OPTIMIZATION OF IOV SECURITY WITH TRUST MODEL

A Thesis Submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

Electronics and Communication Engineering

By

Indu

Regd. No. – 14SECE3021001

Under the supervision of

Dr. Priestly Shan (Supervisor)

Dr. Sibaram Khara (Co supervisor)

GALGOTIAS UNIVERSITY
UTTAR PRADESH
2020

STATEMENT OF THESIS PREPARATION

1. Thesis title: Optimization of IOV security with Trust model
2. Degree for which the thesis is submitted: Doctor of Philosophy in ECE
3. Thesis Guide was referred to for preparing the thesis.
4. Specifications regarding thesis format have been closely followed.
5. The contents of the thesis have been organized based on the guidelines.
6. The thesis has been prepared without resorting to plagiarism.
7. All sources used have been cited appropriately.
8. The thesis has not been submitted elsewhere for a degree.

(Signature of the student)

Name: Indu

Roll No.: 2200293619

APPROVAL SHEET

This thesis entitled Optimization of IOV security with Trust model by Ms. Indu is approved for the degree of Doctor of Philosophy.

Examiners

_____

_____

Supervisor (s)

_____

_____

_____

Chairman

_____

Date:_____

Place:_____

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis, entitled "Optimization of IOV security with Trust model" in fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Electronics and communication Engineering and submitted in Galgotias University, Greater Noida is an authentic record of my own work carried out during a period from March 2015 under the supervision of Dr. Priestly Shan (Supervisor) and Dr. Sibaram Khara (Co-supervisor).

The matter embodied in this thesis has not been submitted by me for the award of any other degree of this or any other University/Institute.

Indu

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Dr. Priestly Shan
Supervisor
Deptt. of ECE

Dr. Sibaram Khara
Co-Supervisor
Deptt. of ECE

The Ph.D. Viva-Voice examination Indu Research Scholar, has been held on ……..

Sign. of Supervisor(s) Sign. of Co-Supervisor(s) Sign. of External Examiner

ABSTRACT

The Internet of vehicles is rapidly gaining commercial as well as researcher's interest as it has enhanced the capabilities of VANET by merging it with IoT. Trust plays crucial role in IoV network for providing reliable services in network. Trust management among nodes (vehicles) can enhance IoV security by isolating untrusted vehicles and revoking the information with malicious content. But it is quite difficult to model trust in such a dynamic network where node leave and join network in random fashion. Existing trust models for IOV are either rater-based models or ratee-based models. In Rater based models, every vehicle will store the trust value of all others vehicles in its routing table and when any node sends message request nodes checks it's the trust value from its table and according rely on the node. But these models do not work well when any new nodes send message whose trust value is not available in node. Conversely, in ratee-based trust models, each node stores its own trust value rated by different nodes. But cold start problems and scalability are two major issue associated with these models. To fill these gaps, designing a trust model that overcome the disadvantages of rater and ratee based model is significantly required. Our main motive is to propose a trust model that is neither ratee based nor rater based. To accomplish this goal, foremost objective is to augment basic concept of trust by studying existing trust models. This will help to gain the knowledge of of trust, challenges in modelling the trust, types of trust models and factors influencing trust in IoV network.

In this thesis, we propose a Probability distribution Based trust Model (PDTM) to secure communication in IoV. The model is neither ratee based nor the rater based. It stores and update the trust at online centers as each node is connected to the internet. The proposed model is decentralized, scalable, Probabilistic in nature, sensitive to Privacy Concerns and robust against Attacks. This trust model is built using SUMO and MATLAB tools. The trust model framework has been tested in the presence of both types of trust and untrusted nodes for various trust metrics like Number of available hops, PDR and trust value. Simulation shows that the malicious vehicles are

clearly separated from the trusted vehicles using probability distribution curve drawn using statistics of nodes. The nodes will be considered as trusted only if its PDF lies in the range of mean +/-2 standard deviation of the curve. Simulation is carried out for different trust threshold values (θ = 0.65,0.7,0.75) and the metrics viz, PDR, Trust value Average, no. of available hops and success rate are estimated. The results, concludes that the proposed PDTM can be adopted in securing vehicular communication in IOV application. Moreover, this scheme does not introduce much overhead as other cryptographic schemes do. The comparison of this model with ratee and ratee based model proves that PDTM is superior to them in the terms of success rate, transaction number growth and computation time.

ACKNOWLEDGEMENT

Working as an Assistant Professor and doing research for the degree of Ph. D in Galgotias University was quite magnificent and challenging experience for me. In all these years, many people directly or indirectly contributed in shaping up my career. It was hardly possible for me to complete my doctoral work without the precious and invaluable support of these personalities. I would like to give my small tribute to all those people.

Initially, I would express my sincere gratitude to my supervisor, Dr. Priestly Shan, for his valuable guidance, enthusiasm and overfriendly nature that helped me a lot to complete my research work. I give sincere thanks to my Co- supervisor, Dr. Sibaram Khara for his valuable guidance in solving all the hurdles that cropped up at various stages of this work.

I express my gratitude to Dr. B. Mohapatra, Dean of School of Electrical, Electronics and communication Engineering for his support. I would like to convey my deep regard to Dr. Mirza Tareek Beg and Dr. Sandeep Tayal for his wise counsel and indispensable advice that always encouraged me to work hard for completion of the thesis. I thank Dr. Jatin Gera and Dr. Vishal Nangal for their consistent motivation and support.

Finally, this work would not have been possible without the confidence, endurance and support of my family and friends. My highest gratitude goes to my parent and in-laws for their relentless supports, blessing and encouragement. Special mention goes to my husband, Divyansh Sharma, CFA whose time I stole to write this thesis.

I dedicate this thesis to my mother who passed away during the research period. R.I.P.

INDU

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

API	**A**pplication **P**rogramming **I**nterface
AU	**A**pplication **U**nit
CA	**C**entralized **A**uthority
CAS	**C**ollision **A**voidance **S**ystem
C-ITS	**C**ooperative **T**ransportation **S**ystems
DST	**D**empster–**S**hafer **T**heory
DSRC	**D**edicated **S**hort **R**ange **C**ommunication
ECC	**E**lliptic **C**urve **C**ryptography
FCC	**F**ederal **C**ommunications **C**ommission
GPS	**G**lobal **P**ositioning **S**ystem
HMM	**H**idden **M**arkov **M**odel
HTTP	**H**ypertext **T**ransfer **P**rotocol
HTTPS	**H**ypertext **T**ransfer **P**rotocol **S**ecure
IoT	**I**nternet **o**f **T**hings
IoV	**I**nternet **o**f **V**ehicles
ITS	**I**ntelligent **T**ransport **S**ystems
MANET	**M**obile **A**d-hoc **NET**work
OBU	**O**n **B**oard **U**nit
PDA	**P**ersonal **D**igital **A**ssistant
PDR	**P**acket **D**elivery **R**atio
PDTM	**P**robability **D**istribution- based **T**rust **M**odel

P2P	**P**eer **to P**eer
QOS	**Q**uality **o**f **S**ervice
RPT	**R**eal-time **T**ransport **P**rotocol
RTM	**R**atee based **T**rust **M**odel
RSA	**R**ivest, **S**hamir and **A**dleman
RSIs	**Road S**ide **I**nfrastructures
RSU	**R**oad **S**ide **U**nit
SUMO	**S**imulation of **U**rban **Mo**bility
TraCI	**T**raffic **C**ontrol **I**nterface
VANET	**V**ehicular **A**d-hoc **NET**work
V2H	**V**ehicle **to H**uman
V2R	**V**ehicle **to R**oadside Unit
V2S	**V**ehicle **to S**ensor
V2V	**V**ehicle **to V**ehicle
WAP	**W**ireless **A**ccess **P**oint
WHO	**W**orld **H**ealth **O**rganization
WSN	**W**ireless **S**ensor **N**etwork

LIST OF PUBLICATIONS

During this PhD, I published some papers in different journals and conferences. This section presents the details of the articles published during this Ph.D. work.

S.No.	Title of the Publication	Name of Journal/Conference	Database	Impact Factor	Date of Publication/Research Paper
1	A Framework to systematically analyse the trustworthiness of nodes for securing IoV Interactions	Scalable Computing: Practice and Experience	Scopus and Web of Sciences	SJR= 0.172 SNIP= 0.472	Volume 21, Issues 3, pp. 451–462, 1 Aug 2020 https://doi.org/10.12694/scpe.v21i3.1743
2	Review of Nature and Computation Methods of Trust Models in Vehicular Networks	Journal of Advanced research in dynamical and control systems	Scopus and UGC approved	0.27	Volume 11 | 07-Special Issue, August 2019 https://www.jardcs.org/abstract.php?id=2043
3	Internet of Vehicles (IOV): Evolution, Architectures, Security Issues and Trust Aspects	International Journal of Recent Technology and Engineering (IJRTE)	Scopus	Impact factor 1 Citations=1	ISSN: 2277-3878, Volume-7, Issue-6, March 2019 https://www.ijrte.org/wp-content/uploads/papers/v7i6/E2106017519.pdf
4	An Analytic study of Security solutions for VANET	International Journal of computer applications	International Journal	0.33	volume 132 (10), December 2015 10.5120/ijca2015907563
5	Research trends in Security, Architecture, services and Applications of Internet of vehicles (IOV)	IEEE International conference GUCON	Scopus	---	28-29 Sep 2018 10.1109/GUCON.2018.8674992

Chapter 1 OVERVIEW

Internet of Vehicles (IoV) is leading step towards the development of intelligent transportation systems. IoV has vehicular Ad-hoc network (VANET) features by merging it with the Internet of Things. The IoV has influenced transportation industry due to its salient features like ephemeral interactions, reliable internet and high computation capabilities. But security system of IOV network is still hinderance in its deployment. In this network, it is difficult to recognize which node is trusted and how much extent. Although various trust models are available for reliable and secure communication in VANET and IOT, these models are not effective for securing communication in IoV due to involvement of huge data sets. So, there is a need to develop efficient trust model for IoV that can secure network interactions. This chapter presents the introduction to our work trust, motivation behind IOV trust and objectives of my research followed by organization of thesis.

1.1 Introduction

IoV is gaining popularity after VANET in developing Intelligent transportation system. Technological development in the field of automobiles have enabled vehicles to gather, manage, and store traffic-related information to avoid road incidents [1]. However, numerous calamities are still faced randomly where human pay the toll of their precious life in accidents [2]. Every year many persons die in severe road accidents which make it foremost cause of death world-wide [3]. According to WHO report in 2018 [4], accident fatalities rate has reached up to 1.35 million from 1.2 million in 2015[3]. Besides that, growing vehicles on road has made traffic congestion as a global issue that further results in unnecessary fuel consumption, time wastage, and excessive environmental pollution. To overcome these issues and make safe and efficient journey, ITS introduced IoV that create better infrastructure for safe road transportation [5][6]. It emphasis on increasing road safety and driving comfort for drivers as well as passengers through their entire journeys [7]. To support vehicular networking, a dedicated spectrum of 75 MHz at 5.9 GHz band has already been

allotted by the FCC in USA[8]. In 2008, ETSI has also provided a 30 MHz spectrum for vehicular networking in 5.9 GHz band [9]. This Allocation of wide DSRC spectrum empowers various potential applications like real-time traffic management, safety applications, mobile Internet access and on-board entertainment [10].

IoV is an enhancement to the capabilities of VANET by collaborating it with IoT. Internet connectivity to vehicles will take automobiles industry to next level [11][12][13]. Although, IoV network resolves the traffic related issues by reducing traffic congestion, fuel wastage, road accidents, and pollution, it introduces some security challenges.

In IoV, trustworthiness of data and entity play significant role in making reliable decisions. But modelling trust in IoV is quite difficult because of its the empirical nature. IoV network is open for the nodes to leave and join anytime and high internet connectivity features of IoV make it easy target for security threats. IoV network vehicles communicate to spread safety messages related to accidents, road jams, road construction etc that needs to be communicated correctly and timely. But sometimes, malicious users can easily gather, transmit, replay false information to create forgery that may lead to accidents or unnecessary delays. So, there is a need of trust establishment that can help each node in IoV network to detect dishonest node and malicious information sent by these nodes.

Researchers are working on trust models from the time of VANET. Various system related to life-critical applications has been developed for e.g. collision avoidance system[14], traffic view systems[15], crash reporting system[16], safety-related message spreading systems [17] etc. The main focus of these systems is assuring reliable delivery of data among vehicles. Consequently, less heed was paid on assuring the quality of data sent by vehicles. Existing trust models for vehicular network exhibits various limitations. To overcome the limitation of ratee based model and rater-based model, a Probability Distribution Based Trust model (PDTM) is proposed for IoV where nodes neither stores the reputation of other nodes nor that of their own. The proposed method is a hybrid trust model that will estimate the

trustworthiness of sender as well as the data send by the sender. PDTM separates the trusted and non-trusted nodes by collecting their statistics during the interaction. The entity-based trustworthiness is estimated by comparing trust value by pre-set threshold. The trust value indicates the degree upto which node can be trusted using its behaviour in last interaction. Data based trustworthiness is estimated by collecting the node statistics during interaction. The PDTM is simple, distributed in trust computation, scalable and robust against forgery and Sybil Attack because of non-locality principal. Moreover, it has very low complexity.

1.2 Motivation

The following section includes the various scenarios related to IoV domain that motivate the need for trust model. These scenarios explain the issues related to traffic routing and nodes trust that may occur in the IoV domain. The motivation behind IoV is daily life traffic congestion. The motivation behind trust management is Dishonest nodes in IoV environment. This section initially explains how traffic congestion may occur due to lack of traffic situation awareness and then explains how agents could easily be misled if the information being received is not treated critically.

1.2.1 Traffic Congestion

This section presents the scenarios where drivers in a city encounter traffic congestion. The malicious users can easily capture, modify, replay and delete the important traffic-related resulting in traffic congestion. For example, Selfish vehicles may send a fake message of accident ahead. As a result of this, all vehicles on road will go on nearby alternative road. This may create traffic jam on alternate road. The congestion delays described could be avoided through trusted situational awareness of congested roads.

Sybil attack may counterfeit traffic flow scenario by disseminating false messages with multiple identities, that often causes traffic congestions and vehicular accidents. In sybil attack, malicious node will play the role of several distinct nodes to

cheat the other vehicles, or destroy the security rules with its multiple identities which are illegally obtained by the way of forgery, theft or conspired sharing. Sybil attack may bring serious threats to VANET. For example, sending false messages and fabricating traffic scenarios affect the normal travel.

Unexperienced driver: A driver (D1) is unfamiliar with the city and is passing through it to reach a destination (S1). D1 relies on typical GPS system, follows its directions and choose shortest path to reach S1. The shortest path was through the main road due to which D1 stuck in congestion and was delayed in reaching S1. If D1 had chosen any side road avoiding the main road, he would had saved precious time rather than getting struck in congestion.

Experienced Driver: A Driver (D2) driving a car needs to reach the destination in minimum time. D2's destination is the parking garage of his office. D2 has also turned on a GPS system, that suggests a similar route to that of D1's via main road. But D2 has been living in that area for long time, so, is familiar with city's internal routes. D2 knows well that the route suggested by GPS is shortest path but it will be quite congested, so he will be delayed a bit longer. Thus, D2 ignores the GPS suggestion and choose a side route to reach his destination. During D2's detour, numerous things may go wrong. For e.g., while Driver D2 is trying to reach his destination via side route, D2 might be unaware of an accident that could cause him to be late for office. D2 might be unaware that the side route has also had growing popularity with the veterans. Even though side path is not as jammed as main road, still taking a main road route could have saved D2 some time.

1.2.2 Dishonest Drivers

In IoV, vehicles in a city communicate with each other about traffic scenarios. The driver in the vehicle fully trusts on the received information. But some nodes are malicious, self-centric and dishonest. They may take advantage of network by disseminating fake message to other nodes that their current road is highly congested. Consequently, the node takes another road that he believes less congested and is delayed unreasonably. Moreover, there may be self-centric nodes that refuse

providing services due to selfishness reasons. These scenarios can be avoided through trust modelling.

1.2.3 Traffic causalities

The growth of traffic casualties has become a serious matter all over the world. The reliable communications between vehicles will help in decreasing traffic casualties[18]. A massive growth has been predicted in on-road vehicles [13] that would be challenging for connected vehicles market [19].

1.3 Problem Formulation

The problem of trust modeling has been addressed in the different network like P2P, adhoc, VANET, IoV etc. using different methodologies. But the literature survey related to vehicular network trust modelling concludes that existing trust-based models are designed for VANET, the trust modelling in IoV network is still in infant stage. Due to internet connectivity the IoV networks are more prone to malicious activities. So, there is a need to design trust model for IoV network. The trust schemes designed for IoV networks are either entity centric or data-centric. But there is no single combined trust framework that can calculate entity as well as data trustworthiness. So, there is a need to design hybrid trust model for IoV network.

To enhance the security and Scalability in IoV, it is quite important that instead of centralized server, nodes should itself compute the trustworthiness of other nodes and data received. But in most of the existing models trusted centralized servers issue a digital certificate or the key for behaviors of other vehicular nodes. This trust computation by Centralized server does not suits well to distributed IoV network and affect network scalability. Thus, it is required to design a trust framework to compute trust in distributed manner. Some trust models like RTM utilize cryptography to guard the routing information throughout communication which increases the computational complexity as well as time complexity. Thus, Security in such models is achieved at cost of quality of service (QOS). But since IoV is a dynamic network it requires low computation complexity and a less delay to maintain the QoS. So, we will design a

decentralized trust framework to secure IoV using minimum computational overhead and minimum time complexity so that the security of Network can be enhanced without negotiating the Quality of service.

The literature shows that existing trust models are not robust against various common attacks like middle man attack, forgery etc. So, there is a need to design a robust trust model which can be deployed effectively against malicious behavior. Our aim is to find an approach to make the proposed trust model robust against the malicious behavior so that the network can withstand effectively in the presence of malicious peers. Some trust models are grounded on past interactions history which is unfeasible to implement in vehicular network. Some trust models require the unique identities of each node to be known which violates user privacy. Some trust models are not robust enough against attacks in network. Furthermore, most of the trust models are rater-based in which all node stores the reputation of other nodes with which they interacted previously. These models do not work efficiently when a node encounters an unknown node. Although the mentioned problem with rater-based trust model is addressed by some researchers by providing the ratee based trust model in which all nodes store their own reputations ratings provided by others. But there are two limitations of ratee based trust models which are unaddressed i.e. cold start problem and scalability problem.

To address these issues, we propose PDTM, where nodes store neither their own reputation nor that of other nodes during any transactions, trust is considered as a service and stored online at trusted center making use of Internet of things, nodes are capable of calculating the trust of the corresponding nodes but the update is not stored locally rather updated online. This is done to improve interactions between the vehicles and its transaction time. As most of the interactions in IoV are very short term and dedicated trust management system makes it very difficult to manage especially if we are using encryption policies whether public or private. In our proposed work the nodes are capable of calculating trust of the corresponding nodes post communication and updating online as each node has internet connection. It also collects the trust of the existing node even before the communication has started thus eliminating dedicated storage for trust in dynamically changing topologies and

accelerated routing updates for lower routing overhead and improved QoS.

1.3.1 Problem Statement

To design a trust-based security mechanism for IoV application that is lightweight (low complexity) updatable, supports heterogeneous devices and can be applied to routing IoV layer. We need to design Trust based policy that provides Decentralized Trust calculation, Scalable, Probabilistic in nature, Robust against Attacks.

1.4 Research Objectives

This Research work has two main goals. First one is to investigate the basic concept of IoV, trust, trust evaluation mechanism, existing trust models for IoV that gives better understanding of the trust concept and challenges. Second one is to provide a model for evaluating trustworthiness of nodes as well as data. To achieve these goals, we have set following objectives:

1. ***To explore the state of art of IoV, its architectures, applications, services, trust, trust establishment techniques and challenges.***

   Understand the basic concept of IoV, architectures of IoV, concept of trust, trust establishment techniques and evaluation mechanism according to the latest research done in both vehicular network and IoT. Identify the challenges for modelling trust in IoV network.

2. ***To explore the trust evaluation mechanism and management approaches in different networks especially VANET and IoV***

   Investigate trust management techniques and fameworks in various networks like Social Sciene, E-Commerce**,** distributed systems P2P, WSNs, Ad-hoc networks, VANETs, IoT and IoV. Identify the various methodology as well as the pros and cons of approaches used to obtain the research gaps.

3. ***To Propose a trust definition and framework for modelling the trust worthiness of nodes during interaction in IoV network***.

Design a to hybrid trust model for IoV to fill the research gaps. The model will be based on probability distribution and it will validate nodes as well as data.

4. ***To Evaluate proposed model by implementing it in appropriate simulator.***

   Simulate the proposed model to evaluate its performance based on various evaluation metrics like PDR, Trust Dynamics, Available no. of hops, and success rate. The proposed model is simulated to show how malicious nodes are separated from the normal nodes to secure the IoV interaction

5. ***Compare proposed model to the existing trust model in IoV network.***

   Compare proposed framework with existing model to ensure how it is better than the already existing models in IoV network and obtain results in comparison with ratee and ratee-based model.

Table 1.1 Objectives and Methodology

S.No	Objective	Methodology
1	To explore the state of art of IoV, its architectures, applications, services, trust, trust establishment techniques and challenges.	Conducting literature study related to IoV, architecture of IoV, trust concepts, its related properties and techniques used for trust modelling
2	To explore the trust evaluation mechanism and management approaches in different networks especially VANET and IoV	Conducting literature review of various trust models mainly related to VANET and IOV to identify the methodologies used in it.
3	To Propose a concept of trust and trust framework for modelling the trust worthiness of nodes during interaction in IoV network.	Theoretical trust framework to suit IoV features considering QoS trust, Distributed trust, Probabilistic approach for aggregation
4	To Evaluate proposed model by implementing it in appropriate simulator.	Simulation using SUMO as network simulator and MATLAB as event simulator for evaluation metrics PDR, No. of hops, trust dynamics and success rate.
5	Compare proposed model to the existing trust model in IoV network.	Simulation-based comparison of proposed model with rater and ratee based trust model using success rate, transaction no. and computation time.

1.5 Research Contributions

The foremost contribution of my research involves introduction to a probabilistic trust concept along with designing of hybrid trust framework in the IoV environment that evaluates the trustworthiness of nodes as well as data. The second contribution is the simulation of the proposed trust model to show how malicious and normal nodes are separated on the basis of PDR, no. of available hops, Trust dynamics, success rate. The third contribution is to compare proposed PDTM with rater and ratee-based trust models in terms of success rates.

1) **A Probabilistic concept of trust along with a definition of trust as a measure of probability.**

2) **Hybrid a trust framework for modelling the trust worthiness of nodes and data in IoV environment**
   - A Threshold-based trust approach is proposed to ensure the node trustworthiness. This approach authenticates network nodes comparing their trust values with preset trust threshold. Since threshold-based approach is able to validate nodes without involving complex computation. So, node interaction can be established in timely manner that suits to the dynamic and decentralized nature of IoV network.
   - A Trust initialization and storage mechanism to handle the cold start problem and scalability issues faced by existing models.
   - A joint probability-based approach is presented to update the trust at online centres. The trust is calculated by evaluating the trust worthiness of data using various statistics collected during interaction.

3) **Performance Evaluation of proposed PDTM using network simulation**
   Computer simulations used to evaluate the effectiveness of the proposed trust model in separating malicious nodes from the trusted nodes and discarding them. By using this model, the malicious nodes will no longer be able to harm the network.

4) **Comparison of the proposed PDTM with the existing trust model in IoV network.**

   Simulation based performance comparison shows that the Proposed PDTM is better than the ratee based and rater-based models in terms of computation time, transaction number growth and success rate.

1.6 Thesis Organization

The complete thesis is organized into six chapters as follows:

Chapter 1 presents importance of trust, difficulties in modelling trust in IOV, motivation behind IOV trust, the problem formulation and objectives of this research work followed by detailed structure of the thesis.

Chapter 2 presents the background of VANET and IoV and the state of art of trust in IOV.

Chapter 3 involves literature reviews of trust model proposed in different networks like P2P, distributed networks, ad-hoc networks, VANET, IOT etc. In the end this chapter involves some challenges identified in modelling trust and research gaps.

Chapter 4 proposes probabilistic concept of trust and hybrid trust framework, trust modelling, and methodology involved in PDTM implementation.

Chapter 5 presents the results and discussions. The Proposed PDTM is evaluated to ensure that the problems identified in research gaps are resolved. The chapter also involves the performance comparison of proposed PDTM with ratee and rater-based models.

Chapter 6 gives concluding remarks of the work and future aspect for the proposed work.

Chapter 2 LITERATURE REVIEW

The IoV is a special Class in the IoT. It is now becoming a popular solution to deal with road safety issues. The IoV provides uncountable opportunities and each automotive manufacturer can get benefit from that. Since IoV is evolved from the concept of VANET, a discussion of VANET and IoT is vital to comprehend IoV. This chapter explains features, applications and the complexities of IoV. As the work in this thesis is based on trust management, So, this chapter also includes the state of art of trust in IOV.

2.1 Background on VANET

VANET is a network of vehicles[20] that aims on improving road safety and driving efficiency. VANET [21]considers moving car as a node and uses ad hoc technology and wireless LAN for vehicular communications. VANETs are distinguished from other kinds of MANETs in terms of high node mobility, ample energy, hybrid network architectures and ample computing powers.

2.1.1 Conventional VANET

VANET architecture comprises of mainly three divisions as shown in Figure 2.1 [22]. These three domains are in-vehicle, ad-hoc and infrastructure division.
The components involved in architecture are vehicular node and road-side unit (RSU). On-board unit and Application unit (AU) installed in vehicle form in vehicle division. Ad-hoc division is comprised nodes interacting independently without an infrastructure. Infrastructure division includes RSUs and hotspots internet access. AU is an entity that is embedded or pluggable in vehicle and executes applications using OBU. Examples of AUs are device for hazard-warning, navigation system having communication capabilities. The AU can communicate with the network only through OBU that performs all mobility and networking functions. Single OBU can support multiple AUs at same time. OBU allows for communication among vehicle and vehicle with infrastructure[22][23]. It delivers communication services to the AUs.

Nodes can connect to the infrastructure available in their range via access point (WAP) or router.

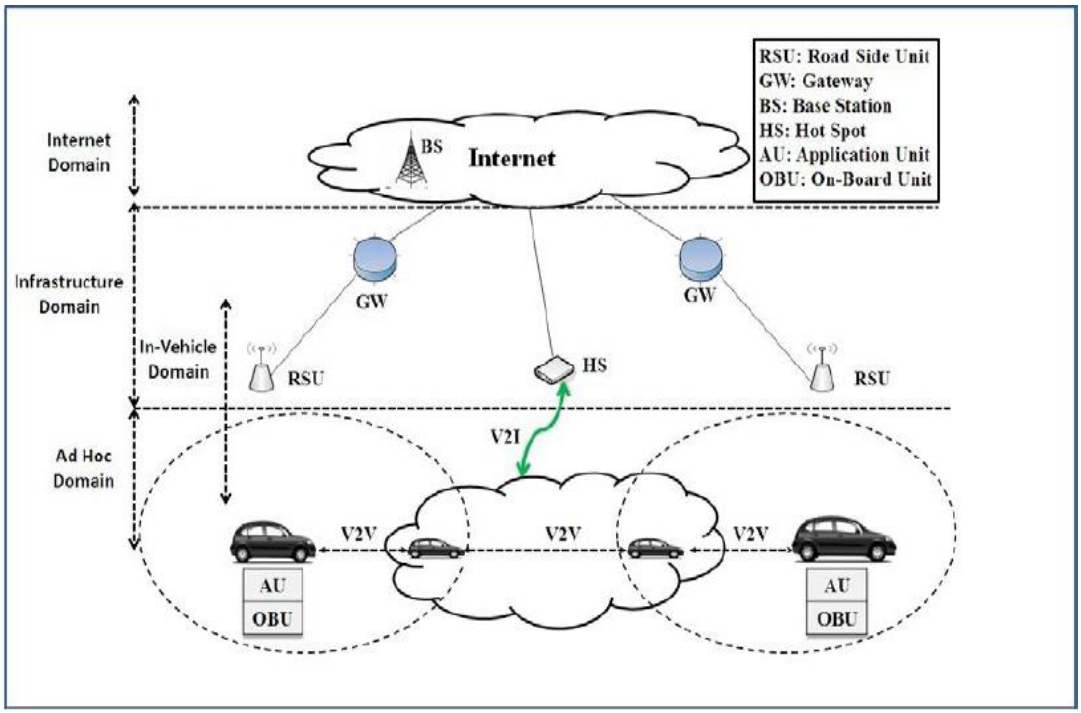


Figure 2.1 View of VANET Architecture

2.1.2 Limitations of VANET

Although VANET provides huge opportunity in the transport field [24], it has numerous limitations like lack of purely ad-hoc architecture [25], non-availability of cloud computing [26], device incompatibility [27], untrustworthy Internet connection[28], low service accuracy.

1. **Lack of purely ad-hoc architecture** The VANETs framework is not able guarantee universal facilities using intelligent transportation system (ITS) applications. When a vehicle moves outside from ad-hoc network range, it does not get the services of that network[25].
2. **Non-availability of cloud computing** – Due to vehicle limited computed and storage capability and cloud computing service in VANET, big data mining based decisions are not supported by it [26].

3. **Incompatibility with personal devices-** Even after the significant growth of PDs in our day-to day life, these PDs are not supported by VANETs[27].
4. **Unreliable Internet connection** - Internet connectivity is not guaranteed in VANET current framework. So, it is less popular commercially because commercial applications are dependent on reliable Internet connection [28].
5. **Low service accuracy**- In ITS, the services are less accurate as the computations are done using local knowledge of the traffic.
6. **Cooperative operational dependency –** The Operations of VANET are extremely dependent on support of its users that reduces the reliability of services of VANETs.

Developed countries like the America attempted to deploy VANET but could not deploy it fully because of less commercialization scope[18]. This lead to the birth of a new network called IOV[29] that merged conventional VANET with Internet of things (IoT)[30]. IoV can be a network to overcome the limitations of VANETs like commercialization problems and growing traffic casualties.

2.2 Internet of Vehicles

IoV refers to the progression of traditional **VANET,** that refers to the real-time communication among its different entities like vehicles, RSU, pedestrian, RSI, sensors using navigation systems, mobile-communication technology, smart-terminal devices etc. It allows the vehicles in network to gather and share safety related information with each other and infrastructures using VANETs. Moreover, it performs the processing, computation, sharing of information on platforms, like Internet systems. Using this information, the information platforms effectively guide and supervise vehicular nodes. In IoV, vehicles are assumed as smart object furnished with an influential multisensory platform, calculating units, communication technologies, internet connectivity. IoV can handle large amount of data and enable the communication among different network elements to provide road safety services to passengers and drivers[31]. The concept of IoV has been explored by various researchers recently but it has not evolved to its fullest. Transportation system in

Japan and Europe have tried to implement IoV partially. In United states, security chips are mounted in vehicles to recognize their identity online [32]. In Delhi, registered autos, all government buses, electronic vehicles are furnished with GPS [33]. European Commission is contributing to design Cooperative Transportation Systems (C-ITS) [34]. The developed countries counties like UK, US and Australia has started putting their efforts on 'Connected Vehicles' [35]. Google has tied up with various companies to develop an Android system for the 'connected drive' [36]. A CarPlay' system is developed by Apple to enable driver to use all iPhone services through car display with voice support [37]. All these above-mentioned steps are leading toward progress of IoV.

2.2.1 Definition

Internet of Vehicles is network of vehicles interacting with one other and with the pedestrian/human's handheld devices using internet connection [38]. This creates system having intelligent devices as its participants. The IoV builds a vehicle sensor platform, that collect information from the network environment, different vehicle and the drivers. All this is done for traffic management, accident avoidance, safer navigation, and pollution control. Different researchers have tried to define IoV in recent literature. Table 2.1 presents the definitions of IoV

Table 2.1 Definitions of IoV

Study	Definition
[39]	IoV is propitious paradigm for the future of automobiles, that will certainly boost automobile market and accelerate the innovations in services and applications of internet.
[40]	IoV technology is referred as dynamic communication systems which enables communication between vehicles as well as public networks using different types of interactions like V2V, V2R, V2H and V2S
[41]	In IoVs, every vehicle and RSU are enabled with internet and capable of interacting with one another using DSRC.
[42]	IoV is a sub set of IoT that has achieved significant progressions using various communication technologies.

2.2.2 Network architecture

The three key network components of IoV are clouds/servers, connections and Vehicles (Figure 2.2). A general architecture of IoV network is shown in Figure 2.3.

Figure 2.2 Key Network elements of IoV

The following subsections describe the IoV components and their roles in network in detail.

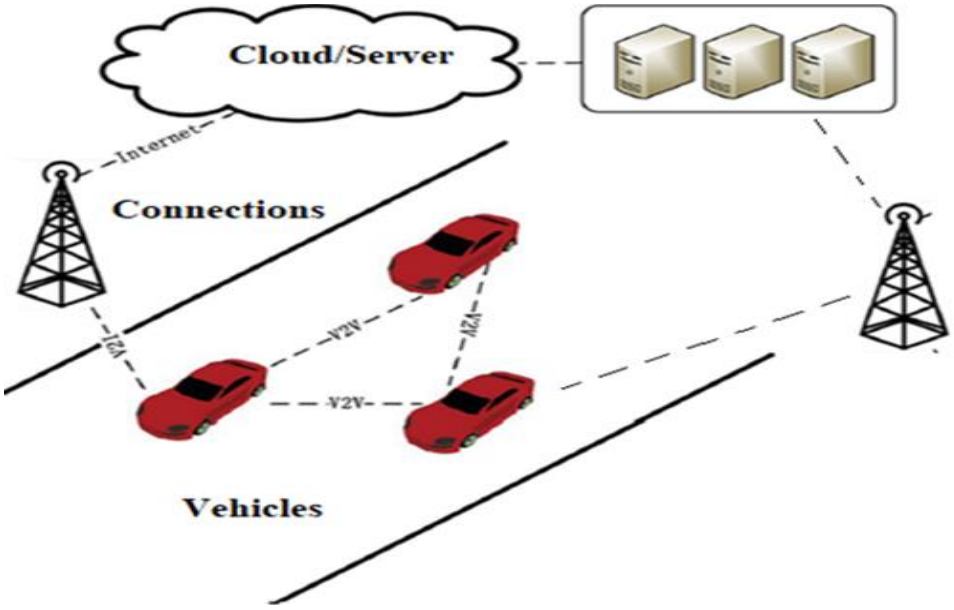


Figure 2.3 Network Model of IoV

Vehicles in IoV are the smart nodes having sensors, internet connectivity and communication devices equipped with them. Sensors are used gather the information whereas communication devices are utilized in establishing communication with other network elements. To process this gathered information and control all devices, the vehicles are also equipped with an operating system. Vehicles in IoV perform dual

role: one as a client to use services from Internet and second as peers for distributed computation. Evidently, IoV is a network having peer-2-peer (P2P) as well as client-server (CS)computing model. In P2P model, vehicles team up and help other vehicles to execute distributed computing functions. The Servers are categorized in of two types i.e. cloud data centre or a normal computing node. With these servers IoV can perform various complicated tasks and applications.

