DESIGN OF SECURE SESSION INITIATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS

A thesis

submitted in partial fulfillment of the

requirements for the award of the degree of

DOCTOR OF PHILOSOPHY
in

Electronics and Electrical

Engineering By

Sandeep Kumar Arora
41400177

Supervised By

Dr. Gulshan Kumar

Lovely Professional University, India

LOVELY PROFESSIONAL UNIVERSITY
PUNJAB
2022

Declaration

I do hereby acknowledge that:

The present thesis entitled **"***DESIGN OF SECURE SESSION INITIATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS***"** is a presentation of my original research work done under the guidance of my supervisor. Wherever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature, and acknowledgment of collaborative research and discussions.

I further declare that there is no falsification or manipulation in terms of research materials. I hereby confirm that the thesis is free from any plagiarized material and does not infringe any rights of others.

I carefully checked the final version of the printed and softcopy of the thesis for completeness and incorporation of all suggestions of the doctoral committee.

I hereby submit the final version of the printed copy of my thesis as per the guidelines and the same content in CD as a separate PDF file to be uploaded in Shodhganga.

Date: 24 April, 2022 **Signature of Candidate**

Certificate

I certify that the candidate Sandeep Kumar Arora (R.No. 41400177) has carried out his thesis work “DESIGN OF SECURE SESSION INITIATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS,” under my supervision. To the best of our knowledge:

i) The candidate has not submitted the same research work to any other institution for any degree/diploma, Associateship, Fellowship, or other similar titles.

ii) The thesis submitted is a record of original research work done by the Research Scholar during the period of study under our supervision, and

iii) The thesis represents independent research work on the part of the Research Scholar.

Supervised By:

Gulshan Kumar

Dr. Gulshan Kumar
Associate Professor,
Lovely Professional University, India

Abstract

Research Area: Vehicular Adhoc Network (VANET) is an emerging technology that needs to be integrated with every vehicle these days. VANET is rapidly adopted by many countries to prevent road accidents and injuries. Moreover, it is used for traffic management in metro cities to save time for the user.

Research Problem: Although VANET is beneficial but dangerous as the VANET nodes can communicate over the public networks. Public networks are open for all and any illegitimate node can create the session without authorization and take full control over the network. The attacker nodes can steal the information easily over the public network if the session is not secured. Moreover, the VANET has limited computation and storage so the authentication scheme should be designed in such a manner that it must have less overhead and cost. The challenge lies in designing a secure session scheme that requires lesser computation, lesser cost, and better Quality of Services (QoS).

Research Approach: The research was carried out to protect the VANET from various threats and to secure the session. We have proposed two various schemes which used blockchain and smart contracts-based architecture and also used Elliptic Curve Cryptography (ECC), hash, implicit certificate, etc. as the cryptographic primitives.

Research Findings: The information exchanged by the vehicles in all two proposed schemes are secured and free from unauthorized access. Further, the Quality of Services (i.e. Throughput, delay, etc.) is drastically improved by securing the session and preventing the VANET from unauthorized access. Besides that, the scheme proposed is resistant to forgery, modification, impersonation, etc. The accomplishment of security goals has been proved with the help of (*Automated Validation of Internet Security Protocols and Applications* (AVISPA). We have also demonstrated that the proposed scheme requires less overhead and less communication cost.

Research Implications: The investigation reveals that the proposed method is superior as compared to the conventional methods in terms of QoS and security. Consequently, the proposed schemes are the best-recommended protocols and the most suitable alternatives to the existing protocols to secure the VANET network.

Acknowledgment

The happiness which comes from long practice, which at first is like poison, but at last like nectar, leads to the end of suffering; - this kind of happiness awakens one to self-realization and abandonment of ignorance

(18.37) Bhagwat Gita

The journey of completing PhD. research work is a lot more than reading and writing research papers. It is a journey of self-enlightenment and experiences which elevates one to think and interpret beyond horizons. The journey is tedious but rewarding, confusing but funny, frustrating at times but never short of satisfaction. Whatever name one may address this journey but undoubtedly, it could have never been accomplished without the help of some wonderful people who walked with me through all the highs and lows. I owe my deepest gratitude to the Lovely Professional University (LPU) for giving me the platform and resources to pursue my research ambitions. My sincere thanks to my Ph.D. supervisor, Dr. Gulshan Kumar for his guidance and valuable support throughout the Ph.D. I am indebted to my co-supervisor, Dr. Himanshu Monga who has supervised my research work in the early phase of my Ph.D.

I convey my gratitude to the executive dean of Lovely faculty of technology and sciences (LFTS), Dr. Loviraj Gupta; Head of examination and division of academic affairs (DAA), Mr. Navdeep Singh Dhaliwal; for providing all sorts of administrative and technical support required to accomplish my research objectives at Lovely Professional University (LPU). A special thanks to the heads of the School of Electronics and Electrical Engineering (SEEE), Dr. Bhupinder Verma, and Dr. Gaurav Sethi for allowing me to use the lab and other facilities required to conduct the research. I must thank the head of the department (HoD), Dr. Kamal Kumar Sharma, and colleagues of SEEE, LPU for encouraging, and motivating me throughout the thesis. I would also like to thank my friends, to name a few, Dr. Rajan Miglani, Dr. Gurjot Singh Gaba, Er. Ravinder Kumar and Er. Harish Chander.

Last but not least, I owe the deepest debt of gratitude to my beloved family, especially to my mother, who even in her old age continues to melt like a candle to shine the light for me. A heartfelt prayer for the departed soul of my father who before passing away cultivated the skills within me that leads to the accomplishment of this program. My heartiest gratitude to my wife who stood behind me as a pillar of strength. The love and affection given by my both sisters and brother and her family motivated me to accomplish my research goals. I am thankful to the relatives who showered blessings on me. Great thanks to my in-laws for understanding me and forgiving me for all those instances when I had not attended family events due to ongoing Ph.D. assignments.

In honor of my parents and homeland

Table of Contents

List of Figures

List of Tables

List of Publications

Publication 1 **Sandeep Kumar Arora**, Himanshu Monga, “*Performance evaluation of MANET on the basis of Knowledge Base Algorithm*,” in Optik, vol. 127, pp. 7283–7291, 2016. *{*SCIE Indexed, IF = 2.187*}*; DOI: 10.1016/j.ijleo.2016.04.138

Publication 2 **Sandeep Kumar Arora**, Gulshan Kumar, Tai-Hoon Kim, “*Blockchain Based Trust Model Using Tendermint in Vehicular Adhoc Networks*,” in Applied Sciences, vol. 11, pp. 1-14, 2021. *{*SCIE Indexed, IF = 2.458*}*; DOI: 10.3390/app11051998

Publication 3 **Sandeep Kumar Arora**, Gulshan Kumar, “*Blockchain Inspired Light Weight Trust Based System in Vehicular*,” in Vehicular Communications (In communication) *{*SCIE Indexed, IF = 6.1*}*

List of Abbreviations

AES	Advanced Encryption Standard
AODV	Adhoc On Demand Distance Vector
AVISPA	Automated Validation of Internet Security Protocols and Applications
BAN	Burrows–Abadi–Needham
BARS	Blockchain Based Trust Management Systems
BFT	Byzantine Fault Tolerance
CA	Certificate Authority
CL-AtSe	Constraint-Logic Based Attack Searcher
CTS	Clear to Send
DDoS	Distributed Denial of Services
DHKE	Diffie Hellman Key Exchange
DKG	Distributed Key Generation
DoS	Denial of Services
DPoS	Distributed Proof of Stake
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing
DSRC	Dedicated Short-Range Communication
ECC	Elliptic Curve Cryptography
ECQV	Elliptic Curve QuVanstone
EED	End-to-End Delay
FCC	Federal Communications Commission
GBT	Gradient Boosting Technique
HLPSL	High-Level Protocol Specification Language
ITS	Intelligent transportation system
IVC	Inter Vehicle Communication

MAC	Medium Access Control
MANET	Mobile Adhoc Network
MD5	Message Digest5
MEC	Mobile Edge Computing
MITM	Man in the Middle
NS-2	Network Simulator-2
OBU	On Boar Unit
ODAM	Optimized Dissemination of Alarm Messages
OFMC	On-the-Fly Mode-Checker
PBFT	Practical Byzantine Fault Tolerance
PDR	Packet Delivery Ratio
PKI	Public Key Infrastructure
PoB	Proof of Burn
PoS	Proof of Stake
PoW	Proof of Work
PUF	Physical Unclonable Function
QoS	Quality of Services
RSU	Road Side Unit
RTS	Request to Send
SA-KMP	Secure and Authenticated Key Management
SUMO	Simulator for Urban Mobility
UMB	Urban Multihop Broadcast
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VANET	Vehicular Adhoc Network
WAVE	Wireless Access for Vehicular Environment
WHO	World Health organization

Chapter 1

Introduction

This chapter gives an overview of the Wireless Adhoc networks, Mobile Adhoc Networks (MANETs), and Vehicular Adhoc Networks (VANETs), problem statement and motivation, research questions and objectives, research methodology followed by an outlining of the thesis.

1.1 Introduction to Wireless Adhoc Networks

When two or more nodes want to exchange the data with wireless communication and network capability with central administration and form a dynamic network is named Mobile Adhoc Network (MANET). Moreover, nodes do not require any extra infrastructure to exchange information. All nodes can act as a router to route the data packets to the destination. The MANET provides a great opportunity to connect and exchange information with some severe challenges [1]. All the nodes dynamically communicate with each other and also provide the necessary network functionality in the absence of any fixed infrastructure. It means that data management and routing management are also required in these types of networks. Therefore, Adhoc networks are complex kind of wireless networks. Adhoc networks can save the cost of wiring by establishing the network in an emergency without any wiring. It saves space as well as the cost of the network and can be used in mobile phones because of its ready availability [2].

1.2 Types of Adhoc Networks

The wireless Adhoc network can be divided into two main types:

- **Quasi-Static Adhoc network:** In this type of network, nodes may be static or portable and because of power controls and link failures, the resulting network topology may be so active. The sensor network is the best example of these types of networks [14].

- **Mobile Adhoc network:** In MANET, the nodes may be mobile and move fast relative to each other. We will discuss the further types of MANET in the next section.

1.2.1 Mobile Adhoc network

MANET is a group of independent network mobile devices that are connected over various wireless links. The network topologies are dynamic and also have a bandwidth constraint. This type of network by itself or incorporate into local area networks.

MANET can be further divided into two types:

- **Vehicular Adhoc Networks:** This type of network is implemented in vehicular communication. Vehicles can inform other vehicles about traffic-related or accidental information.
- **Internet-Based Mobile Adhoc network:** In this type of network the nodes are mobile and connected to the backbone or internet services.

The set of applications of MANET is set from small, static networks to large and highly dynamic networks. Conventional routing cannot be used in the MANETs environment due to its high mobile architecture. Due to its high mobility security is the other concern that we need to take care in these types of networks.

1.2.2 Adhoc Sensor networks

It includes a large number of sensors spreads over a large geographical area. Each sensor is capable of handling mobile communication and also has some computational capability to process the data. The routing protocols determine the connectivity and route the packages accordingly. It is highly flexible and deployed almost in all environments. There are many advantages of these types of networks which includes:

- Use to build a large-scale network.
- Implementation of complex power-saving modes depending upon the state of the art.

With the above advantages, sensor networks are also used in so many applications these days. For example, forest fire detection is the best application of a sensor network. In large buildings or for commercial use sensors networks can be installed without any kind of wired setup for temperature and humidity level detection.

1.3 Vehicular Adhoc Networks

As per the report published by World Health Organization (WHO), road traffic injuries and accidental deaths predominantly increased due to driver carelessness, increasing population, and heavy traffic congestion [1]. So, there is a need for Intelligent Transportation System (ITS) and Vehicular Adhoc Network (VANET) can make it more convenient to which provides services to the end-users and are useful for road safety and reduce the congestion on the road.

VANET offers many features of Mobile Adhoc Networks (MANETs) with additional services like Inter-Vehicle Communication (IVC). It is used to communicate among the vehicles on the road and is useful for information exchange between Road Side Units (RSUs). In VANET vehicles can communicate within a range of 100-1000m. It consists of two communication units: a) An On-Board Unit (OBU) which is fixed inside the vehicle b) Road Side Unit (RSU) which is placed on the road and acts as an access point used to collect and disseminate the data [2,3].

By considering the above facts, Federal Communications Commission (FCC) in the United States has proposed a frequency range of 5.85-5.92GHz to support Vehicle to Vehicle (V2V) communication and Vehicle to Infrastructure (V2I) communication. The mobility is very high in this type of network so to support this high mobility, minimization of delay, and high data rate the establishment of Dedicated Short-Range Communication (DSRC) is developed [4]. Moreover, Wireless Access for Vehicular Environment (WAVE) is developed by the IEEE research group which is a set of special standards utilized by VANETs. In the case of high mobility and latency, routing is a challenging task [5,6,7]. VANET deals with two wireless access standards: (i) IEEE 802.11p manages the physical and Medium Access Control (MAC) Layer and (ii) IEEE 1609 manages the higher-layer protocols [8].

A survey by Indian road safety up to the year 2019 was conducted and it is found that there is a consistent increase in road accidents and accident-related deaths and injuries up to the year 2010 and after that the level is still stable for the injuries/deaths. Figure 1.1 shows the data on deaths by accidents from the year 1970 to 2019.

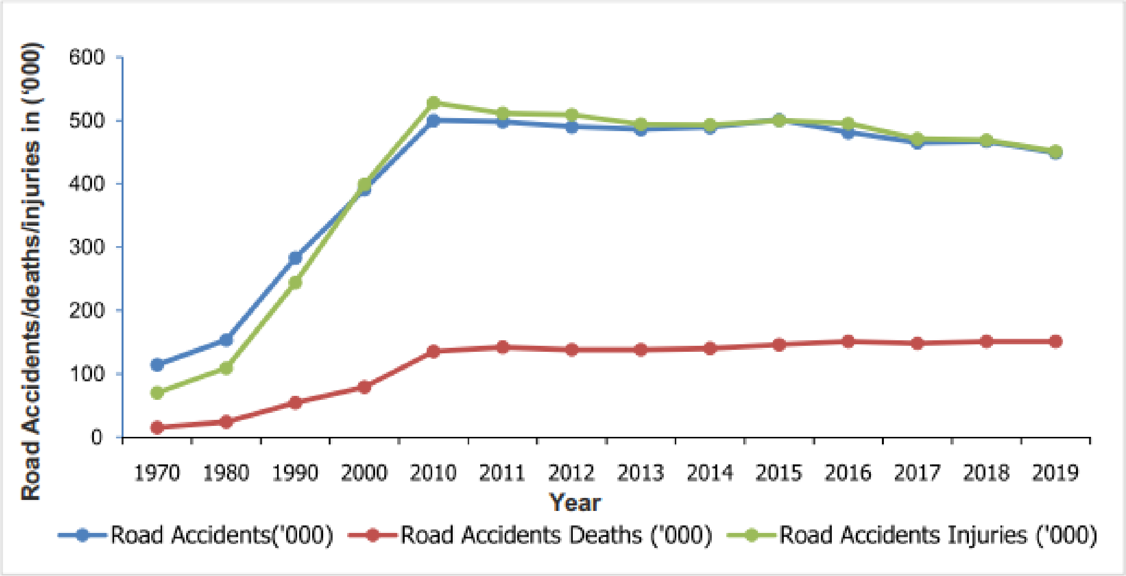


Figure 1.1: Trends of road accidents, deaths, and injuries [9].

So, from that analysis, we found that there is a need for Intelligent transport systems which can reduce the number of casualties on the road in the upcoming years and this can be solved by the Vehicular Adhoc Network (VANET).

One more fact by Indian road safety is released for 2019 as shown in Figure 1.2 and from this, we can analyze that which category of vehicle is more responsible for accident/death. It will be clearly shown in the graph that the two-wheelers accounted for the highest share of 37% of the total persons killed followed by pedestrians i.e. 17%. This is the main reason that helmet wearing has been made mandatory in the Amended Motor Vehicle Act passed by Parliament in 2019 [9].

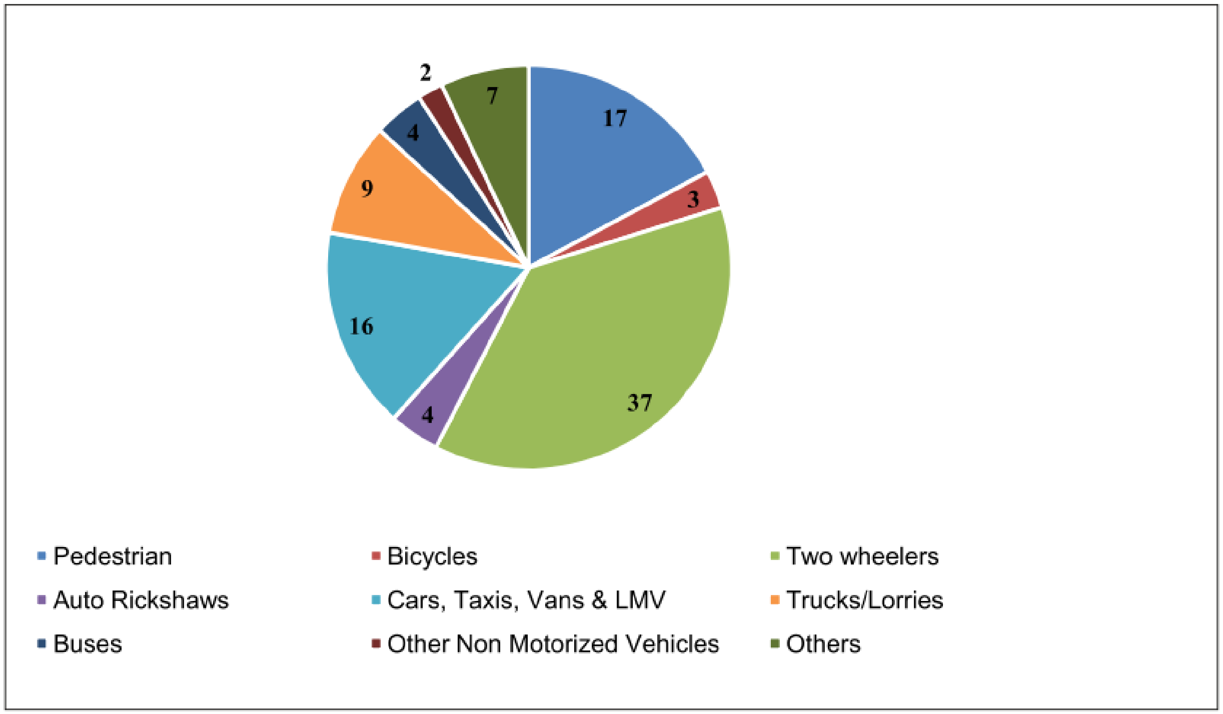


Figure 1.2: Persons killed in 2019 by vehicle category [9].

1.4 Problem Statement and Motivation

The advances in mobile communication and recent trends of adhoc networks allow different architecture deployment for VANET in highways and urban and rural areas. Applications have to be selected by the mean of Quality of Service (QoS). The VANET supports V2V and V2I communication. In V2V communication vehicles can exchange information without relying on the fixed infrastructure and can be employed for safety, security, and dissemination applications. V2I communicates with the roadside infrastructure and is mainly used for information and data gathering applications. VANET has so many applications and we have summarized a few important applications which are used in real-time. [10].

1. Safety applications- To reduce accidents on the road this can be used. But the main thing is this application is sensitive to delay. Hence, we need to pick a suitable routing and security technique to reduce the latency or delay.

2. Efficiency applications- This application is useful to reduce traffic jams on the road. Through this, we will be able to locate the vehicle in real-time and improve its mobility on the public roads.
3. The comfort applications-This type of application is driver-based and provides comfort to the driver. The driver can fetch some important information from the vehicular network like weather, nearby refuel stations, hotels, etc.
4. Interactive entertainment-This is related to sharing information via the internet, chat, music, etc. But the challenge is availability and synchronization between the vehicles.

To achieve these applications is not at all an easy task. There are certain challenges present in these types of a network that we need to explore now [10].

Security and Privacy is the major challenge in Adhoc networks which we need to improve in this area. Due to the frequent topology changes and high mobility in these networks, this is the major concern we need to focus on and motivates me to do the research in this area. Besides those challenges, another major issue is to prevent attackers from interfering with both the integrity of exchanged messages and the availability of the system. Some characteristics of VANETs pose challenges to meet the security requirements, which required novel protocol solutions with some of the following characteristics [11,12,13]: low overhead, minimum hop count, pre-stored information about the nodes. Despite the existing security protocols providing the solution to existing problems but still we need to improve and test the new authentication protocols to secure the session and preserve the privacy of the network. Attackers always look to steal identity-related information to impersonate and get unauthorized access. Disclosure of identity-related information during the exchange of authentication messages or privacy leaks resulting from authentication failure messages could compromise data and location privacy [12].

According to the Juniper research, the damages caused by cyber-attacks in 2019 amounted to $2 trillion. Due to that companies are ready to invest the money to provide proper security to their networks. It is estimated by 2030, the global cybersecurity spending will be $2 billion to mitigate network attacks.

One of the possible measures to secure the session in VANET and prevent the network from being damaged we need to embed the authentication and key agreement protocol in a decentralized manner [14]. It enables only legitimate entities to communicate, thus preventing attacks and their consequences. However, the challenge is the design of that decentralized system which is having less overhead and prevents the various types of network attacks. Less overhead is preferable due to limited computation and limited storage in the VANET network.

1.5 Research Questions and Objectives

The main goal of this thesis is to implement security in the session created between the vehicles to exchange information.

- **Research Question 1 (RQ1):** Which routing protocols are implemented in Adhoc networks and how we can measure their performance?

  - Research Goal 1 (RG1): *To compare the different routing protocols for VANET and find out the best-suited protocol which will give better performance in a high mobility scenario.* The goal is to inspect the various routing protocols used to route the information among the nodes. The different Quality of services like throughput, packet delivery ratio, and delay will decide the nature of routing protocols and their applications.

- **Research Question 2 (RQ2):** Why the session is required to exchange information? What are the various cryptographic primitives used to secure the session and how the secret key is established between the different vehicles?

  -Research Goal 2 (RG2): *To develop a session initiation scheme in the application layer for secure communication among nodes.* The goal is to establish and secure the session created among the nodes for communication. Conventional methods are centralized in nature and do not tamper-proof. To develop a decentralized trust-based method that can use ECC, hash, certificates, etc. that can be used to secure the session and the Quality of Services can also be improved by using the decentralized model. RG2 intends to disclose the assumptions, system model, and the use of different consensus algorithms to secure the session.

- **Research Question 3 (RQ3):** What are the various efficient and robust cryptography primitives? How these primitives can be used to form privacy-preserving, robust, and efficient mutual authentication and secret key establishment protocols for resource-constrained VANET environments?

  -Research Goal 3 (RG3): *To implement an efficient authentication protocol based on public-key cryptography for authentication between vehicles.* The goal is to construct efficient and robust security protocols for the various specific environments (VANET, industrial IoT, etc.) of the VANET that can overcome the vulnerabilities in conventional methods. The protocol is desired to protect against unauthorized access and also enable legitimate devices to exchange secret keys for protecting their communications from attackers. However, the existing security protocols are not suitable because they make use of X.509 explicit certificates and other cryptography primitives that are expensive for resource-constrained VANET nodes. RG3 intends to use assumptions, the proposed model, and the process of combining cryptography primitives using smart contracts to prepare novel and efficient authentication.

- **Research Question 4 (RQ4):** What are the various attacks that can be performed on VANET networks and methodologies that can be used to detect them and verify the robustness of the proposed methods against the possible security threats. How one can analyze the QoS through the identified tools, and how to make inferences from the results obtained?

  > **-Research Goal 4 (RG4):** *To develop a mechanism for analyzing vehicular networks from various attacks and examine the robustness of the proposed scheme through simulation.* The protocols developed as an outcome of RG2 and RG3 should be validated in context to robustness through some scientific tools (e.g., Automated Validation of Internet Security Protocols and Applications (AVISPA)) and methods (e.g., Burrows–Abadi–Needham (BAN) logic). The security protocols have hidden underlying vulnerabilities that sometimes developers could not see, therefore security analyzer tools and methods must be used before

implementing the protocol for practical applications. Figure 1.3 is linked with the research goals and outcomes of the thesis.

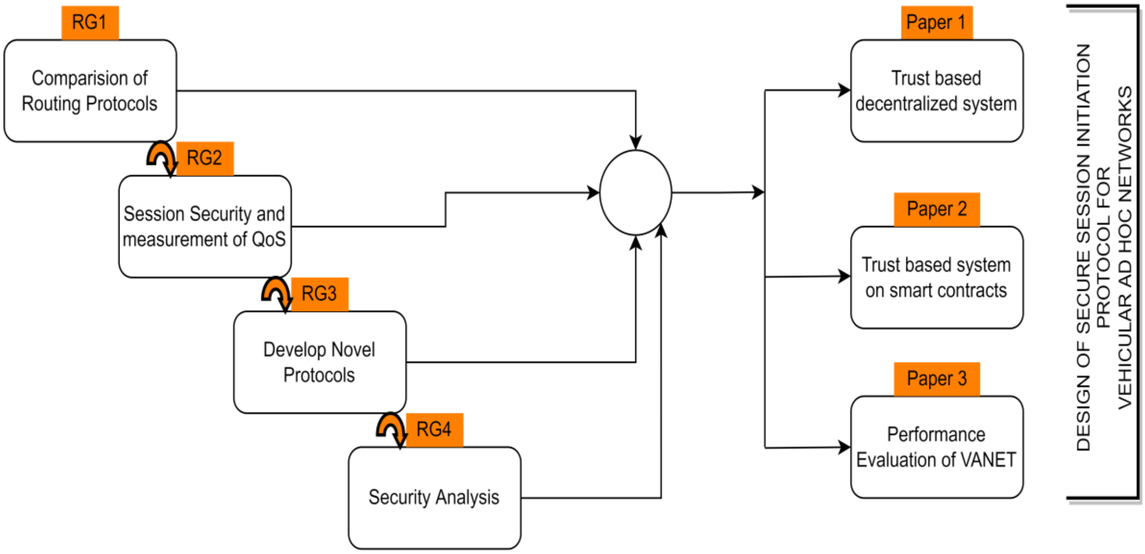

RG1
Comparision of Routing Protocols
RG2
Session Security and measurement of QoS
RG3
Develop Novel Protocols
RG4
Security Analysis
Paper 1
Trust based decentralized system
Paper 2
Trust based system on smart contracts
Paper 3
Performance Evaluation of VANET
DESIGN OF SECURE SESSION INITIATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS

Figure 1.3: Research goals and outcomes.

