S. Krauss, *Microscopic Modeling of Traffic Flow: Investigation of Collision Free Vehicle Dynamics*. PhD thesis, University of Cologne, 1998.

[129] A. Wegener, M. Piórkowski, M. Raya, H. Hellbrück, S. Fischer, and J.-P. Hubaux, "TraCI: An Interface for Coupling Road Traffic and Network Simulators," in *Proceedings of the 11th Communications and Networking Simulation Symposium*, pp. 155–163, ACM, 2008.

[130] OpenStreetMap, "OpenStreetMap." Available online: https://www.openstreetmap.org (Accessed: 16th October, 2017).

[131] M. Haklay and P. Weber, "OpenStreetMap: User-Generated Street Maps," *IEEE Pervasive Computing*, vol. 7, pp. 12–18, Oct 2008. doi: 10.1109/MPRV.2008.80.

[132] BS ISO, "ISO 26262-9:2018 – Road Vehicles – Functional Safety – Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses," tech. rep., British Standard – International Standardization Organization, December 2018.

[133] B. Schneier, "Attack Trees," *Dr. Dobb's Journal of Software Tools*, pp. 21–29, 1999.

[134] IEC, "IEC 61025: Fault Tree Analysis (FTA)," tech. rep., International Electrotechnical Commission (IEC), 2006. ISBN: 2-818-8918-9.

[135] BS ISO, "ISO 26262-3:2018 – Road Vehicles – Functional Safety – Part 3: Concept Phase," tech. rep., British Standard – International Standardization Organization, March 2018. Reference Number: ISO 26262-3:2018(E).

[136] ETSI, "ETSI TR 102 893 V1.2.1 (2017-03): Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA) ," tech. rep., European Telecommunication Standards Institute, March 2017.

[137] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner, "Using SAE J3061 for Automotive Security Requirement Engineering," in *Computer Safety, Reliability, and*

Security (A. Skavhaug, J. Guiochet, E. Schoitsch, and F. Bitsch, eds.), (Cham), pp. 157–170, Springer International Publishing, 2016.

[138] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "Threat and risk assessment methodologies in the automotive domain," *1st Workshop on Safety Security Assurance for Critical Infrastructures Protection (S4CIP)*, vol. 83, pp. 1288–1294, 2016.

[139] A. Ruddle *et al.*, "Deliverable D2.3: Security Requirements for Automotive On-board Networks based on Dark-side Scenarios," tech. rep., EVITA, 2009.

[140] R. Kroh, A. Kung, and F. Kargl, "Sevecom - D1.1: - VANETS Security Requirements," tech. rep., SEVECOM, 2006.

[141] G. Rafael and A. Crespo, "Oversee - D1.4 - Functional Requirements Analysis," tech. rep., OVERSEE, 2010.

[142] SafeTRIP, "Deliverable - D2.2.1 - Legal Issues & Personal Data Management Aspects Analysis - Initial Version," tech. rep., SafeTRIP, 2010.

[143] J. P. Stotz *et al.*, "Deliverable 1.1 - Security Requirements of Vehicle Security Architecture," tech. rep., PRESERVE, June 2011.

[144] T. Leinmuller, R. K. Schmidt, E. Schoch, A. Held, and G. Schafer, "Modeling Roadside Attacker Behavior in VANETs," in *IEEE Globecom Workshops*, pp. 1–10, Nov 2008.

[145] C. Laurendeau and M. Barbeau, "Threats to Security in DSRC/WAVE," in *5th International Conference on Ad-hoc Networks (ADHOC-NOW)*, pp. 266–279, Lecture Notes in Computer Science, Springer Berlin/Heidelberg, August 2006.

[146] R. Moalla, H. Labiod, B. Lonc, and N. Simoni, "Risk Analysis Study of ITS Communication Architecture," in *Third International Conference on the Network of the Future (NOF)*, pp. 1–5, IEEE, Nov 2012.

[147] S. Bhattarai, S. Rook, L. Ge, S. Wei, W. Yu, and X. Fu, "On Simulation Studies of Cyber Attacks Against LTE Networks," in *23rd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, IEEE, Aug 2014.

[148] D. Ren, S. Du, and H. Zhu, "A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs," in *IEEE International Conference on Communications (ICC)*, pp. 1–5, IEEE, June 2011.

[149] K. Bayad, M. Rziza, and M. Oumsis, "Information Security Risk Analysis of Vehicular Ad Hoc Networks," in *Mobile Networks and Management* (R. Agüero, Y. Zaki, B.-L. Wenning, A. Förster, and A. Timm-Giel, eds.), pp. 192–205, Springer International Publishing, 2017.

[150] S. Tayal and M. Tripathy, "VANET Challenges in Selection of Vehicular Mobility Model," in *Second International Conference on Advanced Computing Communication Technologies (ACCT)*, pp. 231–235, Jan 2012.

[151] ISO, "BS ISO/IEC 27000:2014, Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary," tech. rep., BSI Standard Publication, February 2014. ISBN: 978-0-580-83266-6.

[152] A. M. Sanzgiri and S. Upadhyaya, "Feasibility of Attacks: What is Possible in the Real World- A Framework for Threat Modeling," in *Proceedings of 2011 International Conference on Security and Management (SAM 2011)*, July 2011.

[153] A. Panchenko and L. Pimenidis, "Towards Practical Attacker Classification for Risk Analysis in Anonymous Communication," in *Proceedings of the 10th IFIP TC-6 TC-11 international Conference on Communications and Multimedia Security*, CMS'06, pp. 240–251, Springer, 2006.

[154] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, vol. 13, pp. 8–15, 2006.