Connections in IoV: IoV involves wireless connection among various entities like vehicle, RSU, sensor, Internet, pedestrians. Two main wireless connections are V2V and V2R. V2V wireless link connects vehicles with other vehicles in ad-hoc way by creating VANETs. A newly developed standard IEEE 802.11p marks a crucial step towards next phase development of inter-vehicular communication. However, V2V connection link is limited to major network effects. V2R link connects the vehicle with infrastructure available on roads like traffic signals, warning signs on road, toll booths etc. Only Smart RSU like traffic signals compatible with the network will be able to communicate with the vehicle. With connections, IoV's can exchange data amongst vehicle, roadside infrastructure and Internet. This will help to support numerous applications by IoV like Internet services and ITS.

Servers IoV: Severs might deliver different facilities to vehicles. These data servers have huge computing power and storage capacity for real time data about accident etc. Therefore, all progressive and cutting-edge applications must involve these cloud servers. These are operated through internet and from numerous remote locations as a result these are immune from natural disasters and other calamities. Cloud data centers provide flexibility in terms of network bandwidth, memory, storage, CPU cycle which can be consumed on demand. In case of specific requirements resources can be resources can be automatically scaled as per workload. This new innovative approach can not only improve productivity but also enhance capacity at fraction of cost for IoT information processing.

Currently, several architectures have been proposed for IoV table 3 provides a summary of these architectures.

Table 2.2 Comparison of Architecture

Study	Layers	Security	Interactions
Sejin chun et al. [43]	Two	Not specified	V2V, V2R,
Liu Nanjie [40]	Three	Security as service	V2V, V2R, V&I, V&P
Wan et al. [44]	Three	Cross layered security	V2V, V2R
Gandotra et al. [45]	Three	Not specified	D2D
F. Bonomi [46]	Four	Cross layered security	V2V, V&I
Kaiwartya et al. [47]	Five	Security plain	V2V, V2R, V&I, V&P, V&S,
Juan and Sherali [48]	Seven	Security as layer	V2V, V2R, V&P, V&S, R&P,V&I, D2D
Darwish et al. [49]	Thirteen	Cross layered security	V2V, R&P, V&I, V&S, V2R, D2D

2.3 Interactions in IoV

IoV uses different wireless access technologies (WAT) to create connections with cloud/servers because of its heterogeneous nature. These WAT are categorized into three types i.e. 1) vehicular communication, 2) cellular mobile communication 3) short range static communications (see Figure 2.4).

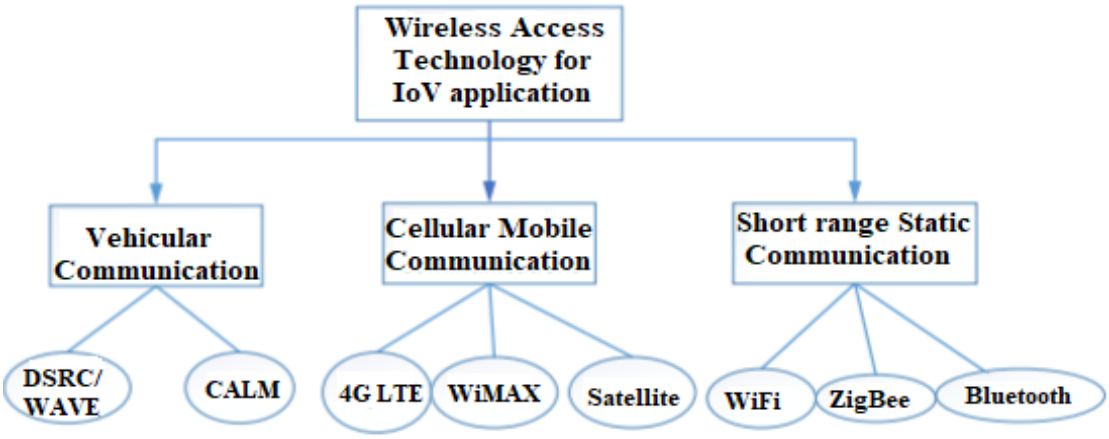


Figure 2.4 Wireless access technologies for IoV application

IoV provides traffic management and safety by involving various communication among network components. Figure 2.5 shows interactions involved in IoV

1. *Infrastructure and vehicle interaction* - It enables the vehicles interaction with nearby infrastructure like parking, hospital etc. in case of emergency. For e.g. accident related data is reported from the OBU on the vehicle, to the server/cloud. Cloud forwards it to the respective Infrastructure i.e. hospital in the case.

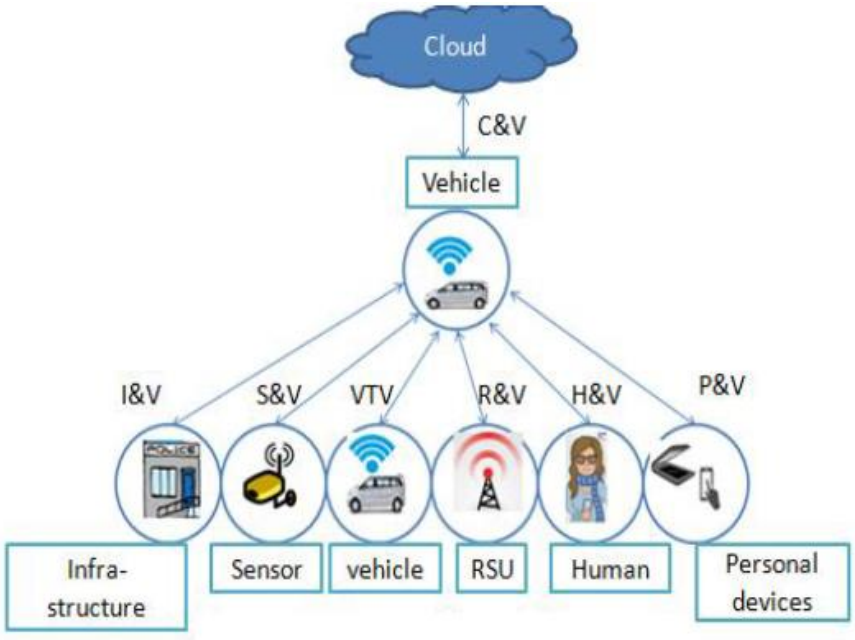


Figure 2.5 Types of Interactions in IoV

2. *Sensor and vehicle interaction*- In S&V interaction, vehicles interact with the sensors on sign boards, traffic lights, roads to gather traffic alerts and updates. The vehicular sensors sense its vicinity events to provide collision avoidance and lane change alters
3. *Vehicle to Vehicle interaction*- Interaction between vehicles involves the dissemination of information like Proximity between the vehicles, speed of other vehicles within a particular range of a Vehicle, Tyre burst related accidental information.
4. *RSU and vehicle interaction*- RSUs are static devices that is generally mounted over dedicated locations like at roads intersection, parking space. Vehicles interact

with fixed RSUs connected to the internet to provide entertainment related facilities.

5. *Human and vehicle interaction:* It enables the vehicular nodes to connect with pedestrians/bicyclists to convey their intent to them so that they can act accordingly.
6. *Personal devices and vehicle interaction:* Vehicles can interact with different personal devices like cell phones, PDA, laptops etc. in it.
7. *Cloud vehicle interaction:* Cloud/server is main hub through which whole data will pass. Vehicles support inadequate storage and computation for applications such as in-vehicle entertainment, location-based services, as these applications involves large computations and big storage. In vehicle-cloud interaction, vehicular nodes can call cloud-based services independently. Common protocols used for Vehicle-cloud interactions are HTTPS, RPC, HTTP, and direct API calls. For Vehicle to cloud interaction in lov, each vehicle has a unique API key

2.4 Application of IOV

The IoV applications are quite vast and miscellaneous. These applications are classified into three kinds (1) Safety-related application (2) Efficiency- related Applications (3) Comfort- related applications. Figure 2.6 provides the detailed taxonomy of IoV applications.

2.4.1 Driving Safety application

The driving safety applications are based on M2M communication. The main goal for these applications is to prevent or mitigate the accidents by avoiding collisions. These applications augment performance of driver and his driving quality by automatically controlling the wheels. So, they diminish the efforts required for quality driving. Safety-related applications are Collision Avoidance and Emergency call.

1. **Collision Avoidance-** Collision avoidance system (CAS) involves M2M communication and prevents accidents by exchanging traffic related information between vehicles. It uses radar/sensors (like lasers and cameras) to notice crash,

and accordingly alert the driver. Safety related application are generally referred as cooperative collision avoidance system [50], that extends CAS by disseminating CAS data to neighbouring vehicles[51][52]. CCAS provides cooperation among the vehicles to reduce multiple vehicles. CarTALK 2000 [53] is an example of CCAS. Authors in [54] defined special policies for congestion-control during emergency.

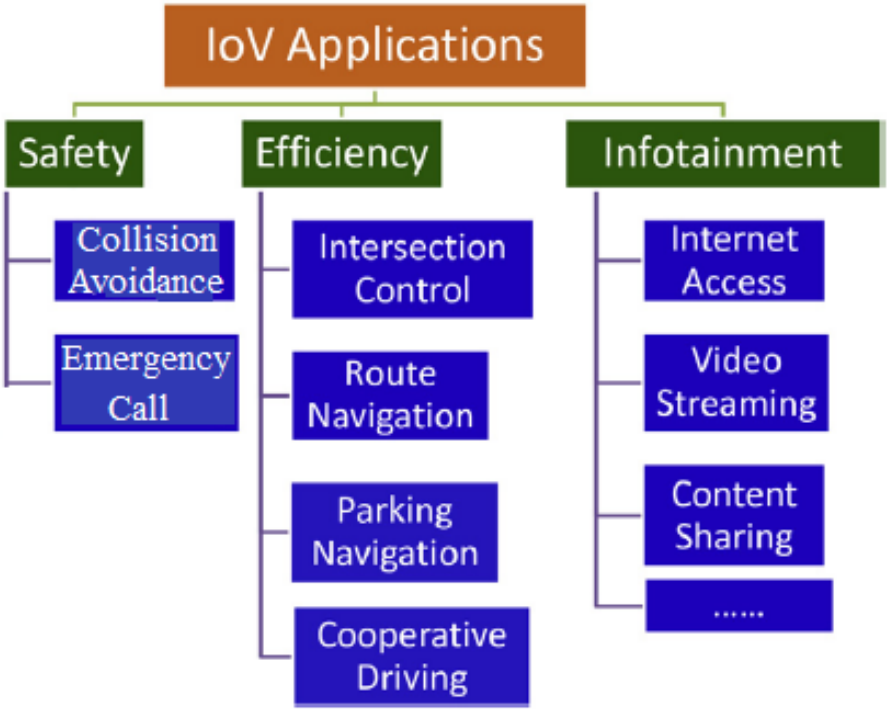


Figure 2.6 Taxonomy of IoV applications

2. **Emergency Call-** IoV enables the Emergency call system in vehicles which is used to contact police, fire etc. during emergency time. It is manual as well as automatic. This call conveys situations of vehicle including cause of emergency, number of passengers, location, direction, speed etc.

2.4.2 Transportation efficiency-related application

Main aim of Efficiency- related applications is to augment vehicular mobility within IoV. Some Efficiency- related applications are as follows

1. **Intersection control:** The IoV control road traffic at junctions by scheduling traffic lights in accordance with volume of traffic. This will diminish unnecessary time wastage at junctions and thus improve the driving efficiency. Traffic-light

scheduling can be achieved based on V2V communication [55] or using V2I communication [56][57][58].

2. **Route Navigation:** IoV overcomes the drawbacks of GPS navigations. Authors in [59] proposed to build real-time information-based navigation route. Work in [60] proposed an algorithm for route-selection optimizing road utility.
3. **Parking Navigation:** IoV is helpful in searching for a vacant parking space in urban environment. Authors in [61] proposed a smart-parking scheme. In study [62], free parking places are discovered automatically.
4. **Cooperative Driving:** This application is utilized in driving a a queue of vehicles as one vehicle. Study [63] discussed the cooperative driving for blind crossings and proposed a safety driving pattern for vehicle's collision-free movements at crossings.

2.4.3 Infotainment

Due to internet connectivity, IoV provides better Infotainment services that includes file sharing among vehicles mainly video sharing. These applications depend on on reliable Internet connection. Various schemes proposed for video streaming by researchers are SVC-based streaming [64], Vehicle to vehicle live video streaming[65], Cooperative Video Streaming [66] etc.

2.5 Characteristics of IoV

IoV mainly consists of vehicle nodes which are quite different in functioning from wireless nodes. As a result, there are numerous characteristics which might bring few tests for development of IoV technology and also bring some positives with them.

1. *Extremely dynamic topology*: Vehicles move at very high speed as compared to other mobile nodes. This results in frequent changes in vehicular network topology.
2. *Changing network density*: The network density may be extremely high during peak hour whereas it could be low in case of fewer vehicles on the road. In both the given scenarios network can disconnect frequently.

3. *Large scale network:* In dense urban areas like highways, centers of city, entrances to city etc. the network scale can be large. This might result in network congestion.
4. *Predictable mobility:* Nodes of MANET move in random direction whereas vehicles follow a set road path. These vehicles have to follow traffic rules like stopping at red light, obeying road signals which make their movement predictable.
5. *Adequate storage:* Vehicular nodes have enough space available with them as compared to other network nodes. This is because vehicular nodes are cars rather than tiny handheld devices.
6. *Numerous communication environments:* There are two forms of communication available for operations of vehicular network. In cities the communication is complex where areas are separated by trees, buildings and other kind of hindrances; as a result, there is not always line of sight communication. In highway driving, the communication is easy and straight.

2.6 Challenges in IoV

The IoV applications are reasonable distinct from other similar networks. Therefore, the IoV network arise some challenges in its implementation.

1. *High Node mobility:* The high node mobility and the dynamic network topology causes recurrent link failures or network disconnections that may lead to message loss. So, it is quite challenging to establish long connection link.
2. *Real-time Communication:* Delayed transmission of message sometime makes it meaningless. For e.g. in case of emergency situation like a car crash, the average delay time in sending the signals might result in loss of life. Therefore, signals must be sent in real-time in these circumstances.
3. *Consistency and reliability of Service:* Services of IoV require more than 99% of accuracy in order to install trust amongst its users. In case of accidents and other life-threatening situation reliability of service is crucial. But due to large scale coverage, complex network model and poor topology of network attaining

consistency and reliability of service is tough. To accomplish these, new innovative techniques must be used in order to design network architecture.

4. *Large scale deployment:* Another big challenge in IoV is its high scalability. IoV requires huge number of nodes and deployment area. Therefore, a need for high scalability of IoV technology exists.
5. *Network Security:* IoV is an open network in which vehicles randomly join and leave. Also, the Internet connectivity makes the network more vulnerable to security threats. Any malicious node may disseminate false information or temper with transmitted information for its own benefit. So, there is a need of security management in IoV network.
6. *Balancing Privacy and security:* It is quite challenging to maintain a balance between privacy and security of information in IoV network. IoV share lot of trustworthy information which might violate privacy in case of leakage in public by the receiver. Therefore, information sharing must be done so that privacy is protected.
7. *Sustainable Service:* One of the most challenging tasks is providing sustainable service of IoV which requires use of high intelligence methods, along with friendly network mechanism design.

   Out of all these above-mentioned challenges, security is most important challenge that should be resolved before IoV deployment.

2.7 Security Threats in IoV

Security plays an important role in IoV network deployment. In IOV, vehicles are connected through internet which makes them vulnerable to security threats. These vehicles operate in a dynamic environment in which data has security risk of being tempered, stolen, mis-routing that might result in disastrous consequences like accidents. Apart from security, safety of humans is of utmost importance because innocent lives are at stake. As compared with other traditional networks in which safety of personnel's is not of major concern. Moreover, except security issues, IoV features like frequent disconnections of nodes from network and high node mobility present few security challenges like data protection, position detection, trust group

formation and certificate organization. To address these challenges there are some security schemes. Dependability on Traffic information dispersed by other vehicles or infrastructure can enable some mischievous users to broadcast traffic jam or an accident ahead as a warning to empty traffic on their own route. Not only this, any person can update internal network of node by altering internal onboard devices and also updating ECU firmware. IoV allows automated vehicle identification where users can recognize themselves for example while crossing toll. However, in case of compromised security hackers can steal personal information. These instances demonstrate that IoV may links the vehicles to normal users as well as hackers. So, there is a need of security schemes in IoV to protect it from mischievous users who might take partial or full control of the vehicle and temper with safety related information.

2.8 Security Schemes in IOV

The Security schemes for IOV are classified into two main categories namely encryption-oriented schemes and trust-oriented schemes.

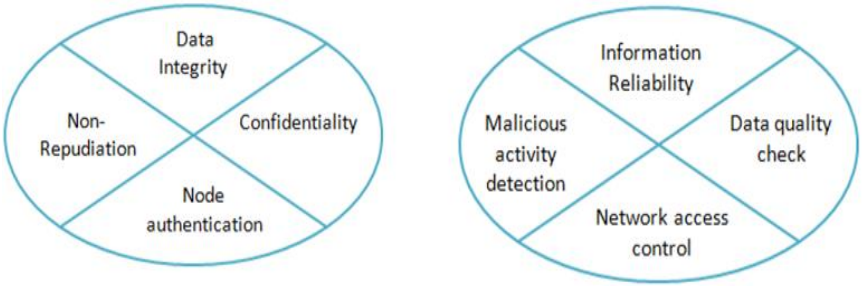
2.8.1 Encryption oriented schemes

Encryption schemes are mainly of two types (1) symmetric (2) Asymmetric. symmetric schemes utilize same key for both encryption as well as decryption, it involves low computation complexity and is faster as compared to asymmetric encryption. Since the reception delay sometimes makes the information meaningless, so symmetric encryption is better suited for IoV but it suffers from some limitations like less scalability due to difficulty in key exchange, increased communication load due to, more storage requirement and extra power consumption [15]. Due to the above-mentioned limitations, asymmetric encryption is preferred for IoV as it is more scalable and don’t suffer from the problems related with key management. Commonly used algorithms for asymmetric encryption in IOV are Elliptic Curve Cryptography algorithm (ECC)[17] and Rivest, Shamir and Adleman algorithm (RSA) [16]. But asymmetric encryption has high computation complexity. In nutshell, it can be said

that both types of encryption schemes have their benefits; however, they don't resolve IOV security issues completely. Encryption is considered as a hard security solution that provides safety by ensuring non repudiation, node authentication, data integrity and confidentiality see figure 2.7(a). Hard solutions are not able to detect the changing behaviour of nodes where any node acts good for some time and then turns into malicious node. Therefore, hard security solutions do not suit well in realizing node and data trustworthiness.

2.8.2 Trust oriented schemes

Trust oriented schemes handles soft security measures that are totally dependent on node's behavior like trustworthiness of information sent/received by nodes, detection of malicious activity (see figure 2.7(b)). In IoV, data Security of data depends upon the behaviour of nodes. For instance, consider a scenario, in which an ambulance is searching for shortest and uncrowded route to pass through it. At that time if a selfish node claimed that the chosen route is congested, then ambulance will take alternate route due to that patient may expire on the long way. So, there is a need to model the trustworthiness of nodes as well as data. And thus, trust-oriented schemes seem more appropriate and fruitful to secure IOV environment.



(a) Hard Security measure (b) Soft security measure

Figure 2.7 Security scheme measures

2.9 Trust concept and definitions

Security and trust are inter- dependent. When we consider the security of an information/ data, the trust automatically comes into scenario. In human relationship,

the security of any information shared with any person is based on the trustworthiness of person. The same concept works in IoV also. The security of any information shared by any vehicle depends on the vehicle itself. So. trust management between nodes is necessary to ensure data security. According to [67], the definition of trust is as follows:

"Trust is considered as a relation among network entities built depending upon the observation of previous interactions"

Basically, trust specifies relation between trustor and trustee node. The trustor node is the one that faith other node to act in desired way whereas the trustee node is the one that maintains this trust acting in that expected way. The degree of trust is usually measured in terms of trust value that is affected by time, situation, context and other factors (see Figure 2.8). An entity is considered as trusted if it behaves in an expected way continuously. When this concept of "trust" is applied in IoV, it signifies that entities in IoV behave as expected.

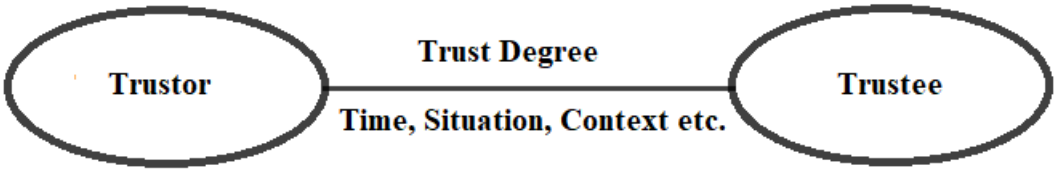


Figure 2.8 Concept of trust

2.9.1 Definitions of Trust

Computer science and social science have different definitions of trust [68][69]. These definitions differ in practical application areas and in point of view of researchers. Even though these definitions are taken from social science, there isn't any unanimity on computer networks trust definition [70]. However, the trust concept is used to achieve safety for ad-hoc networks [71][72]. Authors in [73] and [18] specified that these mechanisms of trust provide strategy to increase security of Ad-hoc network. Moreover, A.Hamid et al.[74] described trust as a key component for security in VANET. Author in [70] defined trust as faith between entities. The table 2.3 collate

various meanings of trust in literature.

Table 2.3 Different meanings of trust in literature

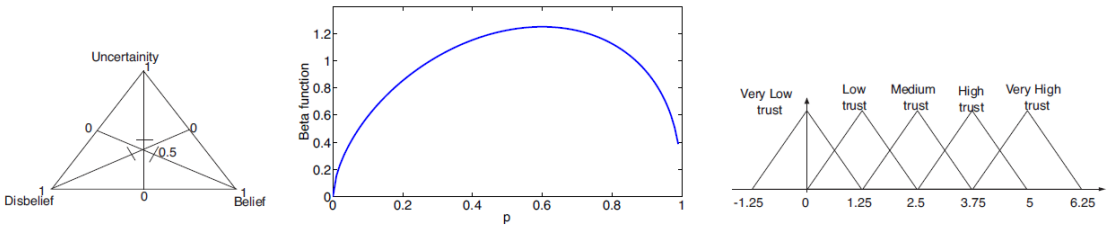
[70]	Considered trust as confidence of an entity has over other obtained from past interactions
[75]	Trust is useful for detection of node behaviour as well as for enhancing the performance of network
[67]	Defined trust as a relation amongst various nodes built from experiences of previous behaviour.
[74]	Considered trust as an important constituent to build trustworthy network that augment network security
[76]	A trust is a rating provided to interacting nodes that decides whether node is trusted or malicious.
[77]	Trust is an expectation about futuristic behaviour on the basis of earlier experience
[78]	Trust indicates a level of dependence of one node on other.

2.10 Trust Metrics

Trust can be evaluated using various metrics, parameters and different ways. These trust metrics can be classified as follows:

1) *Trust scale:* In some trust models, the level of trust is measured by continuous or discrete values. For instance, in study [79][80][81] the trust is defined by a continuous value between 0 and 1 whereas in study [82] the trust is represented by discrete value in range [−1, 1]. In some trust models threshold-based policies are used for trust measurement. For example, in study [82], if normal satisfaction wrt interactions is larger than predefined value, node is considered to as trustworthy.
2) *Trust facets:* Some trust models estimates the trustworthiness of node by a confidence value and a trust value together [83]. Shortest distance between origin (0,0) and (*t*,*c*) on two-dimensional plane represents trustworthiness where (t, c) represents (trust, confidence) pair. Study [84], represented trust using triplet space (Figure 2.9a).

3) *Trust logics:* Some trust-based schemes used probability logic for trust evaluation. In studies [85], [86] probability metrics is used to estimate trust. In [87], the trust metric is the packet delivery ratio. Study [88] used Beta distribution which utilize good and bad experiences to obtain the trust value (Figure 2.9b) Some trust models like [89][70] represent trust via fuzzy logic. The fuzzy logics use some labels for assigning values (Figure 9c).



(a) Trust as belief function (b) Probability based trust (c) Fuzzy logic based trust

Figure 2.9 Representation of trust metrics

2.11 Characteristics of trust

The characteristics of Trust vary in accordance with the characteristics of network. The main characteristics of trust in IOV network can be brief as below:

1. **Dynamicity:** Unlike static value, the trust variable (T) for IoV network should be dynamic in the sense that it needs to be computed and updated regularly.
2. **Subjectivity:** The Trust required for IoV network is subjective in nature which means that each node in network can have distinct view about a same node.
3. **Time dependent:** The Trust changes with change in perception of a node and perception is time dependent. So, the trust IoV trust may grow/decrease with time.
4. **Asymmetric:** The Trust in two nodes in IoV network satisfies asymmetric property. It means that if node P trusts node Q at a level, then node Q also trusts node P not necessarily at same level.
5. **Context dependent: The** Trust in IoV nodes depends on situation. It means that node P can trust the node Q for forwarding the information but not for selflessness.

6. **Transitive:** The transitivity means the trust can be travel trusted path. For example, if node P trusts node Q and node Q trusts node R, then node P trusts trust node Q at a certain level.
7. **Composability:** Trust from different paths can be composed together to form single opinion value.

2.12 Trust management

Existing trust management schemes seems suitable to IOV network due to its empherical and self- organizing characteristics [90]. Hence, researchers have recommended various techniques to improve trust management in IoV. Gomez et al.[91] defined trust management as a unique method to address some unresolved threats. Study [92] presented a scheme of trust formation for normal nodes so that nodes can take correct decision and limit detrimental behaviour of evil ones. Additionally, study [93] stated that trusted interaction in VANET is critical in order to provide a reliable traffic safety. The studies [91], [92], [94], provides few of the trust management recommended by researchers. Table 2.4 shows collate various meanings of trust in literature.

Table 2.4 Trust management Definitions

[94]	Trust management means to ensure the reliability of traffic warning and prevent the dissemination of false traffic warning.
[91]	Trust and reputation management is considered as a mechanism to handle security threats.
[92]	considers trust management as a technique to guarantee security in VANET.
[95]	Trust management has direct impact on quality of applications and services.
[96]	Trust management plays significant role in protecting the reliability and integrity of application

According to explanations given above trust management is primary method to confirm security of VANET. Trustworthy relation among entities is consequence of the trust formation in VANET environment [97]. Nowadays different models are

being projected for managing trust in different networks. For example, [95], [98], [99]. Authors in [98] provided a Situation aware trust model to augment driving efficiency.

2.13 Classification of trust computation techniques.

Various techniques that are widely used for trust computation are as follows. Figure 2.10 shows classification of these computation techniques.

2.13.1 Trust Composition

It refers to the components which needs to be considered for computation of trust. The trust components are mainly of two types.

- *Quality of Service Trust: It* refers to device competence to respond a service demand. It is defined as the belief that IoV network is capable of providing eminence service in the response of service demand. It is assessed by the reliability, cooperativeness, etc. Authors in [100] used transaction performance for QoS trust measurement. In [101], PDR and energy consumption are used for measurement of QoS trust. In our work we used QoS trust as it is not necessary that owners of nodes are socially connected and driver of the node can be changed.

- *Social Trust:* Social Trust refers to a node's assurance to perform well in response of any service demand. Social trust is obtained from social relation among users of IoV nodes and measured by privacy, honesty etc. In [102] social contact and community of interest are utilized as measure of social trust. In [103], social trust is measured by honesty, connectivity, unselfishness and intimacy.

2.13.2 Trust Computation

Trust computation means how the trust is computed. Generally, there are two methods for trust computations i.e. distributed trust computation and centralized trust computation.

- *Distributed trust computation:* In this type of computation, network nodes itself compute the trust value for the node with which it interacts without any centralized entity.
- *Centralized trust computation:* In Centralized trust computation, the trust is computed by a centralized entity for both the nodes involved in interaction. The centralized entity can be any physical cloud or online trusted server.

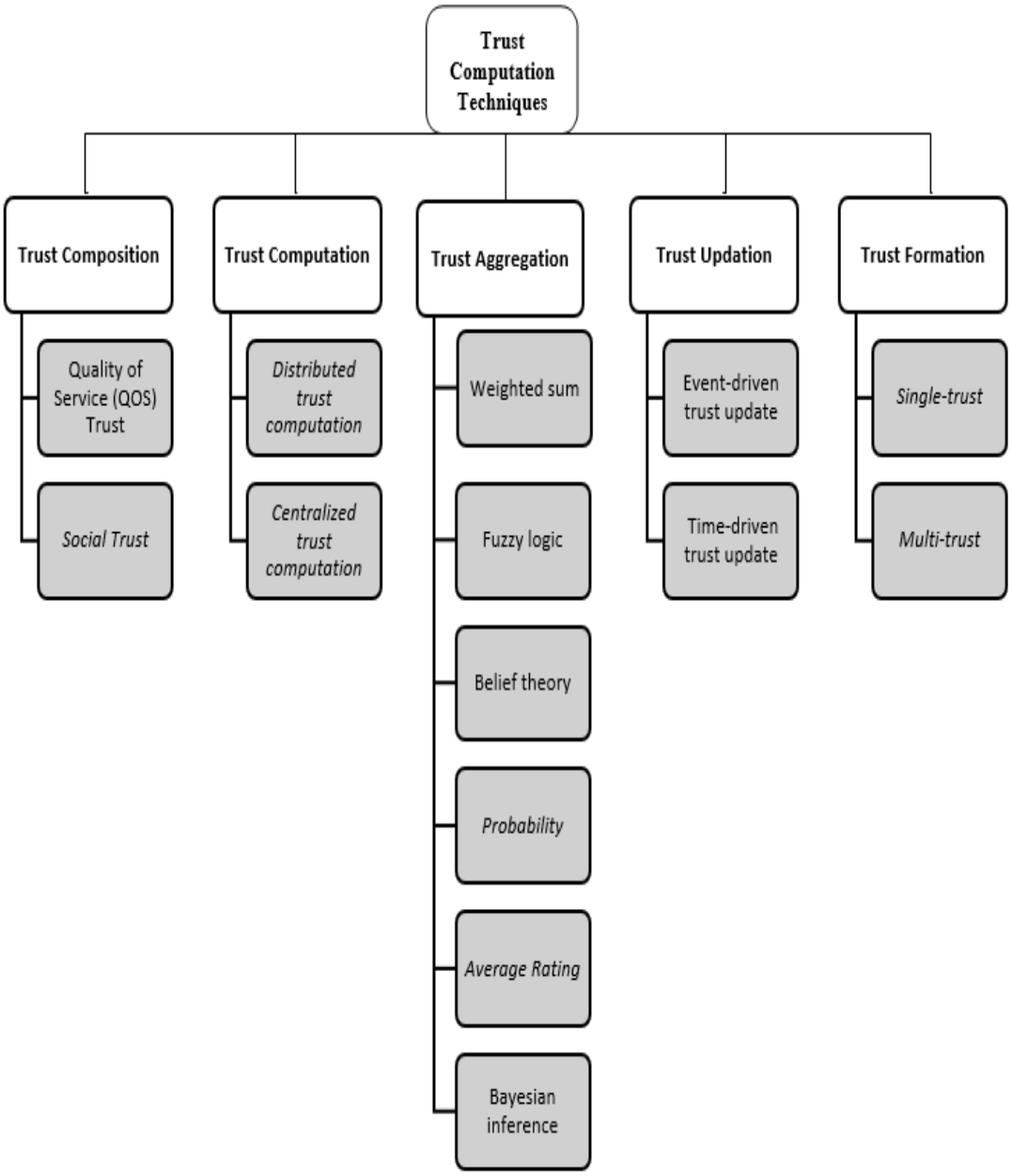


Figure 2.10 Computation Techniques

2.13.3 Trust Aggregation

It is the process of combining the trust evidence collected in form of observations, ratings, opinions etc. Various methods used for aggregating trust are as follows

- *Weighted Sum:* This technique is used to combine values of direct and indirect trust. Study [56] [60] [68], utilized weighted sum technique to combine feedbacks in such a way that the raters having higher reputation have a higher weight. Weights assigned can be static as well as dynamic.
- *Fuzzy Logic:* Fuzzy logic deals with the approximate reasoning instead of fixed value. Authors in [7] used fuzzy membership function to compute trust.
- *Belief Theory:* Belief theory or Dempster–Shafer theory (DST), is a framework for reasoning with uncertainty. Trust model in [67] used Dempster-Shafer Theory to the compute trust of agents in the autonomous systems. DST involves two ideas: obtain the degrees of belief from subjective probabilities and Dempster's rule [22] to combine the degrees of belief.
- *Probability: Trust can be aggregated using* subjective beliefs logic operators [31], [32] or on the basis of probability distribution.
- *Average Ratings:* In this aggregation technique the average of all the rating values is evaluated to calculate the overall trust.

2.13.4 Trust Updation

Trust updation is used to update the node's trust value. Generally, there are two methods for updating trust value - event-driven trust update and time-driven trust update.

- *Event-driven trust update:* In this method, trust values of node are updated after every interaction or node encounter. This method is like a feedback regarding service quality
- *Time-driven trust update:* In this method, the trust is updated periodically using evidence from direct interaction or recommendations. If no interaction or recommendation evidence is obtained, the trust decays over time that can be modelled using an exponential decay function [104].

2.13.5 Trust Formation

It means how to obtain complete trust from numerous trust properties. Methods used for forming trust are categorized as mentioned below

- Single-trust formation: It utilize one trust characteristics to obtain complete trust in a trust model. For instance, service quality is only characteristics used to form trust in service-oriented IoT systems [102].
- Multi-trust formation: It utilize several trust characteristics to obtain complete belief. For instance, In [103] honesty, intimacy and competence etc. are used. This trust can be formed by combining them using weighed sum or using minimum threshold policy.

2.14 Types of trust models

On the basis of whether the entity or data is being evaluated for trustworthiness, the Trust models are classified as follows

2.14.1 Entity-based models

The entity-based models are accountable for trust computation of vehicular entity only in IOV network. In these models, the received data will be considered as trusted only when its sender is trusted. The entity-based model is responsible to evaluate trust in IoT participants considering the behavioural tendencies. The aim of calculating the entitiy-based trust is to recognize the non-trusted user who can attempt to attack network or compromise the network services. The study [105], presents a survey of entity-based trust model and trust computation techniques used in IoT. The entity-based models are further categorized depending upon whether trust is computed by a centralized authority or in distributed fashion. In computation of distributed trust, the social relationships among entities are considered.