1.7 Research Methodology

The standard procedure of research methodology has been adopted while designing the system which provides better security to the session as well as prevents various attacks. The research methodology is primarily classified into three parts: analytical, theoretical, and experimental. The overall flow of the research methodology is illustrated in Figure 1.4 and discussed as follows:

Analytical refers to reading and understanding the literature to find the best-suited routing protocols and present security frameworks. It further includes an understanding of the adversary model and setting up security goals.

Theoretical refers to designing the system model and proposing the security protocols using a decentralized trust model and smart contracts. The proposed model should not be prone to attacks despite the attacker having more computation capabilities.

Experimental refers to the implementation of the approach to evaluating its performance through estimations, simulations, or real-time implementations together with robustness evaluation using scientific tools. Eventually, the proposed scheme is compared with the conventional schemes to establish superiority.

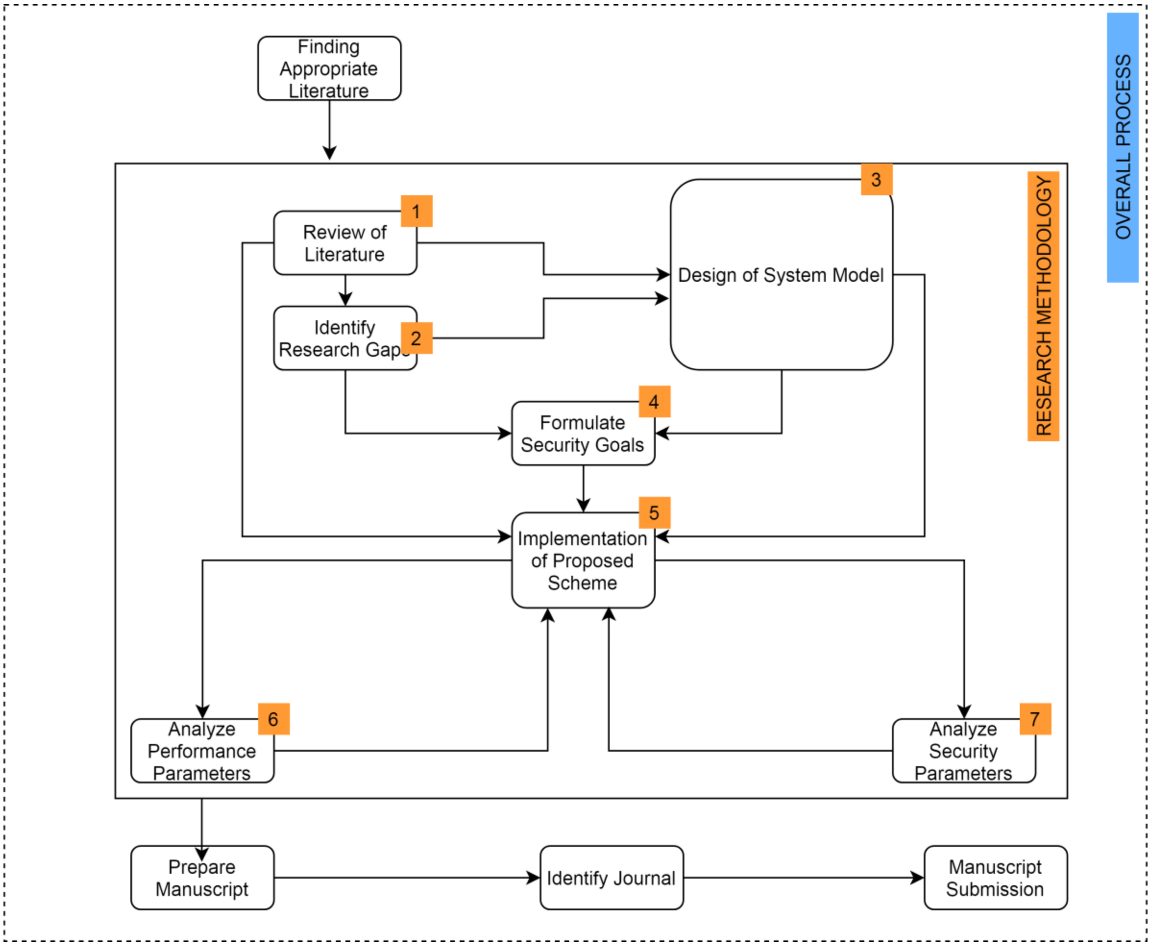


Figure 1.4: Process flow of Research Methodology.

1.8 Contribution of Thesis

The thesis contributes three novel contributions in the form of securing sessions and providing security to the VANET and MANET networks. These networks can be secured from various threats discussed in section 2.3

Paper-I presents a blockchain-based trust model using tendermint in a vehicular Adhoc network. The main contribution of the paper is to secure the session by restricting the unauthorized access of vehicles. The proposed scheme utilizes a trust mechanism based on a gradient boosting technique for validating the messages received from the neighboring vehicles. It eliminates the problem of malicious nodes entering the network and also overcomes the problem of power consumption. Simulation results also show that the proposed techniques are effective in terms of providing a better Quality of Services.

Table 1.1: Contribution, applied primitives, and schemes for comparison

	Research Contributions	Applied Primitives	Comparison with papers
I	Blockchain Based Trust Model Using Tendermint in Vehicular Adhoc Networks	Message Digest, Blockchain, PoW, PoS and tendermint	[38],[39], [43], [46] and [106]
II	Trust Based System on Smart Contracts in Vehicular Adhoc Networks	ECC, Blockchain, PoW, Smart contracts	[76], [82] and [90]
III	Performance evaluation of MANET on the basis of Knowledge Base Algorithm	Knowledge base algorithm	[119], [125] and [130]

Paper-II discusses the impact of applying smart contracts on the VANET networks. Besides, it also discusses the various threats on the VANET and how we can overcome those by applying the blockchain and smart contracts. A novel scheme is proposed in this paper which provides a novel two-way authentication and key agreement through encryption and signature mechanism. Furthermore, smart contracts are used to overcome the problem of overhead and the proposed system is also examined in AVISPA and found secure against potential attacks like MITM, impersonation, replay, etc.

Paper III discusses the impact of various attacks on the Quality of services and analyzed the robustness of the network with and without attacks. A novel knowledge base algorithm is applied to achieve an effective route for data communication. A network simulator has been used to perform the impact of various attacks on the network.

All these contributions together accomplish the objectives of the thesis in section 1.3. Table 1.1 provides the details of cryptography primitives applied to the various contributions along with details of the scheme taken into consideration for comparison purposes.

1.9 Thesis Outline

The remainder of the thesis is organized as follows:

Chapter 2 contains preliminary studies on an overview of routing protocols, security fundamentals, threats, and the various requirements of security. The chapter also includes a discussion on implicit certificates, mutual authentication, and key establishment, an introduction to blockchain, and several attacks on blockchain and its features.

Chapter 3 includes the various conventional schemes based on authentication schemes and mutual key establishment based on public key infrastructure and various decentralized schemes proposed by the various researchers in the field of VANET and the Internet of vehicles. The chapter ends with a summary of research gaps identified after reviewing the literature.

Chapter 4 elaborates the proposed approach and system model of the first research contribution, "Blockchain Based Trust Model using Tendermint in Vehicular Adhoc Networks". Moreover, it also presents the simulation parameters, results, and comparison with conventional schemes.

Chapter 5 uncovers the second research contribution, "Blockchain Inspired Light Weight Trust Based System in Vehicular Networks". The methodology from system initialization to the implementation of smart contracts key agreement has been discussed in this chapter. The last few sections of the chapter include the security analysis through AVISPA and performance estimations.

Chapter 6 elaborates on the third contribution, "Performance evaluation of MANET on the basis of Knowledge Base Algorithm". The methodology from system initialization to the implementation of the knowledge base algorithm has been discussed in this chapter. The last section of the chapter describes how the various types of attacks affect the Quality of services.

Chapter 7 summarizes the research gaps and the security requirements in the VANET framework and how it has been addressed by the proposed schemes. Moreover, it also provides how the proposed research would benefit society and researchers in the current era and future.

Lastly, the appendices cover the NS-2 and AVISPA installation guide, and BAN logic rules and also present the briefing of ECC used in the thesis work.

Chapter 2

Preliminaries

2.1 Overview of Routing Protocols in VANET

Routing is a major challenge in delivering the data from the source to the destination. The major parameters that we need to focus on for routing protocols are traffic management, mobility, and Quality of Services (QoS) [17].

Routing protocols can be divided according to the type of architecture and mode of operation:

2.1.1 Type of Architecture

This can be further divided into Infrastructure and Adhoc based.

- In Infrastructure mode, the fixed access points are used by VANET so that the vehicles can obtain the routing and traffic information directly with help of the internet. This can provide communication between vehicles and fixed access points. The cost will be very high in these types of architecture
- In Adhoc mode, all vehicles can exchange information among themselves. In this mode, there is no need to centralize access points for communication. The nodes themselves can act as routers to send the packet to the destination and such type of architecture is used to detect traffic jams, collisions, and detection of accidents.

2.1.2 Mode of operation

- Routing protocols can be further divided due to the working mode. It can be categorized by topology, geographic, opportunistic, and dissemination. We have surveyed the topology-based and geographic-based routing protocols which we have implemented in this research report. Topology-based routing can be classified further into two types: *Proactive and Reactive.*

- Proactive protocols keep the information about the route inside the routing tables regardless of the use of stored routes [17]. When a client sends a message, the node has to follow the route which is defined in the table. These protocols have high control message overhead because control messages are sent periodically to keep updated the nodes about the route. The Destination-Sequenced Distance Vector (DSDV) [17] is an example of a proactive protocol.
- Reactive protocols do not keep the information before sending the packets. When a node wants to send a packet then the route is determined by the nodes [16,17]. Route discovery is initiated by the flooding method. When a route is established it is stored in the routing table until the destination becomes unreachable. In such types of protocols, the message overhead is very less even though the latency is high. The Adhoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are examples of such protocols [16].

2.1.3 Infrastructure Based

Infrastructure-based routing protocols can be further divided into Urban Multihop Broadcast (UMB) [18] and Optimized Dissemination of Alarm Messages (ODAM) [19].

- In UMB communication among vehicles can take place using multihop transmissions as a way to send the messages to the destination via intermediate nodes. However, this type of communication is challenging in urban areas due to obstacles present between the vehicles. This protocol overcomes problems related to packet collisions, interference, and hidden nodes. UMB uses two control signals Request to Send (RTS) and Clear to Send (CTS). It can work in two modes.
- In directional diffusion mode, the source node chooses the farthest node concerning its position to recognize the messages and continue the diffusion. In intersection mode, the repeaters are installed at the intersection of roads and conduct the diffusion and these repeaters must possess a straight view line to all the parts of the road. When the intersection is discovered on the way, new diffusions will be initiated in all directions.

2.1.4 Greedy perimeter Stateless Routing (GPSR)

It is based on the location of the nodes and it is an efficient routing protocol for wireless and mobile communication [28].

It is based on greedy and parameter forwarding. The first will send the packet to the neighbor node closest to the destination and the second is selected in the case when greedy forwarding is not used. The decision is taken by hop by hop rule in this protocol and it does not require an end to end path establishment [11,30,31]

2.1.5 Geo Networking Protocol

It is a routing protocol standard from European Telecommunication Standards Institute (ETSI); therefore, it's an important geographic routing. Packets are forwarded according to the positions of the nodes by assuming the use of a Global Position Satellite (GPS) [29]. In this, there are two types of packet delivery: geounicast and geobraodcast. The nodes use the location table used that maintains the position of the neighbors which is used to decide on the forwarding of packets. Several evaluations have been already presented in [32] where the authors evaluated the performance of various variants of geobroadcast algorithms.

2.3 Routing Protocols based on Metrics

This section presents strategies for the nodes to select the optimum path based on metrics. This summary helps the researchers to analyze the routing protocols for VANETs. We will define some metrics and their global importance which decide path quality to destination.

- **Minimum hop count:** This deals with the minimum hop count to reach the destination. It should be minimum for better path selection [26].
- **Distance:** It is used to select the node that is closer to the destination as the best candidate node [7].
- **Route Cost Metric:** This metric is based on packet delivery ratio and it also includes the level of link stability [27].

- **Packet Reception rate:** It gives the idea about data dissemination and its efficiency and it is related to the data losses in the network [9].
- **Density:** Traffic density is a very important parameter to find a reliable path. Using beacon messages, the neighbor nodes can be found to realize the density of nodes [28].
- **Speed:** Speed can be used to derive other metrics like link quality, link lifetime, and movement direction [18].
- **Link/route lifetime:** It is the shortest period in which the two nodes can interchange the data in a particular link [22].
- **Link quality:** It is used for the selection of links with the fewest neighboring vehicles, buildings, and obstructions which affects the quality between vehicles [18].

2.2 Security Fundamentals

There are various security aspects that we need to discuss which are used further in this thesis and whose knowledge is necessary. The few important security fundamentals [20] are discussed as follows:

- **Asymmetric Key Cryptography:** It is a cryptography system that uses different public and private keys. The public key is sent publicly by the owner and the private key needs to be kept secret. A sender can use the receiver's public key to encrypt the information. The private is available to the receiver only and nobody can decrypt the information. Elliptic Key Cryptography (ECC) is the most significant scheme that works on the principle of asymmetric key cryptography also known as public-key cryptography.
- **Symmetric Key Cryptography:** It is a cryptography system in which only a single key is used to encrypt and decrypt the information. Therefore, the sender and receiver must negotiate the security key before starting the communication. As we know that establishing the secret key over the wireless channel is susceptible to interception. As a result, in some applications, asymmetric cryptography is used to exchange symmetric keys. Advanced Encryption Standard (AES) is an example of symmetric-key cryptography.
- **Digital Certificates:** Digital certificate is used to ensure that the message is not altered while communicating. It enables the receiver to verify the authenticity. It is one of the important components of security to detect forgery and tampering. It is equivalent to a

handwritten signature but a digital signature is more difficult to forge. These are constructed with the help of asymmetric cryptography. Examples of digital signatures are (X.509), and implicit certificate Elliptic Curve QuVanstone (ECQV).

- **Hash Algorithms:** Cryptographic hash functions are one-way functions that transform the arbitrary-sized message into a fixed-size message digest. The hash algorithm takes into consideration every single bit of the message while execution, hence a minor variation in the message produces a completely different output. There are many variants of hash algorithms (SHA-128, SHA-256) and Message Digest (MD5).

  The hash algorithm should exhibit the following properties:

  1. Two different input messages should not produce an identical message digest.
  2. Hash algorithms must process the inputs quickly with little burden on the computing processor.
  3. It should be computationally infeasible to retrieve the message from a given hash.

2.3 Threats

Threats refer to the exploitation of vulnerabilities by the attacker to accomplish malicious goals. The consequences of the threat range from benign to severe. The attacks are classified into two categories [21]:

2.3.1 Passive

Passive attacks are silent attacks where the adversary intends to eavesdrop on the messages exchanged in the network with no intentions to modify or harm the network resources. An attacker can capture the messages to retrieve the information by unauthorized access. A message may contain sensitive information which can be misused by an attacker to perform illegal activities.

2.3.2 Active

In these types of attacks, an attacker can modify the messages to disrupt routine network operations. Few active attacks are summarized as follows:

- **Denial of Services (DoS):** When the adversary has intentions to hinder the services provided to legitimate entities. It can be performed by flooding the victim's device with malicious requests. The legitimate device will exhaust the services and process the fake requests which fail to provide services to legitimate users. In Distributed Denial of Services (DDoS) multiple machines can do the same which is done by DoS.
- **Man-in-the-middle:** In this attack, the attacker is smoothly able to initiate the session with communicating parties and they never realize that they have connected with a legitimate user or attacker. An attacker will try to intercept the sensitive information and misuse it without authorization. It is possible only if the attacker has sufficient information to impersonate the identities.
- **Modification:** Considering the vulnerabilities of the wireless medium, it is believed that the attacker can intercept the communication. Therefore, the attacker can modify the received message to get privileged access, confidential information, and maybe to generate a secret session.
- **Impersonation:** The attacker can intercept the messages to collect the private information of devices/users such as keys, passwords, etc. for impersonating the identity of legitimate entities.
- **Known Key:** The attacker can try to generate new keys from the old expired (known) keys.
- **Replay:** The attacker can capture the messages to replay later for getting access to unauthorized privileged information or account.

2.4 Security Requirements

To overcome the threats mentioned in section 2.3, the security administrator must ensure the attainment of the following security properties [22,23,24]

- **Confidentiality:** To prevent the disclosure of information to unauthorized parties.
- **Integrity:** To protect the data from unauthorized modifications.
- **Availability:** To ensure disruption-free network services.

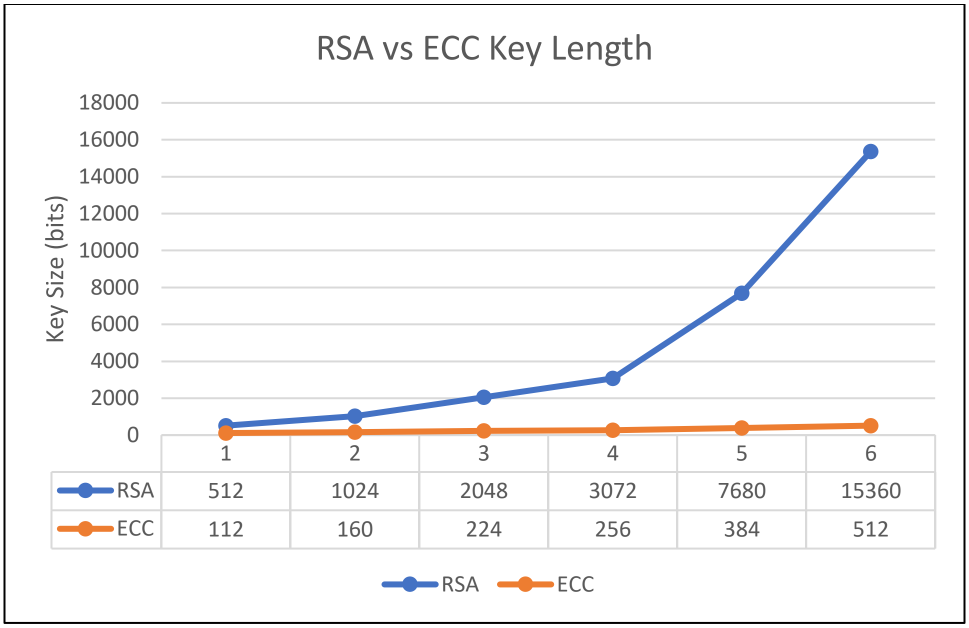
- **Anonymity:** To keep the identity of the communicating entities private.
- **Untraceability:** To prohibit the trace of the message journey, i.e., origination and destination.
- **Freshness**: To ensure newness in the information.
- **Key Security**: To keep the session keys confidential.
- **Mutual Authentication**: To verify the authenticity of each other before establishing a secret key.

These properties can be accomplished by using cryptographic tools like ciphering, keyed hash functions, message authentication code, digital certificates, etc. [25,26]. However, these mechanisms are difficult to implement in VANET due to limited resources like limited computation power, storage, and limited battery life [27]. One of the possible solutions is to process the compilation in an external node and post-processing store the information like keys etc. in the VANET. But still is challenging due to limited storage. The other possible solution is the use of cryptography protocols to secure the session in the VANET [28,29,30]. Vehicles can perform the mutual authentication and use of the decentralized network with the help of blockchain and smart contracts which is described in the section

2.5 Implicit Certificates

To verify the authenticity of each other before the connection establishment digital certificates are very useful. Identical to X.509 explicit certificates, implicit certificates are composed of (a) identification data (b) public key, and (c) digital signatures [25]. For user identification, public key is used to verify the trust between third parties. In explicit certificates, digital signature and public key are the two different elements whereas in implicit they are included to save the bandwidth requirement.

The advantage of implicit certificates over conventional X.509 certificates are rapid computation, the small size of the certificate, and low computation power [31]. Figure 2.1 depicts the comparison of symmetric and asymmetric key size requirements to attain the same level of security. Moreover, it is clear from the figure ECC has fewer key size requirements to attain the same level of security as compared to RSA [32].



	1	2	3	4	5	6
RSA	512	1024	2048	3072	7680	15360
ECC	112	160	224	256	384	512

Figure 2.1: Key length comparison [32].

2.6 Mutual Authentication and Key Establishment

It is the process to protect the network from malicious nodes. It is performed before the key establishment process to allow the legitimate nodes to negotiate a security key and access the security key and access the authorized resources. This technique should be robust enough to protect the users from network attacks. The existing agreement protocols incur a high computation cost. But due to high mobility and less computation power in VANET, we cannot apply the conventional protocols. Therefore, we need to use smart contracts using blockchain to reduce the overhead and decrease the high computation and storage requirements [33].

2.7 Introduction to Blockchain

Blockchain is one of the popular technologies that is built upon a Peer-to-Peer system named Bitcoin [34]. Network peers have the same copy of the blockchain data and each copy cannot be modified. Moreover, it is using the public key to protect the user’s privacy and also to provide anonymity. Therefore, it provides a decentralized, transparent, tamper-proof, and secure data storage environment.

Block is the basic unit of blockchain and is responsible for recording the valid transaction information confirmed by each peer in the network. Figure 2.2 describes the structure of blocks. It consists of a block header with metadata and a block body with transaction data. The Block header contains three sets of metadata:

- Hash of the previous block
- Timestamp, the difficulty of mining, and Nonce (random number)
- Merkle root

In the consensus process, various consensus algorithms have been proposed [35], such as PoW (Proof of Work), PoS (Proof of Stake), DPoS (Distributed Proof of Stake), and PBFT (Practical Byzantine Fault tolerance), Ripple, Tendermint, and Paxos, etc.

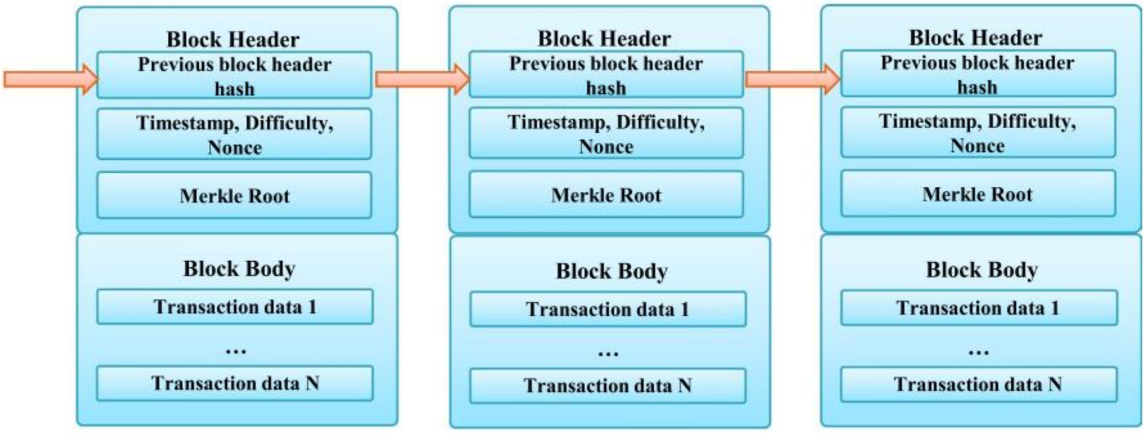


Figure 2.2: Data structure of blocks.

Some typical applications of different consensus algorithms have been shown in Table 2.1. Initially, the bitcoin system was just used to enable the exchange of cryptocurrencies and did not use smart contracts. Smart contracts are the trusted digital contracts generated by Sbazo [36]. The main feature of smart contracts is that the rules are made in advance and executed automatically. Recent platforms like Ethereum [37] and Hyperledger have smart contract programmability, and people can deploy many different applications on them.

According to the network access control mechanisms, blockchains are divided into three types:

- **Public Blockchain:** In a public blockchain everyone can access and read the chain. Moreover, everyone can send transactions and participate in the consensus.

- **Private Blockchain:** Limited nodes can participate in a private blockchain. This type of chain has strict management access control.
- **Consortium Blockchain:** This type of chain is also known as a partially decentralized chain. Some nodes have authority in advance to participate in the consensus.

Table 2.1: Applications of consensus algorithms.

Consensus Algorithms	**Applications**
PoW	Bitcoin, Litecoin, Ethereum
PoS	Ethereum, ADA
DPoS	Bitshare
PBFT	Hyperledger
Ripple	Ripple
Tendermint	Tendermint
Paxos	Google Chubby

Public blockchains apply to the systems where public participation and transparency are required. The miners participate in the consensus to earn the rewards based on the complexity to solve the computational problem. The data in the private blockchain is invisible and have a faster speed of transaction.

There are some other classifications of blockchain also named Permission blockchain [38] and hybrid blockchain [39]. When the node needs permission to join the blockchain then there is a role of permission blockchain. The private and consortium chain belongs to this category. A hybrid chain is developed after the development of public and private chains.

