Faculty of Computer Science and Information Technology

Secure Trust-Based Algorithm using Blockchain Technology to Prevent Attacks in VANET

Kuhanraj Balan

Master of Science
2020

Secure Trust-Based Algorithm using Blockchain Technology to Prevent Attacks in VANET

Kuhanraj Balan

A thesis submitted

In fulfillment of the requirements for the degree of Master of Science

(Computer Science)

Faculty of Computer Science and Information Technology
UNIVERSITI MALAYSIA SARAWAK
2020

DECLARATION

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

……

Signature

Name: Kuhanraj Balan

Matric No.: 17020126

Faculty of Computer Science and Information Technology

Universiti Malaysia Sarawak

Date : 13 July 2020

ACKNOWLEDGEMENT

Ideas shape the course of history - John Maynard Keynes

My Masters journey began with an idea of packing myself with a few additional skills before stepping into the real world. The path was not easy but as I got to the peak, I realized that it would not have been possible without the contribution of a few beautiful souls.

First and foremost, I would like to thank my beloved parents, Mr. Balan and Ms. Kala Devi, and my siblings, Vinodraj and Kirtana who have been my greatest pillars of strength in this journey. A very special person, my better half, Komala Devi for her continued and unfailing love, support and understanding during my pursuit of Master's degree and helped me to keep things in perspective. Also, not forgetting my beloved uncle, Mr. Sevalingam and his friends, Mr. Dana Raja and Ms. Low Moi Jun for their endless care and support throughout my stay here in Sarawak.

Thank you, Dr. Adnan Shahid Khan, for your guidance as my supervisor over the last four semesters. I am forever in your debt for having confidence in me and my capabilities. I deeply appreciate your patience and indispensable advice to improve this research. My heartfelt regards to my mentors, Professor Dr. Narayanan Kulathuramaiyer, Associate Professor Dr. Johari Abdullah, Mr. Rajan Thangaveloo, Ms. Seleviawati Tarmizi and Ms. Emylie Conia Abdul for assisting me in getting my thesis evaluated on time.

Also, I truly appreciate Yasir Kiani for his time and effort in guiding me with his experience and knowledge in the field of VANET. In addition, I would like extend my sincere gratitude to my fellow comrades in arms, Kosheila Sundram Pillay, Suresh Ramachandran, Siva Raja Sindiramutty, Logasshini Nilavezhilan, Thamayanthi Nadaraja and Pavithra Madheuan for being there with me through thick and thin. Thank you for

tolerating all my bad smoke grenade throws during our Counter Strike LAN party sessions, although it was done on purpose.

My sincere thanks to Universiti Malaysia Sarawak (UNIMAS), for funding my Master's degree under the Vice Chancellor Research Zamalah (ZPNC) Scholarship. It has been so far the best form of encouragement I have ever received to come back and pursue my studies again in the Land of the Hornbills. Thank you, Research Innovation & Management Centre (RIMC), UNIMAS for efficiently managing my fees and my monthly allowance and my sincere thanks to the Centre of Graduate Studies (CGS), UNIMAS for assisting me with all my doubts and queries during my submission.

Last but not least, I would like to thank brother Shankar Ram, sister Karishma, brother Vikneswaren and brother Sekhar as well as the rest of the members of Sri Maha Mariamman Temple Association of Kuching for giving me the opportunity to serve the Almighty by giving me a small role in the efforts of rebuilding the temple for the Indian community in Kuching, Sarawak. Thank you and god bless.

ABSTRACT

Vehicular Ad hoc Networks (VANET) is also known as intelligent transportation systems. VANET ensures timely and accurate communications between vehicle to vehicle and vehicle to infrastructure to improve road safety and enhance the efficiency of traffic flow. Due to open wireless boundary and high mobility, VANET is vulnerable to malicious nodes that could gain access into the network and carry out serious network threats such as denial of service attack, data modification attack, impersonation attack, Sybil attack and replay attack. This could affect the network security and privacy, causing harm to the information exchange within the network and increase fatal impacts on the road. Therefore, a secure trust-based mechanism that utilizes blockchain technology has been proposed to increase security and privacy while minimising the aforementioned attacks. A series of experiment has been conducted using Veins simulation tool to assess the performance of the proposed solution in the terms of packet delivery ratio, end to end delay, packet loss and transmission overhead. The simulation results show that under network attack, the proposed solution incurs a better packet delivery ratio at 0.75, smallest percentage of packet loss at 25.5%, a shorter end to end delay of 0.13 seconds and lesser transmission overhead at 5.0% as compared to existing protocols.

Keywords: Trust model, blockchain, privacy, authentication, security, packet delivery, VANET

Algoritma Berasaskan Amanah yang Menggunakan Teknologi Blok Rantai untuk Mencegah Serangan dalam VANET