2.14.2 Data-based trust models

Data transmission is a basic requirement of network. Data based approach computes the level of trust for every received message rather than entity itself. Instead of trust

computation of entity only, these models are accountable computing the reliability of data also. The data-based trust model in IoT focusses on evaluating the trustworthiness of events and data or it detects erroneous data. However as compared to entity-based less work is focused purely on data-based approach for modelling trust.

2.14.3 Combined/ hybrid models

These models are accountable for trust computation of vehicular entity as well as received data. IoT network comprises of nodes/entities that interacts with the services. It also involves abundant data that is used in decision making. So, a trust model will be considered as more effective if it evaluates the trustworthiness of both entities as well as data. Hybrid trust model involves in IoT involves the entity trust that is maintained over time and this entity trust is then utilized as a prime factor in determining the trustworthiness of data. But there are some other factors like locality, timeliness and other contextual properties that also affects the quality of data and therefore need to be considered in evaluation of data trust.

2.15 Existing Trust based models

Trust is differently researched in areas of VANET in addition to conventional trio of network safety, reliability and privacy aimed at providing safe, seamless and reliable interactions. Nevertheless, in spite of huge trust-related research in VANET, the concept of trust, trust models and its evaluation mechanism have still been debatable and is under development. This section includes the study of trust model proposed in different networks like P2P, distributed networks, ad-hoc networks, VANET, IoT, IoV etc.

2.15.1 Trust Management in E-Commerce and Social Science

Trust network and reputation for E-Commerce systems, like Yahoo auctions [106], eBay [106], and also Keynote [107] used a central authority of trust to maintain its repute. Moreover, these systems provides utilization of deterministic number for

demonstrating reputation [108]. Mostly recommendation- based trust mechanism is used for online shopping sites. Social Science on the other hand consists of relationship among individual in society [109]. The idea of reputation in society network is natural and people can feel it daily (buying, selling). Therefore, Trust in general help in simplifying difficult task by allocating tasks based on trust to other parties [110]. Authors in [111] presented a framework for trust management in the virtual communities utilizing reputation and direct experience. Using both direct as well as indirect trust recommendations they have provided the concept of semantic distance to rate nodes. Various properties of social trust which model supports are subjectivity, non-transitivity and context-dependency. Ismail and Josang [88] developed beta system reputation for the electronic markets, on the basis of modelling reputation for future probability based on past experience. In this density function of beta probability was used to merge opinion with deprive ratings. Major advantage of this beta system is that it is quite flexible and simple. In study [112] which proposed reputation system ReGreT, that using direct experiences, and reputation. Overall trust is computed using weighted average approach. In [113], trust is computing the trust by assimilating rating with prevailing trust. Moreover, Study [114],[115], specified 'trust is bigger than just subjective probability'. Lastly, trust model in [116] proposed a that agents may revise beliefs on the basis of evidence provided by other agents.

2.15.2 Trust in Peer-to-Peer and Distributed System

In P2P systems, peer refers to computer that is associated with another computer using Internet. Network is distributed in P2P system as there is non-availability of any centralized entity to keep check on peer to peer communication. As a result of this, users will maintain statistical representation of reputation with the help of borrowing tools from realms of Bayesian networks [117], [118][119], game theory [120] and also other domains. With the use of this system selfish misbehavior of routing nodes can be countered by forcing nodes to co-operate with one another. Despotovic and Aberer in [121] summarizes the complaints it receives from peers and is very sensitive to misconduct. The duckling model in [122][123] represented a P2P trust framework wherein principals validate their communication by transferring keying material through out of band physically separate channel. The trust established is two

way where communication can be both either secured or un-secured based on hierarchical graph with slave-master relationship.

In the project named SECURE [124], [125] wherein attempts were made to combine every aspect of trust model into a single structure, which ranged from risk analysis and modelling trust to collaborating models [126] and recognizing entity. This model is an extension to work of [127] to manage trust in security access control systems. The suggested model permits to give its policy like a mathematical function wherein trust in others is determined in terms of other's assessment. Study [117], [118][119] provided trust model by using Bayesian network on the basis of service delivered by agents. These Agent generally form two types of trust in other wherein first refers to other agent's capability to provide service and second is consistency in delivering opinion towards other agents.

The proposed system uses binary events for example failed and successful transaction for trust identification and also weigh direct as well as indirect information. Consistency has two characteristics: if the agent is honest in providing information and is it trustworthy also. Even though the models recommended in [128]and [129] are based on service quality, trust is modelled according to weighted vector for all the services calibrated according to their significance. Researchers in [130] offered a great comparison between generic model of trust UniTEC and a trust updating algorithm. It computed the trust on the basis of new rating and value of old trust. In the original model UniTEC ratings were given in binary form depending on good or bad experience. Maheswaran and Azzedin's model in [131] calculated the trust on the basis of combining reputation and direct trust by weighing the given elements distinctly with more weight assigned to direct trust. Models in [132], [133] suggested a neural network based approach trust modelling.

BambooTrust, represented in [134] [83] is trust management scheme of global computing platform for public like a grid system. This is based on XenoTrust [135] and Bamboo hash table. XenoTrust [135] used performance criteria (dependability, trustworthiness and throughput) to assess others. This event is based on distribution of

trust management in XenoServer platform. Many existing trust systems are dependent on traditional reply/request model, wherein voting is involved which causes communication overhead, whereas event-based system depend on if change has been occurred or not. Authors in [136], showed a model to enable secure alliance in a computer system environment. Mostly, trust model use security policy where permits and prohibitions are based on actions. Researcher who presented B-trust model [137], also projected lightweight distribution of trust scheme for pervasive trust estimation using Bayesian formalization which takes care of user anonymity and Sybil attacks.

2.15.3 Trust in the Ad-hoc Networks

Ad-hoc networks are distributed in nature due to which they are more prone to attacks. [1]-[3]. Trust evaluation is one of the solutions for security of these networks from attacks. Ad-hoc network involves two methods for trust establishment. First method is direct observations of nodes behaviour like PDR while second method is recommendations. Ad-hoc Networks are considered to dynamically change their own structure which leads them to joining and leaving networks repeatedly. MANET's trust relationship are evolving and are subject to attacks as environment as whole is vulnerable to access from a shared wireless medium. To put it differently, a set of trusted subset of nodes is not available. Trust would be developed with time, whereas trust relationship between nodes might also change[138]. Trust system, CONFIDANT [139] as well as CORE [140], uphold a statistically significant representation of reputation after deriving tools from the game theory and realms of Bayesian approximation [141], [142]. Study [140], presents system where game theory is used to model reputation. According to this system, members with great reputation can utilize resources whereas that with bad reputation can be excluded from the community as they refuse to collaborate. In CORE [140], the term referred to as "subjective reputation" is used to present reputation calculated on the basis of 'direct observations'.

CONFIDANT [139] make use of direct and indirect for trust estimation and detection of malicious nodes. It is based on Bayesian methodology. Later on, researchers

upgraded the work in [139] with a more flexible Bayesian reputation and the trust system given in [143] and [144]. The only reason behind CONFIDANT being different from its CORE is because it sends reputation value to all other nodes which would expose the mischievous dispersal of false reputation value. To conclude, if node is behaving in a co-operative way, then only positive reputation value is allocated, else negative reputation value is assigned. Authors in [145], offered an addition to their previous work [83], by utilizing the theory of semiring for evaluation of the process which was developed after modelling the path problem on directed graph. In that graph edges denoted trust relations whereas nodes denoted entities. Here users make opinion toward other nodes utilizing the information given by intermediate. It means this model does not necessarily requires direct communication to form an opinion towards nodes. Authors in [146] also provided a solution for trust management addressing resource constraint for given network.

Bucheggar et al., in [143] modelled a system which appeared to be robust against false ratings. This approach is quite different from the traditional Bayesian model, wherein standard weights are allotted regardless of the time at which observations are taken. This is the reason because of which this new weighted approach is called modified Bayesian approach. To further improve the discovery of mischievous nodes the researchers utilized second hand info only from the trusted nodes or only if it has cleared a deviation test wherein compatibility is evaluated on the basis of own reputation ratings. In [147], authors introduced the concept of belief for trust-based The model in [147] is adapted from Marsh trust model [94], wherein importance and utility of single variable required weight for simplicity. Moreover, the trust is categorized into various categories which is calculated on the basis of sum of all weighted categories. Authors in [148] described trust as uncertainty measure and suggested that trust can be measured through entropy. Authors also presented two model in this article- one is based on probability while another is based on entropy. Authors recommended a model in [149] which is used to define and maintain trust and routing decisions. Main motive of this model is to improve communication safety in MANETs, by providing a safe route using trust. The assumption behind this is all node includes intrusion detection system to sense and distinguish abnormal nodes.

Work in [150], [151] recommended probabilistic solution using distributed trust scheme in order to build trust relationship amongst. Study [96][151], provides directed graph method whereas the work in [97][150] utilized Beta distribution approach for calculating trust. Authors in [98][152], explained a trust model consisting of two elements: Trust evidence distribution (input for evaluation model) and Trust computational model which is also known as evaluation model. This model used swarm intelligence technique. This model mainly addressed retrieval and evidence system using private and public key notions and distributes the certificates of evidence.

2.15.4 Trust model for Internet of things

Evaluation of trust is of prime concern in IoT-enabled systems and services because these systems and services are more prone to malicious activities. Malicious users can be easily misled IoT systems by altering the transmitted data or by disseminating fake data. Data inconsistency is main problem in modelling trust in IoT systems. Herein, we examine the research addressing the issues associated to trust modelling in IoT enabled services. For example, a trust service platform is present in [153] for social IoT. This model uses recommendation, knowledge, and reputation as trust metrics to estimate the trust score using fuzzy-based approach.

Study [154] described a trust scheme to handle misbehaving nodes with their behaviour changing dynamically in IoT network. The model uses static weighted sum approach to model behavioural trust. The study [155] propose an adaptive system for trust management depending upon CoI for the SIoT. This trust model used dynamic weights sum for calculating trust values.

Study [102], provide an adaptive system to manage trust for service composition application. In this model the trust value is computed for suppliers of service. The model is based on Bayesian approach. This scheme motivated central trust computation as fully distributed trust computation is costly in regard of bandwidth,

processing, and power consumption. In distributed computation every node would observe other node's behavior and manage trust value for them. This doesn't meet resource constraints of IoT network.

Authors in [156] proposed a scheme for trust management using dynamic weighted sum techniques where a node is assisted with an assistant node providing best service in specific context. In this scheme recommendation trust is computed for recommender entity. This scheme is mainly utilized by service oriented IoT systems. Study [157] considers a medical sensor network propose a lightweight, attack proof trust scheme.

Authors in [100] presents a scheme for handling the Trustworthiness of nodes in the SIoT. This is *rater* scheme in which all nodes keep the trust data of other nodes with whom it communicated. This study provides two models i.e. subjective model and objective model. If a node encounters an unknown node for interaction then they look various nodes for its value. This process is very time consuming and inefficient. In addition to this the situation may become worse if no other nearby nodes have interacted with it.

Study [158] considers and IoT agriculture scenario and provides a procedure to differentiate reliable and unreliable data from sensors. This study includes humidity and temperature data gathered from sensors installed in green house to central authority. This considered that these sensors would turn out to be untrustworthy gradually because of environmental changes. So, authors in [158] recommended a Bayesian methodology for assessing the trustworthiness of information obtained by these sensors. The drawback of this research is that it didn't think through the spatial or the temporal context parameters to evaluate trustworthiness of data. Thus, this procedure is applicable only to subset of the IoT scenarios having no participation from user. Authors in [159], propose a data base model which gathers information from crowdsourcing. This method computes the data reliability based on fixed weight approach. The work presented in study [160] is the extension of entity centric trust scheme proposed in study [153]. Authors in [160] provides a method to compute data

reliability in SIoT using weighted dynamic sum approach. It used Accuracy, uniqueness, completeness, timeliness etc as data trust metrics. Study [161] proposed a combined trust scheme known as RealAlert for city scenario. It is a policy-based model that used statistical outlier detection technique to recognize untrustworthy node.

Study [162] provides a trust model to secure the relay nodes and IoT devices as well as to guarantee the reliable communication between devices. This is a neuro-fuzzy based trust model that is inspired form processing of brain. This trust model estimates both node behaviour (entity trust) and the data trust. The model used distributed approach to compute entity trust. But the model is more focused on brain data and suitable for application related to neuroscience.

A trust-based decision system is provided in [163] for health IoT solution. In this system, users of IoT network provide reports related to health factor in specific area. The trustworthiness of reporting users (entity trust) is computed by a central authority to recognize misbehaving users who can provide fake reports. Study [163] involves a hybrid trust model for healthcare application in IoT in which authors used quite simple approach to evaluate entity trust. But the authors have not tested it under high malicious nodes. Besides this some parameters such as parameters related with device capabilities, temporal data freshness used in trust computation are not mentioned clearly.

2.15.5 Trust models for VANET

The given literature for vehicular trust network essentially highlights Entity-based, Data-based, and hybrid Model. As per the given literature the entity centric model would be categorized into two different segments: multifaceted trust [164] and sociological trust [165]. The sociological trust concept was given by Gerlach who presented trust model from sociological viewpoint. Trust depends on different attributes which effect trustier solution. At this juncture, author had explained trust in various forms like system trust is dependent on system only whereas situation trust is dependent on the situations without giving regard to trustee, dispositional trust – in

this trustee is dependent on peer's own belief without considering the given situation. Here, belief is formed and trust is evaluated on basis of past information and considering peer's belief as a result of evaluation. Moreover, author has proposed the security architecture for network of vehicles while also considering privacy protecting approach. The only limitation of the given model is that it does not introduce any technique for aggregating various trust forms.

Author [164] proposed multi-faceted trust which included trust depending upon role of node in given scenario, their experience and priority which is combined approach for role and experience-centric trust management. The Role centric trust considers few pre-assigned roles of agents and gives more interest to them in comparison to others. In the given paper, the roles are recognized as expert role, authority role, seniority role and ordinary role. Experience based trusts evaluate a direct communication between vehicles. The given entity can verify an event from other units by sending requests which limits the reports number. Therefore, author introduced priority-based trust by utilizing feedback it received from highly trusted advisors also known as majority opinion approach. However, this model fails to consider a situation where agent does not report occurred events.

TRIP [91] is a proficient model to identify and segregate selfish nodes network which did not have any central authority. The given trust model allows the vehicle to check the data reliability based on assessment of sender's entity and subsequently accepting or rejecting the warning. This trust model only considers the incoming warning signals from vehicles with good reputation score. The limitation for this scheme is that identity and privacy management issues are not considered here. Authors in [166] also proposed an entity trust model which was based on security enhancement scheme that aims at preventing the hackers from sending bogus messages or even altered messages that can cause network disruption. The trust is assessed on basis of direct communication with observed vehicle and also recommendations from neighbours of observed vehicles. Lastly, Bayesian rule is also used in order to evaluate direct trust. In this model, Dempster-shafer theory is used to integrate recommendations from neighbouring nodes.

Author [167] proposed dynamic trust scheme. It is an entity-based scheme using weights. methodology. Authors in [168] presented a scheme in order to compute reputations based on Hidden Markov Model (HMM). The given scheme evaluates the message reliability and also estimates the legitimacy for broadcast messages. Moreover, work in [169] presents scheme for VANET based on reputations. In this reputation value is assessed by using an aggregation algorithm which is based on binary feedback ratings.

Author [170] recommended a data centric trust establishment framework. As per Raya the malicious node should be revoked and to do this security function like S (Vk) = 0 for node should be revoked and S (Vk) = 1 should be used for legitimate nodes. Author also considered the dynamics of event such as location and time. Dynamic trust metric function is used for different attributes of node.

Author [95] presented information-oriented trustworthiness assessment which is based on real time message content validation system (RMCV) scheme. Author has classified this scheme in two parts: information-based trust model and Classification of messages. The Classification of messages component makes use of two different level of clustering algorithm. First level identifies same event messages from the vast number of messages from different events by considering event type, distances and time. The main objective of clustering at second level is to identify the content of message if they are similar of conflicting. The component of message classification creates clusters with group of messages of similar event type and their content. Now comes the next step which is to determine the group which is having most accurate messages. Author has presented second part of information-oriented model of trust which generated overall reliability score while also considering given components: - content conflict, content similarity and routing similarity path. Similarity of content plays a critical role to judge the reliability of messages in cluster. More similar messages mean a high support of information messages about similar event for each other. Routing similarity path defines penalty value in order to support value as more similar path increases the probability of tempering message. Conflict of content

affects the reliability of messages in cluster negatively in case there are additional messages against messages of that cluster. Lastly, compute the trust score on basis of these components.

Authors [171] mentioned the earlier presented trust management schemes were based on past historical interactions which were not effective to assess the ephemeral network e.g. VANET. In order to overcome this weakness researcher suggested an intrusion aware model of trust framework which are having three main modules namely, trust measurement module, decision module and confidence measurement module. Confidence measurement module will calculate the value of confidence (CxK) for each message (x1,x2….xk) on the basis of time, location closeness that will express the freshness of message, verification of location will identify the node's location and verification of time. The decision process works in two stages, at first stage it identifies the message with high trust value as compared to others and in case trust value is higher to minimum threshold value then message will be considered otherwise it will be forbidden.

Authors in [94] presented reputation-based trust model which describes dynamic role dependent evaluation of reputation mechanism in order to filter bogus messages. Here vehicles played different roles: event observer, event reporter and event participants. Event reporter (ERi) refers to vehicles that encounter events directly and are able to calculate the reputation of event j (RjERi) on the basis of detection of frequency. Event observer (EOi) which calculates the value of reputation (RjEOi(t)) that observe succeeding behaviour from event reporter within time t and also reputation value of event directed by different EOs. Event participants (EPn) also calculates the reputation value (RjEPn(t)) for event j at time (t) by combination of EPs and EOs. Lastly, integrating reputation value of event and comparing if it is more than threshold value which is predefined after which vehicles will broadcast message to all neighbours.

Author [172] presented event reputation system to prevent broadcasting of bogus message. This system is built of four functionalities three interfaces and one table

repository. Event confidence value shows degree of trustworthiness as it contains a list of all vehicles which are faced with that event. The threshold values of event reputation and confidence are projected from the on-board sensor device available on vehicle and event type characteristics. In case detection of event is done by the sensor of vehicle directly then reputation value would increase by one and if vehicle obtains an event message from different vehicles than ERS of this vehicle can add the reputation event value into corresponding field of similar event table and if there in case there is no entry with similar event type then a new event record would be generated. Likewise, for event wherein confidence value of event is detected directly by on-board sensor then ERS can add vehicle's identity in confidence list at similar event entry in event table. In case vehicle receives event message from another vehicle then ERS would simply add content to confidence list of messages in field of an event confidence. In case reputation which is detected and confidence value are more than threshold values, it means the event exists and ERS can send warning message to drivers and broadcast it to neighbours. In viewing safety application author has introduced revocation scheme when event gets resolved. Revocation scheme consisted of suppression and degradation function. On the other hand, threshold value of event suppression function can be controlled by setting the event reputation value as threshold reputation value in case the current event reputation value is more than predetermined threshold values.

Work [173] presented RATE mechanism that is data based trust model. In this case RSU differentiates between data consuming vehicles from data providing vehicles and it also shares the information with neighbours. RSUs and passing by vehicles also establish trust by RSU utilizing Ant Colony optimization algorithm and various other factors. In case vehicle detects the event, vehicle generates confidence and observation report. RATE also adds this report in the freshly received observation list (Lro) after which it calculates observation factor. The Observation factor shows the number of observations of an event, observer's confidence on part of evidence and weight of reported vehicle which reflects identity of vehicle. RATE follow given steps:

1. Firstly, RSU would check recent observation list (Lro) and would calculate observation factor at regular interval
2. In case observation factor >= T and event is not in list of evidence (Le) then add event into it.
3. In case observation factor >= T and event is already existing in evidence list then do nothing
4. Lastly, observation factor < T then remove the evidence from list

Finally, trust level is calculated and attached to evidence on basis of feedback and observation factor. RATE mechanism would provide benefit of reducing attacks launched by malicious nodes.

Author in [174] has explained a fuzzy model that evaluates reliability of message in order to ensure that message is received from certified vehicles. The trust value of message is determined by combining level of location exactness, experience and plausibility. Accuracy level of the event location is based on distance between fag node and event location. Experience and plausibility will depend on the history of interaction. Lastly, on basis of combined trust value the decision module would make decision to accept or even reject the message. Study [175] involves a reputation system for VANET using including indirect, direct trust along with opinion piggy backing. Author [176] provides a trust system based on Beacon that determines the reliability of vehicle by utilizing cosine similarity of the vehicle's velocity, claimed position and drive direction with an estimated value. Researcher also categorized event-based trust into different categories: direct and indirect event-based trust. Direct trust was assessed by using movement and position verification system where a receiving vehicle evaluates the reliability of sending vehicle by comparing beacon message and event message. In case of indirect trust, dependability of relationship between receiver and sender should not be higher than trust value between them. Reputation value also considered previous reputation value and indirect trust. Author also used Dempster- shafer theory in order to combine trust events, reputation value, and beacon trust and compare it with the threshold value to take decision.

Author [177] presented RaBTM scheme to disseminate an opinion speedily and prevent the internal attackers from sending bogus messages. Event trust is evaluated from both direct and indirect event messages which create a combined trust. Lastly, overall trust value (Toval) is calculated with combined trust (Tds) and also opinion confidence of RSU (Orsu) and its comparison with predetermined threshold to make decision. Authors [178] described a trust system to prevent attack. It consists of two phases: Trust management and Data analysis. Firstly, in data analysis, traffic data is collected from various vehicles of network and then testimonies of data are combined by Dempster-Shafer theory to assess reliability of data and reliability of node is gaged by recommendation trust and functional trust.

Categorized trust scheme [179] is a combination of both role based and experience based trust system. Wherein Nodes are assessed as per their relations for event reporting duration and assigning category as per their confidence and trust value. Author [180] presented trustworthy event information distribution approach which is hybrid trust model. In case mischievous nodes are determined using k-means grouping algorithm then reliability of data messages of trustworthy nodes is assessed after applying modified threshold random walk on their opinions. In [181], Author suggested a hybrid trust management scheme in order to identify mischievous vehicles and prevent them from being elected as cluster head. This scheme includes a composite metric (i.e., trust values are assigned to vehicles together with their resource availability) for proxy cluster selection and cluster head through intermittent elections. This helps to form reliable and resource efficient vehicular network.

2.15.6 Trust models for IoV

Trust schemes proposed for IoV are discussed in this section. Author [182] presented a scheme which helps investigators to evaluate criminal cases via collection of trustworthy evidence about an event. This also provides two main modules: IOV forensic service and forensic gateway. Firstly, Forensic gateway gathers the data from sources like RSU, cloud, smartphones. Secondly, IOV forensic service module stores evidence inside the database wherein evidences are organized event wise and signed

up by an evidence accumulator. Block chain technique is used to maintain reliability of evidences.

Author in [183] introduced an iterative trust model which is built when past values of vehicles available in network have direct communication with vehicles and feedback with neighbours for trust calculation. The given model uses Dempster Shafer Theorem (DST) in order to absorb ambiguity and deal with insufficient data about the vehicle for rapid trust update. Iterative model considers distinct level of trust model in order to describe node's behavior. This model is scalable and suitable for IoV environment although vehicles display fluctuating behaviour in the presence of less vehicles in neighborhood. Authors [184] introduced a trust management scheme in case of SIoV. The given scheme is a in continuation to the Ratee – Based Trust scheme. It is also ratee-based scheme that enable the node to keep the reputation status rated by a rater in previous communication. It involves a mechanism comprises of CA and also public cryptography. It calculates trust on the basis of these elements: Relationship factor (indicating the relationship between two nodes), Cookies number (giving information about number of cookies received by any node), Centrality (this shows how much a node is to the centre to other node) and Object type (RSUs or OBUs).

Authors [185] proposed a Ratee Based Trust Management scheme. The constituents of this scheme are: Local trust management, Cookies (Digital Certificates), CA server and Relationship management. This scheme calculates the reliability of node using digital certificates and cookies. The cookies include a response value of last interaction amongst nodes and some information associated to service. The centralized authority keeps all cookies to control middle man forging attack. The Relationship management module is responsible to create trust among nodes. Cold start and scalability are two major problems associated with this scheme. Author [186] presented a cluster-based trust mechanism in order to sense abnormal vehicles. The detection make use of two important things one is Cluster based Trust components (this build trust in real time), second is central reputation components. This mechanism is executed proving the reputation and uploading evidence. The

utility of this mechanism mechanisms is Affinity propagation on the basis of clustering and mutual supervision. For evaluating evidence, the intelligent vehicle detects, gages and collects the evidence regarding qualities of one another and reports them to central authority which calculates reputation globally.

2.15.7 Outcomes of Literature Review

Table 2.5. presents a summary of articles on Trust models for IoT, VANET and IoV. These articles were selected following a selection criterion as explained below:

1. Only the Trust models published in standard databases like ACM, IEEE, Elsevier were considered. Some articles that don't belong to these databases but have high citation and good findings were also considered from other databases
2. Second criterion was year when article was published. We included the articles from 2005 to 2020.
3. Conference articles with minimum 2 citations are selected.

Table 2.5 Trust models for VANET and IoV

S. No.	Author	Trust Model	Network	Class	Year	Publisher	Citations
1	M. Nitti et al. [100]	Subjective and Objective Model	IOT	Entity Based model	2014	*IEEE*	332
2	I. R. Chen et al. [102]	Adaptive IoT trust protocol	IOT	Entity Based trust model	2016	*IEEE*	219
3	F. Bao et al. [154]	Dynamic trust management	IOT	Entity Based trust model	2012	ACM	402
4	F. Bao et al. [155]	CoI based trust Model	IOT	Entity Based trust model	2013	IEEE	131
5	Y. Ben Saied et al. [156]	TMS	IOT	Entity Based trust model	2013	Elsevier	396
6	B. Liu et al. [158]	Bayesian dynamic model	IOT	Data-based trust model	2015	IEEE	11
7	C. Prandi et al. [159]	mPASS	IOT	Data-based trust model	2017	ACM	21

8	U. Jayasinghe et al. [160]	Data Centric for IOT	IOT	Combined trust model	2017	IEEE	15
9	Gerlach et al. [165]	Sociological model	VANET	Entity Based trust model	2007	IEEE	75
10	W. Li et al. [161]	Policy-Based Sensing	IOT	Combined trust model	2018	IEEE	58
11	M. Mahmud *et al.* [162]	ANFIS	IOT	Combined trust model	2018	Springer	28
12	H. Al-Hamadi et al.[163]	Trust-based decision making	IOT	Combined trust model	2017	IEEE	59
13	Minhas et al.[164]	Multifaceted approach	VANET	Entity Based trust model	2011	IEEE Journal	50
14	Gomez et al.[91]	TRIP	VANET	Entity Based trust model	2012	Elsevier	114
15	Zhexiong Wei [166]	Trust based Security	VANET	Entity Based	2014	ACM	29
16	Raya et al.[170]	On data centric	VANET	Data-based trust model	2008	IEEE Conference	328
17	Lo and Tsai [172]	ERS	VANET	Data-based trust model	2009	Springer	67
18	Qin Li et al. [169]	Reputation-Based Announcement Scheme	VANET	Data-based trust model	2012	IEEE Transaction	12
19	A. Shrivastava et al. [168]	HMM	VANET	Data-based trust model	2016	IEEE Conference	3
20	Ding et al. [94]	Reputation-based model	VANET	Data-based trust model	2010	IEEE Conference	37
21	Wu et al. [173]	RATE	VANET	Data-based trust model	2011	IEEE Conference	32
22	Gurung et al. [95]	Real time message cntent validation (RMCV)	VANET	Data-based trust model	2013	Springer	47
23	Shaikh and Alzahrai [171]	Intrusion-aware model	VANET	Data-based trust model	2013	Wiley	44
24	Seyed Ahmad Soleymani et al.[174]	FIS	VANET	Data-based trust model	2017	IEEE	76
25	Yao et al. [167]	Weight-based entity centric	VANET	Entity-based trust model	2016	Elsevier	53

26	Wei and Chen [177]	RaBTM	VANET	Combined trust model	2012	Springer	6
27	Wei and chen [176]	BTM	VANET	Combined trust model	2013	IEEE Journal	23
28	M. B. Monir et al. [179]	Categorized trust-based scheme	VANET	Combined trust model	2013	springer	18
29	Rakesh Shrestha [180]	Trustworthy event Information	VANET	Combined	2017	Hindawi	5
30	Wenjia Li [178]	ART	VANET	Combined	2016	IEEE	208
31	Adnan Mahmood et. al [181]	Trust Managemen t Heuristic	VANET	Combined	2019	IEEE conference	6
32	F. Dotzer [175]	Vars: VANETs reputation system	VANET	Combined trust model	2005	*IEEE Inter. Symposium*	169
33	Arpita Bhargava et. al [183]	Computatio nal Trust model	IOV	Entity Based	2017	IEEE conference	3
34	Shu Yang et al [186]	Trust-based anomaly detection scheme	IOV	Data-based trust model	2016	Hindawi	14
35	F. Gai et. al [184]	RTM system for SIoV	IOV	Entity Based trust model	2017	Hindawi	10
36	Fangyu Gai[185]	Ratee-Based Trust Mgmt. System for IOV	IOV	Entity Based trust model	2017	Springer	4
37	Mahmud Hussian [182]	Trust IoV	IOV	Entity Based	2017	IEEE	14

According to the literature review, Trust models are broadly categorized in three 1) Entity based model – calculates the entity trustworthiness 2) Data-based model - calculates trustworthiness of data sent by entity. 3) Hybrid trust models – performs trustworthiness of data as well as entity. Table 2.6. Summarizes trust models existing in each category. These trust models used different methodologies to model trust in network.

Table 2.6 Classification of Trust models for Different Networks

Type of model	Study
Entity based	[154], [155], [156], [100], [102], [187], [165], [164], [166], [91], [167], [182], [183], [184], [185]
Data Based	[158], [159], [170], [169], [168], [172], [173], [94], [95], [171], [174], [186]
Hybrid Model	[160], [161], [162], [163], [177] [176], [179], [180], [178], [181], [175]

Table 2.7 shows the types of network for which the existing trust models are proposed. Out of 37 trust models studied in the literature, existing trust schemes are focused on VANET and IoT, only few are proposed for IoV environment. So, in our work we will focus on modelling trust for IoV network.

Table 2.7 Types of Network and their references

Network	Study
IOT	[100], [102], [154], [155], [156], [158], [159], [160], [161], [162], [163]
VANET	[91], [94], [95], [164], [165], [166], [167], [168], [169], [170], [171], [172], [173], [174], [175], [176], [177], [178], [179], [180], [181],
IoV	[182], [183], [184], [185], [186]

Table 2.8. summarizes various methodologies used in existing trust models. It clearly shows that probability-based approach is the least explored for designing the trust models. Only two out of 37 trust models studied in literature used probabilistic approach. So, in our work we will focus on probabilistic approach to compute the trust.

Table 2.8 Approaches used trust model for IoT, VANET and IoV

Methodology	Study
Weighting	[167], [176], [179], [181], [154], [155], [156], [100], [159], [160]
Ratings	[94], [169], [172], [175], [184], [185], [163]
Probability	[165], [168]
Bayesian network	[166], [170], [178], [183], [102], [158], [161]
Location based	[95], [171]
Fuzzy logic	[91], [174], [153], [162],
Observations/Opinion gathering/ Evidence	[164], [173], [177], [180], [182]

2.16 Challenges in IoV modelling trust

Study of literature related to the trust model in vehicular network depicts that there are various challenges in modelling trust in IoV networks. Some main challenges in modelling trust in Iov network are presents below.

1. **Verification of Trust in Real-Time**: On roads vehicles move at a very high speed therefore it is quiet challenging to model trust in real time. Since vehicles interact for few micro-seconds, it is hard to judge whether node is trustworthy or not.
2. **Highly Dynamic Network:** The areas in which these vehicles function keep on changing for example road conditions close to a remote village might be completely different from a highway [22]. Therefore, Trust model should be developed in a manner it can handle these unpredictable circumstances.
3. **Network Congestion**: Large numbers of vehicles connect through VANET. For example: Millions of vehicles pass through roads of a highly dense urban area. This situation may worsen during rush hour as numerous people commute from work which may lead to network congestion.
4. **Decentralized Network:** As system is divided in various vehicles there is no centralization of network infrastructure. Nodes of IoV network interact with

each other. If a vehicle interacts with node, it is not certain to communicate with same vehicles in future.

In our work we will model the trust in IoV network addressing these challenges. According to the above challenges in modelling trust, trust model should have following characteristics.

1. **Fast computation** – To compute reliability of entity and information in real time for making quick decisions in IoV, trust model should have less complex so that trust computation can be fast. low complexity with also result in low computation overhead.
2. **Distributed trust computation –** Computation of trust in distributed manner is more suited for IoV due to its open, dynamic and self-organizing characteristics. When every node will calculate trust, there will be no need of central server to calculate the trustworthiness of nodes. Moreover, the system will have less chances of complete failure.
3. **Scalable:** Since the traffic is unpredictable so, the trust model needs to be scalable enough so that it can handle variations in nodes quantity avoiding congestion.

2.17 Research Gaps

The various trust models have been studied in the literature to identify the gaps. These Gaps are as follows.

1. Existing trust schemes are mainly focused on VANET and IoT. Very few trust models are proposed for IoV. Additionally, existing trust schemes for IoV either computes the trustworthiness of entity or data only. Trust schemes for IoV are lacking in combined trust model.
2. Most of the trust models use centralized authority for trust computation which violates the dynamic nature of IoV and thus reduces network scalability.

3. Trust schemes are not able to establish a secure communication in minimum time due to centralized trust computation authority, some cryptographic techniques etc. The time delay occasionally makes the traffic alerts useless.
4. In schemes such as Ratee based Trust Management the focus was on the trust issue in the IoV. In RTM scheme all node stores the rating information of their own rated by other nodes in previous interaction making **larger Routing table**.
5. In RTM, trust is estimated using cookies obtained in previous interaction. These cookies can be easily captured and suffer with the middle man attack. In addition to this Cookie or tokens of trust can be intercepted and copied by any intermediate threat to have Sybil attacks in the network.
6. Existing trust model in various network presents mechanism for trust computation after initial trust has been established. Also, each transaction RTM requires existing transactions to be made earlier for estimating the trust. There is no mechanism for trust establishment in initial stages of the network. This incurs the **cold start problem**, which can be solved by establishment of Trusted CA present at cloud when there is presence of internet at each node.
7. As CA server in RTM utilizes the cryptography (PK encryption) computation complexity will rise substantially due to 1) PK cryptography itself is computational expensive where atleast 256-1024 bit key is required.
8. Another Drawback is the scalability of the network, as Private keys (cookies) of each nodes are maintained by CA of the network rising no of nodes will raise the network overhead, computational complexity (encrypting and decrypting) of cookies.