2.8 Several attacks on Blockchain

Blockchain architecture is with immutability and distributed architecture. But the new age of security attacks is emerging, which are sophisticated and can cause irreparable loss. Some of the attacks on the blockchain are discussed as follows [14]:

2.8.1 Sybil attack

In this type of attack, the attacker floods the network with a large number of nodes with pseudonymous identities and tries to influence the network. These nodes are unrelated and operated by a single individual. The objective is to target several nodes or networks as a whole and generate the fork in the ledger if possible so that double-spending and some other attacks can be performed over the chain.

2.8.2 Selfish mining attack

Most blockchains consider the longest chain as the truly latest version of blockchain. An attacker may try to build the blocks on the top of the existing chain in stealth mode so that he can publish his private fork which can be accepted as a new truth as it is the longest chain. By doing so he can do the transactions on a public chain.

2.8.3 Finney attack

If the attacker can mine off the block and put one of the transactions and keep it in stealth mode so it can be used for a double-spending attack. If any merchant accepts the unconfirmed transaction, you can transfer him the earlier transacted currency. Now he can publish the mined block which was kept in stealth mode.

2.9 Features of blockchain

Through the above analysis which is described in related work about VANET, it is concluded that to provide security and privacy to the network more scalable and more reliable network is required. The following features of blockchain can solve these issues described as follows [41]:

- **Decentralization:** Every node has been given equal kind of rights. No node has control over other nodes. If any node stop working it does not impact the overall VANET network.
- **Transparency:** There is no requirement to establish a trust relationship among the nodes because the whole system is open and transparent. It means no node can break the trust for any illegal activities.

- **Collective maintenance:** All nodes are having equal rights so they can be used for maintenance.
- **Reliable database:** It is not possible to tamper with the data in the blockchain because all the network nodes have the same copy of the blockchain ledger. So, if anybody tries to modify the data it can be compared easily with the blockchain data and hence cannot be modified.
- **Automation:** Smart contracts can execute the code automatically. There is no human intervention required to execute the agreement.

Chapter 3

Related Work

To provide security and privacy to the communication between vehicles, several schemes have been proposed. Each scheme has its own merits and demerits. This chapter briefly covers the paradigm, complexities, primitives, and deficits of conventional schemes. In the last, a tabular summary is provided for a clear understanding of the research gaps that need to be filled through the development of the proposed scheme mentioned in this research.

3.1 Overview of Conventional Schemes

So many researchers have contributed a lot of research work in the area of centralized trust management in recent years. Central servers are used to collect, measure and store the trust values of all vehicles, and are believed to be a fully trusted entities not compromised by an attacker [41,42,43]. Vehicles notice traffic-related incidents and issue notices to neighbors. Vehicle feedback is obtained from a centralized reputation-based server. Based on these results, the server can issue certificates based on their credibility values.

In [44] authors have proposed Public Key Infrastructure (PKI) which generates large overhead and cost. This also uses a centralized approach toward vehicular networks which can be proxied and compromised. Moreover, centralized systems have all the processes dependent on the central server. A dynamic key distribution protocol based on PKI is implemented in which vehicles can communicate with each other and keys are obtained from the Certificate Authority (CA) through RSU, which is reducing the load on vehicles. The load has reduced on vehicles but still, the problem of centralization persists [45].

In [46] authors proposed a Secure and Authenticated Key Management (SA-KMP) algorithm based on key agreement protocol which ensures the communication between the vehicles and RSU. The repository has distributed between the entity’s identity and to each vehicle using its corresponding public key. The certificate revocation has been eliminated by distributing the repository which was not done earlier in PKI systems.

Key agreements and digital signatures can be used to ensure the communication security and privacy protection of vehicles. The anonymous certificate method is also proposed to remove the certificate management problem which increases the efficiency of the authentication process. But the problem is still the central dependency. The vehicles can obtain the certificate from its passing RSU and therefore there is no need to check for the certificate frequently which improves the efficiency of authentication. But there is no experimental plan discussed for analyzation of complex networks [47].

Simulation and punishment mechanisms are also shown [42]. In this, the concept of micropayment has been shown. Honest nodes can earn a certain amount of credits, which they can spend on relaying the packets. If any node with a greater packet drop is identified by the receiver, it will be evicted from the network. With the evident increase in the number of vehicles, it is not possible to cope with all nodes using centralized systems. Moreover, if the central system fails, the entire system's failure can be possible.

Blockchain is a very recent technology that also provides the concept of decentralization. A blockchain-based crowdsourcing program introduced by [48] is used to apply for court adjudication. In [49,50] proposed blockchain-based crowdfunding is shown that is a different form of crowdsourcing. In addition, [51] developed a distributed storage and keyword search based on blockchain. The public keys of the entire network are stored in this paper's blockchain. Therefore, blockchain helps to design a trust-based decentralized and tamper-proof network for vehicular networks. It has been summarized that PoW and PoS are the consensuses that are widely used in permissionless blockchain. Tendermint is the open-source consensus protocol that can solve the problem of Byzantine fault tolerance.

The consensus is a part of distributed computing. An agreement is reached between a distributed number of processes [52], and a popular consensus scheme is called Byzantine fault tolerance (BFT). This type of protocol is used to secure the network from node failure. Practical Byzantine fault tolerance (PBFT) [53] is one of the more well-established BFT algorithms since it is based on three rounds before the actual agreement. This ensures that 3f+1 nodes are necessary to reach a consensus if we have f Byzantine nodes [53].

In [54], the author discusses well-known families of consensus algorithms for both permissionless and permissioned blockchains, which include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Burn (PoB), etc. Next-generation deployment has been carried out and the quality of services (QoS) has been discussed [55]. QoS plays a very important role in vehicular networks which defines how much efficient is the network is presented [56]. It consists of packet delivery ratio, end to end delay and the throughput has also been discussed in results analysis [57,58,59].

The self-mining process consumes much amount of power as described [60]. The decentralized key management mechanism has been proposed, which is a lightweight mutual authentication scheme used to prevent many network attacks [61].

Blockchain architecture is used to prevent many network attacks due to its tamperproof environment, and it provides more security to transactions. Moreover, these transactions are transparent on blockchain [62,63].

The distributed consensus in the blockchain creates trust between multiple parties and is referred to as Byzantine consensus. Byzantine consensus is still a research field and is backed by recent advances in blockchain technology. The consensus is broadly divided into proof-based and voting-based. In the proof-based category, bitcoin is the popular one that uses PoW, which requires the miner to solve a difficult problem, and it requires a large number of resources. Moreover, the transactions are very slow, at nearly seven transactions per second. PoS uses stake to determine the mining difficulty, which can be determined as proof for the voting [64].

The proof-based mechanism provides consistency in the network but suffers from a lower transaction rate and large resource consumption. The novel VANET system model using edge computing is implemented, and it uses an individual session key for each vehicle to prevent interference [65,66]. The RFID-based mechanism provides better authentication and prevents many network attacks, and it uses elliptic curve cryptography to secure the session [58]. Moreover, the Telecare medical information system also used the ECC mechanism for preserving the anonymity of the user, and this is suitable in cryptography [67]. Even to secure the localization, the same trust-based mechanism is used in a wireless sensors network, which is based on decentralization [66].

Ring signature and identity-based encryption are also proposed to authenticate the communication between vehicles. Wei et al. proposed a fog-based privacy protection scheme that improves the security of the crowded vehicular network. Fog user identity is anonymous during identity authentication. Central dependency is reduced by proposing the blockchain-based architecture with the Internet of Vehicles [68].

The voting-based consensus is more useful for the permissioned blockchain customer because knowing your customer's methodology nodes will help achieve a consensus over multiple rounds of collective voting. The popular project Hyperledger fabric [69] uses PBFT in its 0.6 version, and R3 Corda employs BFT-SMaRt [70], which is identical to PBFT.

This author proposed Distributed Key Generation (DKG) scheme based on the Ethereum blockchain implemented as a smart contract and using secret sharing to realize DKG. The core building block of blockchain technology is the consensus protocol. In these, we have to rely on a single centralized entity for the necessary protocol setup. But DKG provides us the flexible means for the VANET network for the registration and faulty behavior of the vehicle. Ethereum smart contracts rely on trusted third parties and which is used for the automated registration and participation of the vehicles in communication [71,72]. In the IoT area, [73] proposed a scheme using Diffie Hellman Key Exchange (DHKE) to secure the exchange of data in sensor networks.

Blockchain-Based Trust Management Systems (BARS) used a reputation score-based mechanism which determines the credibility of a vehicle based on historical interactions [74,75]. An authentication and revocation framework for VANETs is also proposed for preserving the privacy of the vehicles but it is failed to address the security [76]. Crypto trust point (cTp) for securing the data among the vehicles has also been proposed [77]. These are not addressing privacy concerns and are focused on securing the data only.

Computational overhead can be reduced [78] by using Mobile Edge Computing (MEC) to offset resource consumption. But edge computing does not make it truly decentralized and it is dependent still on a central server. Reward-based blockchain is also proposed using a unique crypto ID assumed to be issued by the vehicle for safe communication. It is a trust bit system that is using proof of stake consensus which is used to give the rewards if the vehicle is genuine [79]. Consortium-based blockchain generates the data sharing and storage platform but generates more overhead [80]. Dynamic key management is also discussed for heterogeneous ITS systems. These all are schemes focused only on security, not on the privacy of vehicles.

Ethereum is a secure generalized decentralized system built on smart contracts which is better than the bitcoin network in terms of power and resource consumption [81]. Inter-communication between the vehicles can be secured by encryption algorithms. Zhou et al. proposed the method for encryption and authentication which consumes 83% less time as compared to the traditional public-key encryption method [82]. Automated validation of Internet Security Protocols and Applications (AVISPA) provides a modular and expressive formal language for specifying protocols and it is a robust and efficient method used for security verification [83]. Some authentication and privacy solutions also exist for the Industrial Internet of things which is based on biometrics-based which reduces the overhead and some large computations and it is based on cloud computing. The formal security verification is also performed to prove that the session is secured from attacks [84].

We know that real-time data is very important these days and which can be fulfilled by unmanned vehicles i.e. drones. So, to provide security to the drone, a lightweight authentication scheme is proposed which needs to access the data from the drone directly [85] [86]. For a better understanding of the limitations of previous work carried out in the same area, you may refer to section 1.4 in chapter 1.

3.2 Summary of Conventional Schemes

In summary, most of the conventional schemes are insufficient as they are not considering the reasonable threat and security model with low latency and less communication cost. It is evident from Table 3.1 that conventional schemes are vulnerable to the most common threats like a man in the middle, DoS, known key, etc. In addition, Table 3.1 also provides detailed insights into various aspects including the cryptographic primitives, application, communication cost, threats, latency, etc. These concerns make the conventional schemes unfit for the resource-constrained applications of Adhoc networks. Thus, there is a necessity for authentication while preserving privacy with a tamperproof environment comes up. This provides a decentralized environment with lesser communication costs and improved Quality of Services (QoS).

Table 3.1: Review of existing schemes.

Scheme	Cryptographic Primitives						TB	D	C	Applications	T	CC	LT	NASP
	SC	AC	CB	PW	ID	Hash								
[41,42,43]		✓				✓				MANET, VANET	1,3,5	H	M	III, IV
[44,45]		✓				✓				MANET, VANET	1,3	H	M	III, IV
[46]		✓	✓		✓	✓				MANET, VANET	1,3	H	H	III, IV
[47]	✓		✓			✓				MANET, VANET	3	M	M	I, III, V
[48,49,50]		✓				✓	✓	✓	✓	VANET	1,3	M	H	I, VI
[54]						✓		✓	✓	VANET	6,7	M	H	I, VI
[61]	✓			✓		✓		✓	✓	VANET	7	M	M	I, VI
[64]		✓				✓	✓	✓	✓	VANET	2,7,8	M	M	I, VI
[58,67]		✓			✓	✓	✓	✓	✓	VANET	2,7,8	M	H	I, VI
[68]	✓				✓	✓	✓	✓	✓	VANET, IoV	6	M	H	V, VI
[69,70]		✓			✓	✓		✓	✓	VANET	7,8	H	H	V, VI
[71,72]		✓		✓		✓		✓	✓	VANET, IoT	7,8	M	M	I, VI
[74,75]		✓	✓			✓	✓	✓	✓	VANET, IoT	6,7,8	M	M	I, VI
[78]		✓			✓	✓				VANET	1,4,5	L	H	I, III, V, VI
[81]		✓		✓		✓		✓	✓	VANET	2,6,7	M	M	I, VI

SC: Symmetric Cryptography, **AC:** Asymmetric Cryptography, **CB:** Certificate Based, **PW:** Password Based, **ID:** Identification Based, **TB:** Trust Based, **D:** Decentralized, **C:** Consensus, **MANET:** Mobile Adhoc Network, **VANET:** Vehicular Adhoc Network , **IoT:** Internet of Things, **IoV:** Internet of Vehicles, **T:** Threats, **1:** Denial of Services, **2:** Man in the Middle Attack, **3:** Known keys, **4:** Modification of messages, **5:** Node Compromise, **6:** Sybil Attack, **7:** Distributed Denial of Services, **8:** Selfish Mining Attack **CC:** Communication Cost, **H:** High, **M:** Moderate, **L:** Low, LT**:** Latency **NASP:** Non-Accomplished Security Properties

3.3 Summary and Comparison of Conventional Schemes

Table 3.2: Comparative analysis of routing protocols in VANET.

RP	AR	OP	F	AE	Metrics Used	Simulators for Evaluation	Delay in Seconds	%age Delivery Ratio
DSDV [15]	Adhoc	Based on topology	U	Urban	hop count, mobility, lifetime and density of nodes	SUMO [50], NS2 [52]	0.25s (250 nodes), 0.8s (50 nodes)	70%
DSR [16]	Adhoc	Based on topology	U	Urban	hop count, mobility, lifetime and density of nodes	SUMO [50], NS2 [52]	0.30s (250 nodes), 1.3s (50 nodes)	85%
AODV [17]	Adhoc	Based on topology	U	Urban	hop count, mobility, lifetime and density of nodes	SUMO [50], NS2 [52]	0.35s (250 nodes), 1s (50 nodes)	88%
UMB [18,19]	Infra structure	Dissemination	B	Urban	link availability, no. of hops and link reliability	SUMO [50], NS2 [52]	0.5s (250 nodes), 1.2s (50 nodes)	73%
GNP [28,30]	Geography	Based on location	B	Urban	Link availability, no. of hops and jitter	-	-	-
GP [29,32]	Geography	Based on location	B	Urban	Position, velocity and direction	SUMO [50], NS2 [52]	1s (100 nodes), 0.05 s (140 nodes)	30%

RP: Routing Protocol, **AR:** Architecture, **OP**: Operation, **F:** Forwarding, **AE:** Area Evaluated, **DSDV:** Destination Sequenced Distance Vector, **DSR:** Dynamic Source Routing, **AODV:** Adhoc On Demand Distance Vector, **UMB:** Urban Multihop Broadcast, **GNP:** Geo Networking Protocol**, GP:** Greedy Perimeter, **U:** Unicast, **B:** Broadcast, **SUMO:** Simulator for Urban Mobility, **NS2:** Network Simulator 2

In summary, we have compared the routing schemes which has been already discussed in the literature and compared them all based on architecture, metrics, operation, and QoS. It is found that proactive schemes are not that useful because RSU needs high computation due to the large overhead released. But reactive protocols are better to apply for the normal routing operations because of less overhead, though latency is more in that case. Table 3.2 shows the comparison of all the routing schemes used in the literature.

Chapter 4

Blockchain Based Trust Model using Tendermint in Vehicular Adhoc Networks

The Vehicular Adhoc Network (VANET) is a sub-class of the Mobile Adhoc Network (MANET), which is deployed on the road to make the transport system intelligent. Vehicular communication uses onboard sensing and computation [87,88], as shown in Figure 4.1.

Even smart vehicles want to communicate with each other, and this is the basic key in the fifth-generation network (5G) [89,90]. However, due to high mobility and the dynamism of the network, we cannot trust every vehicle. The malicious nodes can enter the network and spread false information in the network, which leads to the failure of the vehicular network. For example, a malicious node can broadcast a message that there is an accident on a road, claiming congestion, but there was no accident and traffic congestion. These types of misbehavior produce risk in the vehicular network. Therefore, trustworthiness is an important factor to deal with, which is a critical issue in the network [89].

In distributed systems, a byzantine consensus is used to exchange information between the vehicles using trust management [52]. The vehicular network helps to provide information about road accidents, traffic congestion, road conditions, etc., and this helps the vehicles to be aware of the critical situations, thus improving transportation safety [41,91].

The trust management program allows vehicles to determine whether or not the received message is reliable [92,93]. Normally, the vehicle’s trust value can be determined based on the ratings produced by the vehicle’s past behavior. Trust management can be categorized into two classes, i.e., centralized and decentralized [42,43]. Centralized systems store confidence values on the central repository, e.g., the cloud repository. These central systems cannot fulfill the stringent quality of services (QoS) specifications because every time node has to ask the central server to test the trust value, which increases the latency of the network. Trust management is to be conducted at the vehicle or RSU level in decentralized trust management systems so that the burden of interaction with the server is reduced to a great extent, which ultimately increases the efficiency of the system [94,95,96]. Moreover, we cannot rely on one node for trust management. Due to the dynamic network, it is difficult to trust each node for the ratings. Therefore, designing an effective decentralized network is still a challenge [96]. In [54], the authors have discussed the families of consensus for the permissioned as well as permissionless blockchain which has been described in the literature.

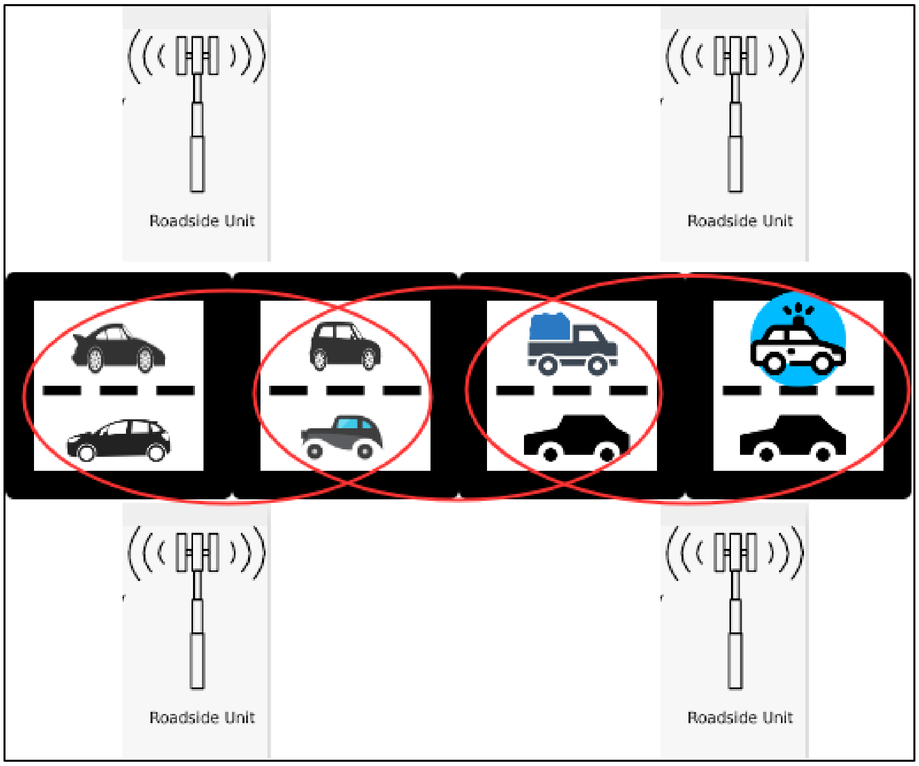


Figure 4.1: Architecture of vehicular adhoc network (VANET).

The proposed system works effectively by retaining the trustworthiness between the nodes in vehicular networks. The internet of vehicles, using big data, is also a trending area, and which explored by game theory, i.e., coalition games for spatial-temporal big data on the internet of vehicles, where the vehicles will be rewarded and penalized according to game rules [97]. Blockchain is one of the innovations in the financial sector that establishes a clear and tamper-proof ledger without centralized banks, so people can transact with absolute trust [98,99]. Therefore, due to the design of the blockchain's trust management system, it can be conveniently carried out between nodes with decentralized systems [100]. Automated-based contention-aware data forwarding has also been proposed, which is based on Bayesian coalition game theory, which improves the routing parameters of VANET [98,101]. The trust between the multiple parties can be generated with the help of Byzantine consensus [64,102]. Due to its high security, blockchain has been commonly used in the non-financial market, i.e., content delivery, key management [103], decentralized storage [104,105], etc. Some popular projects like Hyperledger can also be used as an application of byzantine fault tolerance [69,70]. A blockchain based crowdsourcing program is also defined for court adjudication [48]. The block generation undertaken by the attacker is slow as compared to the normal RSUs, due to the issue of trustworthiness. The benefit of using the cross-blockchain through Tendermint is the interoperability between blockchains, which also reduces the latency and improves the transaction speed. The existing technique has worked on the proof of work consensus, which is not at all a power-efficient method. In the proposed method we have implemented the decentralized cross-chain Tendermint protocol, in which the transaction speed is greater, and this allows us to use and send the data on any blockchain. The existing study has only shown transactions and ratings, but we also worked on the quality of services and calculated the effect on QoS. Voting-based consensus uses less power as compared to the existing study [106,107].

4.1 Our contribution

- A decentralized trust management system has been proposed based on blockchain technology, which permits all the vehicles and RSUs to update the trust value in a decentralized manner, and the active participation of all vehicles and RSUs for the updating procedure.
- We have proposed a proof of authority (PoA), which is better than proof of work (PoW) and practical Byzantine fault tolerance (pBFT), because of the high energy consumption and greater overhead, respectively.
- We have proposed a system model and conducted a simulation which proves that our proposed model is efficient in practical vehicular networks.

4.2 Proposed Approach and System Model

In the proposed system, the system model consists of the following components, as illustrated in Figure 4.2.

4.2.1 Road Side Unit

Roadside units are used to communicate with the vehicles running on the road, and give information and updates about the route. This acts as a bridge between the trusted authority and end-users. Moreover, RSU is also responsible for some of the major tasks, i.e., the collection of ratings and trust value management.

4.2.2 On-Board Unit

This unit is used to broadcast traffic-related information periodically. The information contains speed, multimedia, and the updating of the direction for traffic movement.

4.2.3 Trust Value Management

We assume that the RSUs can calculate the trust values by aggregation of the ratings received from the different vehicles. So, the credibility of the message is judged by the aggregated value of the rating and can be fetched from the trust value management servers [106].

4.2.4 Main Procedures

The proposed model procedure is divided into three parts, as described in Figure 2.

Step 1: Rating generation and uploading

This is the first step toward the decentralization of trust management in a vehicular network. This is the procedure that has to be conducted on vehicles. Some specific rules are required to assess the credibility of the messages and to generate ratings. The messages are divided into groups $\{M1, M2, \dots\dots\dots M_j\}$, where M_j represents the group reporting event, e.g., an accident that happened in one road segment R. All messages have different values of ratings calculated by the RSUs. The vehicle which is near to the event will have more rating value because it is close to the event and will be exactly aware of whether the event happened or not. Therefore, the credibility of a certain message is defined as follows [106]:

$$c_k^j = b + e^{-\gamma d_k^j} \tag{1}$$

where c_k^j is the credibility of the message in group Mj sent by vehicle, d_k^j is the distance between the sender and the location of the event. b and γ are two preset parameters, which control the lower bound and the rate of change of message credibility. Moreover, c_k^j = 0, if k does not report this event. The receiver can obtain a credibility set C^j for event e^j using Eq. (1), where $C^j = \{\, c_1^j, c_2^j, \ldots \ldots \}$. Based on credibility set C, the receiver is able to calculate the aggregated credibility of event e using the gradient boosting technique [107].

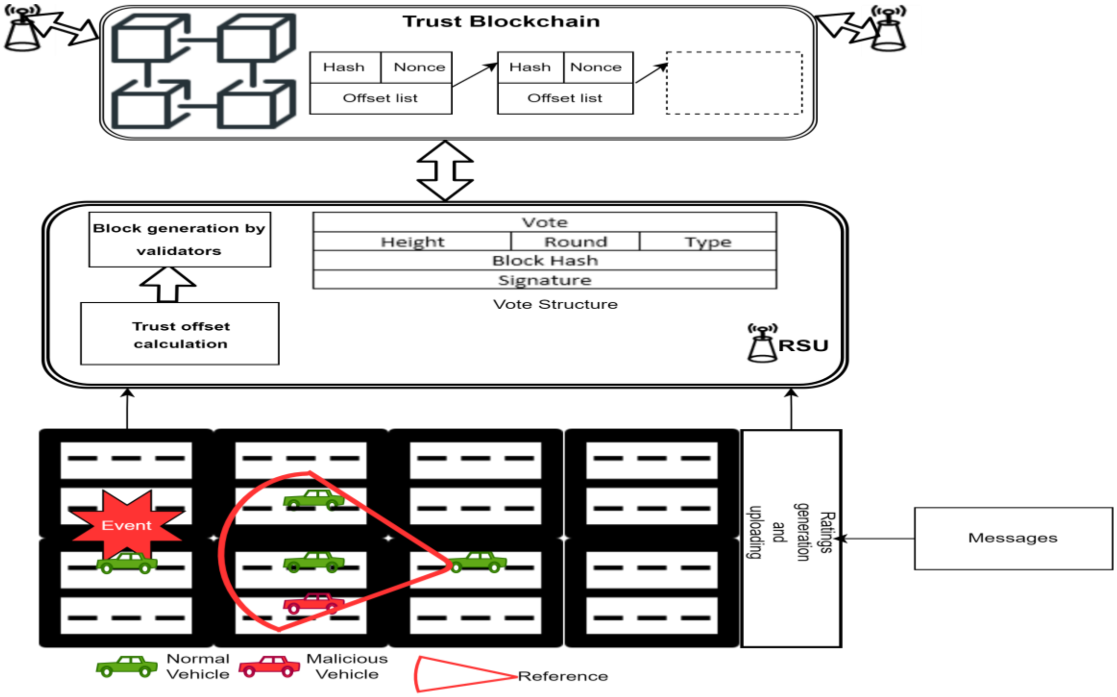


Figure 4.2: Proposed blockchain-based system model for trust management system.