ABSTRAK

Rangkaian Ad hoc Kenderaan (VANET) juga dikenali sebagai sistem pengangkutan pintar. VANET memastikan komunikasi yang tepat pada masanya di antara kenderaan ke kenderaan dan kenderaan ke infrastruktur untuk meningkatkan keselamatan jalan raya dan meningkatkan kecekapan aliran lalu lintas. Oleh kerana ciri batasan tanpa wayar yang terbuka dan mobiliti yang tinggi, VANET terdedah kepada nod jahat yang dapat mengakses rangkaian dan menjalankan ancaman rangkaian yang serius seperti serangan penolakan perkhidmatan, serangan pengubahsuaian data, serangan penyamaran, serangan Sybil dan serangan berulang. Ini boleh menjejaskan keselamatan rangkaian dan privasi, menyebabkan kemudaratan pertukaran maklumat dalam rangkaian dan meningkatkan kadar kemalangan maut di jalan raya. Oleh itu, mekanisme yang selamat dan amanah dengan menggunakan teknologi blok rantai telah dicadangkan untuk meningkatkan keselamatan dan privasi sambil mengurangkan serangan yang dinyatakan di atas. Satu siri pengujian telah dijalankan dengan menggunakan alat simulasi Veins untuk menilai prestasi penyelesaian yang dicadangkan dari segi nisbah pengiriman paket, kelewatan dari hujung ke hujung, kehilangan paket dan penghantaran overhed. Hasil simulasi menunjukkan bahawa di bawah serangan rangkaian, penyelesaian yang dicadangkan menghasilkan nisbah penghantaran paket yang lebih baik pada 0.75, peratusan kehilangan paket yang paling kecil pada 25.5%, kelewatan dari hujung ke hujung yang terpendek iaitu 0.13 saat dan penghantaran overhed yang terendah pada 5.0% berbanding dengan protokol lain.

Kata kunci: *Model amanah, blok rantai, privasi, pengesahan, keselamatan, pengiriman paket, VANET*

TABLE OF CONTENTS

	Page
DECLARATION	i
ACKNOWLEDGEMENT	ii
ABSTRACT	iv
ABSTRAK	v
LIST OF TABLES	x
LIST OF FIGURES	xi
LIST OF ABBREVIATIONS	xiv
CHAPTER 1: INTRODUCTION	1
1.1 Research Background	1
1.2 Problem Statement	3
1.3 Research Aim and Objectives	4
1.4 Research Scope	5
1.5 Contributions of Research	5
1.6 Thesis Organization	5
CHAPTER 2: LITERATURE REVIEW	7
2.1 Introduction	7
2.2 Vehicular Ad-hoc Network	7
2.2.1 Network Model	9
2.2.2 VANET Components	10

2.2.3 VANET Network Architecture Types 12

2.2.4 Standard for Wireless Access in VANET 13

2.2.5 Characteristics of VANET 14

2.2.6 Challenges in VANET 16

2.3 Security Issues 19

2.3.1 Active Attacks 20

2.3.2 Passive Attacks 25

2.4 Current Approaches to Address Security Issues in VANET 27

2.4.1 Anonymous and Lightweight Authentication Based on Smart Card 27

2.4.2 Lightweight Authentication and Key Agreement Protocol 28

2.4.3 Hybrid Approach for Efficient Privacy-Preserving Authentication 29

2.4.4 Efficient, Scalable, and Privacy-Preserving Authentication Protocol 30

2.4.5 Secure Privacy-Preserving Authentication with Cuckoo Filter 31

2.4.6 Benchmark Protocol Method Comparison 32

2.5 Blockchain Technology 34

2.5.1 Blockchain Feature 37

2.5.2 Blockchain Consensus Mechanism 39

2.6 Simulation Tools 45

2.6.1 Simulation of Urban Mobility 45

2.6.2 Network Simulator 2 46

2.6.3 Global Mobile Information System Simulator 47

2.6.4 OMNeT++ 47

2.6.5 Vehicles in Network Simulation 47

2.7 Summary 49

CHAPTER 3: RESEARCH METHODOLOGY 50

3.1 Introduction 50

3.2 Proposed Blockchain in VANET 50

3.2.1 Assumptions 54

3.2.2 Components of Blockchain Scheme in VANET 55

3.3 Research Methodology and Flowchart 57

3.3.1 Stage 1: Formulation of Problem Statement 58

3.3.2 Stage 2: Design of Proposed Solution 59

3.3.3 Stage 3: Validation of Simulation Tool and Evaluation Metrics 73

3.3.4 Stage 4: Simulation and Analysis 78

3.4 Summary 78

CHAPTER 4: PERFORMANCE ANALYSIS 79

4.1 Introduction 79

4.2 System Development 79

4.3 Performance Analysis 85

4.3.1 Packet Delivery Ratio 86

4.3.2 End to End Delay 89

4.3.3 Packet Loss 92

4.3.4 Transmission Overhead 95

4.4 Summary 98

CHAPTER 5: CONCLUSION AND FUTURE WORKS 99

5.1 Introduction 99

5.2 Significance of Research 99

5.3 Research Contributions 101

5.4 Future Works 103

5.5 Summary 106

REFERENCES 107

LIST OF TABLES

		Page
Table 2.1	Summary of Benchmark Method Analysis	33
Table 2.2	Comparison of Simulators for VANET Simulation	48
Table 3.1	List of Notations and Description Used	62
Table 3.2	Default Parameters Set for SUMO Simulation	77
Table 3.3	Default Parameters Set for OMNeT++ Simulation	77
Table 4.1	Packet Delivery Ratio without Network Attack	87
Table 4.2	Packet Delivery Ratio with Network Attack	88
Table 4.3	End to End Delay without Network Attack	90
Table 4.4	End to End Delay with Network Attack	91
Table 4.5	Packet Loss Ratio without Network Attack	93
Table 4.6	Packet Loss Ratio with Network Attack	94
Table 4.7	Transmission Overhead without Network Attack	96
Table 4.8	Transmission Overhead with Network Attack	97