2.18 Summary

This Chapter provides the basic understanding of the VANET, IOV and Trust. In this chapter, we studied the background of VANET and IoV. The chapter involved the concept of IOV with emphasis on its definition, architecture, characteristics, challenges and applications. This chapter also explained the concept of trust, trust metrics, various trust computation techniques and models for different networks like

P2P and distributed systems, Ad-hoc networks, IOT, VANET and IOV. The study of these trust models depicts that trust models in IOV are still lacking in terms of combined trust model. The current research methods in IoV are only either entity based or data based. Based on the many papers some challenges in modelling trust have been identified that needs to be overcome. Besides this, various the research gaps in literature have been identified that will be filled in our work.

Chapter 3 METHODOLOGY

Although the problem of modelling trust to secure interaction between vehicles has been previously explored by many researchers and different types trust models have already been projected by authors in research literature. But literature survey determines trust models projected in the survey belongs to VANET. Only few trust schemes were suggested for IoV. The models proposed in IoV models have focused on modelling the trustworthiness of either entities involved in interaction or the data exchanged during interaction. But in IoV environment, behavior of vehicles changes very rapidly so it is very necessary to model the reliability for both data and entity. Therefore, we have suggested a hybrid trust scheme which assesses the reliability of entities as well as data.

In existing models, node stores either reputation information of all other node with which it interacted previously or that of its own rated by other nodes (Ratee- based). So, the trust schemes are either Rater based or Ratee -based. Moreover, rater-based trust models do not work efficiently if an unknown node is encountered for interaction as the reputation of that unknown node will not be stored with them. The study [184],[185] employs the ratee-based trust models available in IoV. These ratee based models utilize cryptography to secure the data packets exchanged during communication that result in increased computational and time complexity. To solve this problem, we will not use cryptography scheme in our proposed model so that it employs minimum computational overhead and minimum time complexity and security of Network can be enhanced without negotiating the Quality of service.

The ratee based model also suffers from cold start as discussed in research gaps. The term Cold start is derived from cars. As we know when it’s very cold, car’s engine has problems with starting up, but if it is reached at its optimal operating temperature, it runs smoothly. So, “cold start” simply refers to the circumstances that are not yet optimal for car engine to provide the best results. Cold start problem in trust models refers the lack of trust initialization procedure. Existing trust model employs the

procedure of working after initial trust has been established. In our proposed models we will solve the cold start problem by providing initial trust values.

Another issue associated with Ratee based model is the Scalability. The term scalability means the ability of trust model to scale or adjust to network growth. In ratee based model, if large no. of vehicles interacts with a node then this might be difficult for that node to uphold their reputational information in their routing table as the routing table will become lengthy. In our proposed model we will solve this scalability issue by storing the trust values online. Existing Trust models also computes the trust in a centralized manner using trusted centralized authority. One of the main drawbacks for this type of computation is that in case centralized authority fails then whole system would fail. It will affect the network efficiency. To solve this problem the recommended trust model involves a distributed computation for trust. This distributed computation means that trust will be computed by each entity/node instead of a centralized authority. They help in improving the network efficiency because if a node fails to compute the trust then the whole network will not fail.

Herein, we suggest a trust model for IoV application that is hybrid lightweight (low complexity) updatable, supports heterogeneous devices and can be applied to routing IoV layer. The proposed model is Probabilistic in nature. So, it is named as Probability Distribution Based trust model (PDTM). It satisfies the desired characteristics of a trust model identified in the literature survey. These characteristics are fast computations, distributed trust computations and Scalability. The model is Robust against Attacks. This chapter proposes probabilistic concept of trust and hybrid trust framework along with process of trust modelling and updation. It also involves the methodology involved in implementation.

3.1 Probabilistic Concept of Trust

Trust is important component in creating a trustable IoV environment that would help to promote a safer road environment. Trust highly depends on the behaviour of the network components. In this work, we have modelled trust in terms of probability.

According to the concept used in our work we propose below mentioned definition of trust. **"*Trust is defined as a measure of probability of network components to accomplish any particular task/job in a predictable fashion.*"**

According to this definition the network component will be considered as trustworthy only if it behaves in predictable manner and its behaviour is modelled in terms of probability. Since the range for probability exists between 0 to 1 so, trust values will also vary between 0 to 1. The trust parameter will take the value according to the following rule

- If the probability of a network component to performs a task exactly in predictable manner is maximum then the trust value of that network component will be assigned as 1 that represents FULL TRUST.
- If the probability of network component to performs a task exactly in predictable manner is minimum then the trust value of that network component will be assigned 0 that represents FULL DISTRUST.
- If the probability of a network component performs the task partially in predictable manner lies in between minimum and maximum then the trust value of that network component will be assigned in between 0 and 1.

A network component can perform a task in predictable manner only when it behaves in good manner. Such network component is referred as TRUSTED/ NORMAL NODE in proposed trust. Similarly, the network component will not be able to perform the task in predictable manner only when it misbehaves. Such network component is referred as UNTRUSTED/ MALICIOUS NODE in proposed trust model.

According to the proposed definition, the trust involves three main components i.e. Network component Behaviour, predictable manner and Particular task as shown in figure 3.1. Every component plays significant role and functioning in establishing trusted communication. Network Component Behaviour includes end user behaviour, node/vehicles behaviour and RSU behaviour. End user behaviour can be positive or negative. If the user behave is positive then it is considered as trusted user otherwise

untrusted. Vehicle/node behaviour can also be positive or negative. Attacks on a vehicle can change the behaviour of its hardware or software. This may affect the journey of that node on the highway. RSU's behaviour can also be compromised by untrusted users in the network due to which RSU may disseminate fake warning message. Predictable Manner refers to the expectation of network component to behave in desired manner and disseminate the correct messages during interaction. Specific task refers to the applications and services of IoV. The trust is built in network component to accomplish specific task of serving end users with various applications related to driving and safety. Predictable Behaviour of network components increases the trust among them and consequently provide secure vehicular communication.

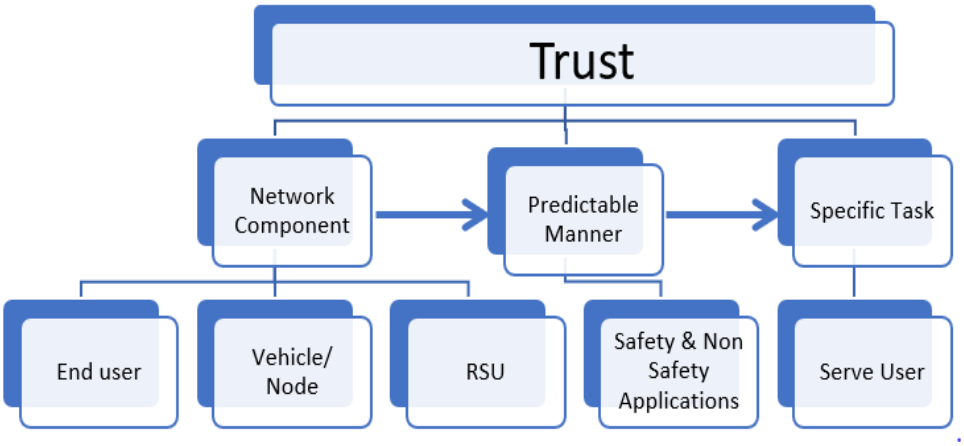


Figure 3.1 Pictorial View of trust

3.2 Probability Distribution Based Trust model (PDTM)

Probability Distribution Based Trust model (PDTM) is a hybrid trust scheme that performs both entity & data-based computations for trust. Moreover, threshold-based trust approach is suggested to assess the reliability of the nodes. This approach authenticates nodes by matching their trust values with preset trust threshold. Threshold is dynamically calculated based upon behavior pattern collected from simulation. Since threshold-based approach is able to validate nodes without involving complex computation So, node interaction can be established in timely manner that suits to the dynamic and decentralized nature of IoV network. A joint

probability-based approach is presented to update the trust at online centers. The trust is calculated by evaluating the trust worthiness of data using various statistics collected during interaction. The proposed PDTM system is neither Ratee based nor rater based because the nodes in proposed model do not store any reputation information about themselves or that of any other node during transactions. Trust is reflected as service and it is kept online at a trusted center using Internet of things. Nodes are also capable of computing trust of other nodes with whom they interact however trust update is not kept locally rather than updated online.

The aim here is to improve interactions between vehicles and reduce transaction time. Although most of the communication in IoV are short term but dedicated trust system makes it quite difficult to manage particularly if encryption policies are used whether private or public. In our proposed model nodes have capability of computing trust of corresponding nodes after communication and updating online as each and every node has internet connection. This model also collects trust of existing node even before communication has started thereby eliminating the need for dedicated storage trust in a dynamically changing topologies and also accelerating routing updates for improved QoS and lower routing overhead. Security and selfishness issue for wireless network can be formulated with the use of combined probability distribution. we design probability distribution system that separates normal node from abnormal behaving node with the use of combined conditional probability. By using simulation, the throughput characteristic, security characteristics, Node behavior like distance and speed with respect to PDR are computed post interaction to calculate trust. Trust model is developed in three steps:

1. Behavior identification of normal nodes in terms of various statistics like PDR, PLR, node distance, Speed, etc.

2. Addition of abnormal node and see the impact on the various statistics of nodes.

3. Segregation of normal and abnormal node through these behavior pattern of statistics the concept of probability distribution.

3.2.1 Architecture of Proposed PDTM

Our IoV system model follows the proposed concept of trust in which vehicles and RSU are considered as network component. Figure 3.2 demonstrates the model for an IoV system with interacting network entities/ components. In proposed architecture, the nodes can perform inter-vehicle interaction to take/ provide service from another node. Nodes can also interact with RSUs. We consider an IoV network with a trusted online server. Trusted severs are used to store the nodes trust value online and provide it when required. Every node in network can freely communicate with each other, perform trust calculation on the basis of nodes behavior during interaction, and update the trust online. In our models we considered both trusted and untrusted node. Trusted nodes are nodes which accomplish their job correctly in IoV system. The actions for a trusted node should alter after receiving any message from other node or from RSU. For instance, whenever a trusted node gets a traffic jam signal or an accident warning, the node is predicted to change its behavior like slow down the speed or take alternate route.

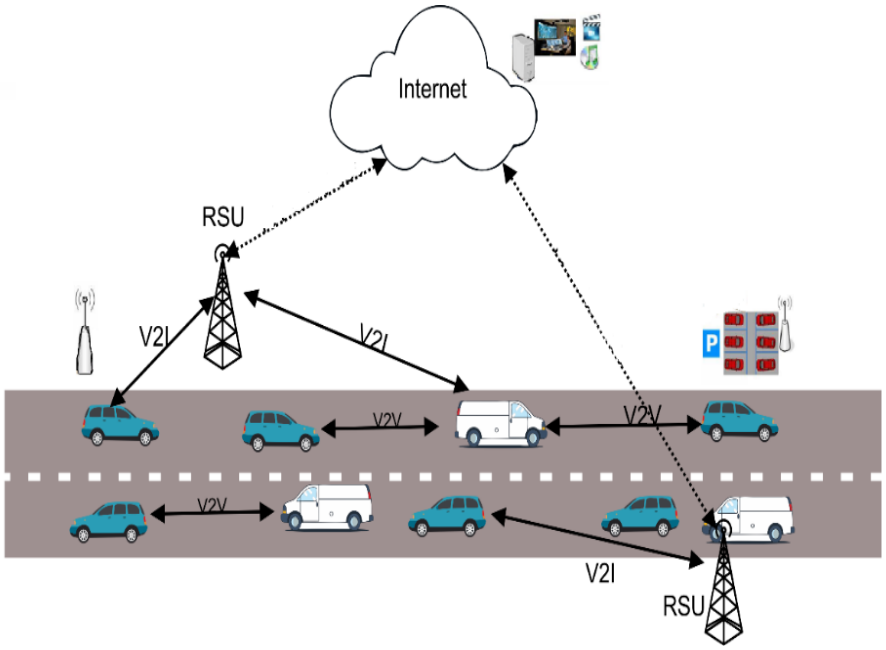


Figure 3.2 Network architecture for proposed PDTM

Malicious node is considered as the one who performs tasks in unpredictable manner and may create problems to another trusted node by launching various attacks. For example, malicious node may disseminate fake traffic jam message or an accident

warning which may cause other nodes to change their route resulting in unnecessary delay. Mischievous node may also disrupt working of the IoV system by misbehaving during interaction with other nodes. Trust value of a node is evaluated depending upon its behavior during the interaction. Its behavior is judge by collecting its different statistics like Node speed, distance, PDR. The trust update is event-based means trust value of a node towards another node will update post interaction only. Each node executes the trust protocol independently.

3.3 System model

The system model of proposed PDTM architecture is generated using various SUMO and TraCI4Matlab.

3.3.1 SUMO

SUMO (Simulation of Urban Mobility) is an open-source simulation software which helps user to generate road scenario including roads, vehicles, human etc. SUMO has special characteristics that it supports an externally imported road scenario that greatly reduce the efforts of generating a mobility model. The SUMO software is available on SourceForge. The software can be downloaded precompiled and packaged for common platforms or downloaded as source code and compiled. The software includes the core agent-based simulation tool, a graphical interface for visualizing a SUMO simulation and tools to help import road network data into the tool. The key input for the SUMO model is the road network that the traffic is navigating.

The most common source of road network data we have used is OpenStreetMap (OSM). We fetch a real map of Manhattan. The map was enhanced by marking areas, points and line denoting the roads, lanes, traffic lights etc. After enhancing the map is downloaded in .OSM file and imported in SUMO using netconvert. SUMO further processes this map to obtain a simulation network using netconvert command. After all these steps we obtained a road network file to simulate the flow of vehicles. Road

network obtained from SUMO showing random vehicles obtained movement is shown in figure 3.3.

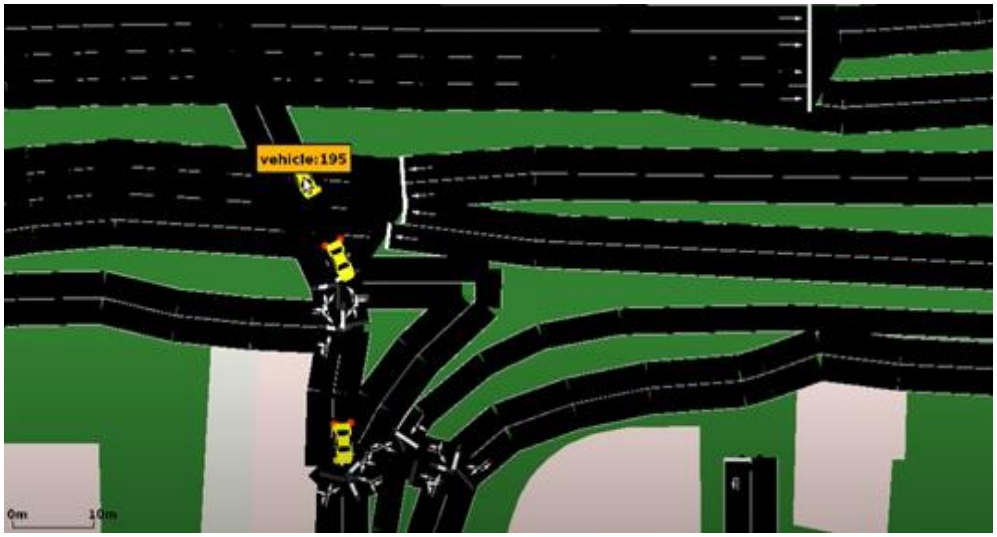


Figure 3.3 Sumo network File

TraCI4Matlab: TraCI4Matlab (Traffic Control Interface for MATLAB) is Application Programming Interface built in MATLAB to enable interaction of applications transcribed in MATLAB & SUMO. It enables MATLAB to control SUMO objects like node, traffic lights, etc. To create MATLAB and SUMO interaction port, the configuration file obtained in SUMO is required to be modified by specifying Input with right input files otherwise the simulation will not run properly. Steps for Using TraCI4Matlab**.**

1. Creating the simulation scenario in SUMO

To use TraCI4Matlab, the first step is to create a simulation scenario in SUMO.

2. Configure SUMO in server mode

To use TraCI4Matlab correctly, the configuration file of the SUMO scenario (the one with extension *.sumocfg*) must include the *traci_server* element configured to the 8813 port, which is the port used by default, as shown in figure 3.4. The *traci_server* element makes SUMO does not execute the simulation immediately, but to enter in a listening state on the 8813 port.

```
<?xml version="1.0" encoding="UTF-8"?>

<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

    <input>
        <net-file value="cross.net.xml"/>
        <route-files value="cross.rou.xml"/>
        <additional-files value="cross.det.xml"/>
    </input>

    <time>
        <begin value="0"/>
    </time>

    <report>
        <verbose value="true"/>
        <no-step-log value="true"/>
    </report>

    <traci_server>
        <remote-port value="8813"/>
    </traci_server>

</configuration>
```

Figure 3.4 Including the traci_server element in the SUMO configuration file

3.3.2 Creating the application in Matlab

Step 1: Execute SUMO from Matlab

Any application in Matlab that uses TraCI4Matlab must start by executing the commands: sumo if it is desired to execute the simulation without visualization or sumo-gui if it is desired to execute SUMO in GUI mode; specifying as a parameter the route where the configuration file of interest is found. This requirement is met through the Matlab's *system* command, as shown in figure 3.5.

```
clear all
close all
clc

import traci.constants

system(['sumo-gui -c ' getenv('SUMO_HOME')...
    '\docs\tutorial\traci_tls\data\cross.sumocfg&']);
```

Figure 3.5 Executing SUMO from Matlab

Step 2: Initialize the connection

After initializing the SUMO server in the previous step, the connection must be established with the function traci.init, as shown in figure 4.6. If the SUMO server was configured to use the 8813 port, the traci.init function doesn't need additional parameters. To use them, it's recommended to use the function help, by writing help traci.init in the Matlab's command window.

```
% Initialize TraCI
traci.init();

traci.inductionloop.subscribe('0');
for i=1:length(steps)

    % Perform a simulation step (one second)
    traci.simulationStep();

    programPointer = min(programPointer+1, length(PROGRAM));
```

Figure 3.6 Connection Establishment

Step 3: Developing the application

Normally, TraCI4Matlab applications include a main loop, in which the simulation's time steps are executed through the command traci.simulationStep. In this loop, the attributes of the SUMO's simulation objects are accessed and modified. The SUMO objects are grouped in various domains. The general structure to access or modify a SUMO object is: traci.<*domain*>.<*get/set_wrapper()*>, where *domain* can take any of the domains listed previously and *get/set_wrapper()* are the functions to access the values (*get*) or modify (*set*) the attributes of the object of interest. For example, if the velocity's value of the vehicle with ID *veh_1* in the current time step is required, the command current_speed_veh01 = traci.vehicle.getSpeed('veh_01') can be executed. To obtain a list of all the commands of a specific domain, write help traci.<*domain*> in the Matlab's command window, where *domain* can take any of the values listed previously. Figure 3.7 shows an example in the case of the lane domain.

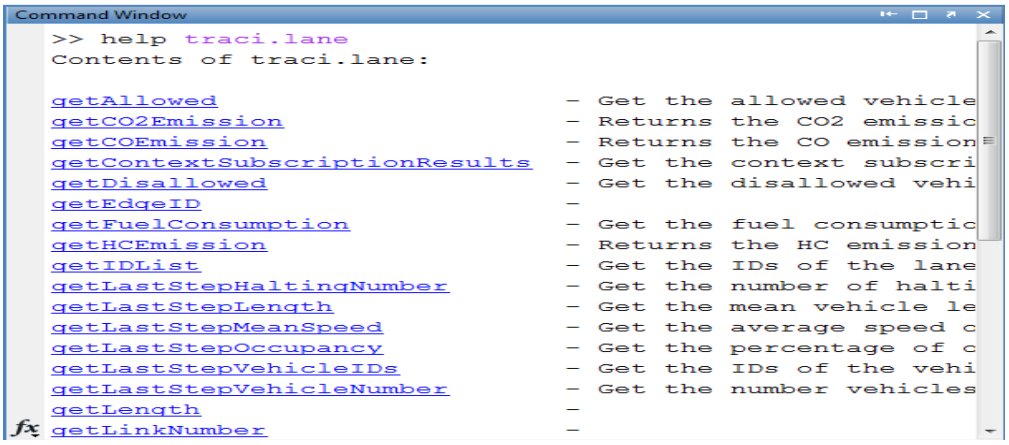


Figure 3.7 Obtaining a list of the functions related to a SUMO object

The simulation's main loop can be executed until a fixed time, or until all vehicles of the simulation have arrived to their destinations. In this case, the traci.simulation.getMinExpectedNumber function is used, as shown in figure 3.8

```
while traci.simulation.getMinExpectedNumber > 0

    % Perform a simulation step (one second)
    traci.simulationStep();

    programPointer = min(programPointer+1, length(PROGRAM));

    indloopSubsResults = traci.inductionloop.getSubscriptionResults('0')
    no = indloopSubsResults(constants.LAST_STEP_VEHICLE_NUMBER);
```

Figure 3.8 Simulation with minimum expected number

TraCI4Matlab includes functions to make TraCI subscriptions. TraCI subscriptions allow retrieving several SUMO by means of a single command. To use TraCI TraCI subscriptions, it's neccesary to know the TraCI constants containing the codes of different attributes related to a TraCI subscription. The TraCI constants can be found by typing edit traci.constants in the Matlab's command window, and locate the *"VARIABLE TYPES"* field. For example, suppose that it's desired to make a TraCI subscription to acces the values of the attributes "LAST_STEP_VEHICLE_NUMBER and LAST_STEP_MEAN_SPEED" of the *induction loop* with ID '0'. In this case, the command shown in figure 3.9 shall be used. Note that the import traci.constants command must be issued at the beginning of the *script*, as explained in the step 1.

```

traci.inductionloop.subscribe('0',{constants.LAST_STEP_VEHICLE_NUMBER,..
    constants.LAST_STEP_MEAN_SPEED});
```

Figure 3.9 TraCI subscriptions

Now, to access the values related to the TraCI subscription, the commands shown in the figure 3.10 shall be issued inside the main loop. Firstly, results are stored in a handle variable which later is indexed with the TraCI constants to which the

subscription was made.

```
indloopSubsResults = traci.inductionloop.getSubscriptionResults('0');
no = indloopSubsResults(constants.LAST_STEP_VEHICLE_NUMBER);
lsms = indloopSubsResults(constants.LAST_STEP_MEAN_SPEED);
```

Figure 3.10 Getting the results of the TraCI subscription

Step 4: Closing the connection

Finally, the connection to the SUMO server is closed as shown in figure 3.11. Later, post-processing of the obtained data can be made thanks to the advantages of the Matlab tools.

```
end

traci.close()

plot(steps, WElaneoccupancy)
hold;
plot(steps, NSlaneoccupancy, 'r')
legend('WE lane occupancy', 'NS lane occupancy')
title('Lane occupancy vs time')
xlabel('t (seconds)')
ylabel('number of vehicles')
```

Figure 3.11 Closing the connection to the SUMO server

3.4 Probability Based Estimation of trust

The proposed probabilistic Trust Based scheme estimates the likelihood that a Node would trust another node until certain degree of accuracy based on last communication. The IoV system gathers information statistics from communications and updates the trust values at data center which can be inquired for further interactions, IoV system can be made effective for providing a node or route with highest number of other nodes which require information. E.g. in case Node A in network wants to interact with Node B, Node A would like to know how much it can trust nodes in neighborhood for relay of information to Node B. In case we can provide all the nodes in system a recommendation service about such required nodes we can solve the given problem.

3.5 Trust Initialization and management in PDTM

We have proposed probability distribution-based trust model (PDTM) that works to disseminate data protocol wherein nodes behave as clients and the online trust center act as a server. This PDBTM protocol is driven by event which means that trust values of nodes can be updated either on occurrence of a communication activity or on encountering an event and trust values are gathered at IoV data center utilizing given recommendations. In case two nodes have direct communication activity, they can note about one another directly and will inform their assessment for trust at any online trusted centers using IoT devices. In case two nodes have indirect communication activity, they can interchange their trust assessment results with other nodes as recommendations. PDTM involves a trust initialization mechanism in which, every node would be given a preliminary value of trust i.e. 0.5 whenever it joins the network. This assignment of initial trust will enable the nodes to participate in the interaction and will solve the cold start problem associated with the existing trust models.

The Proposed PDTM suits well to be decentralized architecture of IOV as there is no centralized authority performing the trust computation. Each entity in network has the capability to compute the trust value itself after interaction and update it online. For the purpose of scalability, nodes keep their evaluation for limited number of nodes wherein it's most concerned. Nodes store the trust value of only limited set of nodes with whom it interacted recently. Besides this all-other trust values will be stored at the online trusted Centre. This will make the network more scalable in the sense that when the number of nodes increase during peak hours then nodes are not required to uphold the trust value of all available nodes as the trust values will be maintained at online centers. This will solve the problems associated with limited storage at node.

3.6 Trust Modelling Process in PDTM

IoV has many advantages for e.g. fast computation, internet connection etc. over VANET which is more useful for obtaining vehicular communication. However, IoV

is accessible and has large data set involved in its calculation. Additionally, IoV is dynamic network wherein vehicles join and leave the network continuously in order to manage with these properties of IoV, we propose a trust model which can secure interaction in IoV. The trust modelling process used in the projected model is shown in figure 3.12.

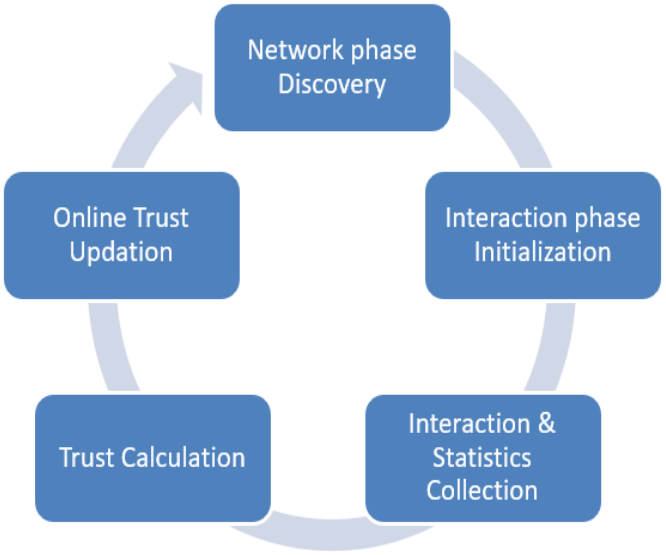


Figure 3.12 Trust Modelling Process

In proposed trust modelling process sender vehicle has to trace another vehicle with whom it desires to communicate in order to get service according to required situation. In case there are multiple service request then receiver node can initiate the network phase discovery with node having a good reputation (high trust value). Once network discovery phase gets completed communication between nodes takes place. During this communication, statistics collected by RSU and used further to compute the new trust value of receiver and sender node. Lastly, Trust value is updated at online centers.

3.7 Algorithm of proposed PDTM

Figure 3.13 displays the flow diagram for probability distribution-based trust model to obtain secure communication in IoV.

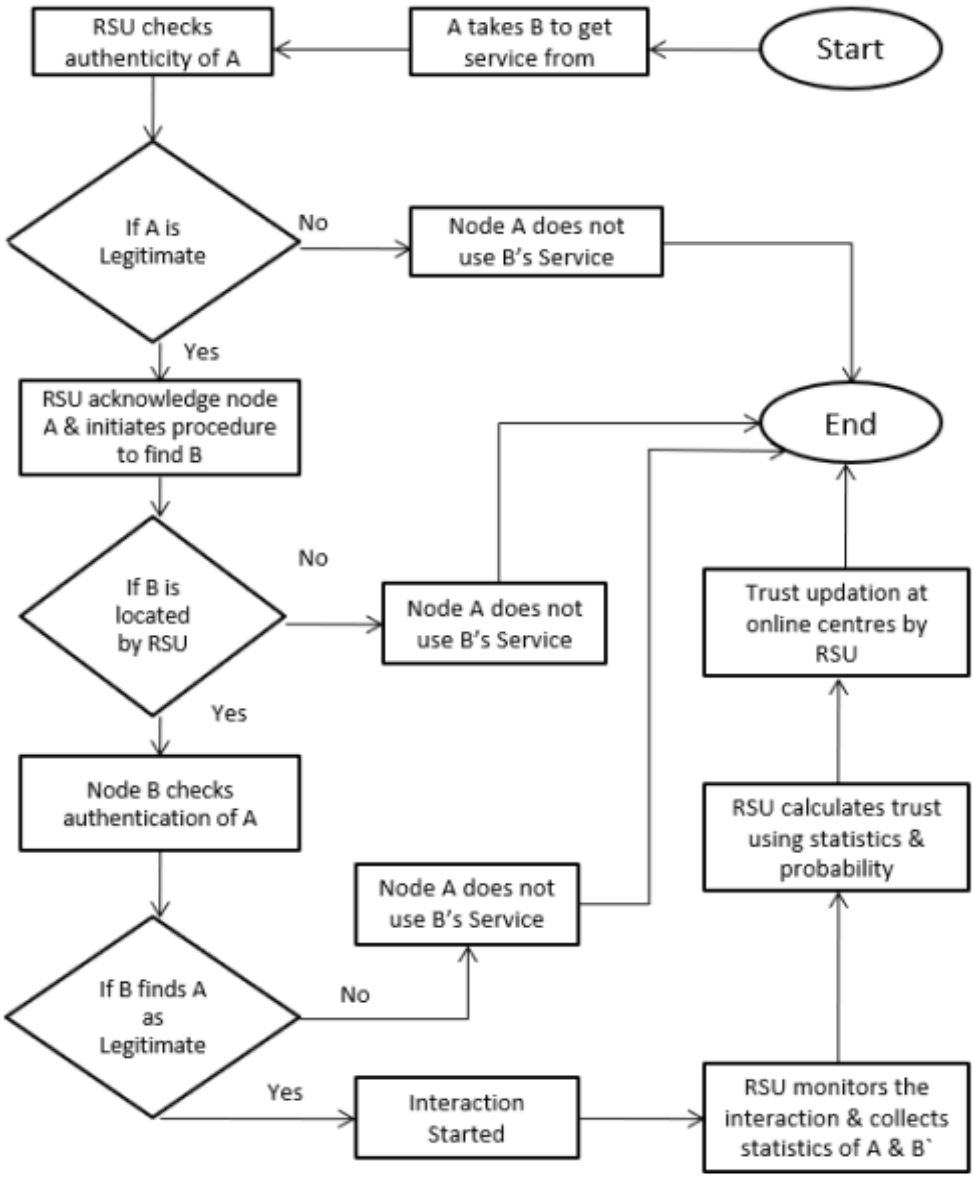


Figure 3.13 Flow Diagram of proposed trust model for IoV

This is to be noted that the proposed flow diagram is inspired from the communication of human in real life. We aim take services from a trusted service provider and after getting service we should update the feedback. (trust value in algorithm is feedback here).

The process initiates when node A tries to interact with node B in order for providing any service. Node A starts by sending a message to RSU to locate node B. When RSU gets request from node A, it initially check the authenticity of A using a trust

threshold (T_o). If A satisfies the condition of minimum level of trust threshold, then it is considered as a legitimate node. If RSU finds A as a trusted Node, it will initiate the process to locate B. After finding B, RSU would repeat the same process to judge reliability of Node B. If node B meets the minimum trust requirement which is set for a node to be a legitimate one, then the communication between A & B will start. If B's Trust value is below T_o then node A cannot communicate with node B. During this communication between both trusted nodes A & B, RSU would collect trust statistics e.g. Packet delivery Ratio (PDR). PDR is calculated by equation 1

$$PDR_t = \frac{Total\ packet\ received}{Total\ packet\ transmitted} \quad \ldots \text{Eq(1)}$$

If value of Statistics (S_t) for every node lies in between a range of mean (m) plus / minus 2 standard deviation (SD) of PDR, in that case nodes behavior would be considered as normal otherwise malicious. Once communication between A & B is completed, RSU would compute new trust value for both node A & B with the use of conditional probability. RSU would then update the newly computed trust value at online centers.

$$if \left\{ \begin{array}{l} S_t > m + 2SD \\ S_t < m - 2SD \end{array} \right\} \quad Malicious\ Behaviour \quad \ldots \text{Eq(2)}$$

and

$$if \left\{ \begin{array}{l} S_t \leq m + 2SD \\ S_t \geq m - 2SD \end{array} \right\} \quad Trusted\ Behaviour \quad \ldots \text{Eq(3)}$$

Every time a failed / successful interaction takes place between nodes, trust will be calculated using the conditional probability and will be updated (i.e. incremented in case of successful communication and decremented in failed communication).

3.8 Routing Table Extensions

We added new trust field in each node's and packet transmitted from the original routing table. Post successful communication between two nodes trust value is estimated and updated to server. Negative trust events are the failed communication

and trust vectors is the node's confidence about another node's credibility post communication.

Trust values will be stored at online centers as shown in figure 3.14. In this notation R[i, j] denotes numeric trust rating for node j, over the interaction i. No matter how the rating is expressed, we need to convert them to numeric values. If a node has never participated in interaction then trust rating value R(i, j) will not be null, the system assigs it smallest amount of trust to avoid cold start problem.

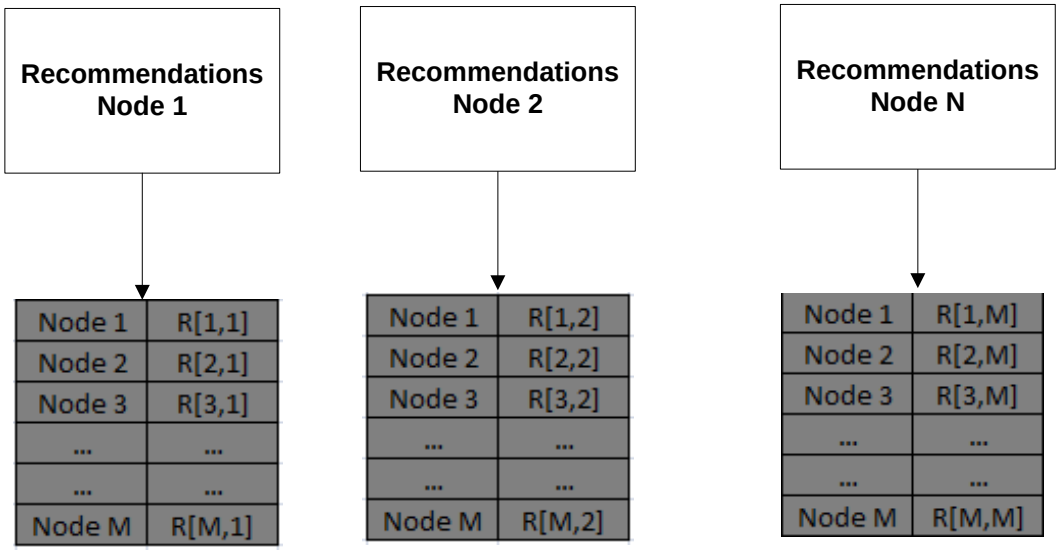


Figure 3.14 Trust rating stored at trusted centres

In Proposed Probabilistic Method each node may store only required working set (trust value of neighboring nodes only or the nodes in its current vicinity as shown in figure 3.15. Working set is calculated by RSU and Recommendation feed is requested via a IoV Call to Server) instead of storing trust of each node in network.