The gradient boosting technique splits the input space into T_m disjoint regions, such as R_{1m}, $R_{2m,}\ldots R_{Tm}$, and then predicts a vehicle with a lower trust value in each region. Here, T_m represents the number of leaves in a tree. Therefore, this is the output of gradient boosting. Thus, the output of the gradient boosting tree is $h_m(x)$ for input x (x indicates the mobile node with trust value), and this is represented mathematically as follows:

$$h_m(x) = \sum_{T=1}^{T_m} b_{tm}\ I\ (x \in R_{Tm}) \tag{2}$$

From Equation (2), b_{tm} denotes the predicted mobile nodes, which consist of lower trust values in the tree. After that, the coefficients b_{tm} are multiplied by a random value γ_m in order to remove the lower trust value mobile nodes in the VANET scenario. So, the updated model is described below:

$$F_m(x) = F_{m-1}(x) + \ \gamma_m h_m(x) \tag{3}$$

$$\gamma_m = \arg\min_{\gamma} \sum_{i-1}^{n} L\ (y_i\,, F_{m-1}(x_i) + \gamma_m h_m(x_i) \tag{4}$$

Using Equations (3) and (4), the lower trust values from the vehicular network will be removed by RSU. Finally, the nodes with higher trust values will be retained by the given formula,

$$F_m(x) = F_{m-1}(x) + \sum_{T=1}^{T_m} \gamma_{T_m} I(x \in \ R_{Tm}) \tag{5}$$

$$\gamma_{T_m} = \arg\min_{\gamma} \sum_{x_i \in R_{Tm}}^{n} L(y_i\,, F_{m-1}(x_i) \tag{6}$$

The RSU may have differences in ratings produced by similar messages, e.g., nine positive and three negative ratings. The former is a majority group, and the latter is a minority group. In the proposed methodology, weighted aggregation solves the problem of ranking conflicts. The offset is between –1 and +1 (normalized value), which is positively associated with the positive rating ratio in this message. The estimation of the offset value of the trust is shown in Equation 7.

$$\sigma_k^j = \frac{\theta_1.m - \theta_2.n}{m+n} \tag{7}$$

where σ_k^j is the trust value offset of vehicle k based on message j and $\sigma_k^j \in [-1,1]$. m and n are the number of positive and negative ratings, whose weights are θ_1 and θ_2, respectively. θ_1 and θ_2 are determined using Equations (8) and (9), respectively.

$$\theta_1 = \frac{F(m)}{F(m)+F(n)} \tag{8}$$

$$\theta_2 = \frac{F(n)}{F(m)+F(n)} \tag{9}$$

where $F(.)$ controls the sensitivity of the minority group of ratings, e.g., $F(x) = x^2$ is less sensitive to the minority group of ratings compared with $F(x) = x$. This strategy has been carried out under the premise that the intruder cannot dominate the majority group. The proposed weighted aggregation is therefore in a position to boost the reliability of the trust value offsets.

Step 2: BFT based consensus for transaction between vehicles

PoW cannot deter the participants from performing selfish mining [60]. If we choose the PoS, we can remove the problem of energy consumption, and speed can also be increased. The joint proof of work and the method for creating a block takes the number of absolute offsets as a stake, and the complexity of it is dependent on the RSU which has more stakes, and can quickly locate the nonce and win the mining election [106] and will publish the block faster as compared to PoW alone, but PoW and PoS both are the mechanisms used for permissionless blockchain, which is more vulnerable to network attacks. So, we want to introduce here the permissioned blockchain consensus in our proposed model, which is more secure than the permissionless blockchain. The proposed block generation method is based on validators and voting power, i.e., Tendermint (consensus without mining).

1. Validators Every node has the same weight in the BFT process. In Tendermint, nodes with a non-negative sum of voting power and nodes with positive voting power are considered as validators. Such participants participate in the consensus through the transfer of signatures and votes to the next generation of blocks.

2. The system model Tendermint consists of three steps (Propose, Prevote, Precommit), and two special steps (Commit and NewHeight).

Obtaining more than two-thirds of the commitment requires obtaining commitments from a total of two-thirds of the validators. When commitments for this block have been signed and transmitted by two-thirds of the validators, the block is said to be dedicated by the network. The vote structure is shown in Table 4.1.

Table 4.1: Vote structure.

Vote		
Height	Round	Type
Block hash		
Signature		

The three steps that we mentioned take one-third of the total allocated time. Every round takes more time as compared to the previous round so that consensus is achieved and the block generates. The proposer is chosen in a round-robin fashion in each round so that the validators are chosen in proportion to their voting power with frequency. The structure of the proposer is shown in Table 4.2.

Table 4.2: Proposal structure.

Proposal	
Height	Round
Block	
Proof of Lock	
Signature	

The first step is Proposal, in which the proposer transmits a proposal by gossiping to their peer. When a proposer is locked into a prior process, the initiative proposes a proof-of-lock.

In Prevote each validator is determined. If the validator is locked on to any previously proposed block, it will sign and broadcast a locked block prevote. If no block has been sent by the validator then it sends a null prevote.

Each validator makes the decision at the beginning of the Precommit phase. The validator signs and transmits a precommit for that block if it has received more than two-thirds of the prevotes for a similar appropriate block. If the node receives two-thirds null votes, then it simply unlocks the block. Each node decides at the end of the Precommit phase. If more than two-thirds of the precommits have been received by the node, then it is entered for the Commit stage. Otherwise, it will start with Propose in the next round. The Commit step is a very important step here, in which two parallel conditions need to be checked before finalizing the round. First, the node will obtain the block that the network has committed. Second, once received and signed by the validator, it broadcasts a commit for that block. All the workflow is shown in Figure 4.3, and we have considered that the elements are uniquely located. This is the one round of consensus for the generation of a block by the RSUs. In this way, RSUs can handle the malicious node if any is present in the network.

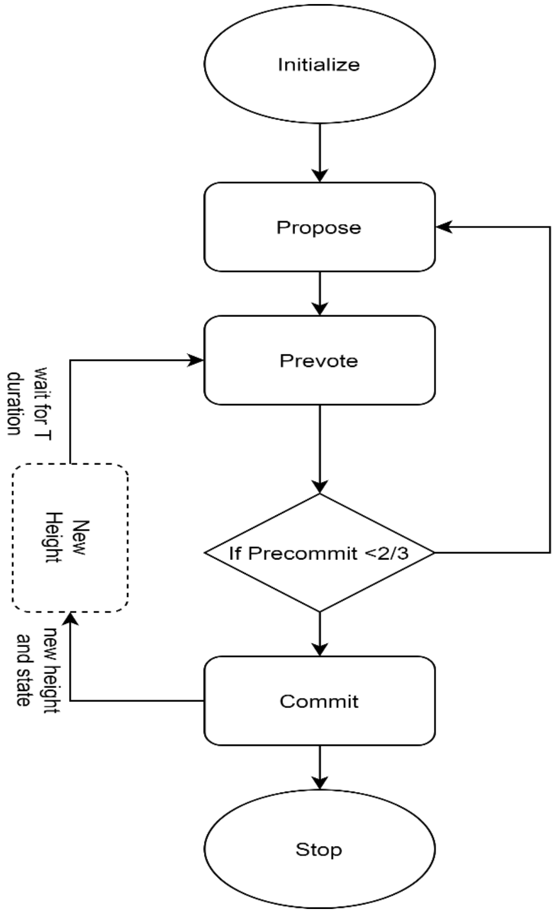


Figure 4.3: Consensus algorithm without mining used by Tendermint.

4.3 Simulation Parameters

To analyze the proposed approach, network performance analysis is selected. The proposed consensus scheme performance was also compared with the existing consensus scheme implemented on VANET. Simulator for Urban Mobility (SUMO) has been used for the vehicular setup, and the simulator parameters are as described in Table 4.3.

Table 4.3: Simulation parameters.

Parameter	**Value**
No. of Nodes	100
Maximum Vehicle Speed	40 m/s
Length of Vehicle	3 m
Width of Vehicle	2 m
Number of RSUs	7
RSU coverage	1 Km

4.4 Implementation and Results

The performance of Tendermint, considering the different numbers of nodes, is shown in Figure 4.4. In this, we have considered four scenarios in which 100 nodes are considered at the maximum, and it is also shown that Tendermint can process thousands of transactions per second, which ultimately increases the throughput level, and the delay of the system is reduced.

4.4.1 Performance Metrics

This section reflects the theoretical study and the feasibility of the consensus suggested in VANET. The network output is measured in terms of the packet delivery ratio, and the end-to-end delay. Evaluation of the results is achieved by running the simulation, and statistical analysis is conducted by averaging the collected values to a mean value.

4.4.2 Packet Delivery Ratio (PDR)

This applies to the ratio of packets received successfully to the cumulative number of packets transmitted across the network [56]. Mathematically, it is given by:

$$PDR = \frac{P_r}{P_s} \tag{10}$$

where P_r is the total number of packets received and P_s is the total number of packets sent.

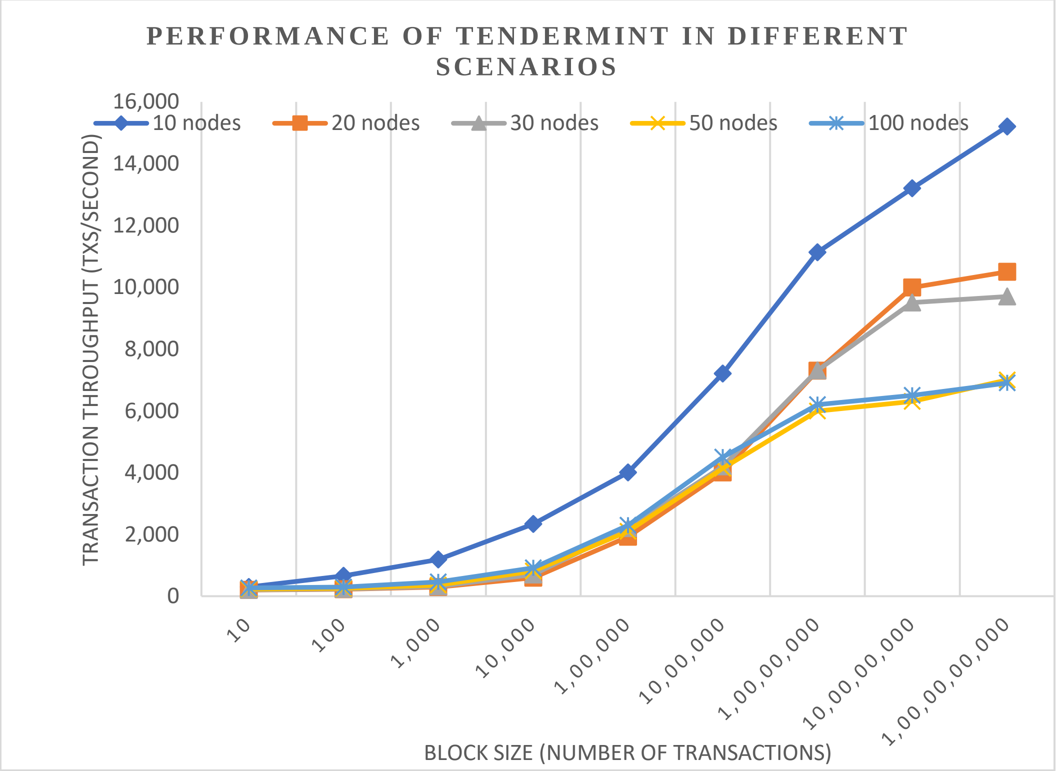


Figure 4.4: Performance of Tendermint.

Figure 4.5 illustrates the packet delivery ratio for the proposed consensus scheme, i.e., Tendermint incurred a higher PDR, improved by 7.8%, 5.6% and 2.4% compared to PoW, PoS and Hybrid, respectively.

4.4.3 End-to-End Delay

End-to-End Delay (EED) is defined as the time it takes for a packet to get from the source to the destination [57,65]. End-to-end delay impacts the PDR significantly on the network. Mathematically, it is given by:

$$EED = \sum T_A - T_S \tag{11}$$

where T_A is the arrival time of the packet and T_S denotes the sent time of the packet.

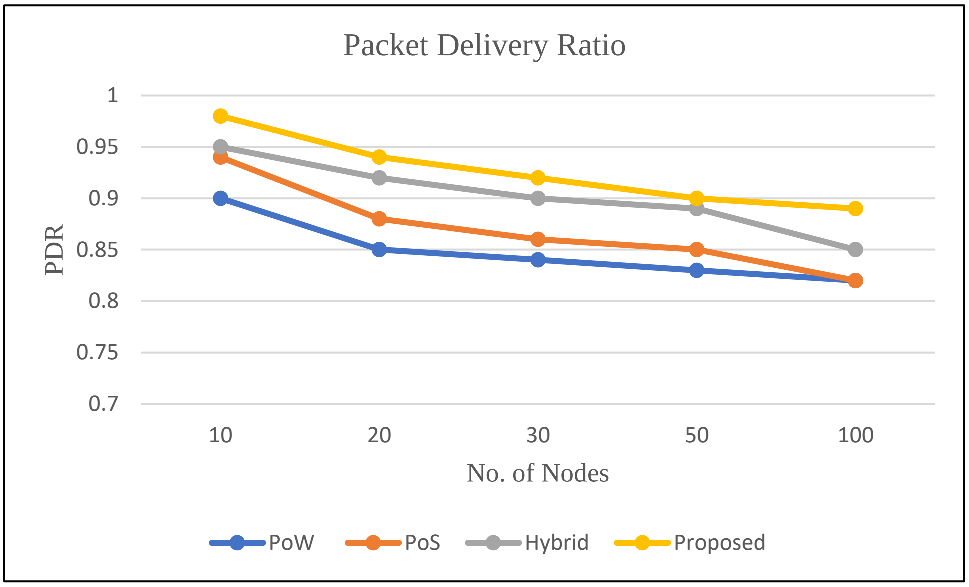


Figure 4.5: Packet Delivery Ratio.

Figure 4.6 shows the simulation results, and the proposed solution incurred low end-to-end delay, with a difference of 15.60%, 3.60% and 11.80% compared to PoW, PoS and Hybrid. The average delay in the case of the proposed scheme is 0.15 s, which is far better than other schemes, which are compared in Figure 4.6.

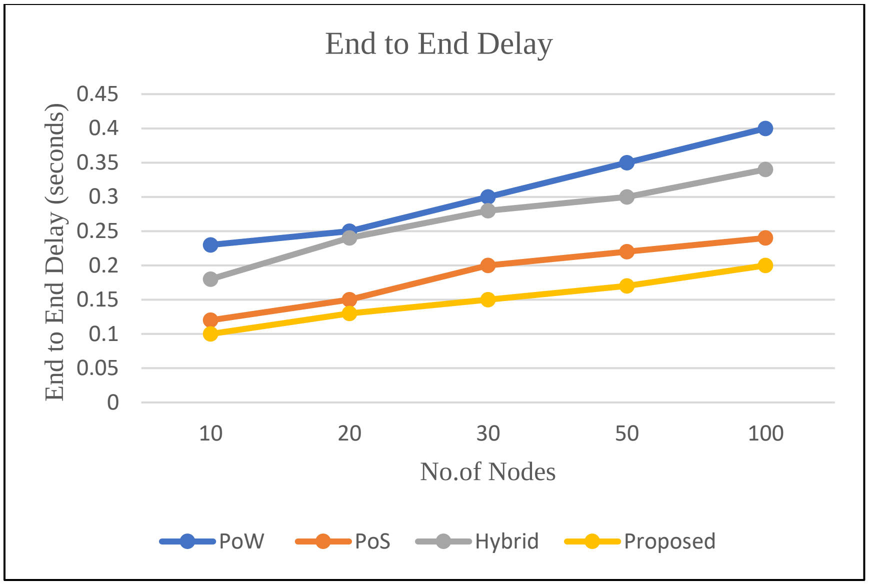


Figure 4.6: End-to-end delay.

4.4.4 Performance Analysis of Ratings

As we have already shown, the end-to-end delay is greater in the case of PoW, i.e., it is also reflected in the rating calculation. The latency is shown in Figure 4.7, and it is low, with a difference of 0.48 s, 0.44 s, and 1.46 s as compared to PoW, PoS and Hybrid.

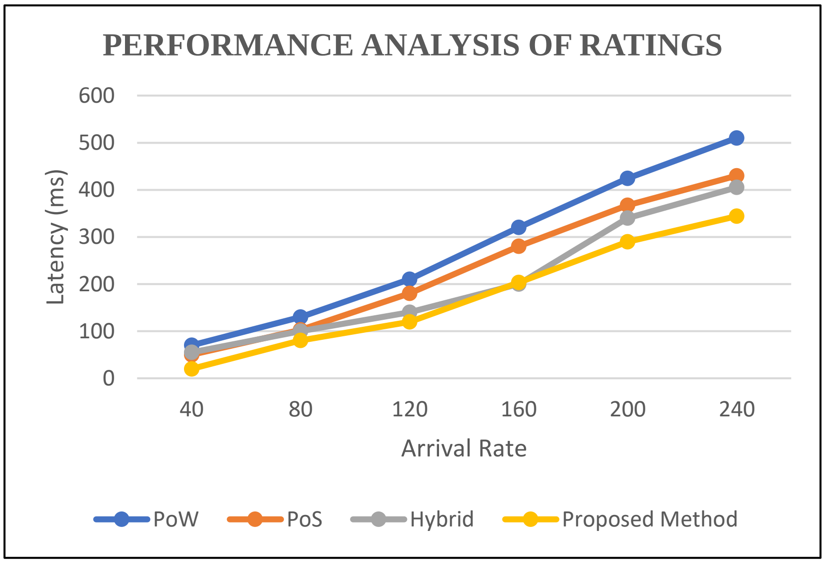


Figure 4.7: Performance analysis of ratings.

4.4.5. Comparative Analysis of Results

In this section we have analyzed and compared the results, and found that our proposed scheme is more efficient as compared to the literature [106]. Table 2, shown below, gives the comparison.

Table 4.4: Comparative analysis of results.

Consensus Scheme	Latency
PoW	15.60%
PoS	3.60%
Hybrid	11.80%
Proposed Scheme	3.65%

As the traffic increases, the load on the system will increase. The computation power of the RSU should be good enough to process a huge amount of data because the processors in the cars are not that powerful, and this is the reason we have given the computation role to the RSUs.

4.4.6. Performance Evaluation in terms of Security Analysis

We have analyzed the following performance metrics: communication cost and authentication delay. Communication cost is calculated based on the total number of vehicles using different variables used for the transmission of messages in the vehicular network. Communication cost is further calculated with respect to message authentication communication cost.

4.4.7 Message Authentication Communication Cost

Traditional Public Key infrastructure requires certificate and signature information for the message authentication. The total message size that is proposed by Zhang [82] is 257 bytes. Wang [76] has proposed a scheme which is using the 190 bytes message size. When we use the system with blockchain to 140 bytes as shown in Figure 4.8.

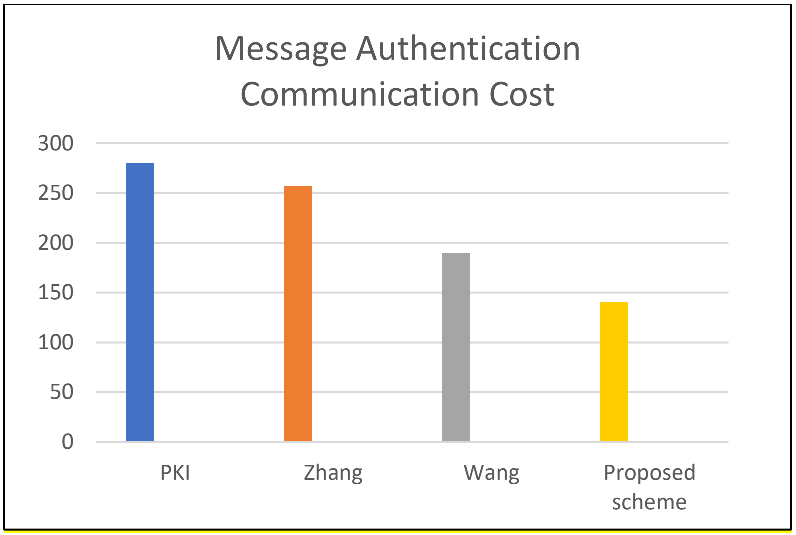


Figure 4.8: Message authentication cost.

4.4.8 Authentication Delay

PKI needs to check the certificate revocation table for authentication. But in the proposed system information is managed through the smart contracts and stored in blockchain which reduces the query time of the certificate. Wang [76] used two-way authentication through participation and Zhang [82] requires the proper participation of the CA. The proposed scheme has better efficiency and less latency due to the introduction of blockchain which will be locally performed on the nodes to reduce the delay as shown in Figure 4.9.

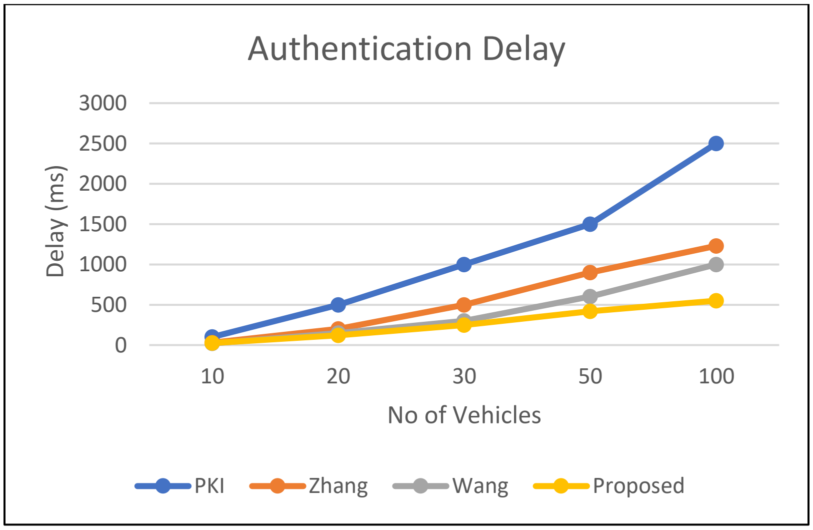


Figure 4.9: Authentication delay.

4.5 Theoretical Analysis

4.5.1 Free from Deadlock

This means that no node at any point in time will wait for another node. No node will wait for a separate node to transmit or accept a request, vote, start to validate a block or add a block to its line.

4.5.2 Message Spoofing Attack

This is when a malicious vehicle enters the system and tries to send fake messages about accidents on the road when there was no accident. This is called message spoofing. We propose the double layer mechanism here to defend against this kind of attack. The first layer will use the gradient boosting technique (GBT), based on machine learning mechanisms, able to provide trustworthiness between the vehicles. The credibility of the message is checked by the receiver, which analyzes the different messages and their ratings broadcasted on the network. Tendermint based on Byzantine fault tolerance acts as a second layer, using the permissioned blockchain, which is much less vulnerable as compared to the permissionless blockchain.

4.5.3 Overwriting Proposed Blocks

This is when the nodes clash to reject the existing block and suggest their new block. To resist this form of attack, after consensus has been achieved, all nodes must agree on the same block to connect to the chain.

4.5.4 Temperproof Environment

It is difficult to change or tamper with the messages stored by the RSUs using blockchain. All the RSUs store the same blockchain version and continuously add new blocks to the blockchain. The involved RSUs will create fake blocks and broadcast them. They do need to contend with the other blocks included in the blockchain, however. Therefore, the amount of compromised RSUs, in this case, is negligible, due to the use of permissioned blockchain.

4.5.5 Strong Privacy

Tendermint uses a BFT consensus algorithm, whereby appointed nodes send and receive messages and agree on blocks. It includes Propose, Prevote and Precommit messages. These messages included the signature of the node that created the message. A block will generate after the consensus contains a Precommit signature of the node that agreed on the block. Thus, it maintains privacy among the nodes.

Chapter 5

Trust Based System on Smart Contracts in Vehicular Adhoc Networks

5.1 Introduction

Due to the change in the lifestyle, the number of vehicles on the roads is increasing day by day and it is expected that it is going to double in the next 10 years [108]. With the increase in the number of vehicles, it is very difficult for the VANETs (Vehicular Adhoc Network) to handle this number of vehicles and to realize the Intelligent Transport Systems (ITSs). VANETs can be divided into two types viz. Vehicle to Vehicle (V2V) and Vehicle to infrastructure (V2I) [109]. In both systems the messages are exchanged through radio communication. In V2V, message exchanges between the vehicles, and in V2I vehicles can communicate with roadside units (RSUs) [109].

VANET is using the adhoc network such as cloud, WAVE, and cellular [110] is used for the secure message exchange between the vehicles using centralized architectures. The communication due to centralize systems is not transparent and that much secure [111]. As security is concerned the amount of data exchange and the requirement for memory and power is also increased. Due to the nature and sensitivity of the information exchange like identity and location. There must be some ways to prevent malicious behavior by accessing reliable sources with the help of consensus mechanisms [112]. Blockchain can easily solve this problem by using decentralized architecture [113]. The blockchain transactions are recorded in a distributed ledger by using consensus such as proof of work (PoW) and proof of stake (PoS). Each block can be divided into blockhead and body. Each block is concatenated with a hash and all the transactions are recorded in a Merkle root. Blockchain synchronizes all the transactions in a decentralized manner. When the failure of the nodes occurs, it will not affect the entire system.

5.1.1 Our Contribution

- To solve the security problem, we have proposed the blockchain-based VANET architecture with smart contracts. Moreover, this solves the problem of central failure caused by excessive access by managing the public key through a distributed mechanism.
- Due to the tamper-proof feature of blockchain, the information is secured on the chain. The system is using blockchain and smart contracts which reduces the overhead and provides better two-way authentication. Vehicles can communicate anonymously through blockchain which avoids third parties to steal information and privacy.