LIST OF FIGURES

		Page
Figure 1.1	Basic VANET Communication	1
Figure 1.2	Intrusion in VANET Communication	3
Figure 2.1	Structure of WANET	8
Figure 2.2	V2V and V2I Communication in VANET	10
Figure 2.3	The Classification of Attacks in VANET	20
Figure 2.4	DoS Attack in VANET	21
Figure 2.5	Replay Attack in VANET	23
Figure 2.6	Sybil Attack in VANET	24
Figure 2.7	Data Fabrication Attack in VANET	25
Figure 2.8	User Location Disclosure in VANET	26
Figure 2.9	Eavesdropping in VANET	27
Figure 2.10	Structure of Blocks in Blockchain	35
Figure 2.11	Data Structure of Block Hashing	35
Figure 2.12	Merkle Tree Structure	36

Figure 2.13 Blockchain Consensus Mechanism 40

Figure 3.1 Proposed Packet Structure with Blockchain Integration 52

Figure 3.2 Generation of Blockchain from Unconfirmed Event Messages 53

Figure 3.3 Flowchart of Research Methodology 57

Figure 3.4 System Design of Proposed Solution 59

Figure 3.5 Flowchart of Proposed Solution 61

Figure 3.6 System Initialization of Proposed Solution 63

Figure 3.7 System Authentication of Proposed Solution 65

Figure 3.8 Message Rating Generation of Proposed Solution 67

Figure 3.9 Trust Value Offset Calculation of Proposed Solution 68

Figure 3.10 Miner Election and Block Generation of Proposed Solution 70

Figure 3.11 Distributed Consensus of Proposed Solution 72

Figure 3.12 Classification of Various Simulators 73

Figure 3.13 Veins Hybrid Simulator 75

Figure 3.14 Veins Simulator Set up 76

Figure 4.1 Packet Delivery Ratio without Network Attack 87

Figure 4.2 Packet Delivery Ratio with Network Attack 88

Figure 4.3 End to End Delay without Network Attack 90

Figure 4.4 End to End Delay with Network Attack 91

Figure 4.5 Packet Loss without Network Attack 93

Figure 4.6 Packet Loss with Network Attack 94

Figure 4.7 Transmission Overhead without Network Attack 96

Figure 4.8 Transmission Overhead with Network Attack 97

LIST OF ABBREVIATIONS

3G	Third Generation
API	Application Program Interface
ASC	Authentication Based on Smart Card
AU	Application Unit
BFT	Byzantine Fault Tolerance
CA	Certification Authority
CFFG	Casper the Friendly Finality Gadget
CH	Cluster Head
CI	Confidence Interval
COaaS	Computing as a Service
CRL	Certificate Revocation List
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CTFG	Casper the Friendly Ghost
DCF	Distributed Coordination Function
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPoS	Delegated Power of Stake
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ESPA	Efficient, Scalable, and Privacy-Preserving Authentication
FBA	Federated Byzantine Agreement

FCC	Federal Communications Commission
GloMoSim	Global Mobile Information System Simulator
GPS	Global Positioning System
GPS	Global Positioning System
GUI	Graphical User Interface
HEPPA	Hybrid Efficient Privacy-Preserving Authentication
IEEE	Institute of Electrical and Electronics Engineers
In- VANET	Intelligent VANET
ITS	Intelligent Transport System
JOSM	Java OpenStreetMap
LAKAP	Lightweight Authentication and Key Agreement Protocol
MAC	Medium Access Control
MANET	Mobile Ad-hoc Network
MOVE	Mobility Model Generator for Vehicular Network
NaaS	Network as a Service
NETA	NETwork Attacks
NS-2.35	Network Simulator 2.35
OBU	On-Board Unit
OFDM	Orthogonal Frequency Division Multiplexing
OSM	OpenStreetMap
PBFT	Practical Byzantine Fault Tolerance
PDR	Packet Delivery Ratio
PKI	Public Key Infrastructure
PLCP	Physical Layer Convergence Procedure

PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof of Work
RPCA	Ripple Protocol Consensus Algorithm
RSA	Rivest-Shamir-Adleman
RSU	Road Side Unit
SD	Standard Deviation
SINR	Signal to Interference plus Noise Ratio
SPACF	Secure Privacy-Preserving Authentication with Cuckoo Filter
SUMO	Simulation of Urban Mobility
TA	Trusted Authority
TCP	Transmission Control Protocol
TraCI	Traffic Control Interface
UNL	Unique Node List
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VANET	Vehicular Ad-hoc Network
VuC	Vehicles using Cloud
WANET	Wireless Ad hoc Network
WAVE	Wireless Access in Vehicular Environments
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network
WWW	World Wide Web

CHAPTER 1

INTRODUCTION

1.1 Research Background

Vehicle Ad hoc Networks (VANET) emerged as a subset of a Mobile Ad hoc Network (MANET) (Ghori, Zamli, Quosthoni, Hisyam, & Montaser, 2018; Junaid, Syed, Warip, Azir, & Romli, 2018) application. VANET is considered as a substantial approach for the Intelligent Transportation System (ITS) (Gillani, Shahzad, Qayyum, & Mehmood, 2013). VANET has recently been the attention of various researchers in the wireless mobile communication field. The aim of VANET is to provide inter-vehicle communication and roadside units to vehicle communication to increase road safety and improve local traffic flow as well as the efficiency of road traffic by providing accurate and timely information to road users (Abbasi & Khan, 2018). In VANET, vehicles are used as network nodes as seen in Figure 1.1.