[155] I. A. Sumra, H. Hasbullah, Jamalul-lail, and M. ur Rehman, "Trust and Trusted Computing in VANET," *Computer Science Journal*, vol. 01, April 2011.

[156] ISO, "BS ISO/IEC 27000:2009, Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary," tech. rep., BSI Standard Publication, July 2009. ISBN: 978-0-580-56554-0.

[157] C. S. Vorugunti and M. Sarvabhatla, "A Secure and Efficient Authentication Protocol in VANETs with Privacy Preservation," in *Proceedings of Ninth International Conference on Wireless Communication and Sensor Networks*, pp. 189–201, Springer, 2014.

[158] M. Mejri and M. Hamdi, "Recent Advances in Cryptographic Solutions for Vehicular Networks," in *International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–7, May 2015.

[159] D. Zax, "A Software Update for Your Car?," tech. rep., MIT Technology Review, March 2012. Available online: http://www.technologyreview.com/view/427153/a-software-update-for-your-car/ (Accessed: 15/10/15).

[160] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)," in *Second International Conference on Network Applications Protocols and Services (NETAPPS)*, pp. 55–60, September 2010.

[161] B. Lipiński, W. Mazurczyk, K. Szczypiorski, and P. Śmietanka, "Towards Effective Security Framework for Vehicular Ad-Hoc Networks," *Journal of Advances in Computer Networks*, vol. 3, no. 2, 2015.

[162] G. Guette and B. Ducourthial, "On the Sybil Attack Detection in VANET," in *IEEE International Conference on Mobile Adhoc and Sensor Systems*, pp. 1–6, Oct 2007.

[163] M. Raya, *Data-Centric Trust in Ephemeral Networks.* PhD thesis, École Polytechnique Fédérale de Lausanne, Switzerland, 2009.

[164] ISO, "BS ISO/IEC 27005:2011, Information Technology - Security Techniques - Information Security Risk Management," tech. rep., BSI Standard Publication, June 2011. ISBN:978-0-580-71714-7.

[165] ETSI, "TS 102 165-1 v4.2.1 (2006-12): Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Methods and Protocols; Part1: Method and Proforma for Threat, Risk and Vulnerability Analysis," tech. rep., ETSI, 2006.

[166] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS Attacks in VANET," *Wireless Personal Communications*, vol. 73, no. 1, pp. 95–126, 2013.

[167] I. A. Sumra, I. Ahmad, H. Hasbullah, and J.-l. Bin Ab Manan, "Behavior of Attacker and Some New Possible Attacks in Vehicular Ad hoc Network (VANET)," in *3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 1–8, IEEE, 2011.

[168] G. N. Nayak and S. G. Samaddar, "Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions," in *3rd International Conference on Computer Science and Information Technology*, vol. 5, pp. 491–495, July 2010.

[169] J. Tobin, C. Thorpe, and L. Murphy, "An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks," in *IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–7, June 2017.

[170] D. Alishev, R. Hussain, W. Nawaz, and J. Lee, "Social-Aware Bootstrapping and Trust Establishing Mechanism for Vehicular Social Networks," in *85th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, June 2017.

[171] M. Chaqfeh and A. Lakas, "A Novel Approach for Scalable Multi-hop Data Dissemination in Vehicular Ad Hoc Networks," *Ad Hoc Networks*, vol. 37, pp. 228 – 239, 2016.

[172] M. Schiller and A. Knoll, "Emulating Vehicular Ad Hoc Networks for Evaluation and Testing of Automotive Embedded Systems," in *8th International Conference on Simulation Tools and Techniques*, pp. 183–190, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2015.

[173] T. Gazdar, A. Belghith, and A. AlMogren, "DTCF: A Distributed Trust Computing Framework for Vehicular Ad hoc Networks," *KSII Transactions on Internet & Information Systems*, vol. 11, no. 3, 2017.

[174] L. H. Son, "Dealing With the New User Cold-start Problem in Recommender Systems: A Comparative Review," *Elsevier Information Systems*, vol. 58, pp. 87 – 104, 2016.

[175] X. Xian, W. Shi, and H. Huang, "Comparison of OMNET++ and Other Simulator for WSN simulation," in *3rd IEEE Conference on Industrial Electronics and Applications*, pp. 1439–1443, June 2008.

[176] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent Development and Applications of SUMO - Simulation of Urban MObility," *International Journal on Advances in Systems and Measurements*, vol. 5, no. 3 & 4, pp. 128–138, 2012.

[177] C. Sommer, J. Härri, F. Hrizi, B. Schünemann, and F. Dressler, *Simulation Tools and Techniques for Vehicular Communications and Applications*, pp. 365–392. Springer International Publishing, 2015.

[178] X. Chen and L. Wang, "A Cloud-Based Trust Management Framework for Vehicular Social Networks," *IEEE Access*, vol. 5, pp. 2967–2980, 2017.

[179] S. H. Bouk, S. H. Ahmed, and D. Kim, "Vehicular Content Centric Network (VCCN): A Survey and Research Challenges," in *30th Annual ACM Symposium on Applied Computing (SAC)*, pp. 695–700, 2015.

[180] M. F. Majeed, S. H. Ahmed, and M. N. Dailey, "Enabling Push-Based Critical Data Forwarding in Vehicular Named Data Networks," *IEEE Communications Letters*, vol. 21, pp. 873–876, April 2017.

[181] S. Olariu, M. Eltoweissy, and M. Younis, "Towards Autonomous Vehicular Clouds," *ICST Transactions on Mobile Communications and Applications*, vol. 11, no. 7-9, pp. 1–11, 2011.

[182] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi, “A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing,” *IEEE Access*, vol. 5, pp. 15619–15629, 2017. doi:10.1109/ACCESS.2017.2733225.