5.2 System Model and Proposed Approach

We are using the decentralized smart contract and Ethereum blockchain to provide a more reliable and secure environment for vehicular communication. Figure 5.1 shows the proposed architecture of VANET using the smart contract in the blockchain. Implementation steps are further explained in the following sections. The section is further divided into four parts.

System initialization has been explained which provides privacy to the users by submitting its identification to the trust blockchain. System authentication is used to provide the authentication and create a session between the vehicles. To make the vehicles more trustable every vehicle data is integrated to Physical Unclonable Function (PUF) and have assigned unique vehicle identification.

5.2.1 System Initialization

To understand this phase, consider any event that occurs on the road and vehicle V_A wants to send the message for which the event has occurred. Any vehicle enters the vehicular network and its ID gets revoked which is provided by the Certificate Authority (CA) as shown in Figure 5.2. Identity has to submit to the trust blockchain which provides privacy to the users. It also provides the necessary information required without revealing the actual data.

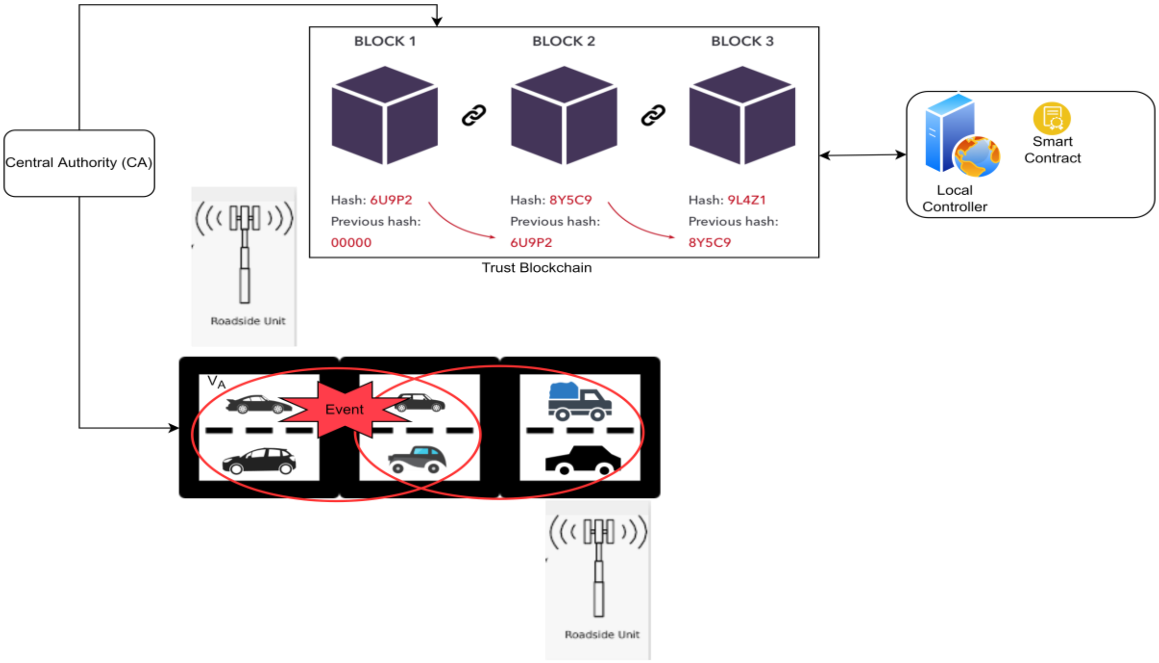


Figure 5.1: Architecture of VANET using smart contract in blockchain.

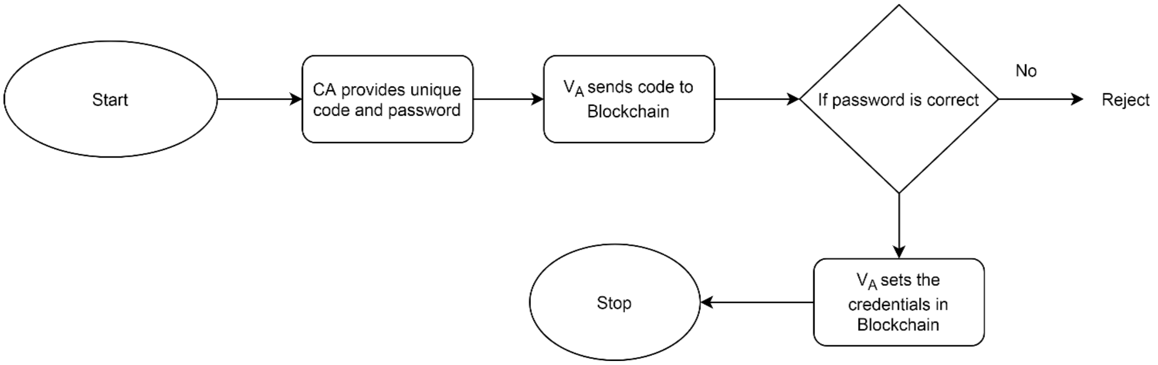

Start
CA provides unique code and password
V_A sends code to Blockchain
If password is correct
No
Reject
V_A sets the credentials in Blockchain
Stop

Figure 5.2: System initialization.

5.2.2 System Authentication

In this phase, the vehicles have to undergo with authentication process so that the proper session can be initialized between different vehicles and the blockchain. Communication and the other data exchange must be secure using the proper authentication and key exchange mechanism. We will discuss the two-party and multi-party smart contracts.

5.2.3 Two Party Smart Contract Algorithm

In order to exchange a secret key, the participants have to agree upon a prime number of p and generator point G. Some properties of the numbers create an impact on the cryptographic solution that we will not discuss here to maintain the simplicity.

Algorithm 1: ECC digital signature process

```
Input: p
Output: $out = (r, s)$
1: Select a random curve E on the field Fp.
2: Define the group G on E(F) and find the order of G.
3: Select a key pair, private key k is generated by random number and public key $K = kG$ using G.
4: Generate random integer r (r<n) and calculate $R = rG$
5: Calculate $e = HASH\ (message, x, y)$
6: Calculate $s = r - e^{k} mod\ n$
7: if r=0 or s=0
8:     move to step 4
9: else
10:    Take the value of r and s as signature
11: end if
12: return $out = (r, s)$
```

After receiving the message and the signature the recipient will follow the below algorithm for verification purposes.

Algorithm 2: Signing of message using public and private keys

```
Input: $(r, s)$
Output: $r_1$
Calculate $sG + H(message)P = (x_1, y_1), r_1 \equiv x_1 mod\ P$
If $r_1 \equiv r\ mod\ P$
    Signature established and verification successful
else
    abort the process
return $r_1$
```

The main thing here to concentrate on is using the tron smart contract and we can use the ecrecover function for signature verification which is a much faster process for the signature verification.

$$ecrecover(bytes32\ hash, uint8\ v, bytes32\ r, bytes32\ s)\ returns\ (address)$$

It is a global function provided by Solidity language and it returns the address of the signers according to the signature itself and with respect to data as well.

The following parameters are required for $ecrecover$ are taken from the sliced content of the signature:

$$r = signature\ [0{:}\,64](Key\ Creation)$$

$$s\ =\ signature[64{:}\,128](Encryption/Signing)$$

$$v\ =\ signature[128{:}\,130](Decryption/Validation)$$

The following slice function snippet we are using for signature verification.

```
function slice(bytes memory data, uint start, uint len) returns (bytes){
bytes memory b = new bytes(len);
for(uint i = 0; i < len; i++){
```

```
b[i] = data[i + start];
}
return b;
}
```

We are not writing the complete slice function for eliminating the complexity. It is available in the repository [114].

To verify the signature in solidity requires a lot of overhead and developers have to write their slicing functions. Since ecrecover can only return the address it can be easy to match whether the signer address is a restored address. By using this smart contract, the vehicles on the roads can be easily authenticated without large overheads and with better accuracy.

The authentication we have shown above is for two vehicles only. But in the case of real-time scenarios, we have multiple vehicles running on the road. So, in that case, we need multiparty authentication and the same can be achieved by using the same key exchange algorithm.

5.2.4 Connecting Solidity with Smart Contract

The smart contracts were coded in solidity, a contract-oriented high-level language for smart contract designing using Remix IDE.
Figure 5.3 shows the network model for executing the smart contracts consists of:

1. **Vehicles:** Vehicles denoted by V_A to V_N have their account in the blockchain and it is using a pair of public and private keys for the communication to be encrypted.
2. **RSU's:** These are used to handle the traffic on the road and it is situated on roadsides. Furthermore, RSU can also act as the certificate authority which is used for the registration of vehicles. A certificate contains an expiry date and a public key of the vehicle. It does not contain the real identity of the vehicle to preserve privacy.
3. **Assumptions made**
   - (i) Blockchain can scale the results according to the increase in the number of vehicles.
   - (ii) It is beyond the adversaries capability to compromise more than 50% of the RSU's.

For initializing the smart contract, we need to use the trust management and data sharing architecture which is having the blockchain account (16-bit address). Moreover, the vehicles are integrated already inside a physical unclonable function (PUF) which is assumed to be System-on-Chip (SoC) which provides them a unique crypto ID (vID). This provides safety against malicious attacks and makes it more reliable for communicating between them. Smart contracts are used to enable safe and secure communication. Vehicles can only send the data after being registered and this all is performed by certificates and vehicles registry as shown in Figure 5.3.

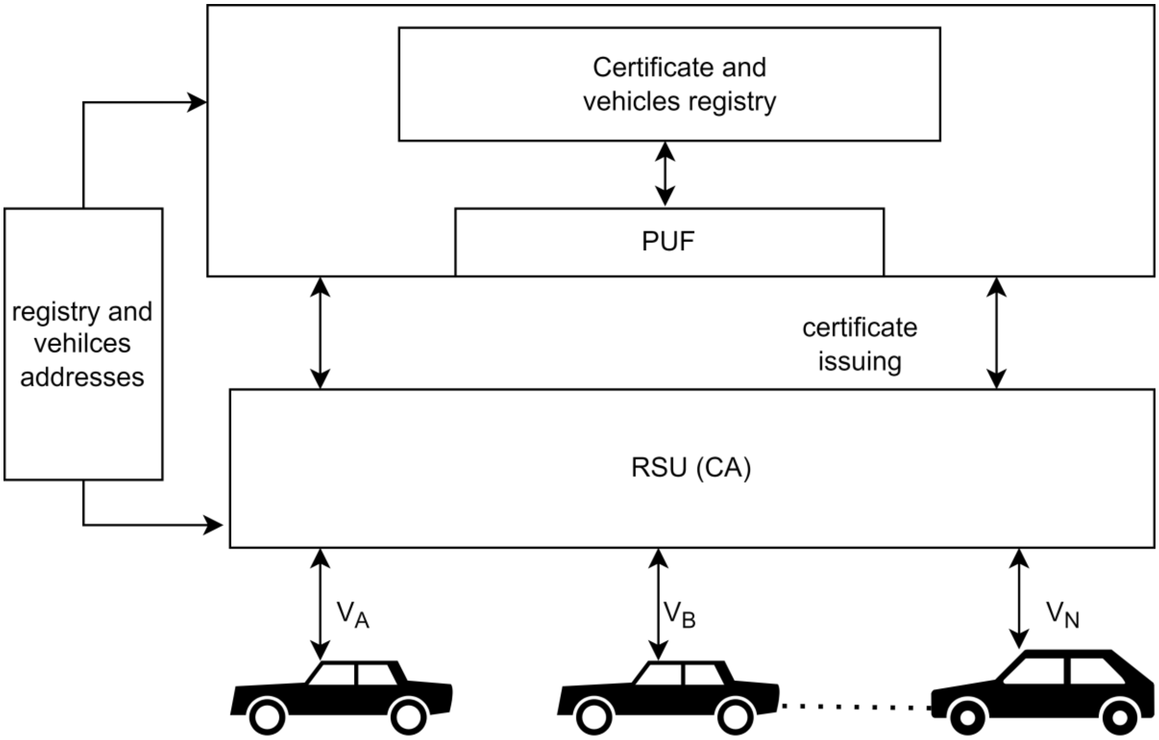

Certificate and vehicles registry
PUF
registry and vehilces addresses
certificate issuing
RSU (CA)
V_A
V_B
V_N

Figure 5.3: Information flow of trust management architecture.

5.2.6 Steps Involved in Smart Contract Flow

1. **Compilation:** Solidity IDE, Remix is used to compile the smart contracts. After compilation, smart contracts can be deployed on CA_j nodes.
2. **Deployment:** After successfully compiling, the contracts are deployed on the RSU nodes CA_j. CA_j broadcasts the address of the smart contracts so that the interaction between the vehicles and RSU can be performed.

Algorithm 3: Vehicles and RSU nodes smart contract initialization and flow

```
Input: $CA_j, V_i$
Output: Smart Contract (SC)
1: Initialization: $CA_j$  //initialization of miners
2: Create node and make account by $CA_j$  //account creation by private keys
3: $CA_j.account$     // sign by private keys and allocate some Ether
4: $\boldsymbol{V_A\ initialization}$   // vehicle 1
5: Create node and make account by $V_A$   //output address
6: $V_A\ .account$    // sign by private keys
7: $\boldsymbol{V_B\ initialization}$   // vehicle 2
8: Create node and make account by $V_B$  //output address
9: $V_B\ .account$    // sign by private keys
10: Run $CA_j$, $V_A$ , $V_B$
11: Deploy smart contracts
12: Interact $CA_j$, $V_A$ , $V_B$
```

5.3 Experimental Setup and Performance Evaluation

In this section, the experimental setup and performance evaluation have been performed. The inferences obtained from the performance analysis are presented in this section.

5.3.1 Experimental Setup

The experimental setup is performed on a computer equipped with Intel Core i5 @2.4Ghz and 8GB of RAM with the Windows 7 operating system. A block header is approximately 508 bytes [37]. Let us take that blocks are generating every 10 seconds (360 in one hour), then the storage overhead for one blockchain is 1602MB/year. Architecture is built on the SHA-256 hash algorithm. The time consumption for SHA-256 is less than $t_1 = 0.01ms$ per 1KB of input [82]. Time consumption to authenticate one public key is $T = t_1$ ($\log_2 n$), where n is the number of certificates issued.

5.3.2 Performance Evaluation

We have analyzed the following performance metrics: communication cost, authentication delay, storage cost, and RSU's overhead.

Communication cost is calculated based on the total number of vehicles using different variables used for the transmission of messages in the vehicular network. Communication cost is further calculated with respect to message authentication communication cost. Storage cost is the overall memory that is required to store the various variables like hash functions, symmetric and asymmetric keys, signature, and timestamp. RSU overhead is also an important parameter because the authentication is to be done by RSU and we need to reduce the overhead to reduce the load on the RSU's.

5.3.2.1 Message Authentication Communication Cost

Traditional Public Key infrastructure requires certificate and signature information for the message authentication. The total message size that is proposed by Zhang [82] is 257 bytes. Wang [76] has proposed a scheme that is using the 190 bytes message size. When we use the system with the blockchain and smart contracts the message size is reduced to 128 bytes as shown in Figure 5.4.

5.3.2.2 Authentication Delay

PKI needs to check the certificate revocation table for authentication. But in the proposed system information is managed through the smart contracts and stored in the blockchain which reduces the query time of the certificate. Wang [76] used two-way authentication through participation and Zhang [82] requires the proper participation of the CA. The proposed scheme has better efficiency and less latency due to the introduction of smart contracts which will be locally performed on the nodes to reduce the delay as shown in Figure 5.5.

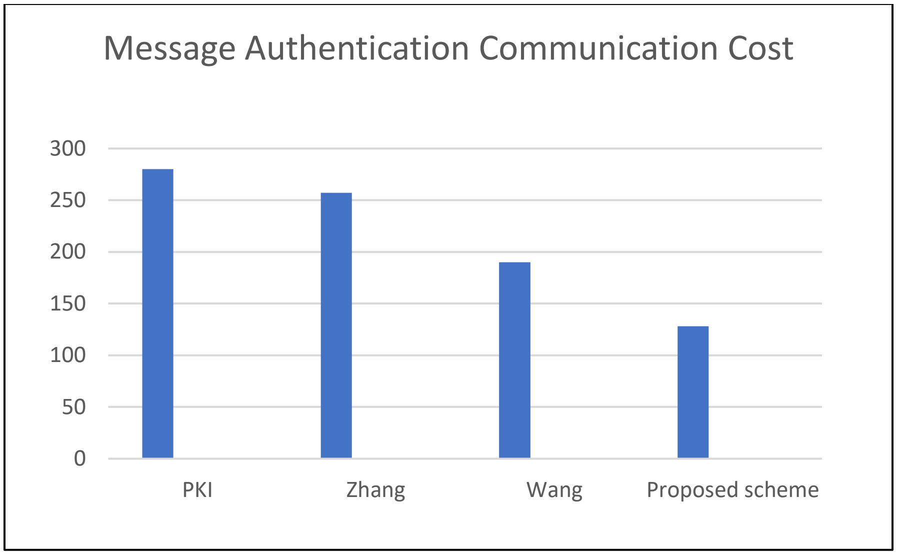


Figure 5.4: Message authentication cost.

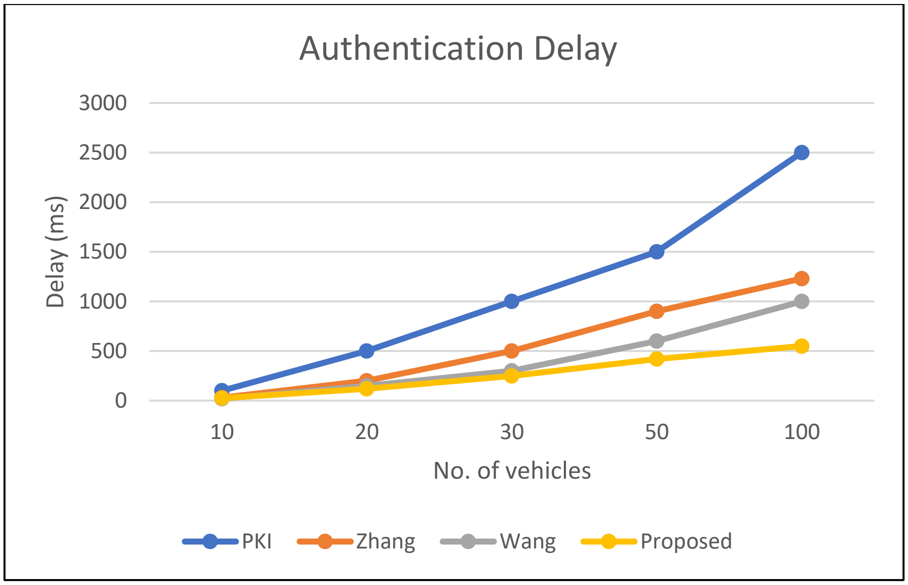


Figure 5.5: Authentication delay.

5.3.2.3 Storage Cost

Figure 5.6 shows the graph between the storage cost and bytes stored. It is the amount of space required for storing all the parameters. As you can see that the storage cost is lower in the case of the proposed scheme because of less overhead and ecrecover function. This clearly justifies the need for message dissemination in the case of the dense vehicular network.

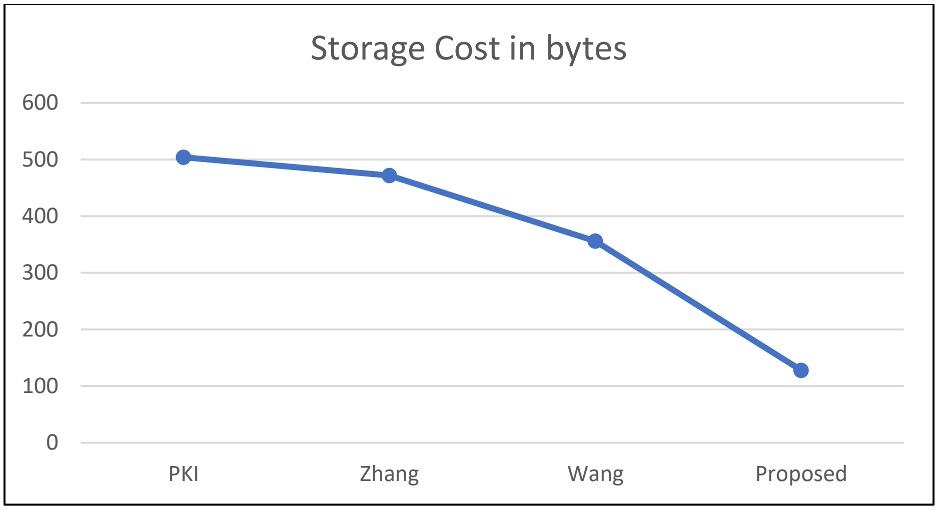


Figure 5.6: Storage cost.

5.3.2.4 RSU Overhead

In our proposed scheme, the message authentication task has been assigned to the RSU's. It has assumed that each vehicle sends the message in 200ms. As u can see in Figure 5.7, the proposed scheme has less RSU overhead as compared to the other schemes.

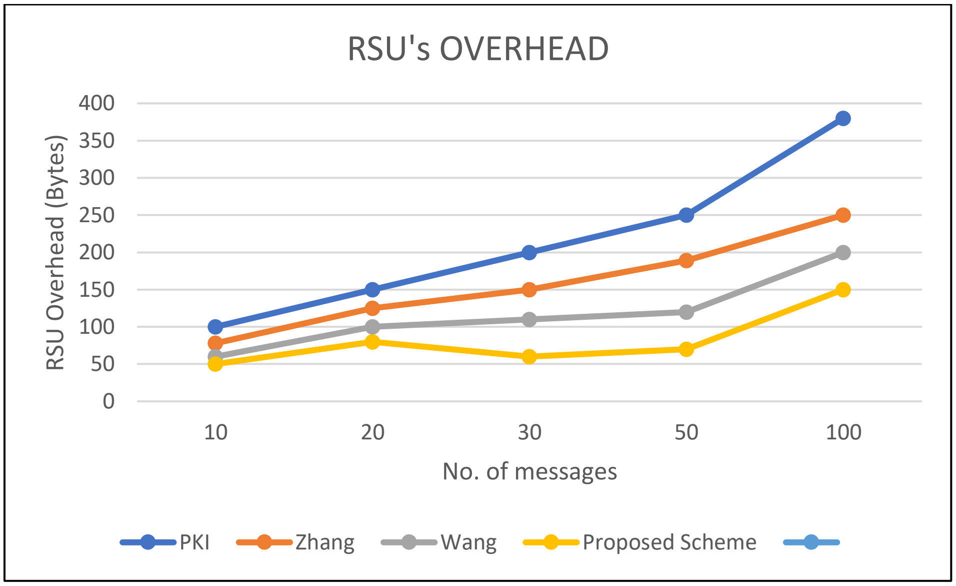


Figure 5.7: RSU's overhead.

5.4 Security Analysis

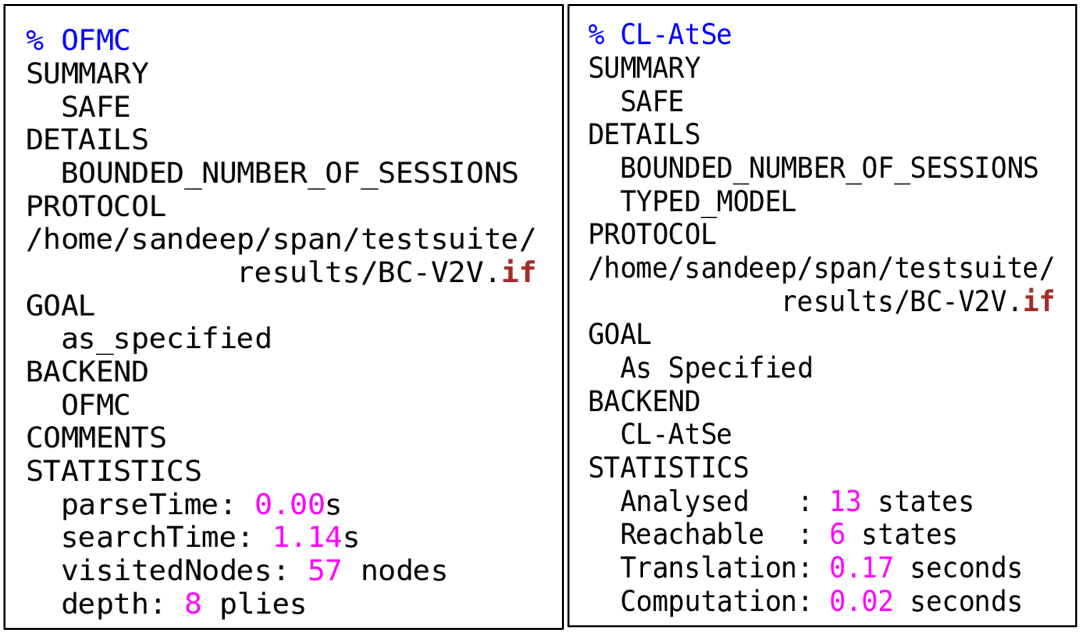
The strength of the proposed protocols has been analyzed through formal and informal analysis. The inferences obtained from this analysis are presented in this section.

5.4.1 Formal Analysis

In this section, formal security verification is performed against the man in the middle and replay attack. We have used the "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool [115] to perform this validation. There are four backends used by AVISPA viz. namely "On-the-Fly Mode-Checker (OFMC)", "Constraint-Logic Based Attack Searcher (CL-AtSe)", "SAT (Boolean satisfiability problem) based model checker (SATMC)", and "Tree Automata Based on Automatic Approximations for the analysis of security protocols (TA4SP)", which are used by the AVISPA. These help us in automatic execution analysis of the security protocols. "High-Level Protocol Specification Language (HLPSL)" is using the high-level implementation of the security protocols into the "Intermediate Format (IF)" using the HLPSl2IF translator. The IF acts as input to one of the four backends to produce the "Output Format (OF)" which explains the protocol is lying under the "safe", "unsafe" or "inconclusive". AVISPA is a widely used tool for the verification and validation of security protocols [116,117,118].