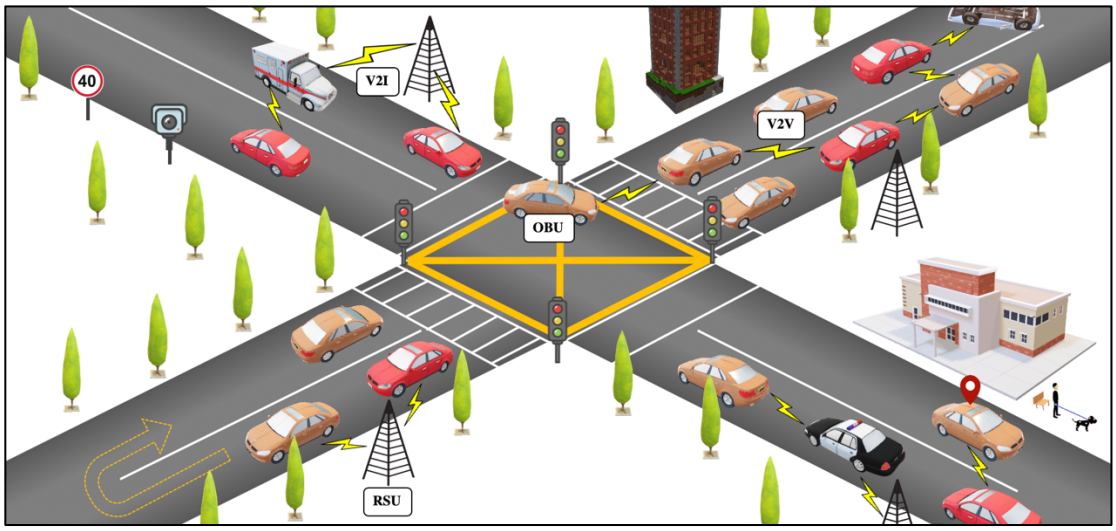

Figure 1.1: Basic VANET Communication (Khan et al., 2019)

As can be seen in Figure 1.1, VANET is comprised of vehicles equipped with On-Board Units (OBUs), fixed infrastructure known as Road Side Units (RSUs), and a wireless medium to allow the components to communicate with each other (Mishra, Singh, & Kumar, 2016). There are two types of communications in VANET, which are vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications. The OBUs and RSUs in VANET establish a connection among themselves with the help of dedicated short range communication (DSRC) in a single or multi-hop communication (Malik, Nanda, Arora, He, & Puthal, 2018; Hasrouny, Bassil, Samhat, & Laouti, 2015; Patel & Jhaveri, 2015). VANET offers various services and applications to the users, most of which are concerned with the safety of the drivers, infotainment, and navigational aid (Zeadally, Hunt, Chen, Irwin, & Hassan, 2012).

The main aim of VANET is to ensure safe driving by enhancing the flow of road traffic and, thus, minimizing the occurrence of vehicle accidents (Hasrouny, Samhat, Bassil, & Laouiti, 2017) which can have fatal impacts. Apart from providing on-board entertainment system, VANET strives to upgrade road safety and driving condition by detecting events or conditions information which can be shared with other nearby vehicles (Mejri, Ben-Othman, & Hamdi, 2014). There are two types of information shared in VANET, which are safety (vehicle speed warning, curve warning) and non-safety information (value-added comfort application) (Bhoi, Khilar, Singh, Sahoo, & Swain, 2018). By default, safety information is given a higher priority in VANET as compared to non-safety information since safety information notifies drivers of expected dangers and to respond early (Azees, Vijayakumar, & Deborah, 2016; Ghaleb, Razzaque, & Zainal, 2014).

1.2 Problem Statement

Despite the benefits offered by VANET, it comes with challenges, especially in terms of security and privacy of users and transmitted messages (Qu, Wu, Wang, & Cho, 2015). Figure 1.2 shows the exchange of sensitive information and traffic changes within the vehicles in VANET. It can be seen that there is a possible intruder in the network which may lead to a serious communication issue. A lack of authentication of this information can result in malevolent attacks which present harm to drivers (Xi, Sha, Shi, Schwiebert, & Zhang, 2007). Techniques such as pseudonyms (Florian, Finster, & Baumgart, 2014) and anonymous authentication (Li, Lu, & Guizani, 2014) has been developed to achieve the goal of preserving privacy of users in the network. However, these techniques may not be secure because reported traffic information can be utilised to link the pseudonyms to the users as vehicles do not change the pseudonyms during information exchange (Rabieh, Mahmoud, & Younis, 2017).

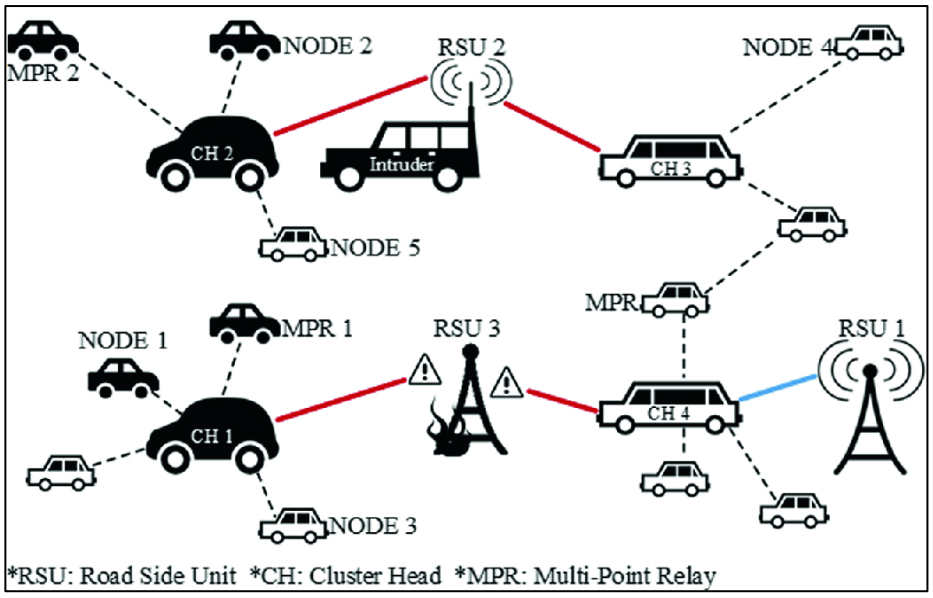

Figure 1.2: Intrusion in VANET Communication (Begum et al., 2016)