3.8.1 Routing table message extension

Initial routing message is extended by adding two new trust fields which are TREQ and TREP. TREQ is trust Request and TREP is trust reply. In the procedure of discovering trusted routing path, all routing requests and their replies contains trust evidence, like the ratings about source as well as destination, which were employed to estimate the trustworthiness of Source and Destination.

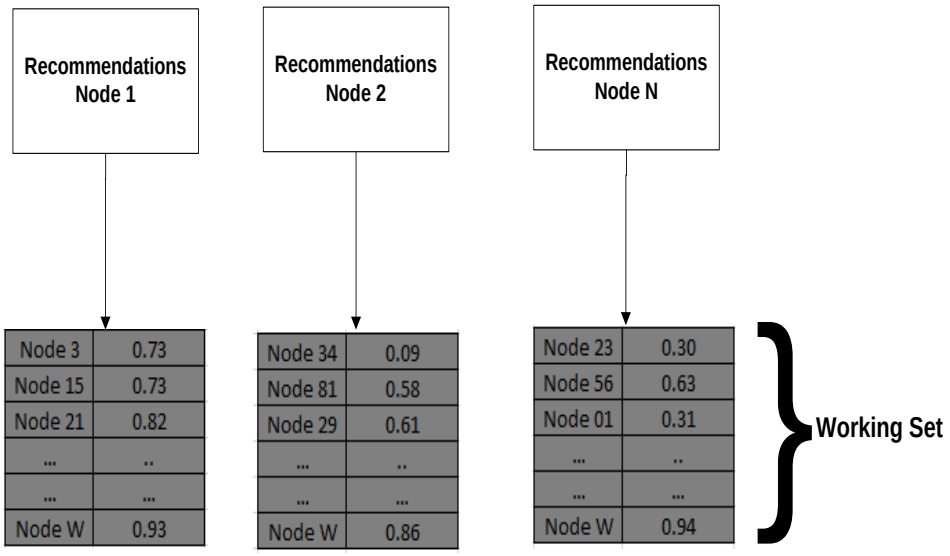


Figure 3.15 Working sets in routing table

3.9 Conditional Probability Estimation using Statistical Analysis of Joint probability distributions

We use a probabilistic distribution-based model to compute direct trust in a node Figure 3.16. While doing so we measure the reliability and genuineness of immediate interacting nodes by taking part in communication. Whenever a node transfers information it keeps the receiver in promiscuous mode. Moreover, as early as it hears its immediate node neighbor about forwarding packet, node checks for reliability of packet after verifying for necessary modifications. If integrity check passes, it would confirm that node had operated in decent fashion and this makes value of direct trust vector increase on basis of behavior properties. Likewise, in case integrity check becomes unsuccessful its corresponding trust vector can be reduced.

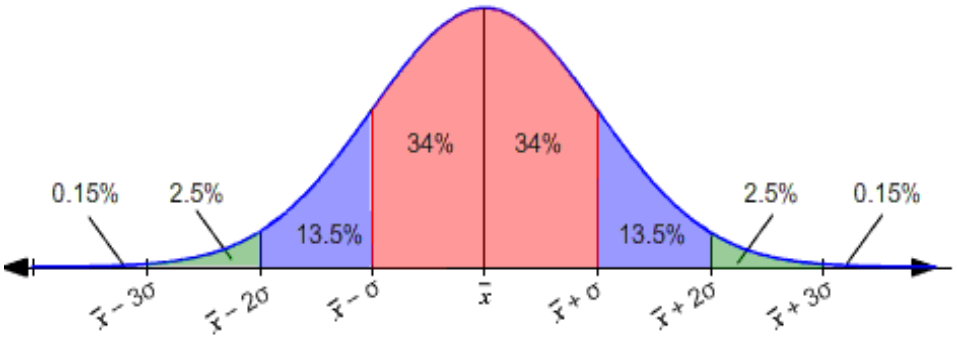


Figure 3.16 Probability distribution for estimating the trust for nodes

The direct trust for node B given by node A as T_{AB} is computed by equation 4

$$T_{AB} = P(S_1 | P_{Ns1}) \times P(S_2 | P_{NS2}) \ldots\ldots P(S_m | P_{NSm}) \quad \text{... Eq(4)}$$

Wherein $P(S_1 | P_N)$ signifies the estimated trust for node B through A if utilizing statistics S_1 given the distribution of S_1 as P_{s1} and also Conditional probability being$P(S_1 | P_{Ns1})$ This $P(S_1 | P_{Ns1})$ projects the probability of having normal statistic S1 if trust distribution for statistic S_1 is specified as P_{S1}. Neighbourhood based trust is not considered in our model because the neighbouring nodes are continuously changing and chances of communication with same neighbourhood node are very less. we have used behavioural approach for calculation of trust. Trust value of a node is calculated by using node statistics collected from simulation.

Equation 5 is the normal distribution given input variable X, mean μ and standard deviation σ

$$Normal\ Distribution\ (x, | \mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad \text{... Eq(5)}$$

of the Probability density function (PDF) of a given statistic S_m which can be modeled as equation 6

$$PDF\ (S_m, | \rho, \tau^2) = \frac{1}{\sqrt{2\pi\tau^2}}\, e^{-\frac{(S_m-\rho)^2}{2\tau^2}} \quad \text{... Eq(6)}$$

Here ρ is mean of statistic S_m and τ is standard deviation. The mean (ρ) and also standard deviation (τ) is collected by implementing network in normal mode without the presence of malicious nodes. For instance, if S_m is let's say Packet delivery ratio (PDR) then during normal interaction we can collect no. of packets received and sent for fixed given time frame t to calculate packet delivery ratio. It has been statistically observed that probability distribution of trust is Gaussian in nature because of the fact that there are very few nodes that have very high trust value and very few nodes that have very low trust values. Most of the nodes have trust values closer to the mean trust.

3.10 Trust Updating Policy

Trust in between nodes can adjust fast with escalation of successful or unsuccessful interaction. For instance, nodes A and B interact, how and when to bring up-to-date trust opinion between nodes would follow a policy that can be derived as

1. Firstly, A will request to service trust vector of corresponding node B, in case trust is better than predetermined minimum threshold trust, communication between nodes begins
2. Node A and B communicate with one another and during this interaction they collect various statistics about communication like Node Distance, PDR, Node Speed etc.
3. By utilizing statistics communication can be classified as positive (normal) or negative (abnormal) on the basis of existing probability distribution function projected using normal and abnormal communication.
4. We can combine probability distribution using conditional probabilities to evaluate trust of existing node.
5. Every time after normal interaction incident happens starting with node A to B, B's Trust of Node B stored at cloud server as communication, Trust(A,B) is updated (increased).
6. Every time after abnormal interaction incident happens starting with node A to B, B's trust of Node B is stored at cloud server as communication, Trust(A,B) is updated (decreased).
7. Every time when trust of successful or unsuccessful event changes, trust value would be re-computed by means of conditional combined trust.
8. Whenever fresh opinion has been taken by an interaction corresponding trust of node will be updated at server.

3.11 Trust Based routing in PDBTM

This section presents different phases for communication and updating trust between two nodes. Figure 3.17 shows complete flow of interaction and trust update Node A

and B are communicating node. RSU monitoring entity collects statistics for communication of node and updates to IoV server through IoV service endpoints which is API. During mobility the API call may get affected. However, in PDTM we considered full internet service provided to all the nodes all the time.

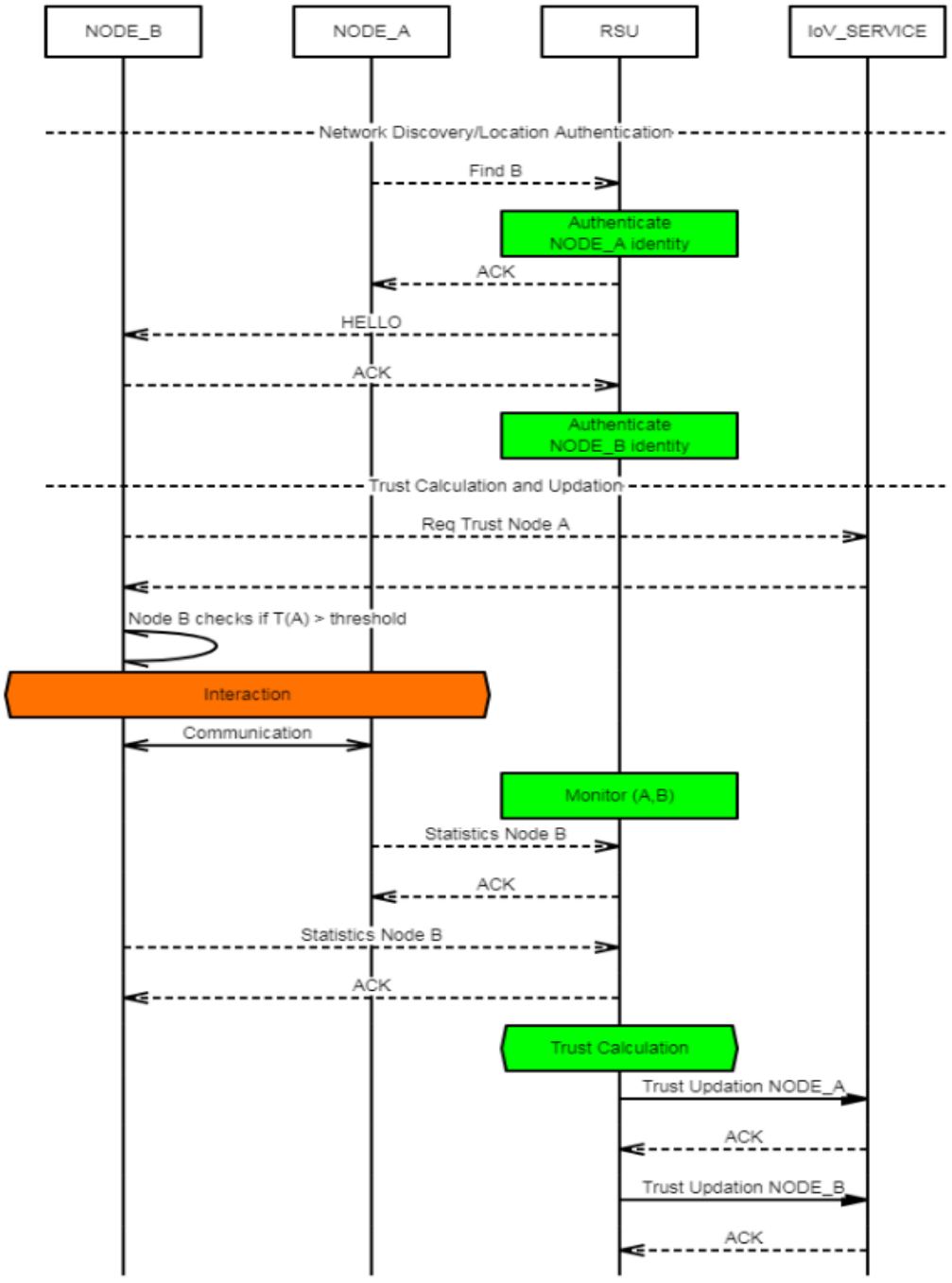


Figure 3.17 Network Discovery and Interaction

Step 1 Network discovery phase

Node A & B want to interact amongst themselves therefore the situation initiates RSU to find node B. If node B exists in neighborhood, RSU primarily validates Node A. If node A is genuine (denoted by trust value of A> predetermined threshold) then RSU sends acknowledgement to node A and starts the process to find node B. After finding node B, communication phase would start between Node A and Node B.

Step 2: Interaction phase

During this phase, initially node B would need to authenticate if it trusts node A or not. Therefore, node B would directly make an IoV call to know if node A is reliable or not. As node B is already authenticated by RSU so IoV service would send trust values of node A to B. Node B would check trust value for A, in case it is larger than predetermined threshold after which node B can initiate communication.

Step 3: Interaction and Statistics collection

RSU would monitor the communication of node A and B and it will gather the statistics of both A and B.

Step 4: Trust collection and updation

By using collected statistics and also conditional probability, T_{AB} is computed. By utilizing conditional probability and current calculated trust T_{AB}, the trust for node A can be updated at IoV center through RSU using equation 7.

$$\mathrm{TAB(New)} = \mathrm{P(TAB/TAB(old)} \qquad \ldots \mathrm{Eq(7)}$$

3.12 Benefits of Proposed PDTM

- This model allows vehicles to differentiate reliable signals from unreliable one in single communication between the nodes.
- Trust as a Service would eliminate identity forgery, this is due to the fact that Trust is taken as a service would lead to decreasing the chance of vehicles being ill-advised by other mischievous vehicles who can forge their own trust.
- Probabilistic Scheme is scalable, as it requires no or very low overhead when nodes want to interact and trust of corresponding nodes would be updated after

communication at the cloud level greatly reduces amount of traffic needed for estimating other nodes reliability.

- The suggested Recommendation based System calculates and regularly maintains the likelihood or Probability that a Node can trust another given node up to a certain degree of accuracy on the basis of earlier communications with the node that the system (IoV) was aided by the Trusted CA.
- For Assessment of Trust between Pairs and solving a cold start problem a probabilistic trust as an authority is recommended.
- Probabilistic Distribution Trust is a special procedure to prove a node's identity and legitimacy by estimating probability of upto what extent a node can be trusted after interactions.
- The Benefit of Probabilistic trust establishment is isolation of Sybil Attack because of non-locality principal and very low complexity and once link is established it becomes very scalable i.e. no need of a CA to validate node.

3.13 Simulation Scenario

This simulation setup of our proposed trust model for IOV involves SUMO and MATLAB. The main aim of conducting simulation is for studying how effectively PDTM trust model works in presence of malicious/non-trusted nodes in IoV network. To accomplish this, the PDTM is Simulated on SUMO with 1.4.0 version and the MATLAB with 2016a version. SUMO is traffic simulator that is used for obtaining the traffic patterns whereas the MATLAB is utilized as an event simulator. MATLAB has been chosen here for simulation since there are a number of V2X applications that can be easily designed to mitigate traffic problems. In our work we used real world map. The traffic scenario for real-world map of Manhattan city used in our work is generated using sumo and is presented in (Figure 3.18). This research work has considered Manhattan city map because it is a standard test map. Any Indian city can also be considered. The proposed model is suitable for any city. This figure depicts the top-view for a traffic scenario nearby an intersection of two roads having tall buildings. The objects visible in light green colour are the vehicles moving on roads.

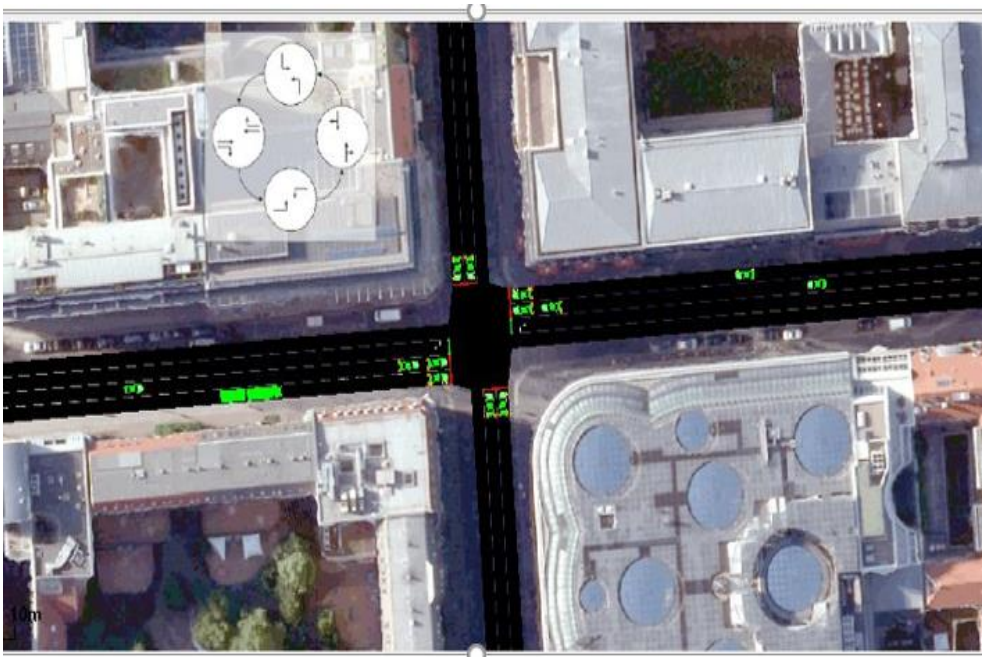


Figure 3.18 Traffic Scenario - Open Street Map for a Manhattan City

In simulation arrangement, the behaviour of every node may change dynamically. It is not necessary that a node that is trusted for during one interaction will remain trusted in every interaction. So, trust of both nodes is being calculated after every interaction between nodes and this trust will be updated online post interaction. This online storage of trust will solve the storage issue and improve the network scalability. The parameters which are provided as an input to the system during simulation are summarized in Table 3.1.

The Simulation is conducted by arbitrarily setting some of the available nodes as the untrusted/abnormal nodes. Preliminary trust value assigned with each node is 0.5 irrespective of whether it is a trusted or an untrusted node. This initialization of trust value will prevent the PDTM from cold start problem. But as the time passes and node starts interaction with each other, the trust value for normal nodes will start increasing as a result of every successful interaction whereas that of malicious/abnormal/untrusted node will start decreasing as a result of their malicious behaviour or misbehaviour during interaction. Besides Trust value the metrics chosen to detect misbehaviours are PDR, available number of hops and Success rate.

Table 3.1 Simulation Parameters

Simulation Parameters	Values
Monitoring Area	1000X1000 meters
Number of nodes (n)	30-110
Range of Communication	250 meters
Interval between Packets	2 ms
Data Packet Length	923 bits
Symbol rate	256KB/S
Bit rate	512KB/S
Simulation time	180 (s)
No Malicious Nodes	10%
Routing Protocol	A-STAR
Mac Layer Protocol	802.11p
Trust Range	[0, 1]
Preliminary trust value of each node	0.5
Trust Threshold	0.65, 0.70, 0.75

For simulation of PDTM trust model, a dynamic IoV environment is considered that consists of 30-100 entities/nodes in having initial 10% malicious node percentage. All these nodes randomly move in 1000*1000meters square area and has range of 250m for communication. The total time of simulation is taken180mins (3hrs). The proposed PDTM is evaluated by three metrics i.e. Number of available hops, PDR, trust value and success rate. Then the malicious node percentage is increased to check the effect of malicious node percentage on proposed model PDTM. Also, the performance of PDTM is compared with existing RATEE based trust model for different percentages of malicious nodes (mp= 10%, 20%, 30%, 40%). Simulation is conducted for three different value of threshold to study the impact of threshold value on evaluation metrics like PDR, average number of available hops. This study of different threshold will show how the value of evaluation metrics (PDR, number of available hops) vary for trusted and untrusted node under normal threshold policy (θ= 0.65), slightly strict (θ= 0.70) and highly strict threshold policy (θ= 0.75).

Chapter 4 RESULTS AND DISCUSSION

In this unit, the proposed trust model PDTM would be evaluated to ensure that problems identified in research gaps are resolved. The PDTM is analyzed analytically as well as through extensive simulations. An analytic analysis of PDTM is provided with respect to various characteristics requirements of trust model like speed of computation, scalability, distributed computation, robustness etc. The simulation-based performance analysis is done in two Phases 1) simulation-based performance evaluation 2) Simulation based performance comparison. The simulations-based performance evaluation is conducted to depict how effectively the proposed model separates the mischievous nodes from trusted nodes to secure interaction amongst nodes whereas simulation-based performance comparison is done to compare the proposed PDTM and existing Ratee based model [185] under the changing percentage of malicious node. Simulation based performance evaluation is done using the metrics Packet Delivery ratio, Average number of hops available, trust dynamics, and Success rate. The model is simulated to evaluate its success rate under increasing number of malicious node percentage. The proposed model is also evaluated to analyze effect of threshold on these metrics for both trusted and non-trusted node. The Simulation based performance is compared by three given metrics 1) Computation time 2) Transaction growth, 3) Success rates under four different malicious node percentage.

4.1 Analytical Evaluation

Hybrid Trust Model: The PDTM computes the trustworthiness of entity using Threshold-based approach and trustworthiness of data is evaluating by collecting the nodes statistics during interaction. Since the model computes the trustworthiness of both entity as well as data, it is a Hybrid trust model.

Less Computation complexity: As the use of cryptography involves the high computation complexity, the cryptography scheme has not been used in PDTM for authentication of nodes. Node authentication is done in simplest way by comparing

the trust value of node with pre-set threshold. This greatly reduces the computation complexity and the overhead involved in key exchange and management.

Distributed trust computation- The PDTM does not calculate the trustworthiness of nodes involving any central authority. In proposed model each node individually connects with internet to calculate and update the trust value of nodes after every interaction. Thus, trusted is computed and updated in a distributed manner. This distributed trust computation reduces the chances of complete system failure and is more suited for open, dynamic and self-organizing nature of IoV.

Robustness: The model is designed to separate malicious and trusted nodes. Trust as Service eliminates identity forgery, As Trust is taken as a service this results in eliminating the risk of disguising vehicles by other mischievous nodes. Probabilistic trust establishment is isolation of Sybil Attack because of non-locality principal

Scalable: PDTM is scalable in the sense that it requires very low overhead to compute and update the trustworthiness of nodes. In addition to this, nodes in system do not have to maintain the trust dynamics for other nodes in system as trust metrics are stored online at trusted servers. Nodes can maintain the trust value for only small set of nodes with which it plans to have interaction. So, the proposed trust model is scalable enough to handle the large number of nodes avoiding network congestion.

Solution to Cold Start Problem: The proposed model does not suffer from cold start as it involves a trust initialization mechanism. In PDTM every node is assigned with a minimum trust value initially so that it can participate in interaction and its trust is then update as per its behavior during interaction.

Time complexity: This approach authenticates the nodes by comparing their trust values with a pre-set trust threshold. Since threshold-based approach is able to validate nodes without involving complex computation. So, node interaction can be established in timely manner that suits to the dynamic and decentralized nature of IoV network.

4.2 Probability Distribution curve of Selected Statistics

We have used total 5 trust statistics for the evaluation of data-based trust. Three statistics are collected directly (node distance, average speed and packet forwarding whereas two are derived (packet delivery ratio, Packet loss ratio). For each statistic we have calculated the probability distribution using SUMO. The Average Speed (ω) is computed using equation (8) by calculating total distance covered by all normal nodes (***n***) in the network in time frame ***t.*** The Probability distribution of speed of the node is shown in fig 4.1

$$\text{Average Speed } (\omega) = \frac{\sum_1^n Distance\ covered}{n \times t} \qquad \text{... Eq(8)}$$

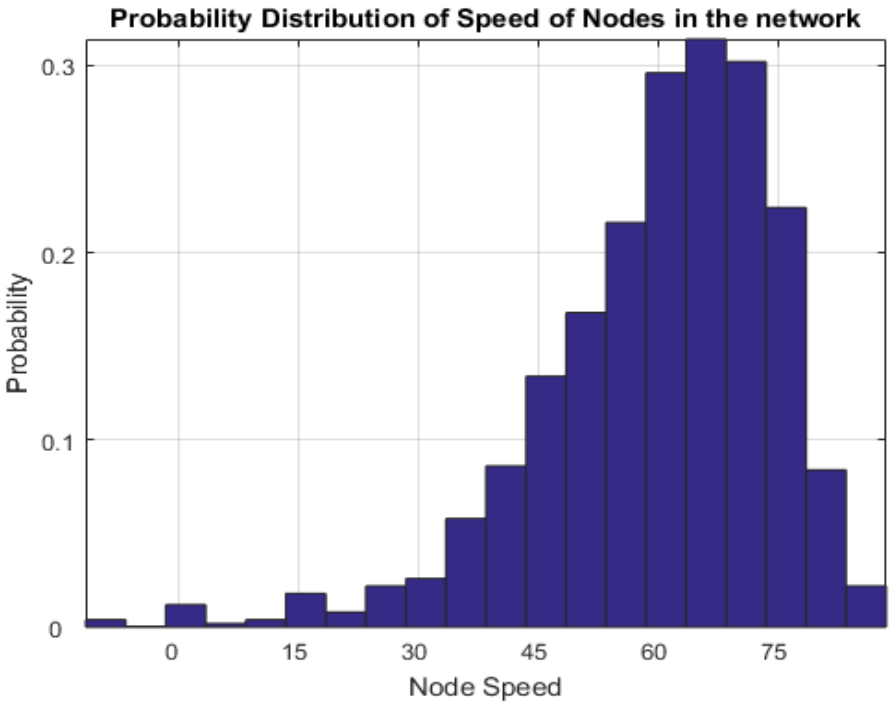


Figure 4.1 Probability Distribution of Speed of Nodes (Km/hr) in the network calculated using SUMO environment.

The packet forwarding refers to the basic method for sharing information across systems on a network. The estimation of probability distribution of forwarding the packet in the system is presented in Figure 4.2.

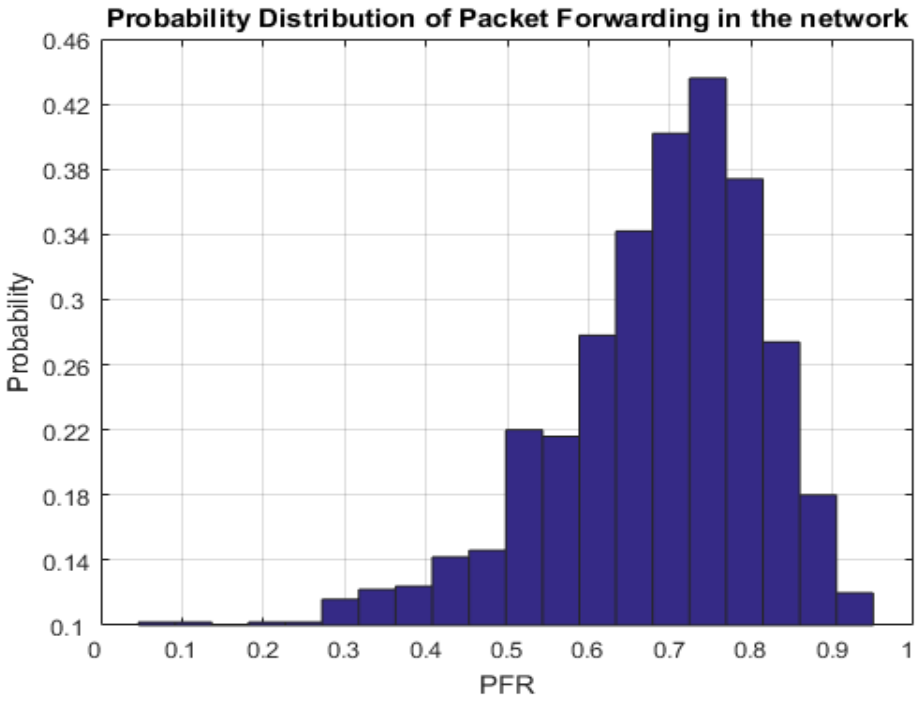


Figure 4.2 Probability Distribution for packet forwarding in the network, calculated using SUMO environment

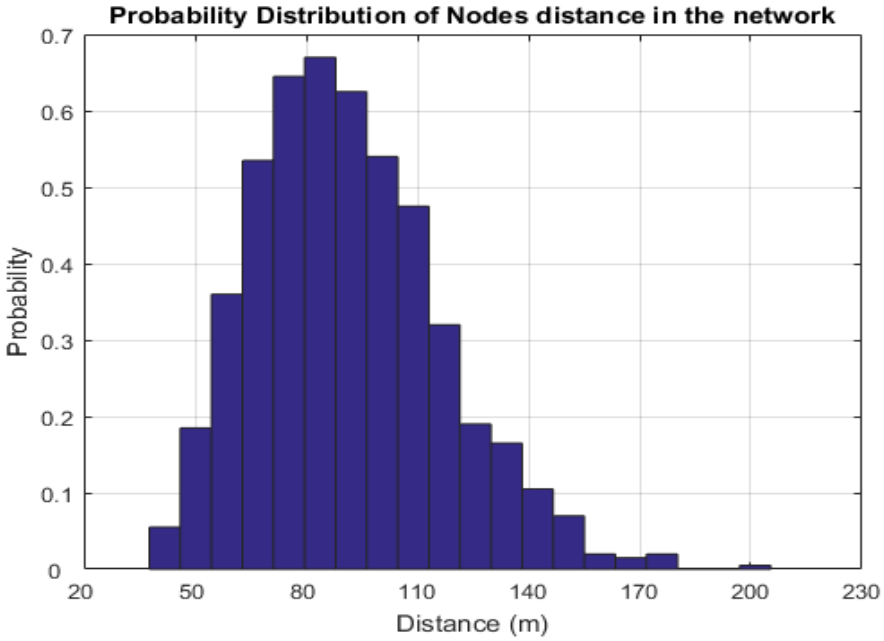


Figure 4.3 Probability distribution of node distance in network, calculated using SUMO

Node Distance refers to the distance travelled by a node and probability distribution

of node distance is shown in Figure4.3. Figure 4.4 depicts PDR for a node. The PDR is calculated as number of packets received divided the no. of packets sent using equation 9.

$$PDR_t = \frac{\sum Packet\ Received}{\sum Packet\ Sent} \quad \text{... Eq(9)}$$

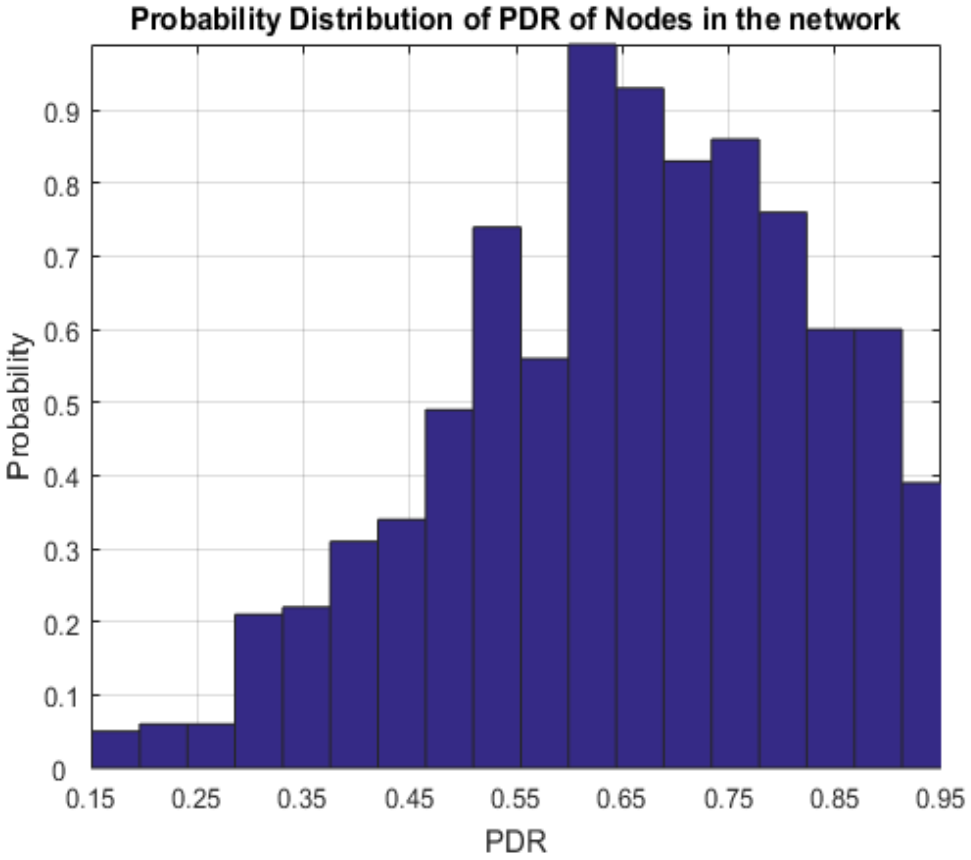


Figure 4.4 Probability Distribution of PDR in network, calculated using SUMO

The **Packet Loss Ratio** is calculated as the number of packets which initiated at source and were received at destination in given time frame ***t*** *using Equation 10.* The probability distribution of packet loss ratio in the network is shown in figure 4.5.

$$Packet\ Loss\ Ratio = \frac{Recieved\ Packets - Routing\ Packets}{Total\ Sent\ Packets - Routing\ Packets} \quad \text{... Eq(10)}$$

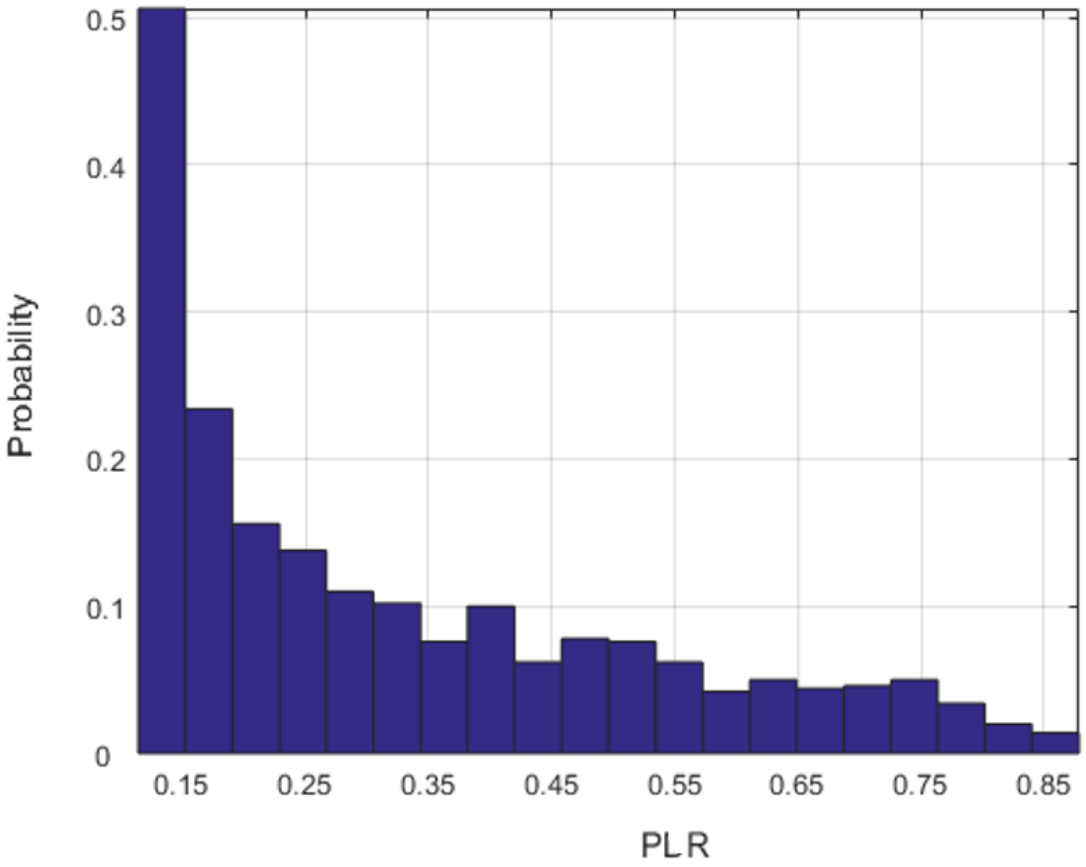


Figure 4.5 Probability Distribution of PLR in network, calculated using SUMO

4.3 Classification of nodes in Abnormal and Normal Nodes utilizing distributions and thresholding.

The probability distribution functions of the various statistics are used to classify the normal nodes from abnormal nodes. We are explaining this by taking speed statistics initially. The PDF for ω can then be used in projecting the abnormal behavior, for instance if ω's PDF is given and we recognize mean μ speed for an average node and standard deviation σ of ω for nodes in normal network we can project abnormal behavior as two standard deviation apart from the mean. Wherein the node can be categorized as either normal or abnormal given, σ, μ and PDF $\left(\frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\frac{(x-\mu)^2}{2\sigma^2}}\right)$ as shown by Equation 11 and 12.

$$\text{Abnormal Node} = \left\{ \begin{array}{l} \omega > \mu + 2\sigma \\ \omega < \mu - 2\sigma \end{array} \right\} \qquad \text{... Eq(11)}$$

and

$$\text{Normal Node} = \left\{ \begin{matrix} \omega \leq \mu + 2\sigma \\ \omega \geq \mu - 2\sigma \end{matrix} \right\} \quad \text{... Eq(12)}$$

Wherein the ω is bounded by $[\mu - 2\sigma \geq \omega \leq \mu + 2\sigma]$ for a normal node and this classification above can also be used for any metric S_m given mean ρ and standard deviation τ as stated by Eq. 13 and 14.

$$\text{if} \left\{ \begin{matrix} S_m > \rho + 2\tau \\ S_m < \rho - 2\tau \end{matrix} \right\} \quad \text{Abnormal Behavior} \quad \text{... Eq(13)}$$

and

$$\text{if} \left\{ \begin{matrix} S_m \leq \rho + 2\tau \\ S_m \geq \rho - 2\tau \end{matrix} \right\} \quad \text{Normal Behavior} \quad \text{... Eq(14)}$$

Therefore, this statistical behavior S_m is limited by $[\mu - 2\sigma \geq \omega \leq \mu + 2\sigma]$ for a normal node, in case the behavior of the node crosses the limit the node is marked as an abnormal node.