In our proposed scheme under HLPSL, we have defined the three basic roles: (a) the role of vehicles, (b) the role of RSU's, and (c) the role of smart contracts between the vehicles and RSU's. We had also simulated the two significant roles (session and goal and environment) and the backend we have covered are OFMC and CL-AtSe [118] because they support the XOR operation. We have not considered other backends because they didn't support the bitwise XOR operation.

Figure 5.8 shows the simulation results under the OFMC and CL-AtSe backends and it helps to predict the security of the designed scheme against replay and man in the middle attacks. The simulation has traversed 57 nodes at a depth of 8 piles. On the other hand, in the case of CL-AtSe backend, 13 states were analyzed, out of that 6 states are reachable with a translation time of 0.17s and computation time of 0.02s.



```
% OFMC
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/sandeep/span/testsuite/
            results/BC-V2V.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.14s
  visitedNodes: 57 nodes
  depth: 8 plies
```

```
% CL-AtSe
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
/home/sandeep/span/testsuite/
            results/BC-V2V.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 13 states
  Reachable  : 6 states
  Translation: 0.17 seconds
  Computation: 0.02 seconds
```

Figure 5.8: Analysis of simulation results under OFMC and CL-AtSe backends.

5.4.2 Informal Analysis

An informal analysis is used to prove the robustness of the proposed scheme from the various attacks. We have used it for tamper-proofing, privacy, and spoofing attacks.

Lemma 1. *Temper proof data*

Proof. It is very difficult to tamper with any block because in blockchain the blocks are arranged in chronological order. An attacker must have at least 51% of the total computation power which is very difficult because the hash rate is very high at this time. Therefore, tempering the blocks are very difficult for an attacker. Hence it is a secure network.

Lemma 2. *Strong Privacy*

Proof. A message exchange between the vehicles including the signature of the vehicle created a message. A block will generate after the consensus and contains the signature of the vehicle agreed upon communication. Hence privacy among the vehicles can be achieved.

Lemma 3. *Prevent from message spoofing attack*

has occurred on a road but actually, no event occurred. This is called message spoofing. The proposed architecture uses certificates to randomize the public keys so that attackers cannot correlate the public key of the vehicle and message spoofing can be eliminated.

5.5 Comparative Analysis with Existing Schemes

In this section, we have analyzed the proposed scheme with the existing schemes such as schemes designed by Wang et al. [76], Zhang et al. [82], and conventional PKI.

5.5.1 Comparative study of communications costs

In our proposed scheme the communication cost calculated is 1024 bits which is very less compared to the other methods because we have used smart contracts which reduces overhead to much extent. On the other hand, communication costs by PKI, Zhang et al. [82], and Wang et al. [76], and were found to be 2240 bits, 2056 bits, and 1520 bits respectively as shown in Table 5.1.

Table 5.1: Message authentication cost comparison.

Scheme	**No. of messages**	**No. of bits**
Proposed scheme	3	1024
Wang [76]	3	1520
Zhang [82]	3	2056
PKI [90]	3	2240

5.5.2 Comparison of security attributes

The comparison attributes and security features for the proposed scheme and others have been shown in Table 5.2. Various features are not supported by or available in PKI [90]. Man in the middle and impersonation is prevented by Zhang [82] and the proposed scheme. It is very clear from the table that the proposed scheme has better security attributes in comparison to conventional methods.

Table 5.2: Comparison of security attributes.

Feature	**Wang [76]**	**Zhang [82]**	**PKI [90]**	**Proposed Scheme**
Denial of services attack	✓	✓	✕	✓
Impersonation attack	✕	✓	✕	✓
Replay attack	✕	✕	✕	✓
Man in the middle attack	✓	✓	✕	✓
Mutual authentication	✓	✓	✓	✓
Session key agreement	NA	✓	NA	✓
Formal security verification by software	✕	✕	✕	✓

5.6 Summary and limitations of proposed work

This section is dealing with the summary part of this chapter as well as the limitations of the proposed work observed. We have introduced the smart contracts in the blockchain and implemented them on the proposed model to achieve less communication cost and less delay due to less overhead and smart contracts applicable on local machines which reduces the delay and message cost. Moreover, we have also introduced the Informal analysis of the system and proved that the proposed technique is free from various attacks like denial of services, man in the middle, replay, etc. As the smart contracts are also suffering from major attacks like Decentralize

Autonomous attack, attacking consensus protocols, etc. which has not been considered in this work and can be considered in future work.

Chapter 6

Performance Evaluation of VANET on the basis of Knowledge Base Algorithm

6.1 Introduction

An increasing interest is achieved in mobile wireless networks as they offer ubiquitous communication. In particular, mobile ad hoc networks facilitate the users to maintain the connectivity to the fixed network or exchange the information in the absence of an access point or base station. This can be achieved by multi-hop communications, which permits the node to reach the far away destination through intermediate nodes as relays. A fundamental problem that is seen in VANET is the selection and preservation of multi-hop paths. Certain factors make an intermittent change in the network topology such as node mobility, signal interference, and power disruption; as a consequence, the links are broken down in the path and an alternate path must be found.

Literature provides us with solutions to avert the degradation of the system performance, taking into account various metrics of interest. An ample amount of methods is advocated in the papers [119], [120], [121], and [122] to avoid the packet losses and restrain the latency and overhead due to path reconstruction.

VANETs possess no access point or base station to accomplish the communication thereafter leading to an efficient and uncomplicated establishment of the network. The place that experiences exposure to a natural catastrophe inhibits communication with the farther world [123]. In this work, our fundamental focus is made on the stability of the routing path, which is subjected to link failure caused by the mobility of the node. Header numbers are defined over each node based on their mobility. These header numbers are allocated with aid of a knowledge-based learning algorithm.

Knowledge-based learning algorithm is a machine learning algorithm that recruits previously learned network and make denouement based on attained knowledge. This enables us to learn when efficient and adequate prior knowledge is available. The protocol which is taken under consideration to relay the data packets from origin to destination is (Ad hoc on-demand distance vector) AODV protocol [124]. In particular, AODV is a reactive protocol or an on-demand routing protocol that is acknowledged on demand. For attaining the optimal path in the transport of data packets from source to destination, a minimum number of hops is the most prioritizing and imperative condition that has to be realized [125]. AODV uses sequence numbers instead of routing tables for path establishment so that the intricacy of looping can be minimized [126].

6.2 Our Contribution

- The link which is subjected to link failure is stabilized by the acknowledgment of a knowledge-based learning algorithm. Initially, we derive an expression of the sustained state which inhibits any link failure but due to mobility battery consumption boosts up making the link expected to be lost.
- This is followed by the infusion of knowledge-based learning algorithm in the network system which allocates the header number to each user based on the available prior knowledge. The header numbers have an inverse relation with mobility. Greater the header number, the insignificant the mobility.
- The above-discussed case is with respect to the ideal case where no foreign attack is affected. In our proposed work two more cases are considered where one case experiences a malicious attack whereas another case experiences a black hole attack. This administers us with the three cases; ideal case, malicious case, and black hole case.
- In the completion of the proposed work comparison between the three performance parameters, throughput, packet delivery ratio and delay are made for each case discussed above.

6.3 Related work

An ample amount of study is done on the energy consumption of the nodes which are associated with a defined cluster, to decrement the chances of link loss. In [119] a centrally coordinated network topology is designed using a lead node. The lead node is such elected that the node which retains the highest energy level is tabbed as the lead node. The selected lead node maintains a table with the contents; node id, the energy of the node, and residual energy. AODV protocol is used for relaying data packets. In particular, usages of certain formulae are made for computation of residual energy and energy consumption between nodes that are one hop apart. Furthermore, the final selection of the most favorable route is made based on per-node despite per flow. The node with the greatest amount of energy appears to be an actively participating node in the ultimate route. Unlike [119], [120] is not centrally coordinated, instead, the link failure is interrupted by the computation of an overall stability factor. Stability factors gauge the stability of each node in the network topology. In the initial stages, self- stability and neighbor stability of each node are resolved which enables us the determination of the overall stability factor. An inverse relation is provided between the mobility of nodes and the stability factor.

In [121] and [122] analogy is undertaken between on-demand routing protocols which enables us to decide on the finest routing algorithm for our work plan. The performance analysis of every protocol is initiated based on certain performance parameters. Protocols correlated in [121] are; AODV, DSR, and DYMO whereas in [122] the same is performed among AODV, DSR, and OLSR. A stochastic model and electrochemical model are designed which cooperate in the maintenance of the exhaustion of the battery. The management is such implemented that the stochastic model and electrochemical cell model are incorporated to achieve the charge management and recovery. This leads to the minimization of the occurrence of latency resulting in the prevention of the degradation of the network. The aim in papers [123], [124], [125] is considerably the same as discussed above but the mechanism is different. Various methods are advocated in the papers [126], [127], [128], and [129] to avoid packet losses and restrain the latency and overhead due to path reconstruction. Auto-configuration protocols are used for the assignment of unique IP addresses to nodes in Mobile ad hoc networks. Without the assignment of unique IP addresses, service provisioning between the nodes is not possible. Such protocols use various heuristics to ensure the uniqueness in IP address assignment; such aspects increase the overall complexity of the VANET system design [130]. The sink is placed anywhere in the target area. The nodes which are closer to the sink easily convey their message to it but the nodes which are at a great distance from it cannot directly forward their data to the sink, they have to send their data to the node which is closer to it than its neighbor forwards its data to sink. In this way, the nodes which are closer to the sink have to send the data of the distant nodes along with their own so they get depleted in terms of energy, as their energy is used in sending their data along with the data of farther nodes [131].

6.4 Knowledge-based learning algorithm

As discussed, prior, the foremost condition of data packets for routing from origin to end node is to persist effectiveness in the network. If the consumption of energy is less than it would result in an increased lifetime of the node which would help in data transmission. In particular, the main aim of our paper is to reduce the possibility of link failure. The parameter used for the assumption of an efficient path in a knowledge-based learning algorithm is the relay number.

Knowledge-based learning algorithm recruits the previously learned algorithm and makes the decisions based on the knowledge attained. This would allow us to make conclusions about when and where efficient knowledge is available. Through previous knowledge and pattern recognition, relay numbers are allocated to each respective node in the network system. An unknown function is given as F: A→ B where F is the actual truth on which input and output are mapped as a ∈ A and b ∈ B. Training data accompanies these instances which would denote the accurate sample of required output producing a function of G: A→B. The function G would provide us an approximate estimation of required output. Probability estimation of each possible outcome is made for every input instance whenever the pattern is supposed to be analyzed based on stability. The yielded function is shown in Eq. (6.1):

$$f(label|a,\forall) = x(a,\forall) \tag{6.1}$$

Here characterization of 'x' is performed by parameter$'\forall'$. The inverse probability of $f(a|label)$ is approximated with the previous probability by the usage of Bayes' rule as shown in Eq. (6.2).

$$f(label|a,\forall) = \frac{f(a|label,\forall)f(label|\forall)}{\sum_{L\in alllabels} f(a|L)f(L|\forall)} \tag{6.2}$$

To attain continuous distribution of labels integration is preferred rather than a summation which is given as Eq. (6.3): -

$$f(label|a,\forall) = \frac{f(a|label,\forall)f(label|\forall)}{\int_{l\in label}^{L\in alllabels} f(a|L)f(L|\forall)dL} \tag{6.3}$$

The algorithm of Knowledge-Based Learning Algorithm is given as follows:

Algorithm 1: Knowledge Base

Input: nodes

Output: range

```
$Vanet()$
$£ \rightarrow networksystem$
$n \rightarrow 0,1,2,3 \dots\dots\dots\dots . N$
$£(t) = \{(X1, Y1) \dots\dots\dots\dots\dots (Xn, Yn)\}$
$where$
$X1 = \{xi1, xi2, xi3 \dots\dots\dots\dots\dots xin\}$
$Y1 = \{yi1, yi2, yi3 \dots\dots\dots\dots\dots yin\}$
$£(t-1) = \{(X1, Y1) \dots\dots\dots\dots\dots (Xn, Yn)\}$
$where$
$X1 = \{x(i1-1), x(i2-1), x(i3-1) \dots\dots\dots\dots\dots x(in-1)\}$
$Y1 = \{y(i1-1), y(i2-1), y(i3-1) \dots\dots\dots\dots\dots y(in-1)\}$
$for\ i = 1 \rightarrow n$
$Computation\ ofnode\ position$
$R \rightarrow RelayNumber$
$if((£(t) == £(t-1))$
$9 \leq R \leq 10$
$elseif(£(t)! = £(t-1))$
$5 \leq R \leq 8$
$else$
$1 \leq R \leq 4$
    $end$
$end$
```

The given algorithm provides the working of a knowledge-based learning algorithm where the network setup is taken as $Vanet()$

Initially, the mobility of the node is monitored which is present at a certain arbitrary point (X, Y). £(t) collectively gives information on the mobility of nodes at the present instant of time. It is followed by delayed £(t-1) which provides us the information of the very same node with x and y coordinates (X, Y) at the previous instant of time. When the data is transmitted from 1 to n (integer number), the relay number(R) is allocated by recruiting £(t-1) along with £(t). If £(t) is nearly equal to £(t-1) 'R' will range between 9 to 10. Whereas if £(t) is not equal to £(t-1) then the 'R' will range between 5 to 8 and if none of the conditions is true then it can be concluded that the network is highly degraded in terms of performance and efficiency ranging 'R' from 1 to 4.

6.5 Proposed Model

Pattern recognition allows the gathering of the knowledge about the mobility of nodes and using these patterns relay numbers are allotted accordingly. Whenever the information is transmitted from one to another node then the power required is inversely proportional to the n^{th} power of the distance (d) between these nodes by $1/d^n$. Here n ranges between 2 and 4 based on the distance between the observed nodes. For successful routing, the SNR (signal to noise ratio) of the second node must be over the threshold value. If

n_i: Origin node

n_j: End node

Ψ: Threshold value

The SNR_jmust satisfy the following condition given in Eq. (6.4): -

$$SNR_j = \frac{P_i G_{i,j}}{\sum_{k \neq i} P_k G_{k,j} + \eta_j} \Psi_j(BER) \tag{6.4}$$

In Eq. (6.4)

P_i: Transmitted power of n_i

$G_{i,j}$: Path gain between n_i and n_j

Ψ_j: Threshold value

$$G_{i,j} = \frac{1}{d_{i,j}^n} \tag{6.5}$$

The methodology is initiated by setting up 4 network setups; 2 setups consisting of 12 nodes that are processed over AODV and DSDV routing algorithms. Likewise, 2 more setups are considered that consist of 24 nodes where each is routed through AODV and DSDV routing algorithm. If this network setup suffers from any link failure then a knowledge-based learning algorithm is applied. The selection of the optimal path is done using a relay number that is inversely proportional to the node mobility. As per the network setup the network configuration for AODV and DSDV routing algorithm is given in Eq. (6.6) to Eq. (6.9) follows:

$$W_{AODV} = \{s, d, r, pl\} \tag{6.9}$$

$$P_{s \to r} = \left\{(l, m) \middle| power_{s \to r \to (l,m)} < power_{s \to (l,m)}\right\} \tag{6.7}$$

$$W_{AODV} = \{s, d, r, pl\} \tag{6.8}$$

$$P_{s \to r} = \left\{(l, m) \middle| power_{s \to r \to (l,m)} < power_{s \to (l,m)}\right\} \tag{6.9}$$

W_{AODV}: Network system of AODV, W_{DSDV}: Network system of DSDV, s: Source node, d: destination node, r: relay node, pl: path loss, P: Path

The equation mentioned above states that whenever the data packets are routed in a particular network starting from the source node to any arbitrary point (l,m) then the required power for direct transmission of data packets from source to relay node is greater than the power required for indirect transfer of data packets. If the path experiences any link failure then the above equation can be modified as Eq. (6.10) and Eq. (6.11):

$$P_{s\rightarrow in\rightarrow pl} = \{(l,m) \big| power_{s\rightarrow r\rightarrow pl\rightarrow(l,m)} < power_{s\rightarrow(l,m)}\} \tag{6.10}$$

$$Data\_Packets_s > Data\_packets_d \tag{6.11}$$

$Data\_Packets_s$: Data Packets at the source node,$Data\_Packets_d$: Data packets at the destination node

As the obstruction occurs in the data packet transmission knowledge-based learning algorithm is acknowledged providing the equations as follows:

$$W' = \{s, d, r_n\} \tag{6.12}$$

$$s = \{s_{t1}, s_{t2}, \dots \dots \dots \dots \dots s_{tn}\} \tag{6.13}$$

$$d = \{d_{t1}, d_{t2}, \dots \dots \dots \dots \dots d_{tn}\} \tag{6.14}$$

$$r_1 = \{r_{t11}, r_{t12}, \dots \dots \dots \dots \dots r_{t1n}\} \tag{6.15}$$

$$r_2 = \{r_{t21}, r_{t22}, \dots \dots \dots \dots \dots r_{t2n}\} \tag{6.16}$$

$$r_N = \{r_{tN1}, r_{tN2}, \dots \dots \dots \dots \dots r_{tNn}\} \tag{6.17}$$

The above-stated equations, Eq. (6.12) to Eq. (6.17) provide information about the mobility samples at the distinct instant of time. Through these mobility samples, the behavior of every node is scrutinized, henceforth, allotment of relay number on the respective node is accomplished. If the range of relay number is between 1 to 10, 'R' represents Relay Number.

$$1 \leq R \leq 10$$

If Rs, Rd, Rr represent the relay number at the source node, destination node, and relay node, then, the relay number of each relay node is given as follows:

$$R_1 = \sum (R_s + R_d + R_{r1}) \tag{6.18}$$

$$R_2 = \sum (R_s + R_d + R_{r2}) \tag{6.19}$$

$$R_N = \sum (R_s + R_d + R_{rN}) \tag{6.20}$$

Eq. (6.18) to Eq. (6.20) is the average sum of relay numbers which is linked in the path of relay node r_1, r_2 up to $i_{n.}$ As discussed, prior that mobility and relay number of respective nodes possess an inverse relation therefore one can conclude that increase in mobility would result in a decrease in relay number. The mathematical formulation is given as follows:

If

$$R_1 > R_2$$

Than

$$M_1 < M_2$$

M_1: Mobility at node 1

M_2: Mobility at node 2

Below shows the schematic representation of the discussed scenario and the considered routing protocols are AODV and DSDV. In Figure 6.1 the red-colored nodes are the selected path nodes because they possess the highest average relay number hence the least mobility.

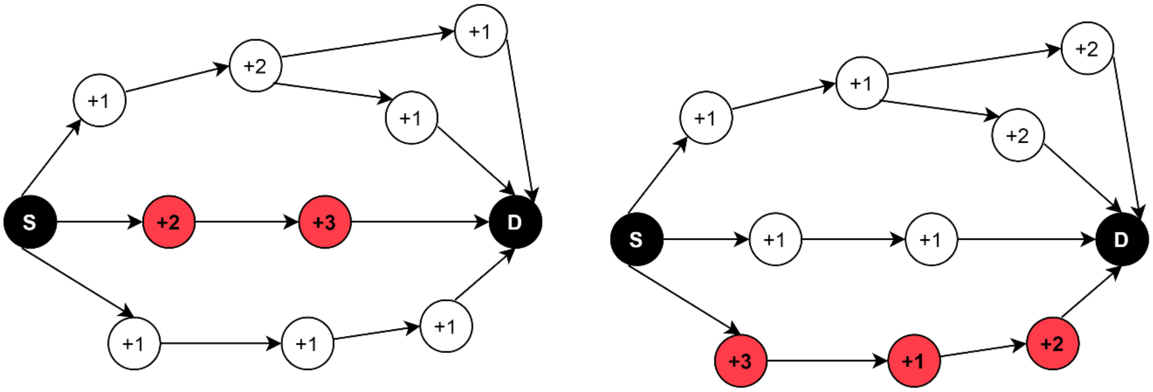


Figure 6.1 Relay number allocation for AODV and DSDV.

The application of a knowledge-based learning algorithm is shown in Figure 6.1 where the most reliable path is selected as the path that consists of the highest average relay number. More the relay number less would be the energy exhaustion of node, which enables the sustainable routing of data packets leading to reduction of link failure possibilities. The work is further extended by the intrusion of certain foreign attacks over the network system; malicious and black hole attacks.

A black hole attack is one of the foreign attacks on the network setup where disorientation happens due to the false reply from the tampered node. In such an attack the affected route acknowledges a false reply (RREP) to the source node after achieving a route request (RREQ) from the adjacent node. This reply is mistakenly assumed to be genuine, henceforth, leading to the construction of false network maintenance. If WB is considered as the network system that is affected by the black hole attack then the equations are modified as follows given in Eq. (6.21) to Eq. (6.28):

$$W_{B(AODV)} = \{s, d, r, B\} \tag{6.21}$$

$$W_{B(DSDV)} = \{s, d, r, B\} \tag{6.22}$$

Here B: Blackhole node

$$s = \{s_{t1}, s_{t2}, \dots \dots \dots \dots \dots s_{tn}\} \tag{6.23}$$

$$d = \{d_{t1}, d_{t2}, \dots \dots \dots \dots \dots d_{tn}\} \tag{6.24}$$

$$r_1 = \{r_{t11}, r_{t12}, \dots \dots \dots \dots \dots r_{t1n}\} \tag{6.25}$$

$$P_{s\to r} = \left\{(l, m) \middle| power_{s\to r\to(l,m)} < power_{s\to(l,m)}\right\} \tag{6.26}$$

If $\quad r \in B$

Then $\quad W_{B(AODV)} \notin \{d\}$

$W_{B(DSDV)} \notin \{d\}$

Therefore, the final selected path W_B is:

$$W_{B(AODV)} \in \{s, d, r\} \tag{6.27}$$

$$W_{B(DSDV)} \in \{s, d, r\} \tag{6.28}$$

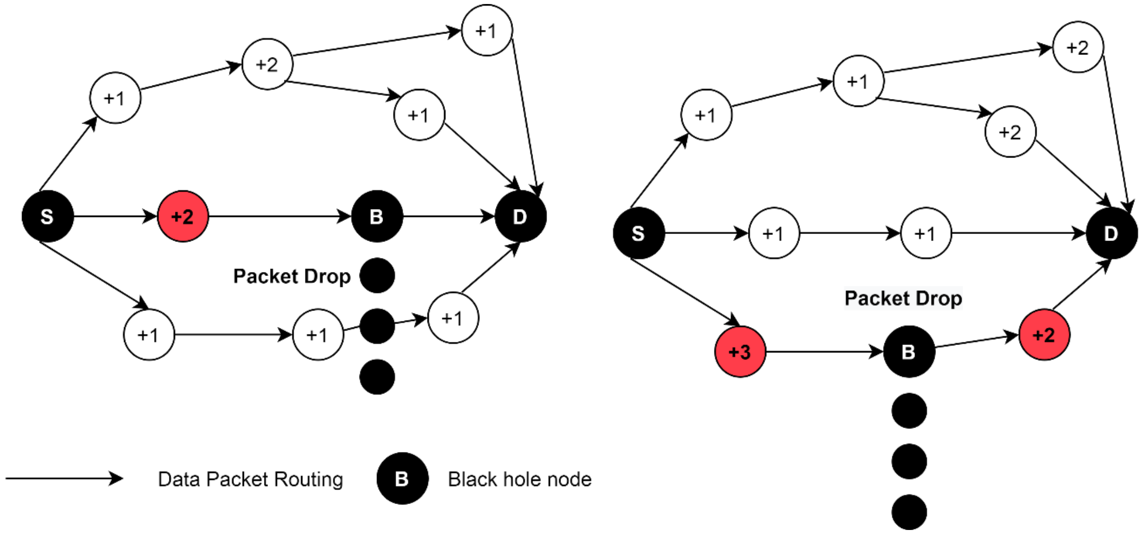


Figure 6.2: Introduction of blackhole node for AODV and DSDV.

The above-shown Figure 6.2 shows the loss of data packets as the node of the selected path is affected by a black hole attack. It would not only lead to the destruction of data packets routing but also to performance degradation. Performance parameters are adversely affected due to the loss of data packets, such as throughput, packet delivery ratio and delay. Another network setup is considered where instead of a black hole attack the network is affected by a malicious attack. A malicious attack is slightly different from a black hole attack as it would impede the communication between nodes and inhibits the transmission of data packets. If W_M represents the network setup suffering from a malicious attack then the equation would be modified as given in Eq. (6.29) and Eq. (6.30).

$$W_{M(AODV)} = \{s, d, r, M\} \tag{6.29}$$

$$W_{M(DSDV)} = \{s, d, r, M\} \tag{6.30}$$

Similarly, the equations can be written for the introduction of a malicious node to the network.

Figure 6.3 shown below shows the intrusion of a malicious node in the network system. It not only degrades the performance of the system but also leads to the loss of the most reliable path. This loss would deduce the throughout, PDR, overhead, and several other performance factors.