The characteristics of VANET (e.g. high mobility, volatility) which are distinct from other wireless communication networks have caused VANET to be susceptible to numerous internal and external attacks such as modification attack and denial of service attack, which could result in longer delay or fatalities. (Engoulou, Bellaïche, Pierre, & Quintero, 2014). Although solutions that can provide secure communication channels against external attacks are available, trust management and privacy protection for vehicles remains unresolved in VANETs (Zhang, Zheng, & Deng, 2018). Therefore, designing a secure VANET demands four key elements to be considered, which are privacy, trust, availability and integrity (Lu, Qu, & Liu, 2019) in order to reduce or prevent any major attacks in the network.

1.3 Research Aim and Objectives

The main aim of this research is to minimize the occurrence of malicious attacks in VANET by proposing a secure trust-based algorithm. In order to achieve the aim, the following research objectives are outlined:

a. To investigate and identify the potential security threats and requirements in VANET.
b. To propose a secure trust-based algorithm using blockchain technology to address trustworthiness of user and messages exchanged in VANET.
c. To evaluate the performance of the proposed solution using Veins simulator in terms of packet delivery ratio, end to end delay, packet loss and transmission overhead.

1.4 Research Scope

This research focuses on mitigating several security and privacy attacks that are impersonation, message fabrication, denial-of-service (DoS), and Sybil attacks. Secondly, this research focuses on the above-mentioned attacks occurring on a highway with straight road. Lastly, the evaluation of the proposed solution is conducted in a simulated environment using the Vehicles in Network Simulation (Veins) simulation tool.

1.5 Contributions of Research

The proposed secure trust-based algorithm implements blockchain technology to mitigate several network attacks in VANET such as impersonation, message fabrication, DoS, and Sybil attacks as well as to maintain the freshness of data in the network. The proposed secure trust-based algorithm uses a dual factor authentication approach to verify the identity of the users as well to ensure safe transmission of messages between vehicles.

1.6 Thesis Organization

A total of five chapter is included in this thesis. Chapter 2 describes the literature related to the research study. This chapter includes an overview of VANET detailing the characteristics, network model, architectures, and challenges of the network. Moreover, this chapter also discusses the security issues faced by VANET in terms of active and passive attacks. Chapter 2 also introduces the concept of blockchain technology and its integration in VANET.

In Chapter 3, a secure trust-based algorithm for VANET using blockchain is proposed. This chapter illustrates the research methodology used as a guideline to carry out this research and thesis writing. Furthermore, this chapter also presents the design and

frameworks of the proposed solution. A detailed explanation of each of the proposed frameworks is included in this chapter as well. This chapter also analyses several simulation tools available for research in VANET to identify the most suitable simulation tool for this research. The selection of a suitable simulation tool along with the simulation environment setup in order to analyse the performance of the proposed solution are discussed in this chapter.

Chapter 4 presents the performance analysis of the proposed solution. In this chapter, the development of the proposed solution is described in detail using the proposed algorithms developed to improve the security and privacy in VANET. Next, the performance of the proposed solution is analysed in terms of packet delivery ratio (PDR), end to end delay, packet loss, and transmission overhead. Each of the performance metrics is compared against several recent benchmark protocols to highlight the efficiency and effectiveness of the proposed solution.

Lastly, in Chapter 5, a conclusion of the thesis is presented with a summary of the contributions made by the research and some future works in VANET which may set a path for future research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter is specifically dedicated to discuss on the overview of the characteristics in VANET. Literature review that is presented in this chapter is in terms of their significance to the research question and available elucidations. This chapter first begins with an overview of VANET covering the characteristics, network model, architecture standards, standard of architecture types, standards of wireless access, security issues and research challenges. Then, the concept of blockchain technology in VANET is introduced in detail, which includes the features, consensus mechanism and scheme. Finally, an overview of similar techniques is discussed and their method of analysis is compared.

2.2 Vehicular Ad-hoc Network

In the last few years, automotive industry has emerged as one of the most attractive topics for researchers due to their enormous potential to improve traffic safety, effectiveness and other additional services. Vehicular Ad-hoc Network (VANET) derives from the root concept of wireless fundamental known as Wireless Ad-hoc Network (WANET) (Ghori, Zamli, Quosthoni, Hisyam, & Montaser, 2018; Jindal & Bedi, 2016). Figure 2.1 illustrates the structure of WANET which divides into three sub categories as follows: Wireless Mesh Network, Wireless Sensor Network (WSN) and also Mobile Ad-hoc Network (MANET). MANET is a superset of two categories where one is VANET and the other with the word Intelligent incorporated in front of VANET, known as In-VANET (Dak, Yahya, & Kassim, 2012).

Safety-critical applications and non-safety infotainment or entertainment-based applications are maintained by VANET. Safety based applications in this context includes collision avoidance, pre-crash sensing and lane changing, which are targeted to reduce road accidents, improve traffic monitoring and manage road safety applications. On the other hand, non-safety applications are used to access various services on the move. For instance, World Wide Web (WWW), interactive messaging, online gaming, payment services, and information or application updates. The significant difference between safety and non-safety applications is that safety applications is applicable for real time message passing. Through wireless access technologies, every vehicular node can access both kinds of services from the nearby infrastructure.