It can be seen on system model let's consider there is an interaction between node A and B, during the time T which can be separated into different time slots, which are $T = \{T_1, T_2, T_3, \ldots T_t, \}$. This is presumed that in every time slot T_i node can observe η times the forwarding manners of any node in network. The PDR for node in different time slots are $PDR_{nt} = \{PDR_{n1}, PDR_{n2} \ldots = PDR\upsilon_{nt}\}$. We can set a bound $\emptyset$ for the PDR as threshold for identifying behavior. During interaction if $\emptyset(A, B)$ is two standard deviation apart the threshold mean packet-forwarding ratio for node ***B*** during any interaction period we mark the node as abnormal node and reduce the trust of node using Equation (15)

$$T_{AB} = P(S_1 | P_{Ns1}) \times P(S_2 | P_{NS2}) \ldots\ldots P(S_m | P_{NSm}) \quad \ldots \text{Eq.(15)}$$

the T_{AB} is utilized for updating trust value for Node B by Node A at IoV center. We used the probabilistic distributions functions to decrease the inaccuracy in calculating the trust for a particular node, that is computed by uniting the earlier trust of node **B** available at IoV center and current time frame estimated joint probability distribution T_{AB}. Through this, we can maintain the probability range [0-1] as well as can select both the normal and the abnormal nodes clearly using probability distributions of

metrics defined above. As shown in figure 4.6 we have used the joint probability distribution of Speed and PDR of node to identify the normal and abnormal behavior. The Circle represent the bound $[\mu - 2\sigma \geq \omega \leq \mu + 2\sigma]$.

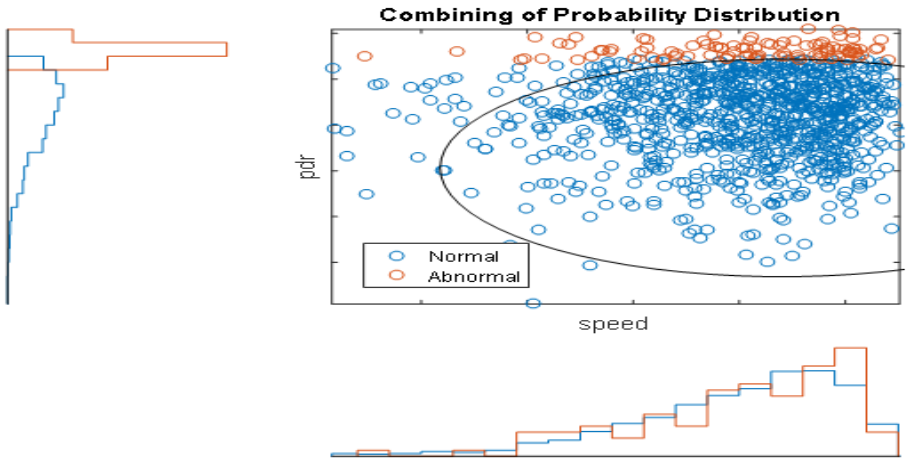


Figure 4.6 Joint Probability Distribution of PDR and Speed in the network for estimating Trust vector of nodes

4.4 Simulation- Based Evaluation

The simulation is conducted to evaluate PDTM in the sense that how effectively the model work under the IoV environment. Simulation of PDTM shows how easily it can filter the trusted node from the malicious nodes using simulation metrics like the PDR, Average no. of hops, trust values and Success rate. The whole simulation is conducted for three different threshold values.

4.4.1 Packet Delivery Ratio

PDR is calculated by dividing no. of packets which receiver node successfully acquired and the total number of packets sent by sender. The PDR of trusted node remains high as it does not discard the reception of packets intentionally and tries to deliver maximum packets received by it where as that of malicious nodes will be comparatively less because they may drop the packet or discard it before reception. The simulation curve shows how the PDR of trusted (normal) and malicious

(abnormal) nodes changes with time. The results depict that for both trusted and malicious node, PDR increases with time. But this increase is high for trusted node as compared to the malicious node. Ideally it is considered that PDR of a well behaving trusted node should be as high as possible. The curves presented in figure 4.7 shows Average PDR of the trusted node wrt time. It shows that the Maximum value of average PDR for normal nodes for different value of threshold are as below

1) For θ = 0.65 PDR is 0.920
2) For θ = 0.70 PDR is 0.818
3) For θ =0.75 PDR is 0.647

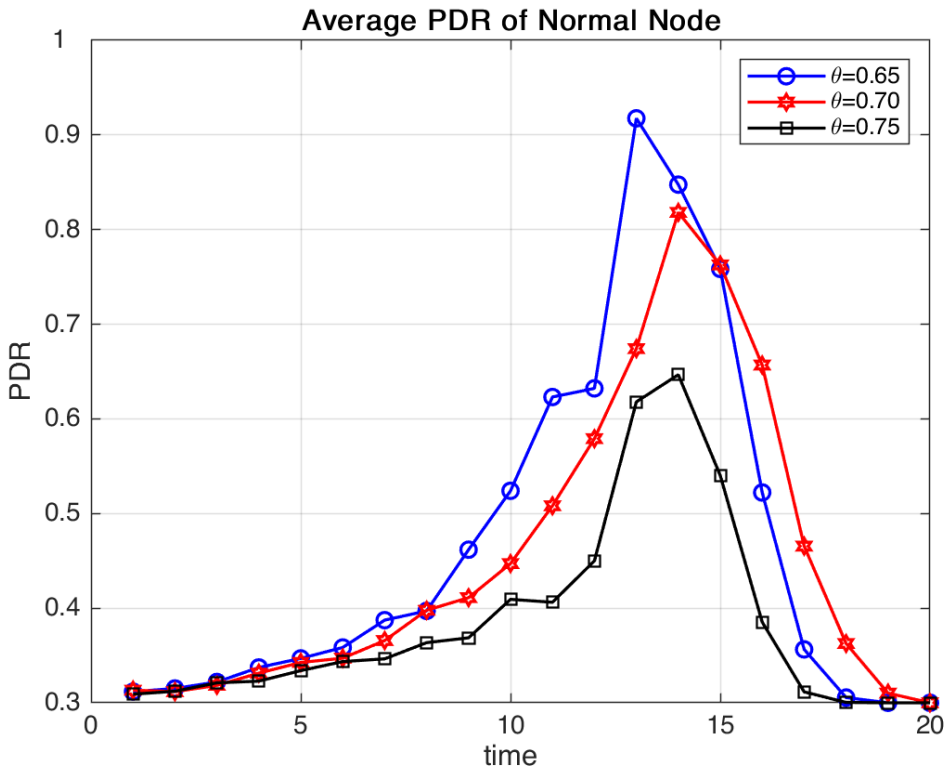


Figure 4.7Average PDR for Normal Node wrt Time

Figure 4.8 shows the Average PDR of the abnormal node wrt time. It shows that the Maximum value of average PDR for trusted nodes for different value of threshold are as below

1) For θ = 0.65 PDR is 0.015,
2) For θ = 0.70 PDR is 0.011
3) For θ =0.75 PDR is 0.009

The comparison of PDR values for trusted and non-trusted nodes shows that both have the positive values of PDR. But the PDR of trusted node is much high and keeps increasing with number of successful interaction whereas PDR of abnormal normal node is less as it does not forward the received packets. The reason behind its not forwarding the packets may be its bad intentions for misguiding the other nodes. PDR of trusted node is always higher than that of abnormal node for each value of threshold.

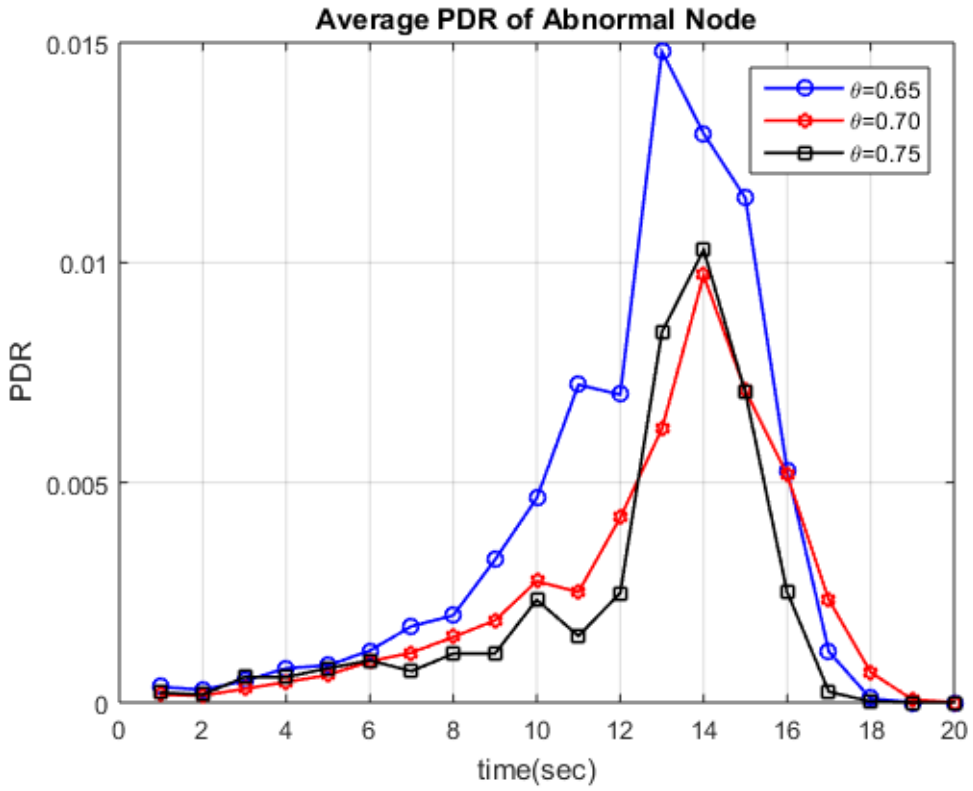


Figure 4.8 Average PDR for abnormal nodes

4.4.2 Effect of threshold policies on Packet Delivery Ratio

Table 4.1 includes Average PDR value for trusted nodes at different values of thresholds (θ = 0.75, 0.70, 0.65) at different time instant starting from t= 0 sec to 20 sec. The value of Average PDR for trusted nodes is zero at t=0 for all value of θ. It means no packets are received yet. With progression of time, the average PDR value for trusted nodes keeps on increasing for all threshold upto t=13sec. After time interval t=14 sec, the Average PDR values are decreasing for each threshold value till t=20 which clearly show that maximum PDR value is achieved at t=14 sec for

threshold θ = 0.75 and θ = 0.70, at t=13 sec for θ = 0.65. The maximum PDR values achieved at θ=0.65 is 92.09% that is very high as compared to the maximum PDR achieved at θ=0.75 i.e. 64.76%.

Table 4.1 PDR value of trusted nodes at different threshold

Average PDR of Trusted Nodes			
time	θ = 0.75	θ = 0.70	θ = 0.65
1	0.31468	0.318341	0.31833
2	0.32025	0.318423	0.318423
3	0.323997	0.327627	0.327628
4	0.324083	0.336802	0.34047
5	0.336921	0.347855	0.351512
6	0.349794	0.358882	0.364355
7	0.353511	0.371736	0.391792
8	0.371829	0.401464	0.404638
9	0.37738	0.415665	0.466699
10	0.417577	0.452209	0.526941
11	0.410383	0.512462	0.625475
12	0.454207	0.581803	0.634675
13	0.629304	0.674873	0.920965
14	0.647604	0.818976	0.849976
15	0.541995	0.764382	0.766205
16	0.388956	0.662389	0.527501
17	0.31613	0.469258	0.35988
18	0.312574	0.314552	0.327105
19	0.303556	0.306136	0.307198
20	0.30183	0.303638	0.305458
Max	0.647604	0.818976	0.920965

The PDR values at almost every time instant is less for higher values of threshold as compared to lower threshold values, for example at time instant t=8 sec, the PDR for θ=0.65 is 0.404638, that decreases for θ=0.70 i.e. 0.401464 and again decreases for θ=0.75 i.e. 0.371829. Likewise, at t=18 sec, the PDR for θ=0.65 is 0.327105, that decreases for θ=0.70 i.e. 0.314552 and again decreases for θ=0.75 i.e. 0.312574. The discussion on PDR values concludes that PDR of trusted nodes decreases significantly (i.e. from 92.09% to 64.76 %) with increase in the threshold limit (which is 0.65 to 0.75). The reason behind this is that under the strict threshold policy the trusted nodes may sometimes be considered as malicious.

Table 4.2 presents the Average PDR for non-trusted nodes at different thresholds (θ = 0.75, 0.70, 0.65) at different time instant starting from t= 0 sec to 20 sec. The value of Average PDR for non-trusted nodes is zero at t=0 for all values of θ and it remains as Zero from t=0 sec to t=10 seconds regardless of threshold value.

Table 4.2 PDR value of non-trusted nodes at different threshold

Time	Average PDR of Abnormal Node		
	θ = 0.75	θ = 0.70	θ = 0.65
1	0.00	0.00	0.00
2	0.00	0.00	0.00
4	0.00	0.00	0.00
6	0.00	0.00	0.00
8	0.00	0.00	0.00
10	0.00	0.00	0.00
12	0.0025	0.003	0.0042
14	0.01	0.0103	0.0135
16	0.0025	0.0052	0.0053
18	0	0.0001	0.0007
20	0	0	0
Max	0.010	0.0103	0.0135

After the time t=10 seconds, the value of average PDR for malicious nodes increases for all the thresholds. It continues to increase up to t=14 Seconds. After that values of Average PDR decreases at every time instant for all the thresholds till t=20 seconds. It means the maximum value of PDR is achieved at time instants t=14 for threshold θ=0.65 is 1.35% that is quite comparable to maximum PDR achieved for θ=0.75 is 1.0%.

For all non-zero PDR values from time instant t=12 to t=18, it is clear that, the PDR value at each instant is less for higher threshold. For e.g. at t=16, PDR for θ=0.65 is 0.0053, which decreases for θ=0.70 i.e. 0.0052 and further decreases to 0.0025 for

θ=0.75. This discussion on PDR concludes that with increase in threshold, PDR values for malicious nodes decreases but not significantly. The Reason behind it is that the untrusted nodes have nothing to do with the threshold policies because their main aim is to affect the PDR.

4.4.3 Average no. of Available hops

Average number of the available hops are estimated for both trusted and non-trusted nodes with progression of time for various trust threshold. It can be seen from Figure 4.9. that with progression of time, the availability of number of hops for trusted nodes is increasing. The reason behind this is the good behavior of trusted nodes. The Availability of multiple hops helps trusted nodes in getting the shortest path. So, behaving in good manner is rewarding.

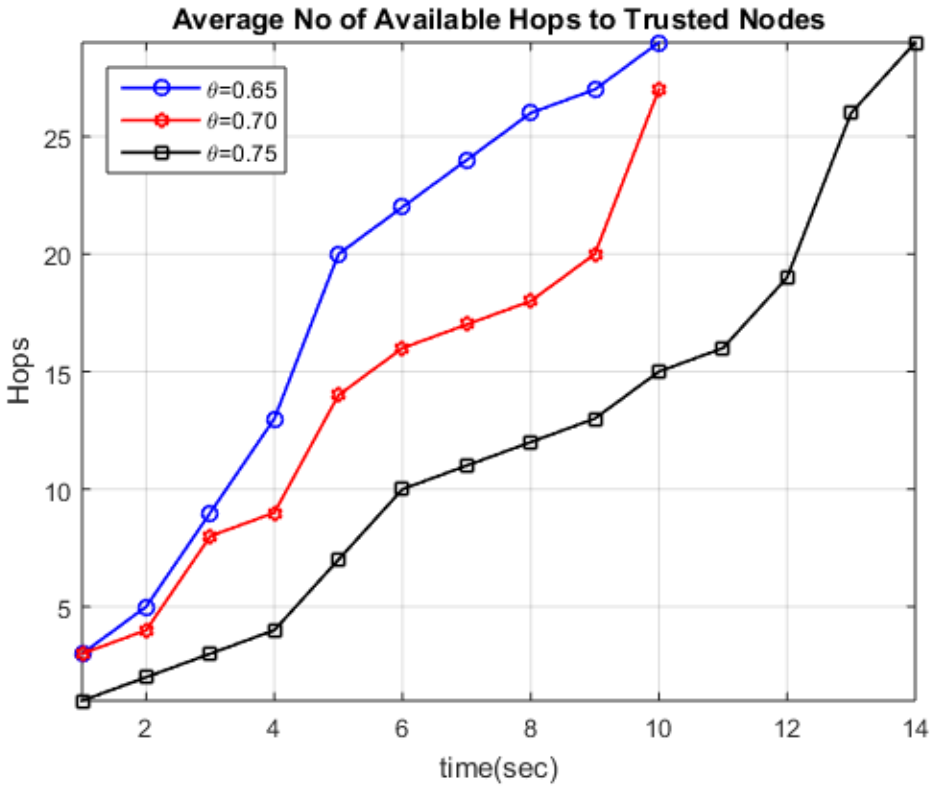


Figure 4.9 Average No. of Available Hops to Trusted Nodes

The curves for available number of hops for non-trusted node shown in figure 4.10 depicts that availability of average number of hops for non-trusted nodes decreases with time and approaches to zero after some time. It is visible in graph that the

average no. of hops drops significantly within the first 10seconds.

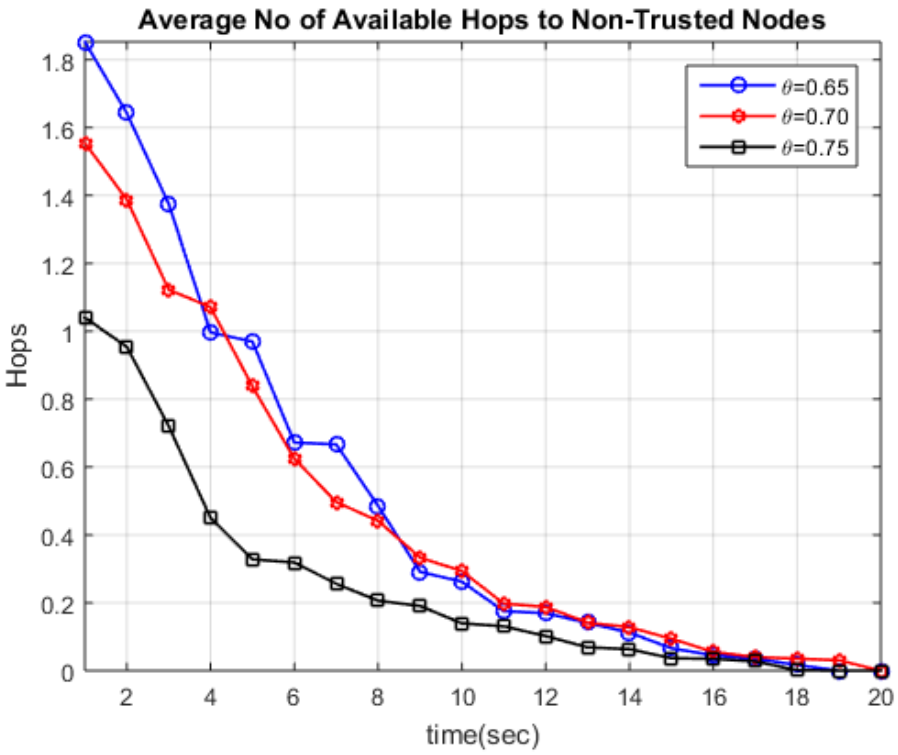


Figure 4.10 Availability of Average number of hops to non-trusted nodes

4.4.4 Effect of threshold policies on Available number of hops

Table 4.3. presents the average number of available hops for trusted nodes at different thresholds (θ = 0.65,0.70,0.75) at different time instants starting from t= 0 second to 20 seconds. Initially, the number of available hops for the trusted nodes is zero at t=0 for all value of threshold (θ). With progression of time form t=0 sec to t=20 sec, the number of available hops for the trusted nodes also progresses continuously for all values of threshold. The reason behind this continuous progression in hops is good behaviour of trusted nodes during the interactions. The readings of Available hops at each time instant for different threshold values shows that availability of number of hops for higher threshold is comparatively less than that for lower threshold values. For example, at t=8 seconds the number of hops available for threshold value θ=0.65 is 24, that decreases for higher value of threshold θ=0.70 to 16 and then further decreases for more higher threshold value θ=0.75 to 12. In addition to this, the Average value number of available hops for threshold value θ=0.65 is 26 that is comparatively higher than that for threshold value θ=0.75 i.e. 17. This discussion on

effect of threshold policies on the number of available hops concludes that growth of value of available hops is greater when threshold policy is less strict θ (θ=0.65) and smaller during more strict policy. The reason behind this is that under very strict threshold policy trusted nodes can be sometimes misunderstood as the non-trusted node.

Table 4.3 Number of hops available for trusted nodes at different threshold

Time	Average No Hops of Trusted Node		
	θ = 0.75	θ = 0.70	θ = 0.65
0	0	0	0
2	2	2	3
4	4	4	9
6	10	9	20
8	12	16	24
10	15	18	27
12	19	27	30
14	29	30	33
16	28	33	41
18	32	38	45
20	36	42	50
Average	**17**	**20**	**26**

Table 4.4 presents number of available hops available for malicious nodes at different thresholds (θ = 0.65,0.70,0.75) at different time instants starting from t= 0 seconds to 20 seconds. Initially the non-trusted nodes contain some available hops to misguide other nodes. But, with progression of time from t=0 seconds to t=20 seconds, the number of available hops for malicious nodes reduces continuously for all threshold values and ultimately becomes Zero at time instants t=20 seconds. The reason behind this reduction in available hops is the misbehavior of malicious node during interaction. The readings of Available Hops at each time instant for different threshold values shows that availability of number of hops for higher threshold is comparatively less. For example, at t= 8 seconds, the number of hops available for threshold value θ=0.65 is 0.49, that decreases for higher values of threshold θ=0.70 i.e. 0.44 and then further decreases for more higher threshold value θ=0.75 to 0.21.

Table 4.4 Number of hops available for non-trusted nodes at different threshold

Time	Number of Hops of Non-Trusted Node		
	θ = 0.75	θ = 0.70	θ = 0.65
0	1.06	1.55	1.8
2	0.95	1.39	1.64
4	0.45	1.07	1
6	0.32	0.62	0.67
8	0.21	0.44	0.49
10	0.14	0.23	0.29
12	0.1	0.17	0.19
14	0.06	0.11	0.13
16	0.03	0.05	0.06
18	0	0.02	0.04
20	0	0	0
Avg	**0.226**	**0.423**	**0.438**

In addition to this, average value of number of available hops for threshold value θ=0.65 is 0.438 is that is comparatively higher than that for threshold value θ=0.75 i.e. 0.226. This discussion on the effect of threshold policies on the number of available hops concludes that the growth of value of available hops is greater when the threshold policy is less strict (θ=0.65) and smaller during more strict policy. But the value is quite negligible for both threshold cases. The reason behind this is that the malicious nodes have nothing to do with threshold.

4.4.5 Average Trust Values

Trust dynamics represents the level of trustworthiness of node while communicating to other nodes. Any node is proficient enough to interact with other only if trust value for both nodes fulfills the minimum requirement. Trust dynamics changes dynamically after completion of each interaction. Trust values of nodes can increase or decrease overtime depending upon behavior of nodes during interaction. Since the

trusted nodes behaves good during every interaction so their trust value should increase with time whereas the trust value of malicious nodes should decrease with time due to their misbehaviour during each interaction.

The simulation curve in Figure 4.11. depicts changes in value of trust with time. Here we have neglected the initial trust values. So, when the interaction started the trust value of node is almost zero which keeps on increasing with progression of time.

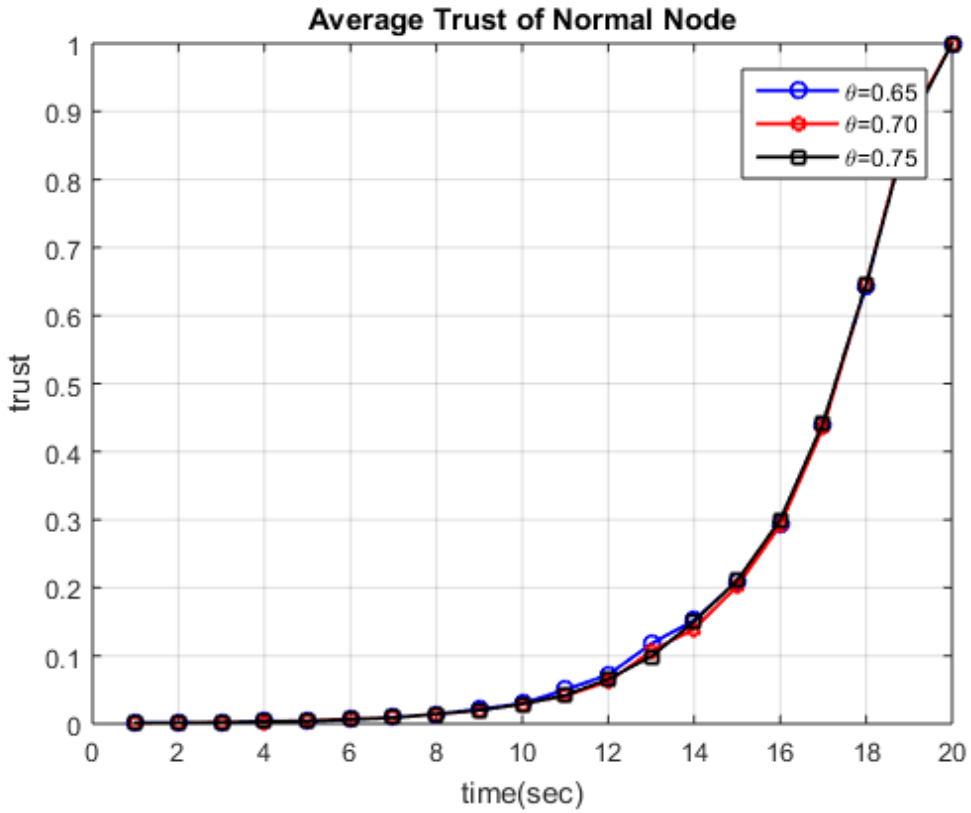


Figure 4.11 Availability of Average number of hops to trusted nodes

Figure 4.12. shows how the trust value of malicious (abnormal) nodes changes with time. In this we have considered 0.5 as original trust value given to malicious nodes so that they can participate in interaction. But with time, trust value of malicious nodes keeps on decreasing due to their misbehaviour during each interaction and ultimately becomes zero after some time.

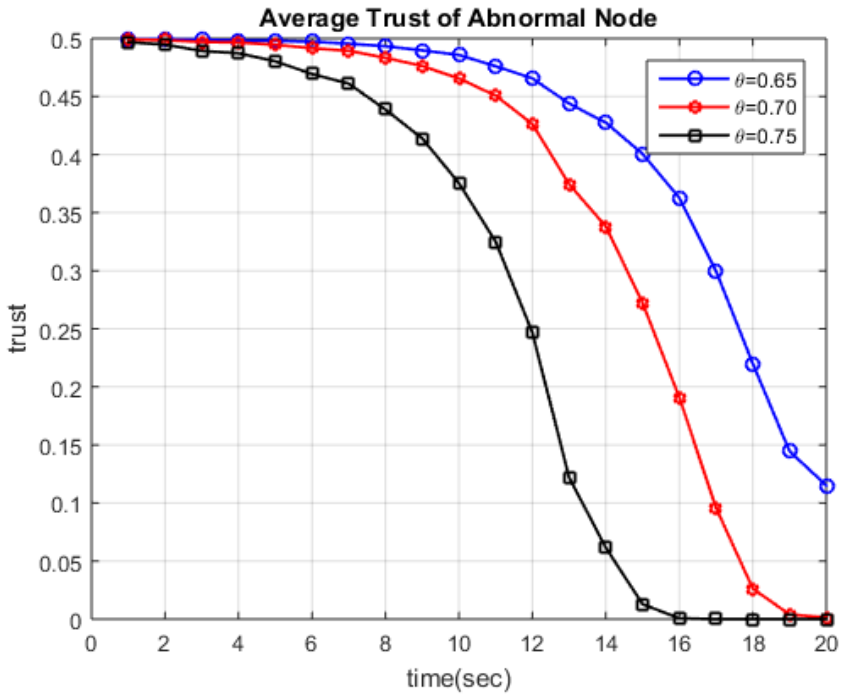


Figure 4.12 Trust dynamics of non-trusted nodes wrt time

Figure 4.13. shows the combined graph of trust dynamics for trusted as well as abnormal nodes.

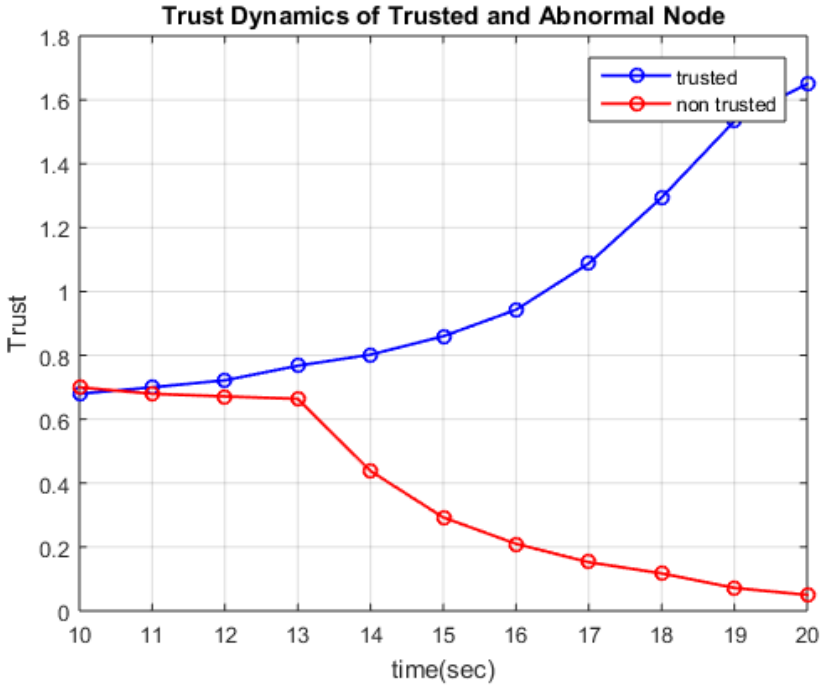


Figure 4.13 Trust dynamics trusted and non-trusted nodes wrt time

The result depicts that the trust values of trusted nodes are continually increasing with

time and that of abnormal node is gracefully decreasing with passage of time. Every successful interaction contributes further increase in the trust dynamics for trusted nodes. Moreover, the reduction in trust dynamic for malicious node would be due to its misbehavior. Initially there is not much difference in the trust dynamics of normal and abnormal node but as the time increases and more events are encountered the difference increases to great extent that helps in clearly separating the abnormal nodes from normal nodes and discarding them.

4.4.6 Effect of threshold on Average trust value

Table 4.5. presents the trust values for trusted nodes at different thresholds (θ = 0.65, 0.70, 0.75) at different time instants starting from t= 0 second to 20 seconds.

Table 4.5 Trust value for trusted nodes at different threshold

Time	**Trust value of Normal Node**		
	θ = 0.75	**θ = 0.70**	**θ = 0.65**
0	0	0	0
2	0	0	0
4	0	0	0
6	0	0	0
8	0.02	0.02	0.02
10	0.04	0.04	0.04
12	0.08	0.08	0.08
14	0.15	0.16	0.16
16	0.3	0.3	0.3
18	0.65	0.65	0.65
20	1	1	1
Avg	**0.224**	**0.225**	**0.225**

Initially, the trust values for the trusted nodes is zero at t=0 for all value of threshold (θ). With progression of time form t=0 sec to t=20 sec, the trust dynamics for the trusted nodes also progresses continuously for all values of threshold. The reason behind this continuous progression in trust value is good behaviour of trusted nodes during the interactions. The readings of trust values at each time instant for different threshold values shows that threshold does not affect the trust values of the nodes as it is seen that trust dynamic for a node remains almost same for all the thresholds. For example, at t=14 seconds the trust dynamic for threshold value θ=0.65 and θ=0.70 is 0.16. This discussion on the effect of threshold policies on the trust vale of normal nodes concludes that the growth of trust value is almost same for all the thresholds. This is because the trust value is more dependent on the behaviour of nodes during interaction rather than the threshold value.