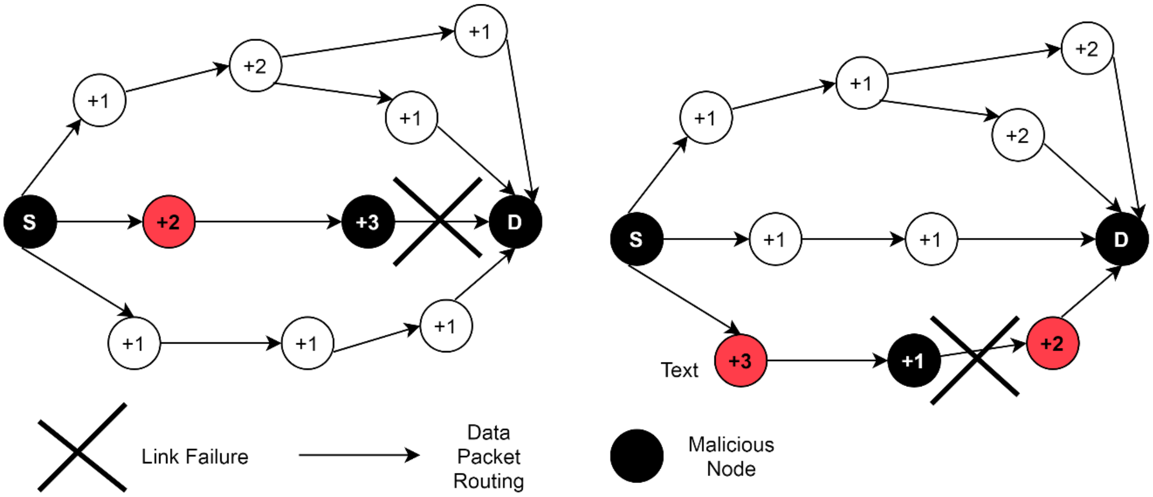


Figure 6.3: Introduction to the malicious node.

6.6 Results and Analysis

6.6.1 Simulation tool and scenario

For the implementation of our work plan, NS2 (network simulator 2) is used in Linux (Ubuntu 12.04). Required parameter values are attained by awk scripts. Designing the scenario of simulation is one of the hefty tasks as a detailed scenario would complicate the understanding whereas the less detailed scenario may provide incorrect results. Our approach should be in such a manner that the user can conveniently perceive the work along with the legitimate outcomes.

6.6.2 Performance parameters

- Throughput: Throughput measures how fast a user transmits data through a network. Even though it seems that bandwidth and throughput are similar but in actuality, they contrast to a great extent. If the bandwidth of a network is A bps but only D bps can be transmitted across the link, then we can conclude that D bps is the throughput. Always A > D. If the bandwidth of a given link is 1 Mbps but only 500 kbps is allowed for transmission, then 500 kbps is the throughput of the system.

- Packet Delivery ratio: The number of data packets lost when sent to the destination is referred to as data packet loss. This not only prevents communication but also degrades the performance of the entire network system. So, every measure should be taken to improve any loss in the data. The origin of packet loss can be link failure or interior or exterior attack. An extensive amount of research is under process to accelerate the reliability of the dynamic network system hence preventing any loss of data. PDR is given as aware of the performance characteristics. The ideal case possesses adequate and reliable parameters whereas malicious and black hole attack parameters portray the degradation in the network.

$$PDR = \frac{\sum Total\ number\ of received\ packets}{\sum Total\ number\ of sent\ packets} \tag{6.31}$$

- Delay: it refers to the time taken for a packet to be transmitted across a network from the source to the destination and it includes various parameters like transmission time, propagation delay, processing delay, and queuing delay.

6.6.3 Simulation parameters

In particular, three cases are implemented in our proposed work, and the performance of each case is evaluated based on three performance parameters; throughput, packet delivery ratio, and delay. Table 6.1 displays certain simulation parameters: -

Table 6.1: Simulation parameters.

Simulation parameters	**Specification**
Simulation time for ideal case	1m 34s
Simulation for malicious case	1m 30s
Simulation time for black hole case	1m
Channel type	Wireless channel
Antenna model	Omni-directional
Radio propagation model	Two ray ground
Number of nodes	100
Number of malicious nodes	1
Number of black hole node	1
Number of packets	50
Traffic type	Constant bit rate (CBR)
Routing protocol	AODV

6.6.4 Simulation results

As discussed before the assessment is made based on throughput, PDR (Packet Delivery Ratio) and Delay hereby, providing the result in Table 6.2 ,Table 6.3 and Table 6.4. In the table shown below analysis can be easily made based on performance parameters hence enabling us to become aware of the performance characteristics. The ideal case possesses adequate and reliable parameters whereas malicious and black hole attack parameters portray the degradation in the network.

Table 6.2: Throughput (Kbps).

No. of Nodes	Ideal Case	Malicious node	Black hole attack
10	450.32	280.05	176.04
20	302	180	150
30	280	165	140
50	265	154	132
100	230	135	131

Table 6.3: Packet delivery ratio.

No. of Nodes	Ideal Case	Malicious node	Black hole attack
10	0.94	0.75	0.36
20	0.92	0.7	0.35
30	0.9	0.69	0.343
50	0.9	0.689	0.34
100	0.8	0.7	0.32

Figure 6.4 ,Figure 6.5 and Figure 6.6 shows the comparison of the considered performance parameters: -

We studied the knowledge-based learning algorithm which is implemented over the routing paths in VANETs- a fundamental issue to provide reliable routes and short routes possible. We focused on the per-node analysis rather than the per-flow analysis. The focal point of our proposed work is to diminish the prospect of network degradation provoked by the energy exhaust of nodes. The use of a machine learning algorithm enables us to determine the optimal path in terms of header number; in particular, we showed some properties for obtaining the optimal path in terms of the header number which refers to the mobility of the node.

Table 6.4: Delay(ms).

No. of Nodes	Ideal Case	Malicious node	Black hole attack
10	50	60	80
20	80	90	100
30	90	100	130
50	100	120	150
100	110	150	200

An approximate expression for the optimal sum of header number is realized. Finally, based on our findings, we proposed an approach to finding and selecting a route that accounts for the expected data transfer time over the path allowing for improving the throughput, packet delivery ratio, and delay.

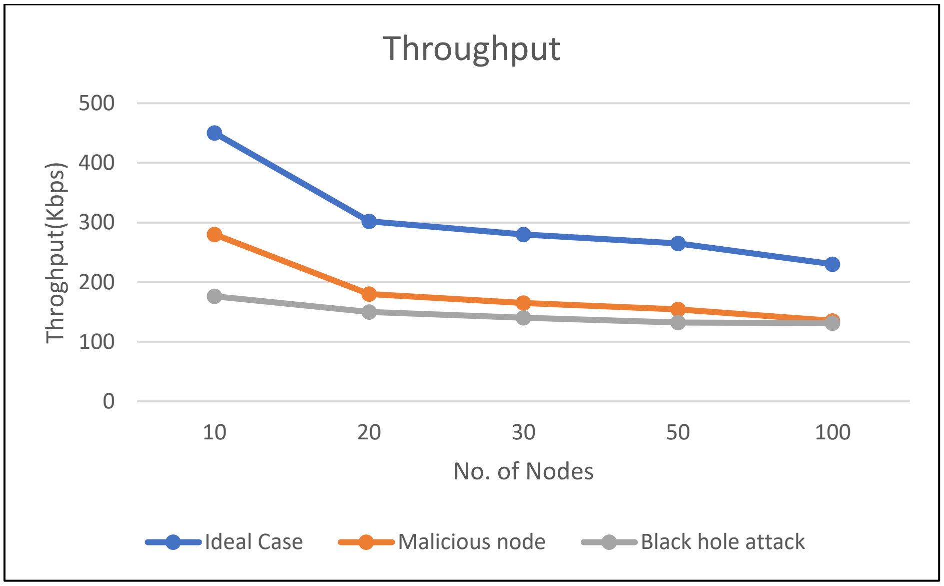


Figure 6.4: Throughput.

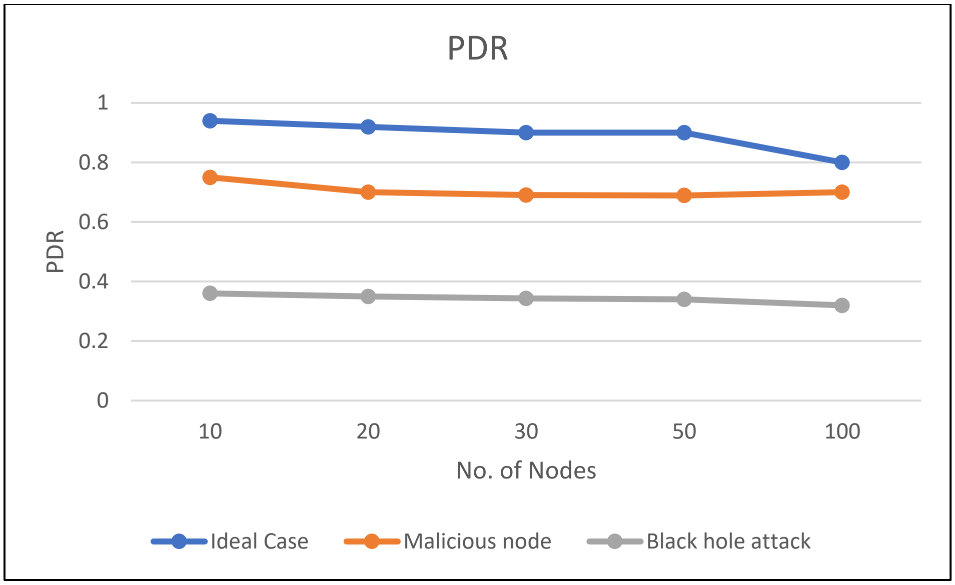


Figure 6.5: PDR.

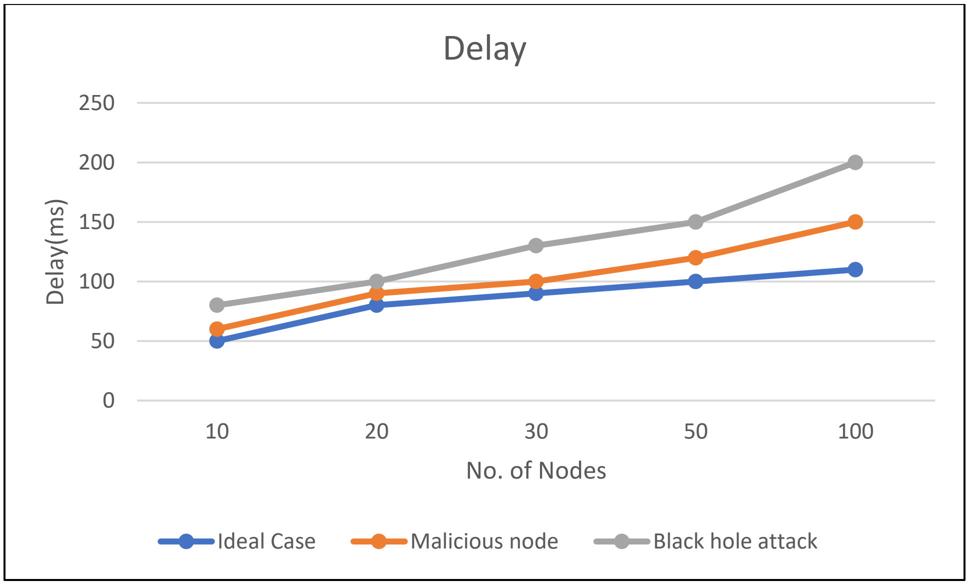


Figure 6.6: Delay.

6.6.5 Comparative Analysis

Comparative analysis is done with the literature [56] [57] and it has been found that the knowledge base algorithm improved the Quality of Services to a significant level as shown in Figure 6.7 , Figure 6.8 and Figure 6.9.

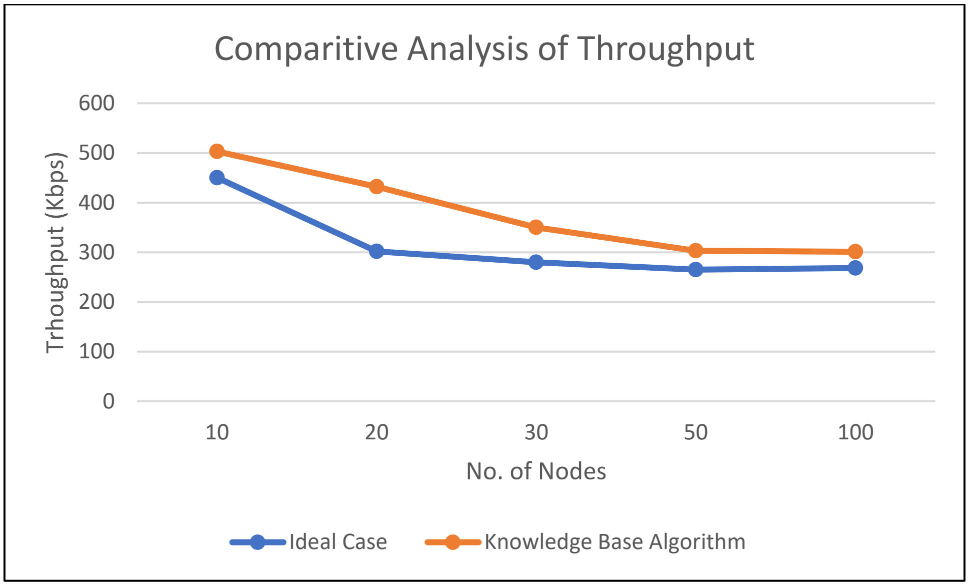


Figure 6.7: Comparative Analysis of Throughput.

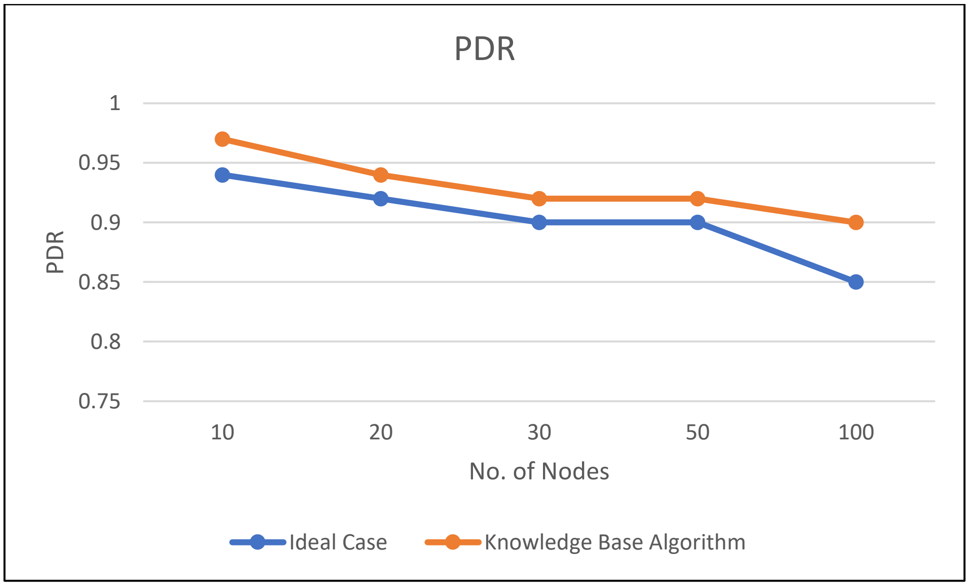


Figure 6.8: Comparative Analysis of PDR.

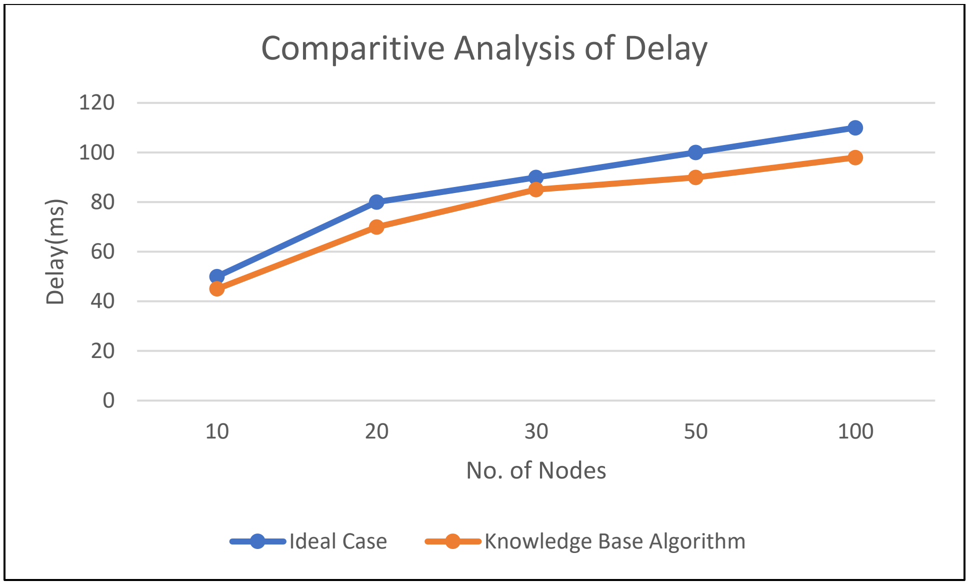


Figure 6.9: Comparative Analysis of Delay.

6.6.6 Summary and Conclusion

We have analyzed the parameters of Quality of services in this chapter. It is presented that by applying the knowledge-based algorithm the throughput, delay and PDR have shown significant improvement in comparison to the ideal case where no knowledge-based algorithm is implemented due to the freshness of the route which leads to less delay and higher throughput. Moreover, the concept of header number is used to select the optimal path for routing for the improvement of QoS.

Chapter 7

Conclusions

7.1 Summary

As road safety is a major concern and with the development of the automobile industry, VANET is very much required application for road security and the safety of passengers. Moreover, it is important to build an intelligent transport system everywhere on the roads especially on national highways to protect the users from road accidents and injuries. However, due to insecure sessions and wireless channels, VANET becomes an easy target for attackers. By considering that facts mentioned above a secure session initiation method and decentralized method for authentication and agreement have been developed in this thesis. VANET is suffering from mobility and high-power consumption. The proposed schemes provide the decentralized system with trust management to improve the QoS by utilizing the least power. Besides that the scheme proposed is effective to prevent the system from common threats like MITM, replay, impersonation, etc. The accomplishment of security properties such as integrity, privacy, freshness, etc. has been verified through security analysis. The proposed scheme is also compared with conventional schemes in terms of communication cost, overhead, and delay and it has been observed that the proposed schemes are more robust and efficient than the conventional schemes proposed in the literature.

We proposed the double layer mechanism here to defend against this message spoofing. The first layer has used the gradient boosting technique (GBT), based on machine learning mechanisms, able to provide trustworthiness between the vehicles. The credibility of the message is checked by the receiver, which analyzes the different messages and their ratings broadcasted on the network. Tendermint based on Byzantine fault tolerance acts as a second layer, using the permissioned blockchain, which is much less vulnerable as compared to the permissionless blockchain. It is difficult to change or tamper with the messages stored by the RSUs using blockchain. All the RSUs store the same blockchain version and continuously add new blocks to the blockchain. The involved RSUs may create fake blocks and broadcast them. They do need to contend with the other blocks included in the blockchain, however. Therefore, the amount of compromised RSUs, in this case, is negligible, due to the use of permissioned blockchain. Moreover, with the integration of blockchain with VANET, there is a significant improvement in the QoS, message authentication, and storage cost as shown in Chapter4.

We have introduced the smart contracts in the blockchain and implemented them on the proposed model to achieve less communication cost and less delay due to less overhead and smart contracts applicable on local machines which reduces the delay and message cost. Moreover, we have also introduced the Informal analysis of the system and proved that the proposed technique is free from various attacks like denial of services, the man in the middle, replay, etc. As the smart contracts are also suffering from major attacks like Decentralized Autonomous attacks, attacking consensus protocols, etc. which have not been considered in this work and can be considered in future work.

It is also presented that by applying the knowledge-based algorithm the throughput, delay and PDR have shown significant improvement in comparison to the ideal case where no knowledge-based algorithm is implemented due to the freshness of the route which leads to less delay and higher throughput. Moreover, the concept of header number is used to select the optimal path for routing for the improvement of QoS.

7.2 Research Impact

The research contribution of the thesis has scientific as well as social impact. But the VANET network suffers from the absentia of security essentials due to the nature of resource-constrained VANET nodes. The proposed work presented in the thesis intends to accomplish the essential security measures against various threats to secure the session by utilizing less computation and fewer resources. The proposed scheme has provided a network that will be tamper-proof and decentralized to avoid the unauthorized access of third parties. Double layer protection is also provided in the research carried out which further enhances the security of the network and makes it more useful for the public to use efficiently with strong privacy. Moreover, the probability of deadlock is very less compared to another system because the nodes do not wait for the other node. Further, the research work provides the foundation for future research as well. The VANET network is the major component of an intelligent transport system that can reduce road accidents and injuries to passengers on daily basis. The security requirements of these types of networks are message integrity, privacy, authorized access, etc. The proposed scheme based on blockchain and smart contracts can exhibit these properties, thus enhancing the trust in the VANET network. Hence we have concluded from the above points that the blockchain brings no dependency on central servers and the network will be more secure and no third party can enter and do the modifications in data due to tamper-proof and strong privacy provided by research carried out. The research work can be further combined with the Internet of Things (IoT), cloud, and fog computing to benefit other closely related sectors.

7.3 Future Aspects

The proposed work can be further extended to address the problems of society and the scientific community. Few long terms goals are summarized below:

1. **Quantum computing:** Quantum computers can easily crack the existing security algorithms. So, we need to modify the security protocols according to the power of quantum computers. Moreover, quantum security has the following benefits less power consumption and less network overhead. Hence new protocols need to develop to protect the VANET network from the attacker having quantum computing capability.

2. **Hashgraph:** It is a consensus algorithm that uses the concept of virtual voting to achieve faster and more secure transactions. It claims to overcome the gap left by blockchain. Moreover, it is a peer-to-peer platform that needs for complete transactional operations.

3. **Fog computing:** Vehicular network is a resource-constrained network. Vehicles have less storage and less computational power. Therefore, more complex computations can be done with the help of authentication whose overhead can be reduced to make complex computations faster.

7.4 Ethical Considerations

The research has been carried out with utmost honesty while ensuring scientific integrity. The thesis contains only real and unbiased findings of experimentation. The schemes and their elaboration are free from all types of plagiarism; moreover, the works referred to conduct the research have been duly credited. We have used only public available cryptography primitives, open-source blockchain and smart contracts schemes, and scientific tools to avoid ethical shenanigans. The literature has been ethically downloaded from the portal provided by the University. Furthermore, only authentic scientific tools have been used to conduct the research.

References

[1] "WHO, Fact-sheet for Road Traffic Injuries," May 2017. [Online]. Available: http://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries/. [Accessed 20 May 2021].

[2] X. Ma, J. Zhang, X. Yin and K. S. Trivedi, "Design and analysis of a robust broadcast," *IEEE Transactions of Vehicular Technology,* vol. 61, no. 1, pp. 46-61, 2012.

[3] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications,* vol. 37, pp. 38-392, 2014.

[4] "Dedicated Short Range Communications," 2018. [Online]. Available: http://www.leearmstrong.com/DSRC/DSRC Homeset.htm.. [Accessed 20 May 2021].

[5] Q. Xu, T. Mak, J. Ko and R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," in *ACM International Workshop on Vehicular Ad Hoc Networks*, 2004.

[6] X. Yang, J. Liu, F. Zhao and N. Vaidya, "A vehicle to vehicle safety messaging in DSRC," in *Workshop on Vehicular Adhoc Networks*, 2004.

[7] X. Yang, J. Liu, F. Zhao and N. Vaidya, "A vehicle to vehicle communication protocol for cooperative collision warning," in *Mobile and Ubiquitous Systems: Networking and Services*, 2004.

[8] P. IEEE draft standard, Sept 2009. [Online]. Available: http://ieeexplore.ieee.org/servlet/opac?punumber¼5325056.. [Accessed 11 June 2021].

[9] "Highway Authority," [Online]. Available: https://morth.nic.in/sites/default/files/RA_Uploading.pdf. [Accessed 11 June 2021].

[10] F. Cunha, L. Villas, A. Boukerche, G. Maia and A. C. Viana, "Data Communication in VANETs: Survey, Applications and Challenges," *Adhoc Networks Elsevier,* vol. 44, pp. 90-110, 2016.

[11] C. Perkins and E. Royer, "Adhoc On-demand distance vector routing," in *Workshop on Mobile Computing Systems and applications*, 1999.

[12] Z. Stampoulis and A. Chai , "A survey of security in vehicular networks," [Online]. Available: http://zoo.cs.yale.edu/ ∼ams257/projects/wireless-survey.pdf. [Accessed 12 May 2021].

[13] Z. Zeadally, Y. Hunt and A. Irwin, "Vehicular adhoc networks; status, results and challenges," *Telecommunication Systems,* vol. 51, pp. 2-3, 2012.

[14] [Online]. Available: 14. https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity. [Accessed 20 May 2021].

[15] C. Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers," in *ACM Conference on Communications Architectures, Protocol and Applications*, New York, 1994.

[16] M. Marina and S. Das, "On demand multipath distance vector routing for adhoc networks," in *International Conference on Network Protocols*, CA, 2001.

[17] C. Perkins and E. M. Royer, "Adhoc on demand distance vector (AODV) routing," in *IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, 1999.

[18] G. Korkmaz, E. Ekici, F. Ozguner and U. Orguner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in *International workshop on Vehicular Ad Hoc Networks*, USA, 2004.

[19] A. Benslimane, "Optimized dissemination of alarm messages in vehicular ad hoc networks," *Lecture Notes,* vol. 30, no. 79, 2004.

[20] H. Suo, J. Wan, C. Zou and J. Liu, "Security in internet of things: A review," in *IEEE International Conference on Computer Science and Electronics Engineering*, Hangzhou, 2019.

[21] I. Butun, P. Osterberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials,* vol. 32, no. 1, pp. 616-644, 2020.

[22] P. Kumar, A. Braeken, A. Gurtov, J. Ianatti and P. H. Ha, "Anonymous secure framework in connected smart home environments," *IEEE transactions on Informatics Forensics and Security,* vol. 12, no. 4, pp. 968-979, 2017.

[23] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos and J. J. Rodrigues, "Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment," *IEEE Internet of Things,* vol. 5, no. 6, pp. 4900-4913, 2018.

[24] P. Gope, A. K. Das, N. Kumar and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics,* vol. 15, no. 9, pp. 4957-4968, 2019.