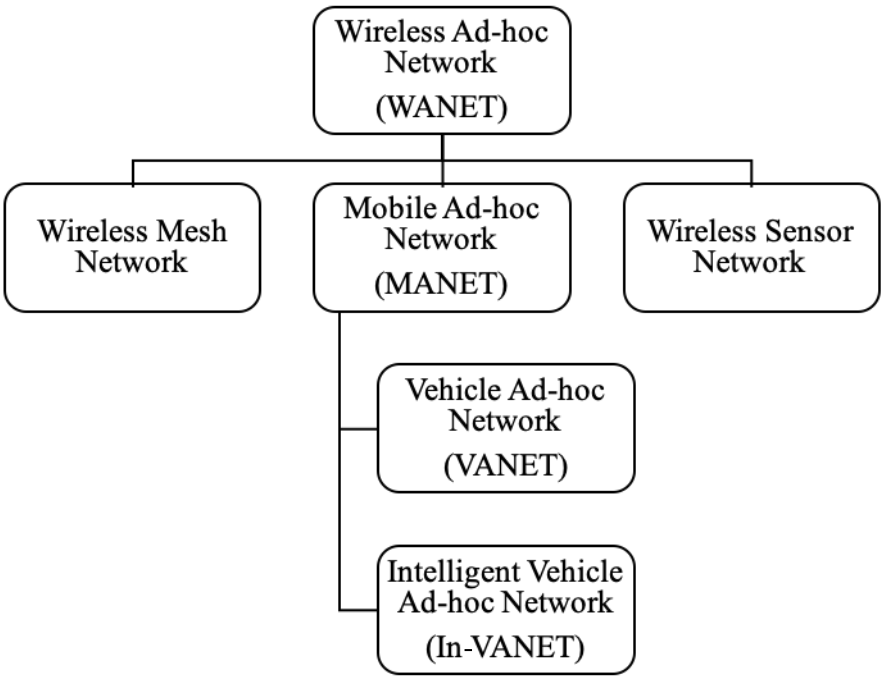

Figure 2.1: Structure of WANET (Dak et al., 2012)

Even though MANET is a superset of VANET, they do have many similarities such as dynamic topology, multi-hop data transmission, distributed architecture and Omni-

directional broadcast. Regardless to the network, route or relay data to the location of arrival is possible by the mobile node itself. Nevertheless, VANET and MANET have several distinguishable differences. The mobility of the vehicular nodes in VANET are easily foreseeable unlike MANET as the vehicles are moving along the direction of the road. In VANET, the nodes do not have a limitation of storage or processing capability for battery power nodes. The topology in VANET also has the tendency to become extremely dynamic as the nodes moves faster in pace. Furthermore, as time passes and location changes, the network density varies significantly in VANET.

2.2.1 Network Model

For both safety and non-safety applications, with the only focus of deploying V2V and V2I in VANET, the vehicular networks are evolving as a growing field of wireless technology. Figure 2.2 illustrates the communication between nearby vehicles of a vehicular node with RSU simultaneously in the VANET system. To certify that no malicious message pass through, RSU receives a message to authenticate the communication from the vehicle. Security related issues between the vehicular node and the RSU is handled by the autonomous server.

The two categories of communications present in the system are V2V and V2I. Both of this communication types are considered an essential component of Intelligent Transport System (ITS). Apart from that, for a successful V2V communication in the system, vehicles equipped with an OBU which includes of Omni directional antennas, processors, Global Positioning System (GPS) unit, and sensors. Furthermore, vehicular nodes do communicate with roadside devices known as RSU when they are placed at a fixed distance from the component depending on the communication range set in the system for a successful and

effective V2I communication with the neighbouring roadside infrastructures. The specified communication is possible either through wireless medium or wired connection and can be a mobile component. V2I communication can be expanded to allow other applications to incorporate such as the Internet as RSU capable of connecting to a network. In addition, the V2V communications permits real-time message passing and emergency message response functionality in case of accidents or traffic jam. This will be very helpful for other vehicles to receive the information early and take an alternative route to prevent traffic congestions.

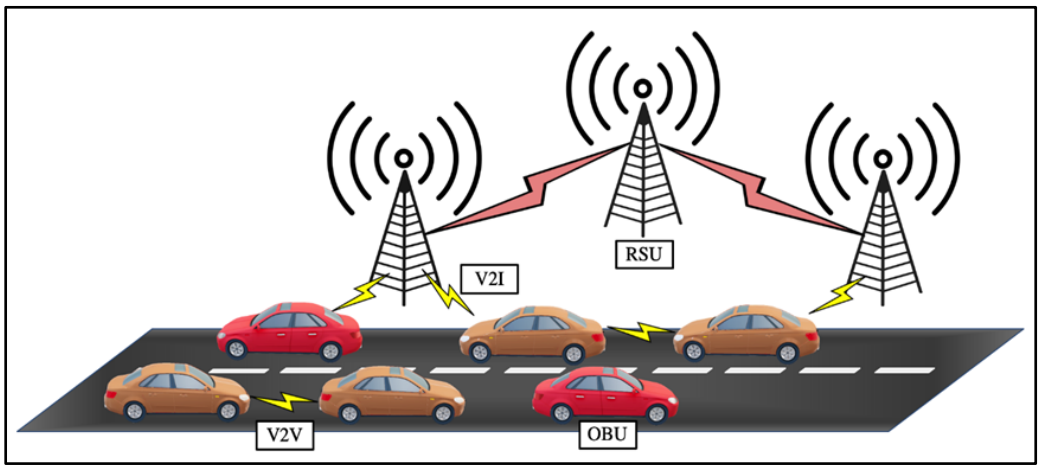

Figure 2.2: V2V And V2I Communication in VANET

2.2.2 VANET Components

Just like any other system with their specific architecture and standards, VANET system architecture composed of three types of domains comprised of in-vehicle, ad-hoc, and infrastructure domains. Application Unit (AU), OBU and RSU are few of the numerous components dedicated specifically for VANET system to function at its topmost efficiency. The architecture with brief explanation is given as follows:

(a) In-vehicle Domain

In-vehicle domain comprises of wired and wireless connections between an OBU and to single or multiple AUs. An OBU is a major component used in V2V and V2I communication. A network device means a device used typically for the purpose of sending and receiving messages including boosting the safety and non-safety messages in an ad-hoc domain; and OBU is equipped with a single network device based on Institute of Electrical and Electronics Engineers (IEEE) 802.11p radio technology. Besides, AU is an embedded-in-vehicle entity whereby several of the entities can be implemented together with a single OBU to share the processing and wireless resources.

(b) Ad-hoc Domain

Ad-hoc domain comprised of two units namely RSU and OBU. RSU is a static node and one or more RSU can be communicated with each other directly or via multi-hop and can be connected to the Internet facility via the gateway. Furthermore, RSU serves the purpose of delivering internet connectivity to OBUs in the network for communication whereas OBU is a mobile node and allows communication between vehicular nodes without the need for a centralized coordination to form a mobile ad-hoc network.

(c) Application Unit

Another embedded in-vehicle entity necessary for VANET system is AU. A single OBU can accept multiple-plugged AUs to share the processing and wireless resources of it. OBU is similar to a manager that manages all the mobility and networking facilities of AUs in the network (Choi, Rajkumar, Mudalige, & Bai, 2009).

(d) On-board Units

This unit is dedicated for the purpose of V2V and V2I communications. In an ad-hoc domain, OBUs serve the purpose of delivering communication services to the AUs and forwards informational data on behalf of them among the network. IEEE 802.11p is the standard commonly used for furnishing an OBU with at least a single network device.

(e) Road-side Units

RSU is a long-range communication device that is placed at stationary along the roadway or at a permanent position at a consistent distance from one RSU to another. RSU is required to be equipped with at least a single network device in the system based on IEEE 802.11p since the internet connectivity to the OBUs are the core purpose of RSU.

2.2.3 VANET Network Architecture Types

The VANET network architecture comprised of three categories namely: Cellular/wireless local area network (WLAN), pure ad-hoc and hybrid network architecture. A brief explanation of the specified network architectures is given as follows:

(a) Cellular/WLAN Network Architecture

The access points used in WLAN network architecture are WLAN/Worldwide Interoperability for Microwave Access (WiMAX). Fixed and cellular getaways are the ways used to connect to the Internet facility. VANET can associate both WLAN and cellular network to introduce such type of network so that a WLAN is used where an access point is accessible or a third generation (3G) connection can be used.

(b) Ad-hoc Network Architecture

Due to the high cost of the cellular/ WLAN network architecture that uses a fixed gateway, access points and other devices to build the network. As a solution to this matter, ad-hoc network architecture is introduced in vehicular nodes and all the RSU or road-side wireless devices for a network connectivity among themselves.

(c) Hybrid Network Architecture

This network architecture is a mixture of both the Cellular/WLAN and ad-hoc network architecture as the name of suggests and a likely solution for VANET system. Hybrid network architecture can provide VANET with a better coverage of network for the issues such as the seamless transition of communication among the various kinds of wireless systems.

2.2.4 Standard for Wireless Access in VANET

There are two standards for wireless access in VANET comprised of DSRC and IEEE 1609- standard for Wireless Access in Vehicular Environments (WAVE). A brief description to the standards is as follows:

(a) Dedicated Short Range Communication (DSRC)

This standard is for communication that ranges from 300 m to 1000 m where the V2V and V2I communication happens. As assigned by the United States Federal Communications Commission (FCC), the DSRC uses a spectrum of 75 MHz at 5.9 GHz that would provide half-duplex with a data transfer rate of 6-27 Mbps. Seven channels were ordered for the DSRC spectrum each with a 10 MHz wide. Of all the seven channels, one channel is dedicated kept for the safety communication purpose in the system; two channels

are dedicated for critical safety of life and high-power public; and the remaining four channels are used as service channels.

(b) IEEE 1609-standards for Wireless Access in Vehicular Environments

This standard is also commonly known as IEEE 802.11p and a necessity for the small range communications of the ITS. The frequency range used for V2V and V2I according to WAVE is 5.85 – 5.925 GHz as it is perfect to generate real-time traffic congestion statistics to further improvise on the VANET performance. In addition, it is also profitable in the sense of transport sustainability. Besides, this standard uses Orthogonal Frequency Division Multiplexing (OFDM) technique for the purpose of signal divisioning into multiple narrow band channels.

2.2.5 Characteristics of VANET

Since VANET is a subset of MANET, VANET shares some characteristics of MANET; but it also has several characteristics that are unique and distinct than MANET due to its high-speed nodes and dynamic topology. The following subsections discuss the characteristics of VANET.

(a) Wireless Communication

Wireless environment is what VANET is made to serve. The communication such as the connection authentication and information exchanges happen through wireless network. Hence, security elements such as confidentiality, integrity and availability have to be preserved in the VANET system at all times.