Table 4.6 presents trust value for malicious nodes at different thresholds (θ = 0.65,0.70,0.75) at different time instants starting from t= 0 seconds to 20 seconds.
Initially a trust value of 0.5 is assigned to all the non-trusted node. But, with progression of time from t=0 seconds to t=20 seconds, the trust value for malicious nodes reduces continuously for all threshold values and ultimately becomes Zero at time instants t=20 seconds. The reason behind this reduction in trust value is the misbehavior of malicious node during interaction.

The readings of trust value at each time instant for different threshold values shows that trust value for higher threshold is comparatively less. For example, at t= 8 seconds, the trust value for threshold value θ=0.65 is 0.50, that decreases slightly decrease θ=0.70 i.e. 0.48 and then further decreases for more higher threshold value θ=0.75 to 0.44. However, this decrease in the value of trust is not much Significant. In addition to this, average trust value of nodes for threshold value θ=0.65 is 0.41 is that is comparable to that for threshold value θ=0.75 i.e. 0.31. This discussion on the effect of threshold policies on the trust value concludes that the growth of value of trust value is not much affected by the threshold policy. The reason behind this is that trust value depends on the behaviour of nodes during the interaction.

Table 4.6 Trust value of non-trusted nodes at different threshold

Time	Trust value of Abnormal Node		
	θ = 0.75	**θ = 0.70**	**θ = 0.65**
0	0.5	0.5	0.5
2	0.5	0.5	0.5
4	0.49	0.5	0.5
6	0.47	0.49	0.5
8	0.44	0.48	0.49
10	0.38	0.46	0.48
12	0.33	0.43	0.47
14	0.26	0.34	0.43
16	0.06	0.19	0.36
18	0	0.03	0.22
20	0	0	0.12
Avg	0.31	0.35	0.41

4.4.7 Success Rate

This rate is calculated as no. of successful attempts divided with the entire no. of communication attempts completed by node to establish the communication between two nodes. In other word it can be said that success rate defines the number of attempts in which a node finds the path for interacting desired node. Ideally the success rate of a trust model should as high as possible.

Figure 4.14 presents the graphs which demonstrates in what way the success rate differs with the no. of communication attempts. This graph depicts that when the number of attempts are increasing the success rate increasing. It means that when the communication attempts are increased then the chances of successful communication are high.

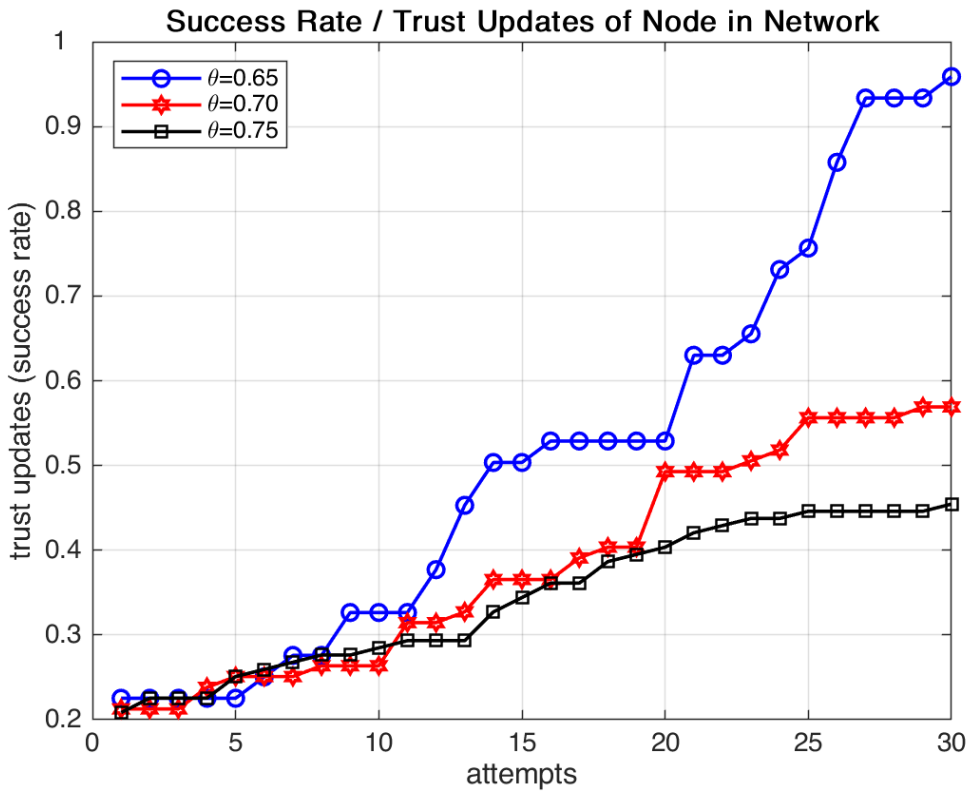


Figure 4.14 Success rate versus number of attempts

4.4.8 Effect of threshold on Success Rate

The Effect of threshold on Success Rate shows that how threshold policy affects the communication in the network. Table 4.7 presents success rate at different thresholds (θ = 0.65,0.70,0.75) with number of attempts. The readings of success rate vs number of attempts show that success rate is low for higher threshold as compare to that at low threshold. For example, at when number of attempts is 30, the success rate for threshold value θ=0.65 is 0.96 that decreases to 0.57 when we make the threshold stricter i.e. θ=0.70 and then further decreases to 0.45 for more higher threshold value θ=0.75. This discussion on threshold effect on success rate concludes that stricter the threshold policy, more difficult is to identify path between nodes for successful communication. Node will have to give more attempts in case of strict threshold policy (θ=0.75) because in strict policy the malicious nodes are immediately separated from the network so more attempts are required.

Table 4.7 Success Rate at different threshold

Attempts	Success Rate		
	θ = 0.75	**θ = 0.70**	**θ = 0.65**
5	0.25	0.25	0.24
10	0.28	0.26	0.32
15	0.33	0.36	0.50
20	0.39	0.50	0.53
25	0.44	0.56	0.76
30	0.45	0.57	0.96
Max	**45.00%**	**57.00%**	**96.00%**

4.5 Simulation- based performance comparison

This simulation is conducted to assess the projected PDTM as compared to existing Ratee based scheme [185] and rater based scheme [100]. The simulation results and their comparative analysis in terms of transaction/ interaction growth, the success rate with various malicious percentage, and system computation time is presented in this section.

4.5.1 Transaction Number Growth

Transaction number is defined as no. of transactions/ communications that takes place amongst any two of the nodes. In this simulation, we have recorded the number of transactions taking place between vehicular node during 10 hours, and the transaction growth is calculated every hour for all the three methods. The simulation outcomes are shown in Figure 4.15. During first simulation hour, growth of transaction no. is less in PDTM as compared to ratee methods and rater method is slowest. The reason behind the same is that in the early stage of network, few nodes are interrelated and share the information which is to be accumulated to evaluate trust.

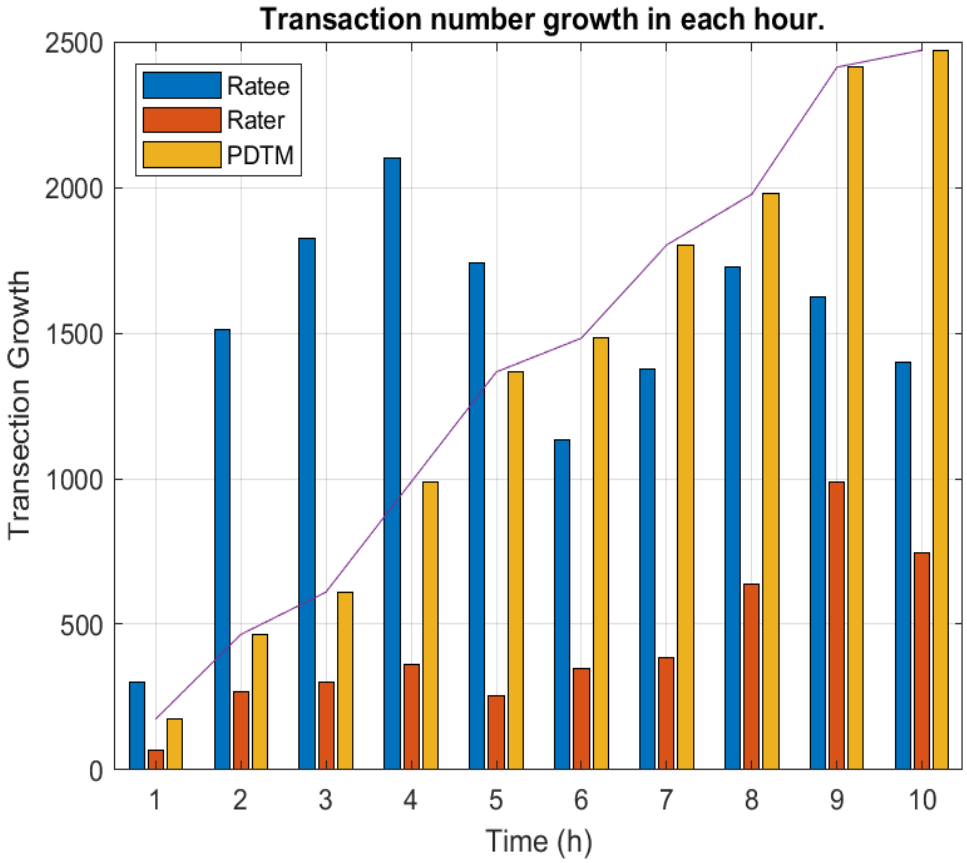


Figure 4.15 Transaction number growth in each hour

The transaction number growth for rater-based models is quite less as compared to both ratee- based and PDTM throughout the simulation. But the comparison of the transaction number of ratee based models and PDTM shows that the transaction growth is initially low in proposed PDTM in comparison with Ratee model. This is due to the fact that in PDTM we have allocated preliminary trust to all given nodes so malicious nodes may also participate in network and does not allow the transaction to take place. But as the time progresses, the proposed model works well as compared to ratee based model as the transaction number growth in PDTM is increasing in a continuous manner with progression of time and peaks at more than 2300 transactions in 9th hour. In long run PDTM has more transaction growth in each hour whereas transaction number growth in ratee-based model fluctuates up and down. During first four hours the transaction growth of ratee based is very high having peak at more than 2000 transactions. But after t= 4 hours it starts fluctuating with peak at 1800 transactions.

Table 4.8 shows the values of value of transaction number for Rater-based, ratee-based and proposed PDTM scheme. The reading clearly shows that the Average value of transaction number is lowest in ratee based among three whereas the transaction number is initially low PDTM but after n=4 nodes PDTM provides better transaction number growth.

Table 4.8 Transaction number growth for various trust schemes

Nodes	Rater-based scheme	Ratee-based scheme	PDTM
1	70	302	174
2	267	1512	465
3	302	1826	610
4	360	2099	988
5	256	1738	1366
6	349	1134	1483
7	384	1378	1802
8	640	1727	1977
9	988	1622	2413
10	744	1401	2471

This discussion on transaction number growth concludes that the for proposed PDTM is better than both rater-based models throughout the simulation and ratee based model in long run because with progression of time the malicious nodes are discarded form the network due to their misbehavior.

4.5.2 Trust Computation Time

The Trust computation time refers to time required for completing a transaction/ interaction attempt. The computation time involves node validation time and trust computation time and measured in milliseconds. In proposed model, validation of node identity and trust calculation is done by individual nodes involved in interaction in distributed manner whereas in ratee based trust model node validation is done based on the cookies by the centralized CA.

Figure 4.16 exhibits results of trust computation time. Both proposed PDTM and ratee-based model follows a direct correlation between trust computation time and no. of nodes. But especially, total computation time in PDTM is lesser in Proposed model. Even when no. of nodes reaches 200, calculation time of PDTM is 36.3ms that is almost half of the computation time of Ratee-based model that is 71.4ms. The reason behind this is that node validation and trust computations is done in distributed manner in PDTM that meets the demand of IoV interactions.

This discussion on transaction number growth concludes that the for proposed PDTM is better than both rater-based models throughout the simulation and ratee based model in long run because with progression of time the malicious nodes are discarded form the network due to their misbehavior.

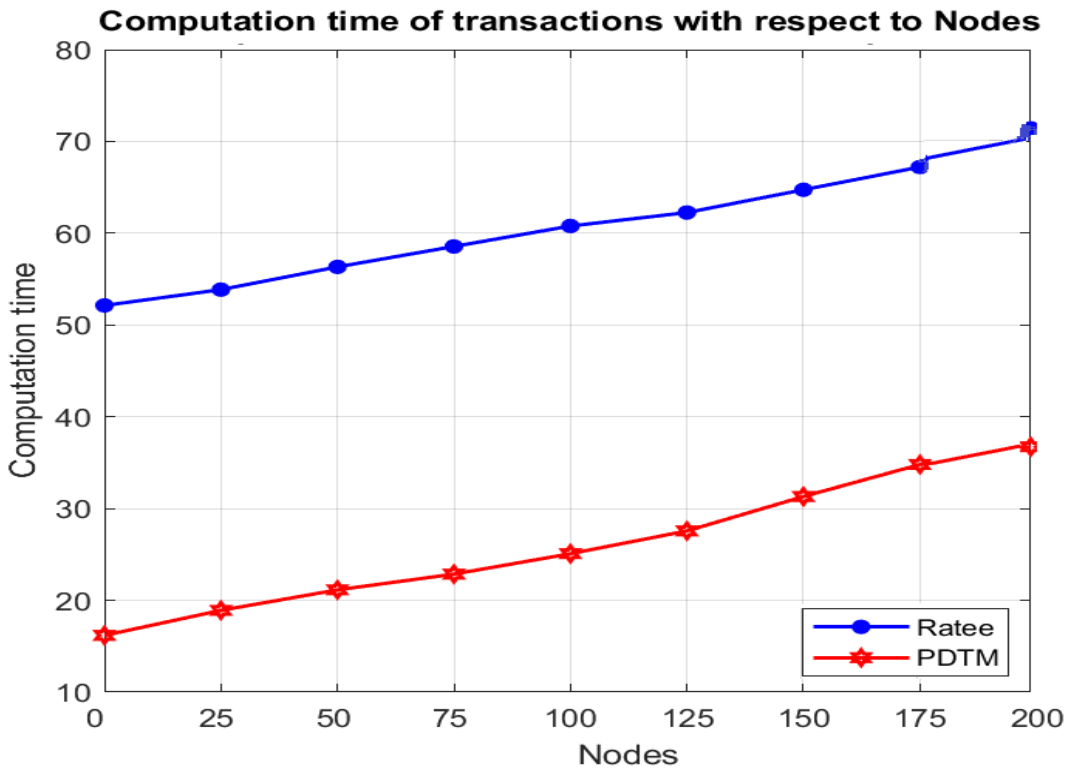


Figure 4.16 Computation time with respect to nodes

Table 4.9. shows the values of computation time for both ratee-based scheme and PDTM under different number of nodes. These readings clearly show that PDTM schemes outperforms the ratee-based scheme in terms of computation time under all

values of nodes.

Table 4.9 Comparison of computation time of Ratee and PDTM scheme

Nodes	Computation Time	
	Ratee	**PDTM**
0	52.1	16.2
25	53.8	18.9
50	56.3	21.1
75	58.6	22.9
100	60.8	25.1
125	62.3	27.6
150	64.7	31.3
175	67.2	34.8
200	71.4	36.3
Average	**60.8**	**26.02**

The Average computation time in Proposed PDTM and ratee based scheme is 26.02 and 60.8 respectively. It means the average computation time of PDTM is less than the half of computation time taken by ratee based scheme.

4.5.3 Transaction Success Rate with different malicious percentage

Here the malicious nodes are those nodes which disseminate misleading information to other nodes. The simulation is conducted for various malicious nodes percentage (represented with mp). The main purpose of this simulation is to examine how the success percentage of proposed scheme rises under various malicious situations.

Figure 4.17 to 4.20 shows the combined graphs of transaction success rate for PDTM and ratee-based scheme under different malicious percentage. The combined simulation results depict that as the time progresses both schemes show increase in

transaction success rate. But on the average the PDTM scheme performs better than ratee scheme at each percentage of the malicious node.

When mp=10%. The average success rate of PDTM scheme is 95.9% amd that for the ratee scheme is 93.4 % so the PDTM is better than ratee-based scheme by 2.5%. Similarly the maximum success ratee of ratee scheme is below 97% and that of PDTM easlily crosses 98% as shown in figure 4.17. It means the PDTM is 1% better than ratee scheme in terms of maximum succeess rate at malicious percentage mp=10%

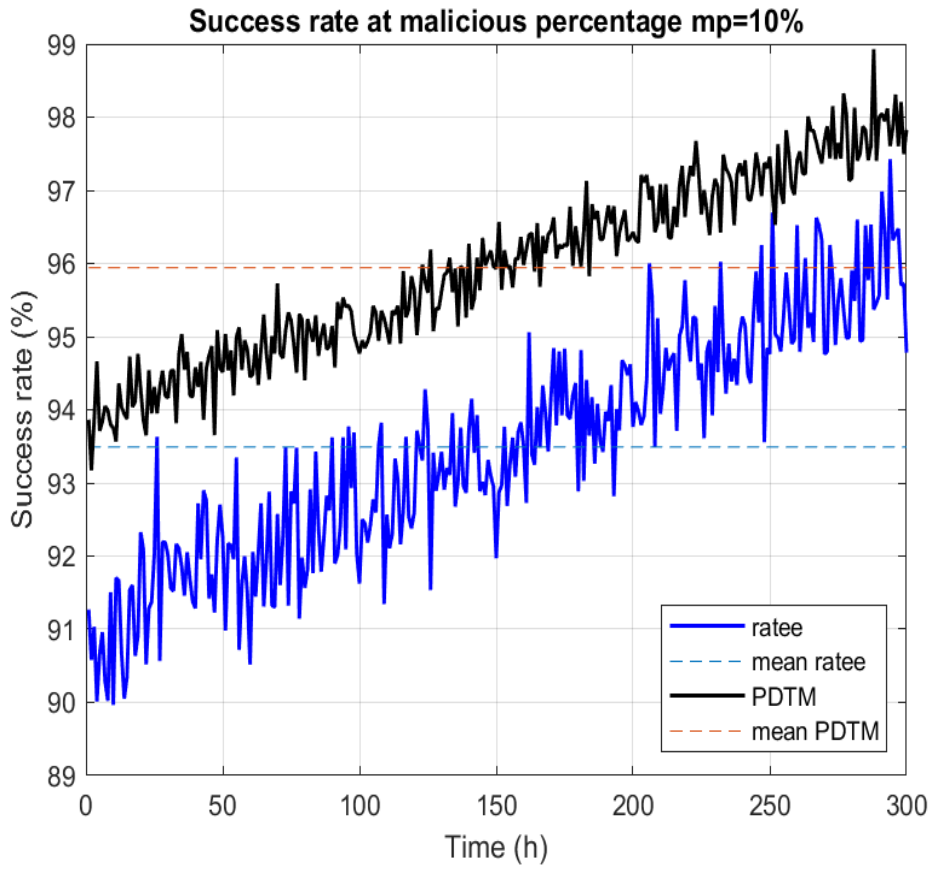


Figure 4.17 Success rate for PDTM and ratee-based scheme at mp=10%

When mp=20% the average success rate of PDTM scheme is 89.9% amd that for the ratee scheme is 84.4 % so the PDTM is better than ratee-based scheme by 5.5%. Similarly the maximum success ratee of ratee scheme is 90% and that of PDTM easlily crosses 95% as shown in figure 4.18. It means the PDTM is 5% better than ratee scheme in terms of maximum succeess rate at malicious percentage mp=20%.

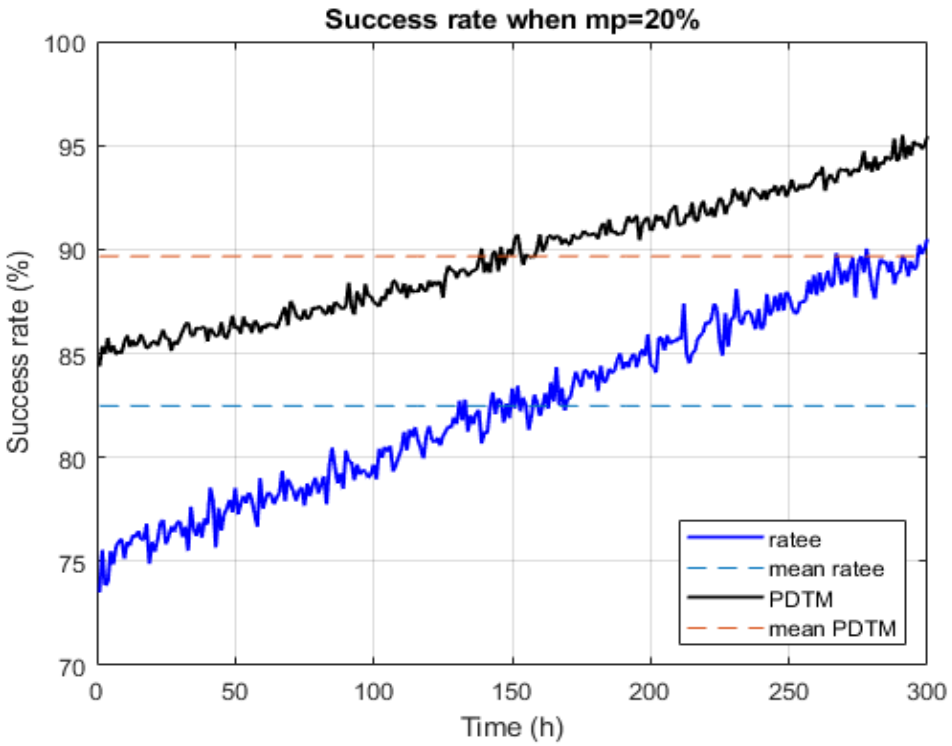


Figure 4.18 Success rate for PDTM and ratee-based scheme at mp=20%

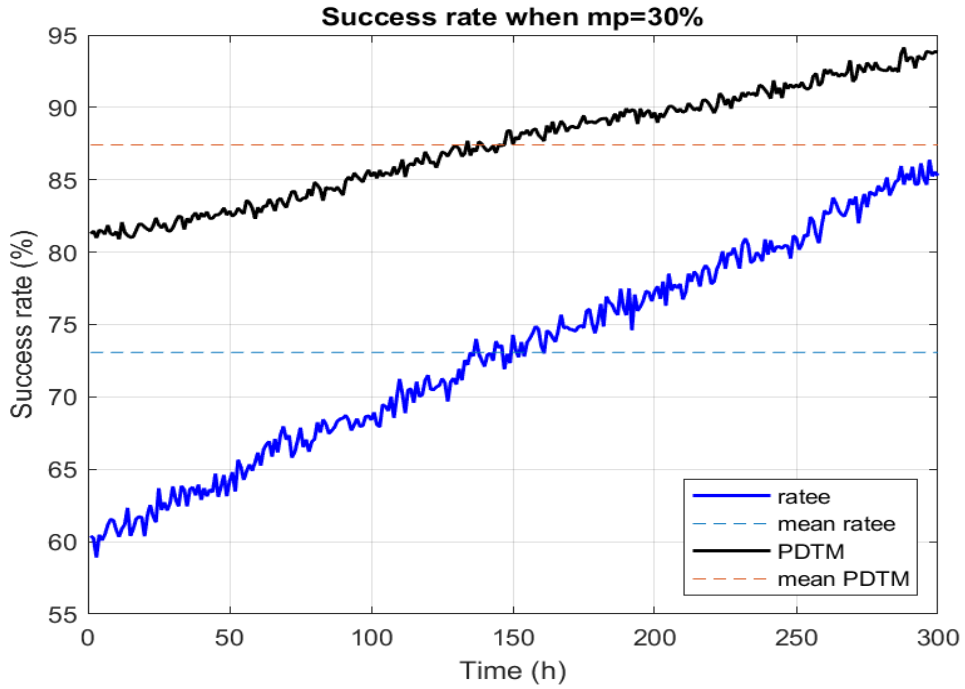


Figure 4.19 Success rate for PDTM and ratee-based scheme at mp=30%

When mp=30% the average success rate of PDTM scheme is 87.5% amd that for the ratee scheme is 73.0 % so the PDTM is better than ratee-based scheme by 17.5%. Similarly the maximum success ratee of ratee scheme is 86% and that of PDTM easlily crosses 92% as shown in figure 4.19. It means the PDTM is 6% better than ratee scheme in terms of maximum succeess rate at malicious percentage mp=30%.

Similarly When mp=40% the average success rate of PDTM scheme is 84.9% amd that for the ratee scheme is 68.0 % so the PDTM is better than ratee-based scheme by 16.9%. Similarly the maximum success ratee of ratee scheme is 85% and that of PDTm easlily crosses 92.5% as shown in figure 4.20. It means the PDTM is 7.5% better than ratee scheme in terms of maximum succeess rate at malicious percentage mp=40%

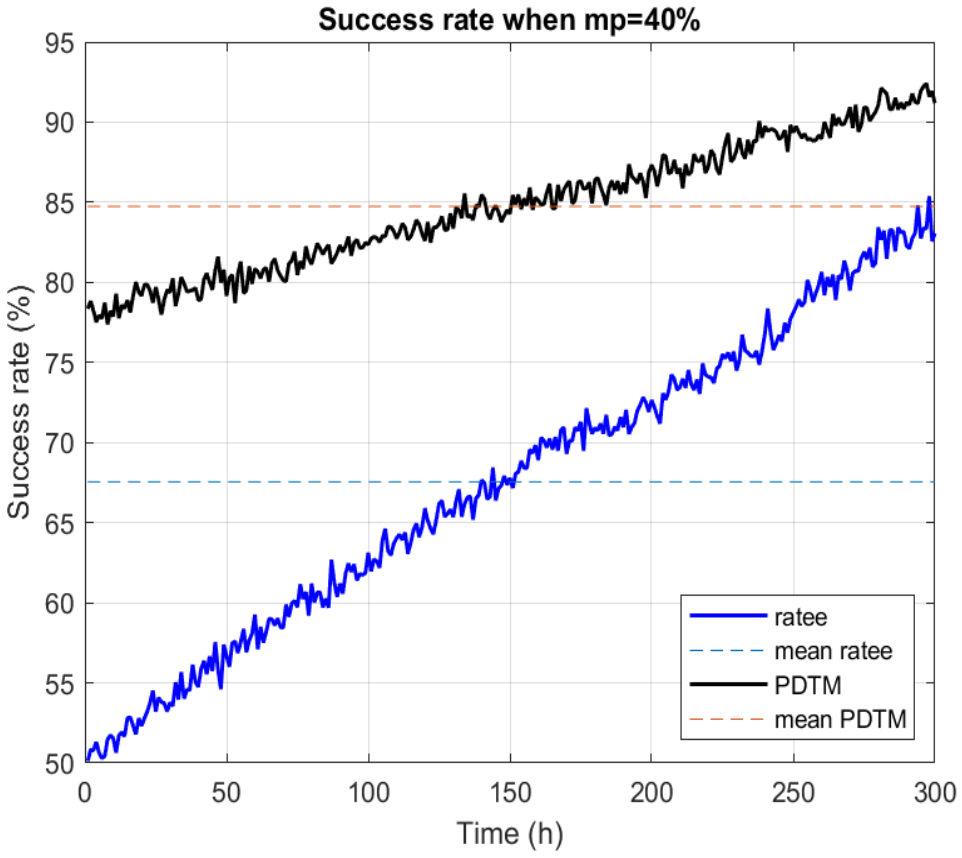


Figure 4.20 Success rate for PDTM and ratee-based scheme at mp=40%

Table 4.10. summarizes the discussion on the success rate comparison of PDTM and

ratee based scheme. The table clearly depicts that shows that with increase in malicious node percentage the average value of both ratee and PDTM decreases. Similarly, the maximum value of PDTM also decreases with increase in malicious node percentage. However, as the malicious percentage grows the mean success rate of PDTM is better than that of Ratee based scheme under each value of malicious node percentage. It means that PDTM can handle the transaction better than ratee based scheme even under high percentage of malicious node Thus, the Proposed scheme beats the ratee scheme in relation of mean and maximum success rate.

Table 4.10 Success rate at different mp of ratee and PDTM

Malicious percentage (mp)	Mean Success rate		Maximum Success rate	
	Ratee- based scheme	PDTM Scheme	Ratee- based scheme	PDTM Scheme
10%	93.4	95.9	97	98
20%	84.4	89.9	90	95
30%	73	87.5	86	92
40%	68	84.9	85	92.5
Avg.	79.7	89.55	89.5	94.375

4.6 Summary

To conclude, the projected model is assessed analytically as well through extensively simulation. The analytical evaluation concludes that PDTM is a hybrid trust model having distributed trust computation with low computation complexity. The proposed model is scalable and robust. It provides the solution to the cold start problem faced in ratee based models. The simulation-based evaluation concludes that the proposed model easily segregates the malicious nodes in the system and prevents them to contribute in communication based on trust dynamics. Result depicts that PDR of trusted node is 0.9209 that is much higher than the PDR of malicious node that is 0.015. The Average no. of hops of trusted node is 26 which is much more than average no. of available hops for malicious nodes that is 0.438. Trust dynamics of trusted nodes are higher than that of malicious node. So, on the basis of values of PDR, number of available hops and Trust dynamics, the malicious nodes can be clearly identified and

discarded. The study of the effect of threshold concludes that threshold policy should not be very strict as in strict threshold policy the trusted nodes are sometimes misunderstood as malicious and it is discarded from network.

The Average computation time in Proposed PDTM and ratee based scheme is 26.02 and 60.8 respectively. It means the average computation time of PDTM is less than the half of computation time taken by ratee based scheme. The discussion on transaction number growth concludes that the for proposed PDTM is better than both rater-based models throughout the simulation and ratee based model in long run because with progression of time the malicious nodes are discarded form the network due to their misbehavior. As the malicious percentage grows the mean success rate of PDTM is better than that of Ratee based scheme under each value of malicious node percentage. It means that PDTM can handle the transaction better than ratee based scheme even under high percentage of malicious node Thus, the Proposed scheme beats the ratee scheme in relation of mean and maximum success rate. The simulation -based comparison of proposed model with rater and ratee based model concludes that the proposed PDTM outperforms the rater based as well as ratee based model in terms of transaction number growth, success rate and computation time.

Chapter 5 CONCLUSION AND FUTURE WORK

Trust plays signification role in securing the interaction in IoV interactions. This thesis provides a comprehensive understanding on the concept of IoV and trust along with the proposed probability distribution-based trust model for secure the IoV interactions. In this thesis the proposed PDTM to evaluated to segregate the malicious nodes from the trusted node. The PDTM scheme is then compared with the ratee and rater based schemes to evaluate its performance.

In this thesis, first research objective related to understanding of basic concept of IoV and concept of trust in IoV is successfully achieved by conducting literature study related to IoV (section 2.2), architecture of IoV (section 2.2.2), trust concepts (section 2.9), its related properties (section 2.12) and techniques used for trust modelling (section 2.13). The subsequent research objective is attained with the help of conducting literature review of various available models proposed in different networks like P2P, distributed networks, ad-hoc networks, VANET, IoT etc (Section 2.15). Literature survey was focused on the types of trust model and the methodology used in them. While achieving this object some challenges in modelling trust in IoV (section 2.16) and research gaps in literature (section 2.17) were identified.

As third objective, we initially proposed a definition of trust as a measure of probability (section 3.1) and then proposed a hybrid trust framework for IoV (section 3.2) is proposed to eliminate gaps identified in the existing work. This proposed framework utilized the concept of probability distribution and so, called Probability distribution-based trust model. PDTM model is the integration of both data as well as entity-based trust model. The reliability of entity is evaluated by using pre-set threshold policy and that of data is evaluated by gathering the node statistics during interaction. The model used joint probability distribution to segregate the trusted and malicious nodes. If the measured statistics lies in the range of mean plus/minus twice of standard deviation then it is considered as trusted otherwise untrusted. The PDTM model also resolved the cold start problem by providing initial trust value to all each node.

Fourth Objective is achieved by Evaluating the performance of PDTM analytically and through extensive simulation. The analytic evaluation of proposed model (section 4.1) showed that model is scalable, robust and involves fast and distributed trust computations, so is well suited for IoV. It provided the solution to the cold start problem faced in ratee based models. The simulation-based evaluation concludes that the proposed model easily segregates the mischievous nodes in the system and prevents them to contribute in interactions (section 4.3). The experimental results (section 4.4) showed that PDR of trusted node is 0.9209 that is much higher than the PDR of malicious node that is 0.015. Additionally, the average number of available hops, and trust value of trusted nodes are also significantly higher than that of non-trusted node. Thus, the malicious nodes can be clearly identified and discarded on the basic of value of PDR, available hops and Trust dynamics. The effects of threshold on evaluation metrics shows PDR, available number of nodes and success rate for both trusted and non-trusted nodes decrease with increase in threshold (θ). But this decrease is less significant in non-trusted nodes. The trust dynamics is not much affected by threshold policy. The effect of threshold policies on various performance metrics concludes that the threshold policy should not be much strict. This is because under very strict threshold policy the trusted nodes can be misunderstood as untrusted.

The last objective is achieved by comparing the proposed model PDTM with other existing model (section 4.5). The comparison result shows that our model is more superior than the model which are based on existing ratee system in terms of transaction number growth, trust computation time and success rate. Moreover, Average computation time in Proposed PDTM is 26.02 ms that is less than the half of computation time taken by ratee based scheme whose computation time is 60.8ms.

Going forward, the research might get extended in following ways :-

1) Current model secures the traffic information exchanged between vehicles. This model might be extended to secure the data transactions in other application scenarios of IoV network.

2) In proposed model, a vehicle and its driver are considered as a single node. Our model might be extended to identify the malicious behaviors of drivers and vehicles separately and discard it.
3) The proposed system might be extended by using better techniques to improve the robustness of the model.
4) In the given thesis, we present a separate approach to assess the reliability of entity and data. Single approach might be used to calculate the reliability of both entity as well as data to make the computation much faster than that in this model.
5) Some Machine Learning Algorithms can be utilized to identify and eliminate malicious vehicles in the network.

References

[1] J. Zhang and K. Wang, “Data-Driven Intelligent Transportation Systems :,” *IEEE Trans. Intell. Transp. Syst. Vol. 12 pp. 1624-1639*, 2011.

[2] D. Singh, M. Singh, I. Singh, and H. Lee, “Secure and reliable cloud networks for smart transportation services,” *17th IEEE Int. Conf. Adv. Commun. Technol. Phonix Park. South Korea, 1-3 July*, no. July, pp. 1–6, 2015.