[25] S. Sciancalepore, G. Piro, G. Boggia and G. Bianchi, "Public key authentication and key agreement in IoT devices with minimal airtime consumption," *IEEE Embedded Systems Letters,* vol. 9, no. 1, pp. 1-4, 2017.

[26] K. Choudhary, G. S. Gaba, I. Butun and P. Kumar, "MAKE-IT: A lightweight mutual authentication and key exchange protocol for the industrial internet of things," *Sensors,* vol. 20, no. 18, p. 20, 2020.

[27] S. Khan, A. I. Alzahrani, O. Alfarraj, N. Alalwan and A. H. Al-Bayatti, "Resource-efficient authentication and session key establishment procedure for low resource IoT devices," *IEEE Access,* vol. 7, pp. 170615-170628, 2019.

[28] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed hash chain," *Journal of Information Security and Applications,* vol. 45, pp. 156-175, 2019.

[29] P. Kumar, A. Gurtov, J. Ianatti, M. Yliantilla and M. Sain, "Lightweight and secure session key establishment scheme in smart home environments," *IEEE Sensors,* vol. 16, no. 1, pp. 254-264, 2016.

[30] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia and G. Bianchi, "Key management protocol with implicit certificates for IoT systems," in *Workshop on IoT challenges in Mobile and Industrial Systems*, 2015.

[31] P. Porambage, P. Kumar, C. Schmitt, A. Gurtov and M. Ylianttila, "Certificate-based pairwise key establishment protocol for wireless sensor networks," in *International conference on Computer Science and Engineering*, 2013.

[32] B. A. Forouzan, Data Communications and Networking, Tata Mcgraw-Hill Education, 2013.

[33] M. N. Aman, K. C. Chua and B. Sikdar, "Mutual Authentication in IoT systems using physical unclonable functions," *IEEE Internet of Things,* vol. 4, no. 5, pp. 1327-1340, 2017.

[34] S. Nakamoto, "Bitcoin: A peer to peer electronic cash system," Technical Report, 2009.

[35] Z. Zheng, S. Xie, X. Chen and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *International Conference on Big Data*, 2017.

[36] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, 1997.

[37] G. Wood, "Ethereum: a secure decentralized generalized transaction ledger," Ethereum Project Yellow Paper, 2014.

[38] H. Sukhwani, J. M. Martinez, X. Chang, K. S. Trivedi and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network," in *Symposium on Reliable Distributed Systems*, 2017.

[39] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *International Conference on Consumer Electronics*, 2016.

[40] C. Wang, X. Cheng, J. Li, Y. He and K. Xiao, "A survey: Applications of blockchain in the internet of vehicles," *EURASIP Journal on Wireless Communications and Networking,* vol. 77, pp. 1-16, 2021.

[41] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transaction of Computer Systems,* vol. 20, pp. 398-461, 2002.

[42] M. E. Mahmoud and S. Shen, "An integrated stimulation and punishment mechanism for thrawting packet dropping attack in multihop wireless networks," *IEEE transactions of Vehicular Technology,* vol. 60, pp. 3947-3962, 2011.

[43] C. Lai, K. Zhang, N. Cheng, H. Li and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Transactions of Intelligent Transport Systems,* vol. 18, pp. 1-16, 2016.

[44] Intelligent Transport Systems Committee, "IEEE trial use for wireless access in vehicular environments (WAVE) security for applications and management messages," IEEE, 2006.

[45] A. H. Salem, A. A. Hamid and M. A. Nasr, "The case for dynamic key distribution for PKI-based VANETs," *International Journal of Computer Networks and Communications,* vol. 6, no. 1, pp. 61-78, 2014.

[46] X. Y. Guo, "Research on the privacy preservation in security communication for VANET," *Shenyang Aerospace University,* 2017.

[47] W. Qinglong, Q. Rui, F. Na and D. Zongtao, "An efficient conditional anonymity authentication scheme for VANETs," *Journal of Beijing Jiaotong University,* vol. 43, no. 5, pp. 80-86, 2019.

[48] A. S. Federico, "The Crowd Jury, A Crowdsourced Justice System for the Collaboration Era," [Online]. Available: https://medium.com/the-crowdjury/the-crowdjury-a-crowdsourced-court-system-for-the-collaboration-era66da002750d8. [Accessed 2 January 2021].

[49] V. Jacynycz, A. Calvo, S. Hassan and A. A. Sanchez-Ruiz, "Betfunding: A distributed bounty based crowdfunding platform over the ethereum," in *International Conference on Distributed Computing and Artificial Intelligence*, Spain, 2016.

[50] H. Zhu and Z. Z. Zhou, "Analysis and outlook of applications of blockchain technology to equity crowdfunding," in *China Finance Innovation*, China, 2016.

[51] C. Cai, X. Yuan and C. Wang, "Hardening distributed and encrypted keyword search via blockchain," in *IEEE Symposium on Privacy-Aware Computing*, Washington, 2017.

[52] D. S. De Angelis, L. Aniello, B. Leonardo, L. Roberto, M. Federico, A. Margheri and V. Sassone, "Applying the CAP theorem to permissioned blockchain," in *Italian Conference on Cyber Security*, Milan, 2018.

[53] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM transaction of Computer System,* vol. 20, pp. 398-461, 2002.

[54] J. Mattila, "The blockchain phenomenon," in *Berkeley Roundtable of the International Economy*, Berkeley, 2016.

[55] European Telecommunications Standards Institute, "Study on LTE-Based V2X Services, V1.0.0: TSG RAN 3GPP; TR 36.885; European," France, 2016.

[56] U. Draz, T. Ali, S. Yasin and A. Shaf, "Evaluation based analysis of packet delivery ratio for AODV and DSR under UDP and TCP environment," in *International Conference on Computing, Mathematics and Engineering Technologies*, Sukkur, 2018.

[57] M. Shorfuzzman, M. Masud and M. Rahman, "Characterizing end-to-end delay performance of randomized TCP using an analytical model," *International Journal of Advanced Computer Science and Applications,* vol. 7, pp. 406-412, 2016.

[58] N. Kumar, K. Kaur, S. C. Misra and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-to-Peer Networking and Applications volume,* vol. 9, pp. 824-840, 2016.

[59] R. Amin, S. K. Islam, G. P. Biswas, M. K. Khan and N. Kumar, "An efficient and practical smart card-based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography," *Journal of Medical Systems,* vol. 39, no. 11, pp. 1-18, 2015.

[60] W. Thin, N. Dong, G. Bai and J. S. Dong, "Formal Analysis of a proof-of-stake blockchain," in *International Conference on Engineering of Complex Computer Systems*, Melbourne, 2018.

[61] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu and W. He, "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Transactions of Vehicular Technology,* vol. 69, pp. 5836-5849, 2020.

[62] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access,* vol. 8, pp. 2482-2498, 2019.

[63] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors,* vol. 19, no. 22, p. 4954, 2019.

[64] G. Zyskind, O. Nathan and A. S. Pentland, "Decentralized privacy: Using blockchain to protect personal data," in *IEEE Security and Privacy Workshop*, CA, 2015.

[65] P. Pukale and P. Gupta, "Analysis of end-to-end delay in vehicular networks," *International Journal of Science and Research,* vol. 5, no. 9, pp. 1122-1125, 2016.

[66] T. H. Kim, R. Goyat and G. Kumar, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access,* vol. 7, pp. 184133-184144, 2019.

[67] R. Amin, S. Islam, G. P. Biswas, M. K. Khan and N. Kumar, "An Efficient and Practical Smart Card Based Anonymity Preserving User Authentication Scheme for TMIS using Elliptic Curve Cryptography," *Journal of Medical Systems,* vol. 39, no. 11, p. 180, 2015.

[68] N. Lasla, M. Younis, W. Znaidi and D. B. Arbia, "Efficient distributed admission and revocation using blockchain for cooperative ITS," in *International Conference on New Technologies, Mobility and Security*, Paris, 2018.

[69] C. Cachin and M. Vukolic, "Blockchain consensus protocols in the wild," *ArXiv,* vol. 1707, 2017.

[70] Clique, "Ethereum Repository," [Online]. Available: https://github.com/ethereum/EIPs/issues/225 . [Accessed 2 July 2020].

[71] P. Schindler, A. Judmayer, N. Stifer and E. Weippl, "Distributed key generation with ethereum smart contracts," in *Cryptocurrency Implementers Workshop*, 2019.

[72] A. Shamir, "How to share a secret," in *Communications of ACM*, 1979.

[73] N. P. Owoh and M. M. Singh, "Applying Diffie-Hellman Algorithm to Solve the Key Agreement Problem in Mobile Blockchain-based Sensing Applications," *International Journal of Advanced Computer Science and Applications,* vol. 10, no. 3, pp. 59-68, 2019.

[74] T. Jiang, H. Fang and H. Wang, "Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis," *IEEE Internet of Things,* vol. 6, no. 3, pp. 4640-4649, 2019.

[75] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "Bars: A blockchain-based anonymous reputation system for trust management in VANETs," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2018.

[76] Z. Lu, W. Liu, Q. Wang, G. Qu and Z. Liu, "A privacy-preserving trust model based on blockchain for Vanets," *IEEE Access,* vol. 6, no. 45, pp. 655-664, 2018.

[77] M. Singh and S. Kim, "Crypto trust point (ctp) for secure data sharing among intelligent vehicles," in *International Conference on Electronics, Information and Communication*, 2018.

[78] X. Zhang, R. Li and B. Cui, "A security architecture of vanet based on blockchain and mobile edge computing," in *IEEE International Conference on IIoT Information Centric Networking*, 2018.

[79] M. Singh and S. Kim, "Trust bit: Reward-based intelligent vehicle communication using blockchain," in *IEEE World Forum on Internet of Things*, 2018.

[80] X. Zhang and X. Chen, "Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network," *IEEE Access,* vol. 7, pp. 58241-58254, 2019.

[81] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Project Yellow Paper, 2014.

[82] F. Zhang, R. Li, Y. Li and J. Song, "Research on identity authentication based on elliptic curve encryption algorithm in V2X communication," *Automotive Engineering,* vol. 42, no. 1, pp. 27-32, 2020.

[83] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, H. P. Drielsma, P. C. Heam, O. Kouchnarenko and J. Mantovani, "Automated validation of Internet security protocols and applications," *Lecture Notes Computer Science,* vol. 35, no. 76, pp. 281-285, 2005.

[84] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos and J. Rodrigues, "Biometrics based privacy-preserving user authentication scheme for the cloud-based industrial internet of things deployment," *IEEE Internet of Things,* vol. 5, pp. 4900-4913, 2018.

[85] M. Wazid, A. K. Das, N. Kumar , A. V. Vasilakos and J. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme on the internet of drones deployment," *IEEE Internet of Things,* vol. 6, pp. 3572-3584, 2019.

[86] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular adhoc networks," *IEEE Access,* vol. 5, pp. 14966-14980, 2017.

[87] H. Zhou, B. Liu, T. H. Luan, F. Hou, L. Gui, Y. Li, Q. Yu and X. Shen, "Chain cluster engineering a cooperative content distribution framework for highway vehicular communications," *IEEE Transactions of Intelligent Transport Systems,* vol. 15, pp. 2644-2657, 2014.

[88] S. He, D. H. Shin, J. Zhang, J. Chen and Y. Sun, "Full view area coverage in camera sensor networks: Dimension reduction and near-optimal solutions," *IEEE transactions of Vehicular Technology,* vol. 65, pp. 7448-7461, 2015.

[89] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Communication Surveys,* vol. 17, pp. 2377-2396, 2015.

[90] R. Wasef, X. Lu and X. Shen, "Complementing public key infrastructure to secure vehicular adhoc networks," *IEEE Wireless Communications,* vol. 17, pp. 22-28, 2010.

[91] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Communication Magazine,* vol. 55, pp. 122-129, 2017.

[92] T. Roosta, M. Meingast and S. Sastry, "Distributed reputation system for tracking applications in sensor networks," in *International Conference Mobile Ubiquitous System*, San Jose, 2006.

[93] S. Li and X. Wang, "Quickest attack detection in multi-agent reputation systems," *IEEE Journal of Selected Topics in Signal Processing,* vol. 8, no. 4, pp. 653-666, 2014.

[94] S. Gurung, D. Lin, A. Squicciarini and J. Bertino, "Information Oriented trustworthiness evaluation in vehicular ad-hoc networks," in *International Conference on Network System Security*, Madrid, 2013.

[95] Z. Li and C. T. Chignan, "On Joint Privacy and Reputation Assurance for Vehicular Ad Hoc Networks," *IEEE Transactions on Mobile Computing,* vol. 13, no. 10, pp. 2334-2344, 2014.

[96] X. Huang, R. Yu, J. Kang and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Acess,* vol. 5, pp. 25408-25420, 2017.

[97] N. Kumar, S. Misra, R. Iqbal and J. Rodrigues, "Coalition games for spatio-temporal big data in the internet of vehicles environment: A comparative analysis," *IEEE Internet of Things,* vol. 48, pp. 310-320, 2015.

[98] N. Kumar, Misra S., R. Iqbal and J. Rodrigues, "Bayesian coalition game for contention-aware reliable data forwarding in vehicular mobile cloud," *Future Generations Computer Systems,* vol. 48, pp. 6-72, 2015.

[99] T. H. Kim, G. Kumar, R. Saha, M. K. Rai, W. J. Buchanan, R. Thomas and M. A. Alazab, "Privacy-preserving distributed ledger framework for global human resource record management: The blockchain aspect," *IEEE Access,* vol. 8, pp. 96455-96467, 2020.

[100] R. Goyat, G. Kumar, M. K. Rai, R. Saha, R. Thomas and T. H. Kim, ". Blockchain-powered secure range-free localization in wireless sensor networks," *Arabian Journal of Science and Engineering,* vol. 45, pp. 6139-6155, 2020.

[101] N. Kumar, R. Iqbal, S. Misra and J. J. Rodrigues, "An intelligent approach for building a secure decentralized public key infrastructure in VANET," *Journal of Computer and System Sciences,* vol. 81, no. 6, pp. 1042-1058, 2015.

[102] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access,* vol. 4, pp. 2292-2303, 2016.

[103] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. Ogah and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transport systems," *IEEE Internet of Things,* vol. 4, pp. 1832-1843, 2017.

[104] C. Cai, X. Yuan and C. Wang, "Towards trustworthy and private keyword search in encrypted decentralized storage," in *IEEE International Conference on Communications*, Paris, 2017.

[105] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communication Survey Tutorials,* vol. 18, pp. 2084-2123, 2016.

[106] Z. Yang, K. Yank, L. Lei, K. Zheng and V. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things,* vol. 6, pp. 1495-1505, 2019.

[107] S. Sangeetha and S. Sathappan, "Self-organized gradient boosting key authentication for secured data communication in mobile adhoc network," *International Journal of Applied Engineering Research,* vol. 12, pp. 7823-7832, 2017.

[108] D. Jia, K. Lu, J. Wang, X. Zhang and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Communications Surveys and Tutorials,* vol. 18, no. 1, pp. 263-284, 2016.

[109] Z. Lu, G. Qu and Z. Liu, "A survey on recent advances in vehicular network security, trust and privacy," *IEEE Transactions on Intelligent Transportation Systems,* vol. 20, no. 2, pp. 760-776, 2018.

[110] G. Yan and S. Olariu, "A probabilistic analysis of link duration in vehicular adhoc networks," *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, no. 4, pp. 1227-1236, 2011.

[111] I. Singh, K. Mishra, A. M. Alberti, A. Jara and D. Singh, "A novel privacy and security framework for the cloud network services," in *International Conference on Advanced Communication Technology*, 2015.

[112] N. Malik, P. Nanda, A. Arora, X. He and D. Puthal, "Blockchain-based secured identity authentication and expeditious revocation framework for vehicular networks," in *International Conference on Big Data Science and Engineering*, 2018.

[113] H. Onishi, "A survey: Engineering challenges to implement vanet security," in *2018*, International Conference on Vehicular Electronics and Safety.

[114] "Tron Repository," [Online]. Available: https://github.com/tronprotocol. [Accessed 4th March 2021].

[115] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos and J. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for the cloud-based industrial internet of things deployment," *IEEE Internet of Things,* vol. 5, pp. 4900-4913, 2018.

[116] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos and J. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in the internet of drones deployment," *IEEE Internet of Things,* vol. 6, pp. 3572-3584, 2019.

[117] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular adhoc networks," *IEEE Access ,* vol. 5, pp. 14966-14980, 2017.

[118] "SPAN: the Security Protocol Animator for AVISPA," [Online]. Available: http://people.irisa.fr/Thomas.Genet/span. [Accessed 4th March 2021].

[119] S. Aggarwal, A. Ahuja, J. P. Singh and R. Shorey, "Route lifetime assessment based routing protocol for mobile adhoc networks," *Indian Research Lab,* pp. 1697-1701, 2000.

[120] R. Dube, C. D. Rais, K. Y. Wang and S. K. Tripathi, "Signal Stability based adaptive routing for adhoc mobile networks," *IEEE personal Communication,* vol. 7, no. 4, pp. 36-45, 1997.

[121] C. E. Jones, K. M. Sivalingam, P. Agrawal and J. C. Chen, "A survey of energy-efficient network protocols for wireless networks," *Wireless Networks,* vol. 7, no. 4, pp. 343-358, 2001.

[122] A. H. Ali, "Centrally coordinated power-aware route selection for MANETs," in *International Conference on Open Source Systems and Technologies*, 2003.

[123] Y. C. Tseng, Y. F. Li and Y. C. Chang, "On route lifetime in multihop mobile adhoc networks," *IEEE Transactions on Mobile Computing,* vol. 2, no. 4, pp. 366-376, 2003.

[124] P. I. Basarkod, S. S. Manvi and D. S. Albur, "Mobility based estimation of node stability in MANETs," in *International Conference on Emerging Trends in Computing Communication and Nanotechnology*, India, 2014.

[125] S. Sarkar and M. Adamaou, "A framework for optical battery management for wireless nodes," *IEEE Journal on Selected Areas in Communication,* vol. 21, no. 2, pp. 179-188, 2003.

[126] G. Zussman and A. Segall, "Energy-efficient routing in adhoc disaster recovery networks," in *IEEE Infocomm*, 2003.

[127] D. De Couto, D. Aguayo, J. Bicket and R. Morris, "A high throughput path metric for multihop wireless routing," in *International Conference on Mobile Computing*, 2003.

[128] S. Muthuramalingam, P. Janani, B. Bavya and R. Rajaram, "An energy-conserving topology maintenance algorithm for MANET," in *International Conference on Network and Communication*, 2009.

[129] C. F. Chiasserini and R. R. Rao, "Energy efficient battery management," *IEEE Journal on Selected Areas in Communications,* vol. 19, no. 7, pp. 1235-1245, 2001.

[130] S. Kahlid and A. Mehboob, "Design and Implementation of ID-based MANET auto-configuration protocol," *International Journal of Communication Networks and Information Security,* vol. 5, no. 3, pp. 141-151, 2003.

[131] K. Sharma and H. Monga, "Improve termite hill routing protocol using ACO WSN," in *International Conference of Computer Science and Engineering*, 2013.

Appendix A

SUMO Installation

Sumo 0.12.3 has been installed on our system. Its installation steps are as follows:

1. Downloaded sumo-src-0.12.3.tar.gz
2. Extracted it to the home folder, here we extracted it to /home/Sandeep/Downloads

   ```
   root@ubuntu:/home/Sandeep/Downloads# tar xvzf sumo-src-0.12.3.tar.gz
   ```

3. Installed important libraries

   ```
   root@ubuntu:/home/Sandeep/Downloads# apt-get install gfortran libproj-dev libxerces-c-dev libfox-1.6-dev
   ```

   Then installed sumo by following commands.

4.
   ```
   root@ubuntu:/home/Sandeep/Downloads# cd sumo-0.12.3
   ```

5.
   ```
   root@ubuntu:/home/Sandeep/Downloads/sumo-0.12.3# ./configure
   ```

6.
   ```
   root@ubuntu:/home/Sandeep/Downloads/sumo-0.12.3# make
   ```

7.
   ```
   root@ubuntu:/home/Sandeep/Downloads/sumo-0.12.3# make install
   ```

With these steps, sumo-0.12.3 got installed for use.

Appendix B

AVISPA Installation

To install AVISPA *v*1.1, you need to extract the archive avispa-package-1.1_Linux-*i*686.tgz in the desired directory, which will create a new sub-directory named avispa_1.0 populated by several files and sub-directories. Then you need to set the environment variable AVISPA_PACKAGE to refer to the absolute path ending in avispa-1.1, and to put the script called avispa in the execution path of your shell. The commands to install the AVISPA in the bash shell environment are:

```
tar -xzf /home/Sandeep/avispa-package-1.1_Linux-i686.tgz
```

```
export AVISPA_PACKAGE=/opt/avispa-1.1
```

```
export PATH= PATH :AVISPA_PACKAGE
```

Now you should be able to execute AVISPA, using the command avispa. Please see the README file for information about the command-line options of AVISPA. The AVISPA package provides a user-friendly mode for XEmacs to allow a simple interaction between the user and the modules of the AVISPA package. To set up the XEmacs mode follows the instructions below:

```
cd $AVISPA _PACKAGE/contrib tar -xzf avispa-mode.tgz
```

This command will create a directory temporary-avispa containing a makefile for installing the XEmacs mode. Follow the instruction in temporary-avispa/help.txt; when done, delete the temporary directory temporary-avispa.

The AVISPA package further provides the hlpsldoc tools for documenting HLPSL specifications in LATEX and HTML format. To set them up, follow the instructions below:

```
cd $AVISPA_PACKAGE/contrib/hlpsldoc tar xzf hlpsldoc.tgz
```

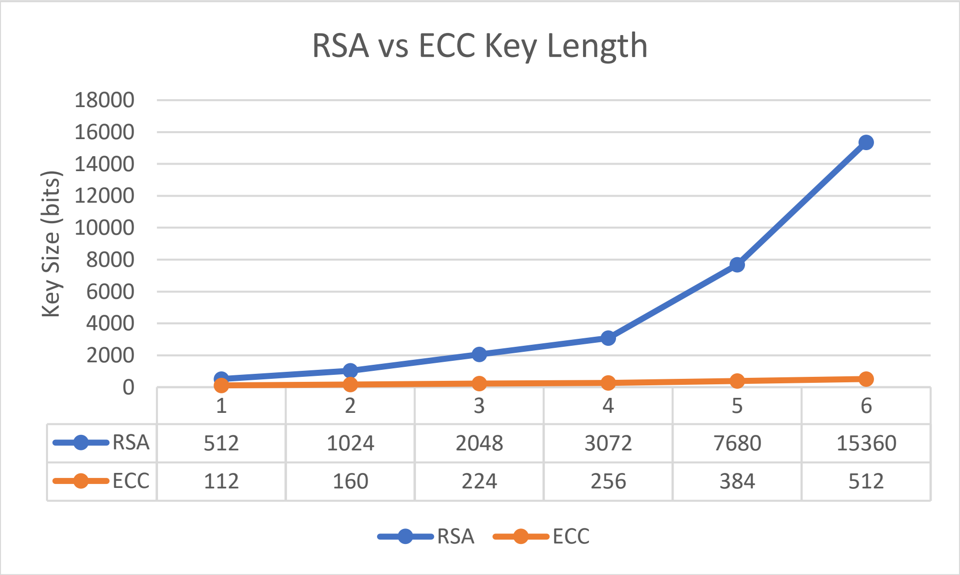
Then follow the instructions in the local INSTALL file. Usage of the hlpsldoc tools is explained in the local README file.

Appendix C

Elliptic Curve Cryptography (ECC)

The security protocols earlier used the RSA algorithm for public-key encryption and digital signature applications. However, with time the key size of RSA got increased that intensified the burden on computing systems. These complications gave rise to ECC. Figure C.1 illustrates the difference in key length between RSA and ECC. The ECC provides equal security with very little key size, thus reducing the burden on the computing system.

In Elliptic Curve Arithmetic (ECA), exponentiation indicates repeated multiplication, (for example, a^2 mod q = (a × a) mod q) whereas multiplication indicates repeated addition (for example, a × 2 = a + a).



	1	2	3	4	5	6
RSA	512	1024	2048	3072	7680	15360
ECC	112	160	224	256	384	512

Figure C.1: Key Length Comparison.

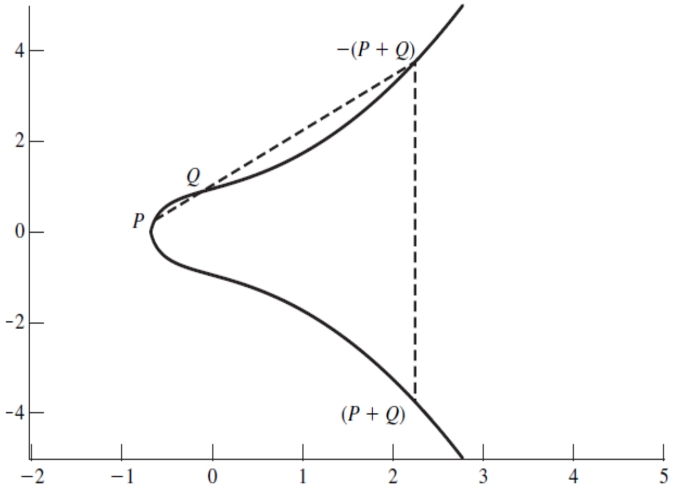


Figure C.2: Example of elliptic curve: $y^2 = x^3 + x + 1$.

The elliptic curves are represented through the *Weierstrass equation*. The elliptic curves are comprised of 2 variables and coefficients. It is worth noting that in cryptography the elliptic curves are restricted to finite fields. The *Weierstrass equation* for elliptic curves can be expressed as:

$$y^2 modp = (x^3 + ax + b) modp$$

Figure C.2 depicts an example of an elliptic curve that meets the following necessary condition of the coefficient set,

$$4a^3 + 27b^2 \; ƒ= 0$$