[3] “World Health Organization (WHO), Global Status Report on Road Safety 2015. Geneva: WHO Press,” 2015.

[4] “GLOBAL STATUS REPORT ON ROAD : https://www.who.int/publications-detail/global-status-report-on-road-safety-2018,” 2018.

[5] T. Report, “Intelligent transport systems (ITS), “Framework for public mobile networks in cooperative its (c-its)s,” *Tech. Rep., Eur. Telecommun. Stand. Inst. (ETSI), Palo Alto, Calif, USA, April*, vol. 1, pp. 1–63, 2012.

[6] E. Hossain *et al.*, “Vehicular telematics over heterogeneous wireless networks : A survey,” *Comput. Commun. vol. 33, no. 7, pp. 775–793*, vol. 33, pp. 775–793, 2010.

[7] R. I. Meneguette, L. F. Bittencourt, and E. R. M. Madeira, “A Seamless Flow Mobility Management Architecture for Vehicular Communication Networks,” *J. Commun. Networks, vol. 15, no. 2, pp. 207–216*, no. May 2014, 2013.

[8] D. Jiang and L. Delgrossi, “IEEE 802 . 11p : Towards an International Standard for Wireless Access in Vehicular Environments,” *Proc. IEEE Veh. Technol. Conf. Singapore, pp. 2036–2040*, pp. 2036–2040, 2008.

[9] “ETSI: European Telecommunications Standards Institute. News Release (September 2008), http://www.etsi.org/WebSite/NewsandEvents/2008 09 Harmonizedstandards ITS.aspx.”

[10] E. Schoch, F. Kargl, and M. Weber, “Communication Patterns in VANETs,” *IEEE Commun. Mag. 46, 119–125*, no. November, pp. 119–125, 2008.

[11] M. Fischer and R. Parkin, *Opportunities , risk , and turmoil on the road to autonomous vehicles*. 2016.

[12] A. Mai., “Connected Vehicles: From Building Cars to Selling Personal Travel

Time Well-Spent. Technical report, Cisco, 2011."

[13] A. Industries, "The road to 2020 and beyond: What's driving the global automotive industry?," 2020.

[14] T. Elbatt, S. K. Goel, and G. Holland, "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications," *Proc. VANET*, pp. 1–9, 2006.

[15] T. Nadeem, C. Liao, and L. Iftode, "TrafficView : Traffic Data Dissemination using Car-to-Car Communication TrafficView : Traffic Data Dissemination using Car-to-Car," *ACM SIGMOBILE Mob. Comput. Commun. Rev. vol. 8*, no. June 2014, 2004.

[16] S. U. Rahman and U. Hengartner, "Secure Crash Reporting in Vehicular Ad hoc Networks," *Proc. MOBICOMM*, 2007.

[17] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-Vehicle Safety Messaging in DSRC," *Proc. VANET*, pp. 19–28, 2004.

[18] A. Jim Barbaresso, Gustave Cordahi, Dominie Garcia, Christopher Hill and K. W. Jendzejec, "USDOT's Intelligent Transportation Systems (ITS) Strategic Plan 2015-2019," *Washington, DC US Dep. Transp. Intell. Transp. Syst. Jt. Progr. Off. 2015*.

[19] "Connected Car Global Forecast 2015," 2015, https://www.sbdautomotive.com/files/sbd/pdfs/536%20connected%20car%20forecast%20ib%2015.pdf , Accesssed on 15 June 2020.

[20] S. Sargunavathi and J. Martin L. M., "Design and Development of CTSR with Direct & Indirect Observations of MANET Applications," in *Part of the Springer book series on Mobile Networks and Applications*, 2017.

[21] Y. Toor, P. Muhlethaler, A. Laouiti, and A. La Fortelle, "Vehicle Ad Hoc networks: applications and related technical issues," *IEEE Commun. Surv. Tutorials*, vol. 10, no. 3, pp. 74–88, 2008.

[22] A. Festag *et al.*, "' NoW – Network on Wheels ': Project Objectives , Technology and Achievements," *Proc. 6th Int. Work. Intell. Transp. (WIT 2008), Hamburg, Ger. Mar*, no. March, pp. 211–216, 2008.

[23] C. Manifesto, "CAR 2 CAR Communication Consortium Manifesto version

1.1.," *Tech. report, CAR 2 CAR Commun. Consort. (C2C-CC), Aug .*, 2007.

[24] M. K. Saini and A. El Saddik, "How close are we to realizing a pragmatic VANET solution ? A meta-survey," *ACM Comput Surv ; 48(2) 1–40; 48(2) 1–40*, no. November, 2015.

[25] S. F. Hasan, X. Ding, N. H. Siddique, S. Member, and S. Chakraborty, "Measuring Disruption in Vehicular Communications," *IEEE T Veh Technol*, vol. 60, no. 1, pp. 148–159, 2011.

[26] A. S. Z. SALIM BITAM, ABDELHAMID MELLOUK, "VANET-C LOUD : A G ENERIC C LOUD C OMPUTING M ODEL FOR V EHICULAR A D H OC N ETWORKS," *IEEE Wirel. Commun.*, no. February, pp. 96–102, 2015.

[27] J. Toutouh and E. Alba, "Light commodity devices for building vehicular ad hoc networks : An experimental study," *Ad Hoc Networks*, vol. 37, pp. 499–511, 2016.

[28] C. C. Z. Baber Aslam, Ping Wang, "Extension of Internet access to VANET via satellite receive-only terminals.," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. Vol. 14, I.

[29] L. Angeles and L. Angeles, "Internet of Vehicles : From Intelligent Grid to Autonomous Cars and Vehicular Clouds," *IEEE World Forum Internet Things*, pp. 241–246, 2014.

[30] S. Vashi, J. Ram, J. Modi, S. Verma, and D. C. Prakash, "Internet of Things (IoT) : A Vision, Architectural Elements, and Security Issues," no. 1, pp. 492–496, 2017.

[31] C. A. Kerrache *et al.*, "TACASHI : Trust-Aware Communication Architecture for Social Internet of Vehicles," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5870–5877, 2018.

[32] T. white H. US, "NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE," 2011, Accessed on 8 July 2020 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[33] Transport Department, "Government of NCT of Delhi, 'Installation of GPS in buses and Autos,'" 2010.

[34] European Commission, “A Digital Single Market Strategy for Europe,” 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 , Accesssed on 20 June 2020.

[35] Brandon Schoettle and Michael Sivak, “PUBLIC OPINION ABOUT SELF-DRIVING VEHICLES IN CHINA, INDIA, JAPAN, THE U.S., THE U.K., AND AUSTRALIA,” *Transport Research Institute*, Report No. UMTRI-2014-30, Aug 2014. Accessed on 8 July 2020. Link https://deepblue.lib.umich.edu/bitstream/handle/2027.42/109433/103139.pdf?sequence=1&isAllowed=y .

[36] “Google, ‘Open Automobile Alliance’, 2015. Available: http://www.openautoalliance.net/.”

[37] “Apple, ‘CarPlay’, 2014. Available: http://www.apple.com/ios/carplay/.”

[38] W. G. Meeting, “White Paper of Internet of Vehicles (IoV),” *50th Telecommun. Inf. Work. Gr.*, no. October, 2014.

[39] C. Jiacheng, Z. Haibo, Z. Ning, Y. Peng, G. Lin, and S. Xuemin, “Software defined Internet of vehicles: architecture, challenges and solutions,” *Journal of Communications and Information Networks*, vol. 1, no. 1. pp. 14–26, 2016.

[40] L. Nanjie, “Internet of Vehicles: Your next connection,” *Huawei WinWin*, pp. 23–28, 2011.

[41] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, “Trust management in social Internet of vehicles : Factors , challenges , blockchain , and fog solutions,” *Int. J. Distrib. Sens. Networks*, vol. 15, no. 1, 2019.

[42] R. Silva and R. Iqbal, “Ethical Implications of Social Internet of Vehicles Systems,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 517–531, 2019.

[43] S. C. ; S. S. ; S. S. ; S. E. ; J. J. and K. Lee, “A pub/sub-Based Fog Computing Architecture for Internet of Vehicles,” *2016 IEEE 8th Int. Conf. Cloud Comput. Technol. Sci.*

[44] J. Wan, D. Zhang, S. Zhao, L. Yang, and J. Lloret, “Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions,” *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 106–113, 2014.

[45] P. Gandotra, R. Kumar Jha, and S. Jain, “A survey on device-to-device (D2D)

communication: Architecture and security issues," *J. Netw. Comput. Appl.*, vol. 78, pp. 9–29, 2017.

[46] F. Bonomi, "The Smart and Connected Vehicle and the Internet of Things," *Synchronization Telecommun. Syst. 2013*, pp. 1–53, 2013.

[47] O. Kaiwartya *et al.*, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[48] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero Ibáñez, "A seven-layered model architecture for Internet of Vehicles," *J. Inf. Telecommun.*, vol. 1, no. 1, pp. 4–22, 2017.

[49] T. S. J. Darwish and K. Abu Bakar, "Fog Based Intelligent Transportation Big Data Analytics in The Internet of Vehicles Environment: Motivations, Architecture, Challenges, and Critical Issues," *IEEE Access*, vol. 6, no. c, pp. 15679–15701, 2018.

[50] H. S. Tan and J. Huang, "DGPS-based vehicle-to-vehicle cooperative collision warning: Engineering feasibility viewpoints," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 4, pp. 415–427, 2006.

[51] R. Miller and Q. Huang, "An adaptive peer-to-peer collision warning system," *IEEE Veh. Technol. Conf.*, vol. 1, pp. 317–321, 2002.

[52] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," *IEEE Commun. Mag.*, vol. 44, no. 1, pp. 74–82, 2006.

[53] D. Reichardt, M. Miglietta, L. Moretti, P. Morsink, and W. Schulz, "CarTALK 2000: safe and comfortable driving based upon inter-vehicle-communication," pp. 545–550, 2003.

[54] X. Yang, J. Liu, F. Zhao, and N. H. Vaidya, "A Vehicle-to-Vehicle Communication Protocol for cooperative collision warning," in *The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services. MOBIQUITOUS. IEEE*, 2004, pp. 114--123.

[55] N. Maslekar, M. Boussedjra, J. Mouzna, and H. Labiod, "VANET based adaptive traffic signal control," *IEEE Veh. Technol. Conf.*, 2011.

[56] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea, and L. Iftode,

"Adaptive traffic lights using car-to-car communication," in *IEEE Vehicular Technology Conference*, 2007, no. 1, pp. 21–25.

[57] L. A. Prashanth and S. Bhatnagar, "Reinforcement learning with function approximation for traffic signal control," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 2, pp. 412–421, 2011.

[58] R. Wunderlich, C. Liu, I. Elhanany, and T. Urbanik, "A novel signal-scheduling algorithm with quality-of-service provisioning for an isolated intersection," *IEEE Trans. Intell. Transp. Syst.*, vol. 9, no. 3, pp. 536–547, 2008.

[59] P. Y. Chen, Y. M. Guo, and W. T. Chen, "Fuel-saving navigation system in VANETs," *IEEE Veh. Technol. Conf.*, 2010.

[60] K. Collins and G. Muntean, "Route-based Vehicular Traffic Management for Wireless Access in Vehicular Environments," in *IEEE 68th Vehicular Technology Conference*, 2008.

[61] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK : A New VANET-based Smart Parking Scheme for Large Parking Lots," in *IEEE INFOCOM*, 2009.

[62] D. Graupner, "Decentralized Discovery of Free Parking Places," in *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, 2006, pp. 30–39.

[63] L. Li and F. Wang, "Cooperative Driving at Blind Crossings Using Intervehicle Communication," *IEEE Trans. Veh. Technol.*, vol. 55, no. 6, pp. 1712–1724, 2006.

[64] A. Razzaq and A. Mehaoua, "Video Transport over VANETs : Multi-Stream Coding with Multi-Path and Network Coding," in *IEEE Local Computer Network Conference*, 2010, pp. 32–39.

[65] M. Xing and L. Cai, "Adaptive Video Streaming with Inter-Vehicle Relay For Highway VANET Scenario," in *IEEE International Conference on Communications (ICC)*, 2012, pp. 5168–5172.

[66] C. Lee, C. Huang, C. Yang, and T. Wang, "A Cooperative Video Streaming System over the Integrated Cellular and DSRC Networks," in *IEEE Vehicular Technology Conference (VTC Fall)*, 2011.

[67] Y. M. Chen and Y. C. Wei, "A beacon-based trust management system for

enhancing user centric location privacy in VANETs," *J. Commun. Networks*, vol. 15, no. 2, pp. 153–163, 2013.

[68] M. Gerlach, "Trust for vehicular applications," *Proc. - Eighth Int. Symp. Auton. Decentralized Syst. ISADS 2007*, pp. 295–302, 2007.

[69] G. Delanty, "Can We Trust Trust?," *Dep. Sociol. Univ. Oxford, chapter 13, 213–237*, 2000.

[70] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks," *Comput. Networks*, vol. 53, no. 14, pp. 2396–2407, 2009.

[71] D. D. K. Nigahat*, "A review of blackhole attack in mobile adhoc network," *Int. J. Eng. Sci. Res. Technol.*, vol. 6, no. 4, pp. 314–319, 2017.

[72] S. Mandala, K. Jenni, M. A. Ngadi, M. Kamat, and Y. Coulibaly, "Quantifying the severity of blackhole attack in wireless mobile Adhoc networks," *Commun. Comput. Inf. Sci.*, vol. 467, pp. 57–67, 2014.

[73] Y. L. Sun and Y. Yang, "Trust establishment in distributed networks: Analysis and modeling," *IEEE Int. Conf. Commun.*, pp. 1266–1273, 2007.

[74] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A Categorized Trust-Based Message Reporting Scheme for VANETs," *Commun. Comput. Inf. Sci.*, vol. 381 CCIS, no. 5, pp. 65–83, 2013.

[75] L. Buttyan, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *Mob. Networks Appl.*, pp. 1–22, 2002.

[76] N. Bißmeyer, C. Stresing, and K. M. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data, 2010 IEEE Vehicular Networking Conference, VNC 2010," *IEEE, Jersey City, New Jersey, USA*, pp. 166–173, 2010.

[77] N. Bismeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," *IEEE Veh. Netw. Conf. VNC*, pp. 78–85, 2012.

[78] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Trans. Dependable Secur. Comput.*, vol. 01, no. 1, pp. 11–33, 2004.

[79] S. Kamvar, M. Schlosser, and H. Molina, "EigenRep: Reputation Management

in P2P Networks," *Proc. TwelJth Int. World Wide …*, no. May, 2003.

[80] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," *IEEE Int. Conf. Commun.*, pp. 2129–2133, 2008.

[81] R. Sherwood, S. Lee, and B. Bhattacharjee, "Cooperative peer groups in NICE," *Comput. Networks*, vol. 50, no. 4, pp. 523–544, 2006.

[82] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, 2004.

[83] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," *Proc. 2004 ACM Work. Wirel. Secur. WiSe*, pp. 1–10, 2004.

[84] G. Lenzini, M. S. Bargh, and B. Hulsebosch, "Trust-enhanced Security in Location-based Adaptive Authentication," *Electron. Notes Theor. Comput. Sci.*, vol. 197, no. 2, pp. 105–119, 2008.

[85] M. J. Probst and S. K. Kasera, "Statistical trast establishment in wireless sensor networks," *Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS*, vol. 1, 2007.

[86] R. Haenni, "Using probabilistic argumentation for key validation in public-key cryptography," *Int. J. Approx. Reason.*, vol. 38, no. 3, pp. 355–376, 2005.

[87] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "Robust cooperative trust establishment for MANETs," *Proc. Fourth ACM Work. Secur. ad hoc Sens. Networks, SASN 2006. A Work. held conjuction with 13th ACM Conf. Comput. Commun. Secur. CCS'06*, no. May 2014, pp. 23–34, 2006.

[88] S. Yu, M. J. Kwon, E. H. Lee, H. Park, and H. Y. Woo, "The Beta Reputation System," in *15th Bled Electronic Commerce Conference*, 2002.

[89] R. Falcone, G. Pezzulo, and C. Castelfranchi, "A Fuzzy Approch to a Belief-Based Trust Computation," in *Lecture Notes on Artificial Intelligence, pp. 73–86, 2003*, 2003, pp. 73–86.

[90] J. Wang, Y. Liu, X. Liu, and J. Zhang, "A trust propagation scheme in VANETs," *IEEE Intell. Veh. Symp.*, pp. 1067–1071, 2009.

[91] F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, 2012.

[92] and W. S. X. Li, J. Liu, X. Li, "RGTE: a reputation-based global trust

establishment in VANETs," in Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13), pp. 210–214, IEEE, September 2013," in *5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13)*, 2013, pp. 210–214.

[93] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," *VANET'12 - Proc. 9th ACM Int. Work. Veh. Inter-NETworking, Syst. Appl.*, pp. 73–82, 2012.

[94] X. Z. Qing Ding, Xi Li, Ming Jiang, "Reputation-based trust model in Vehicular Ad Hoc Networks," in *IEEE international conference on Wireless Communications and Signal Processing (WCSP)*, 2010.

[95] E. B. Sashi Gurung, Dan LinAnna Squicciarini, "Information-Oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks," in *Network and System Security*, 2013, pp. 94–108.

[96] A. Osama and B. Azzedine, "Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services," in *IEEE Global Telecommunications Conference - GLOBECOM*, 2011.

[97] P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi, "Trust Issues for Vehicular Ad Hoc Networks," *VTC Spring 2008 - IEEE Veh. Technol. Conf.*, pp. 2800–2804, 2008.

[98] X. Hong, D. Huang, M. Gerla, and Z. Cao, "{SAT:} Building New Trust Architecture for Vehicular Networks," in *The Third International Workshop on Mobility in the Evolving Internet Architecture*, 2008, pp. 31–36.

[99] Z. Huang, S. Ruj, M. Stojmenovic, M. Cavenaghi, and A. Nayak, "A social network approach to trust management in VANETs," in *Part of the Springer book series on Peer-to-Peer Networking and Applications*, 2014.

[100] M. Nitti, R. Girau, L. Atzori, and S. Member, "Trustworthiness Management in the Social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1–14, 2014.

[101] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Comput.*

Sci. Inf. Syst., vol. 8, no. 4, pp. 1207–1228, 2011.

[102] I. R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition," *IEEE Trans. Serv. Comput.*, vol. 9, no. 3, pp. 482–495, 2016.

[103] I. R. Chen and J. Guo, "Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 49–56, 2014.

[104] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 5, pp. 1200–1210, 2014.

[105] J. Guo and I. R. Chen, "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems," *Proc. - 2015 IEEE Int. Conf. Serv. Comput. SCC 2015*, pp. 324–331, 2015.

[106] P. Resnick, R. Zeckhauser, and E. Friedman, "Reputation Systems," *Commun. ACM*, vol. 43, pp. 45–48, 2000.

[107] J. I. and A. K. M. Blaze, J. Feigenbaum, "The KeyNote Trust Management System," in *University of Pennsylvania*, 1999.

[108] L. K. B. Ganeriwal, Saurabh and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," *ACM Trans. Sens. Networks*, pp. 66–77, 2007.

[109] J. Scott, "Social Network Analysis: A Handbook, 2nd edition ed. Newberry Park, CA: Sage Publications," *vol. 4277, Lect. Notes Comput. Sci. Berlin / Heidelb. Springer, 2006, pp. 894-903.*, vol. 4277, pp. 894–903, 2006.

[110] S. Ries, J. Kangasharju, and M. Max, "A Classification of Trust Systems," *Lect. Notes Comput. Sci. Berlin / Heidelb. Springer*, pp. 894–903, 2006.

[111] A. Abdul-rahman and S. Hailes, "Supporting Trust in Virtual Communities," in *in The 33rd Hawaii International Conference on System Sciences, Maui, Hawaii*, 2000.

[112] J. Sabater, "REGRET : A reputation model for gregarious societies," in *in The Fifth International Conference on Autonomous Agents Montreal, Quebec, Canada*, 2001.

[113] C. M. Jonker and J. Schalken-pinkster, "Human Experiments in Trust

Dynamics Human Experiments in Trust Dynamics," in *in The Second International Conference on Trust Management (iTrust '04), Oxford, UK*, 2004, no. February.

[114] C. Castelfranchi, R. Falcone, and G. Pezzulo, "Integrating Trustfulness and Decision Using Fuzzy Cognitive Maps," in *in Proceedings of the first International Conference on Trust Management (iTrust 2003)*, 2003, no. May.

[115] C. Castelfranchi and R. Falcone, "Trust Is Much More than Subjective Probability : Mental Components and Sources of Trust," in *in The 33rd Hawaii International Conference on System Sciences*, 2000.

[116] K. S. Barber and J. Kim, "Belief Revision Process Based on Trust : Agents Evaluating Reputation of Information Sources," in *in Trust in Cyber-societies, Lecture Notes in Computer Science*, 2001, pp. 73–82.

[117] Y. Wang and J. Vassileva, "Bayesian Network Trust Model in Peer-to-Peer Networks," in *in Agents and Peer-to-Peer Computing, vol. 2872, Lecture Notes in Computer Science. Berlin, Heidelberg: Springer*, 2004, pp. 23–34.

[118] Y. Wang and J. Vassileva, "Bayesian Network-Based Trust Model," in *in The International Conference on Web Intelligence (WI '03), Halifax, Canada*, 2003.

[119] Y. Wang and J. Vassileva, "Trust and reputation model in peer-to-peer networks," in *in The 3rd International Conference on Peer-to-Peer Computing Linköping, Sweden*, 2003.

[120] L. Xiong and L. Liu, "A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities," in *in IEEE International Conference on E-Commerce Technology (CEC '03)*, 2003, pp. 275–284.

[121] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," in *in The Tenth International Conference in Information and Knowledge Management, Atlanta, Georgia, USA*, 2001, pp. 310–317.

[122] F. Stajano and R. Anderson, "The Resurrecting Duckling : Security Issues for Ad-hoc Wireless Networks," in *Security Protocols, vol. 1796. Berlin / Heidelberg: Springer*, 2000, pp. 172–182.

[123] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking To Strangers : Authentication in Ad-Hoc Wireless Networks," *Symp. Netw.*

Distrib. Syst. Secur. (NDSS '02), San Diego, Calif., 2002.

[124] M. Carbone, M. Nielsen, and V. Sassone, "A Formal Model for Trust in Dynamic Networks," *First Int. Conf. Softw. Eng. Form. Methods (SEFM '03), Brisbane, Aust.*, 2003.

[125] V. Cahill *et al.*, "Using Trust for Secure," *IEEE Pervasive Comput.*, vol. 2, pp. 52–61, 2003.

[126] B. N. Shand, "Trust for Resource Control: Self-enforcing Automatic Rational Contracts between Computers," *Univ. Cambridge Comput. Lab. UCAM-CL-TR-600*, 2004.

[127] S. Weeks and P. Henry, "Understanding Trust Management Systems," *2001 IEEE Symp. Secur. Priv. Oakland, California, USA*, 2001.

[128] V. Wang, Yan, "Trust2 : developing trust in peer-to-peer environments," in *IEEE International Conference on Services Computing, Orlando, Florida, USA*, 2005, no. August.

[129] V. Wang, Yan, "Two-phase Peer Evaluation in P2P E-commerce Environments," in *IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE '05), Hong Kong*, 2005.

[130] M. Kinateder, E. Baschny, and K. Rothermel, "Towards a Generic Trust Model – Comparison of Various Trust Update Algorithms," in *in The Third International Conference on Trust Management (iTrust '05), Rocquencourt, France*, 2005, pp. 177–192.

[131] F. Azzedin and M. Maheswaran, "Evolving and Managing Trust in Grid Computing Systems," *IEEE Can. Conf. Electr. Comput. Eng. (CCECE '02)*, pp. 1424–1429, 2002.

[132] V. V. P. Song, Weihua, "Neural Network-Based Reputation Model in a Distributed System," *IEEE Int. Conf. E-Commerce Technol. San Diego, California, USA*, pp. 5–8, 2004.

[133] H. Baohua, H. Heping, and L. Zhengding, "Identifying Local Trust Value with Neural Network in P2P Environment," *First IEEE IFIP Int. Conf. Cent. Asia Internet, Bishkek, Kyrg. Repub.*, 2005.

[134] W. Kotsovinos, Evangelos, "BambooTrust : Practical scalable trust management for global public computing," *ACM Symp. Appl. Comput. Dijon,*

Fr., pp. 23–27, 2006.

[135] B. Dragovic, E. Kotsovinos, S. Hand, P. R. Pietzuch, J. J. T. Avenue, and Ö. Ø. Ò. Ñ. Ø. Ò. Ñ, "XenoTrust : Event-based distributed trust management," *14th Int. Work. Database Expert Syst. Appl. Prague, Czech Repub.*, 2003.

[136] B. Shand, N. Dimmock, and J. Bacon, "Trust for Ubiquitous , Transparent Collaboration," *Wirel. Networks*, vol. 10, pp. 711–721, 2004.

[137] D. Quercia, S. Hailes, and L. Capra, "B-trust : Bayesian Trust Framework for Pervasive Computing," in *in iTrust 2006 - 4th International Conference on Trust Management, Pisa, Italy*, 2006.

[138] N. Boudriga, "Security of Ad Hoc Networks," *Secur. Mob. Commun.*, pp. 285–324, 2009.

[139] S. Buchegger and J. Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of nodes: Fairness in dynamic ad-hoc networks)," *Proc. Int. Symp. Mob. Ad Hoc Netw. Comput.*, no. October, pp. 226–236, 2002.

[140] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," in *in The IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security Portoroz, Slovenia*, 2002, pp. 107–121.

[141] S. Buchegger, J. Le Boudec, J. Le, B. The, and R. Spreading, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks To cite this version : The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks Reputation Systems for Mo- bile ad-hoc and Peer-to-," *https//hal.inria.fr/inria-00466691 Submitt. 24 Mar 2010 HAL*, 2010.

[142] S. Buchegger and J.-Y. Le Boudec, "Coping with False Accusations in Misbehavior Reputation Systems for Mobile Ad-hoc Networks," *EPFL-IC-LCA, Lausanne, Switz. IC*, 2003.

[143] S. Buchegger, "A robust reputation system for mobile ad-hoc networks," *Proc. P2PEcon*, no. 5005, pp. 1–11, 2003.

[144] S. Buchegger, C. Tissières, and J. Y. Le Boudec, "A test-bed for misbehavior detection in mobile ad-hoc networks - How much can watchdogs really do?," *Proc. - IEEE Work. Mob. Comput. Syst. Appl. WMCSA*, no. 5005, pp. 102–111,

2004.

[145] G. Theodorakopoulos and J. S. Baras, “On trust models and trust evaluation metrics for ad hoc networks,” *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 318–328, 2006.

[146] T. J. John S. Baras, “DYNAMIC AND DISTRIBUTED TRUST FOR MOBILE AD-HOC NETWORKS,” *Univ. Maryland, Orlando, Florida, USA*, 2004.

[147] A. A. Pirzada and C. McDonald, “Establishing Trust In Pure Ad-hoc Networks BT - Twenty-Seventh Australasian Computer Science Conference (ACSC2004),” in *in The 27th Australasian Conference on Computer Science, Dunedin, New Zealand*, 2004, vol. 26, pp. 47–54.

[148] Y. L. Sun, W. Yu, and Z. Han, “Information theoretic framework of trust modeling and evaluation for ad hoc networks,” *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–315, 2006.

[149] Z. Liu, A. W. Joy, and R. A. Thompson, “A dynamic trust model for mobile ad hoc networks,” *Proc. - 10th IEEE Int. Work. Futur. Trends Distrib. Comput. Syst.*, pp. 80–85, 2004.

[150] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, “A quantitative trust establishment framework for reliable data packet delivery in MANETs,” *SASN’05 - Proc. 2005 ACM Work. Secur. Ad Hoc Sens. Networks*, vol. 2005, pp. 1–10, 2005.

[151] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim, “Highly reliable trust establishment scheme in ad hoc networks,” *Comput. Networks*, vol. 45, no. 6, pp. 687–699, 2004.

[152] T. Jiang and J. S. Baras, “Ant-based adaptive trust evidence distribution in MANET,” *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 24, pp. 588–593, 2004.

[153] T. U. . L. G. M. Truong N.B.; Won, “A reputation and knowledge based trust service platform for trustworthy,” *Proc. 19th Int. Conf. Innov. Clouds*, no. March, pp. 104–111, 2016.

[154] F. Bao and I.-R. Chen, “Dynamic Trust Management for the Internet of Things Applications Self-IoT 2012 Introduction System Model Dynamic Trust

Management Protocol," pp. 1–30, 2012.

[155] F. Bao, I. R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems," *Proc. - 2013 11th Int. Symp. Auton. Decentralized Syst. ISADS 2013*, 2013.

[156] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Comput. Secur.*, vol. 39, no. PART B, pp. 351–365, 2013.

[157] Shafer G, "A mathematical theory of evidence," *J. Cross. Cult. Psychol.*, vol. 8, no. 1, pp. 123–125, 1977.

[158] B. Liu, Z. Xu, and J. Chen, "TOWARD RELIABLE DATA ANALYSIS FOR INTERNET OF THINGS BY BAYESIAN School of Computer Science and Technology , Nanjing University of Posts State Key Laboratory for Novel Software Technology , Nanjing University , P . R . China College of Instrument Science," pp. 2–6, 2015.

[159] C. Prandi, S. Mirri, S. Ferretti, and P. Salomoni, "On the need of trustworthy sensing and crowdsourcing for urban accessibility in smart city," *ACM Trans. Internet Technol.*, vol. 18, no. 1, 2017.

[160] U. Jayasinghe, A. Otebolaku, T. W. Um, and G. M. Lee, "Data centric trust evaluation and prediction framework for IOT," *Proc. 2017 ITU Kaleidosc. Acad. Conf. Challenges a Data-Driven Soc. ITU K 2017*, vol. 2018-Janua, no. March, pp. 1–7, 2017.

[161] W. Li, H. Song, and F. Zeng, "Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 716–723, 2018.

[162] M. Mahmud *et al.*, "A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications," *Cognit. Comput.*, vol. 10, no. 5, pp. 864–873, 2018.

[163] H. Al-Hamadi and I. R. Chen, "Trust-Based Decision Making for Health IoT Systems," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1408–1419, 2017.

[164] 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 Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 41, no. 3, pp. 407–420, 2011.

[165] Matthias Gerla, "Trust for Vehicular Applications," *8th Int. Symp. Auton. Decentralized Syst.*, 2007.

[166] Z. Wei, F. R. Yu, and A. Boukerche, "Trust based security enhancements for vehicular ad hoc networks," *DIVANet 2014 - Proc. 4th ACM Symp. Dev. Anal. Intell. Veh. Networks Appl.*, pp. 103–109, 2014.

[167] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Networks*, vol. 55, pp. 107–118, 2016.

[168] A. Shrivastava, K. Sharma, and B. K. Chaurasia, "HMM for Reaputation Computation in VANET," in *IEEE International Conference on Computing, Communication and Automation (ICCCA2016)*, 2016, pp. 667–670.

[169] Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang, "A Reputation-Based Announcement Scheme for VANETs," in *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*, 2012, vol. 61, no. 9, pp. 4095–4108.

[170] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," *IEEE 27th Conf. Comput. Commun.*, pp. 1238–1246, 2008.

[171] R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks," *Secur. Commun. Networks*, vol. 7, pp. 1652–1669, 2014.

[172] N.-W. Lo and H.-C. Tsai, "A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, no. 1, p. 125348, 2009.

[173] S. Z. Aifeng wu, Jianqing Ma, "RATE: A RSU-Aided Scheme for Data-Centric Trust Establishment in VANETs," in *7th IEEE international conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, 2011.

[174] S. A. Soleymani *et al.*, "A Secure Trust Model based on Fuzzy Logic in Vehicular Ad Hoc Networks with Fog Computing," in *IEEE Access*, 2017, vol. 3536, no. c, pp. 1–10.

[175] F. Dötzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad-hoc network reputation system," *Proc. - 6th IEEE Int. Symp. a World Wirel. Mob. Multimed.*

Networks, WoWMoM 2005, no. 1, pp. 454–456, 2005.

[176] Y. chih wie Yi- Ming Chen, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *J. Commun. Networks*, vol. 15, no. 2, pp. 153–163, 2013.

[177] Y.-M. C. Yu-Chih Wei, "Reliability and Efficiency Improvement for Trust Management Model in VANETs," in *Human Centric Technology and Service in Smart Space*, springer, 2012, pp. 105–112.

[178] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, 2016.

[179] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A Categorized Trust-Based Message Reporting Scheme for VANETs," in *Advances in Security of Information and Communication Networks*, springer, 2013, pp. 65–83.

[180] R. Shrestha and S. Y. Nam, "Trustworthy event-information dissemination in vehicular Ad Hoc networks," *Mob. Inf. Syst.*, vol. 2017, 2017.

[181] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A Hybrid Trust Management Heuristic for VANETs," *2019 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2019*, pp. 748–752, 2019.

[182] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the internet of vehicles (IoV)," *Proc. - 2017 IEEE 2nd Int. Congr. Internet Things, ICIOT 2017*, pp. 25–32, 2017.

[183] A. Bhargava, S. Verma, B. K. Chaurasia, and G. S. Tomar, "Computational trust model for Internet of Vehicles," *2017 Conf. Inf. Commun. Technol. CICT 2017*, vol. 2018-April, pp. 1–5, 2018.

[184] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the Ratee : A Trust Management System for Social Internet of Vehicles," *Wirel. Commun. Mob. Comput.*, vol. 2017, 2017.

[185] F. Gai, J. Zhang, Z. Peidong, and X. Jiang, "Ratee-Based Trust Management System for Internet of Vehicles," in *Part of the Lecture Notes in Computer Science Springer book series*, springer, 2017.

[186] S. Yang, Z. Liu, J. Li, S. Wang, and F. Yang, "Anomaly detection for internet of vehicles: A trust management scheme with affinity propagation," *Mob. Inf.*

Syst., vol. 2016, 2016.

[187] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, “Trust management system design for the Internet of Things: A context-aware and multi-service approach,” *Comput. Secur.*, vol. 39, no. PART B, pp. 351–365, 2013.

Author's Biodata

Indu is currently working as an Assistant Professor in School of Electrical, Electronics and Communication Engineering in Galgotias University, India. She received her Master of Technology in Electronics and Communication Engineering from Maharshi Dayanand University, India. Her research and publication interest includes wireless communication, Vehicular Ad-hoc Networks and Internet of Vehicles.

Ms. Indu
B.Tech., M.Tech. (ECE), Ph.D (Thesis Submitted)

Assistant Professor
Department of Electronics and Communication Engineering,
Galgotias University
Greater Noida, U.P.
India, Pin 203201

Research Scholar
Galgotias University
Greater Noida, U.P.
India, Pin 203201

Mobile: 7827882127
E-mail: indubhardwaj2011@gmail.com