(b) High Mobility of Nodes

The common case of scenario in VANET would be the high-speed vehicular node movements all the time. As the mobility of the node gets higher, the harder it gets to predict the location or position of a node. Indirectly, this results in protecting the privacy of the node difficult too (Kolte & Madankar, 2014).

(c) Rapidly Changing Network Topology

As mentioned in Section 2.2.1.2, the mobility of the nodes is high and the speed of the vehicular nodes are unpredictably changing at random. Therefore, the location or position of the node varies frequently too. In return, the network topology in VANET have the ability to change frequently too.

(d) Unbounded Network Size

In VANET, the system can be implemented to a place of any size or area for communication to occur at any point of time. This means that the network size of VANET is geographically unbounded.

(e) Real-Time, Time-Sensitive Data Exchange

The vehicular nodes are encouraged to collect data from the RSUs and other vehicular nodes which are motivated by the ad hoc nature of VANET. Therefore, the nodes are required to communicate among themselves more frequently.

(f) Time Critical

VANET system is considered as time critical as it is essential for the nodes to deliver messages within the constricted time frame for a successful and effective communication. It

is also crucial when it comes to decision making based on the message or information delivered to each node to perform the consecutive action accordingly.

(g) Sufficient Energy

In the context of energy, VANET does not experience any issues with the computational resources and energy to perform the computational processes. This characteristic also increases the demand to implement techniques such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) in VANET which allow the unlimited usage of transmission power.

(h) Better Physical Protection

Physically, the nodes and components in VANET are protected better. Hence, it is more challenging to compromise VANET physically and to limit the infrastructure attacks.

2.2.6 Challenges in VANET

(a) Mobility

The major challenge faced in VANET environment is mobility of the nodes which can be an RSU or vehicles that are stuck in the traffic congestion or the one vehicle moving in a fast pace. The nodes within the system itself have challenges in communicating (Hasrouny, Bassil, Samhat, & Laouti, 2015). The mutual communication window during high velocity scenario is kept small which is only for a few seconds due to small transmission range. Besides, the communication system has to cope with the Doppler Effect, frequent link failures, wastage of network bandwidth, and high end-to-end delay for high relative velocity (Lim & D., 2016). Although nodes have high period of message exchange, they must deal

with the problems related to high vehicular traffic density such as frequent data collision, channel fading, message dropping due to expired waiting time, and other interferences.

(b) Volatility

Due to the coverage area of vehicles, the connectivity can be lost with the high mobility and might travel in opposite direction that makes the nodes connectivity extremely ephemeral. Long live context lacks in VANET systems where a hotspot with a long-life password from the user node is required and at the same time impractical for securing volatile connections.

(c) Privacy Versus Authentication

Privacy in keeping their personal details private, protected and not exposed by the drivers will be quite difficult when the system is set to give identity to all the individual vehicles in order to avoid Sybil attack.

(d) Privacy Versus Liability

Each vehicular node has the right to keep its personal details from other nodes while not violating the privacy no matter of the situation. For example, during an accident, the legal investigation is allowed to access data without any denial and it is the advantage of the liability that provides the opportunity for open investigation platform.

(e) Network Scalability

In VANET, network scalability alludes to the capacity of dealing with new nodes without compromising performance. In the structure of VANET, an expansion in the number of vehicles may lead to network congestion and connectivity issue.

(f) Traffic Density

A node in the context of VANET system can be placed in a high-density network such as the traffic jam or in low density network such as the highway roadway with no or less surrounded vehicle. During low density network, an advanced information message dissemination using store-and-forward message is transmitted instead of the immediate message forwarding (Raya, Jungels, Papadimitratos, Aad, & Hubaux, 2006). The same message has the possibility of repeating multiple times by the same vehicle due to this case scenario. In case of high-density network, it is achieved by choosing only selected vehicles given permission to send repeated message. The density of the node influenced by the road and time that is commonly measured as high during the daytime compared to other times (La & Cavalli, 2014). In case of high density, the opposite must be achieved with only selected vehicles allowed to send repeated messages.

(g) Movement Pattern

The vehicular node follows a predefined path instead of a random path as different roads comes with various characteristics. Compared to rural and highway roads, urban roads are usually a dense roadway with numerous vehicles, buildings and other obstacles. As the characteristics of the roadways differ, the movement pattern of the vehicular nodes varies too due to the challenge they pose for an efficient communication (Hasrouny, Bassil, Samhat, & Laouti, 2015). For example, urban roads are not highly ordered as the highway roads in terms of movement.

(h) Heterogeneity

Heterogeneity is also a challenge in VANET system as every single node have their own characteristics depending upon their applications be it either a stationary node such as RSU or mobile node such as the vehicles. Moreover, the nodes can be categorized into different levels according to the requirements of the application (Wu, Liu, Zhang, & Zhang, 2014). To support the heterogeneity characteristics, each vehicular node can be further classified into private, authority and maintenance based on the vehicle whereas RSU can be classified into data emit able and completeness of ad-hoc features (Hasrouny, Bassil, Samhat, & Laouti, 2015). RSUs do not require a privacy feature unlike the vehicular nodes. Therefore, VANET system shall be able to provide services based on the requirements of singular nodes.

2.3 Security Issues

Nodes in VANET are exposed to two types of attacks which are physical and non-physical attack. Physical attack refers to the physical damages done externally to the nodes whereas non-physical attacks are attacks that disrupts message transmission between nodes during communication. VANET is exposed to numerous non-physical attacks because of the open nature of the wireless medium used for communication in the system. There are two types of non-physical attacks in VANET which are active and passive attack. Figure 2.3 depicts a chart of classification of types of non-physical attacks involved in this system.

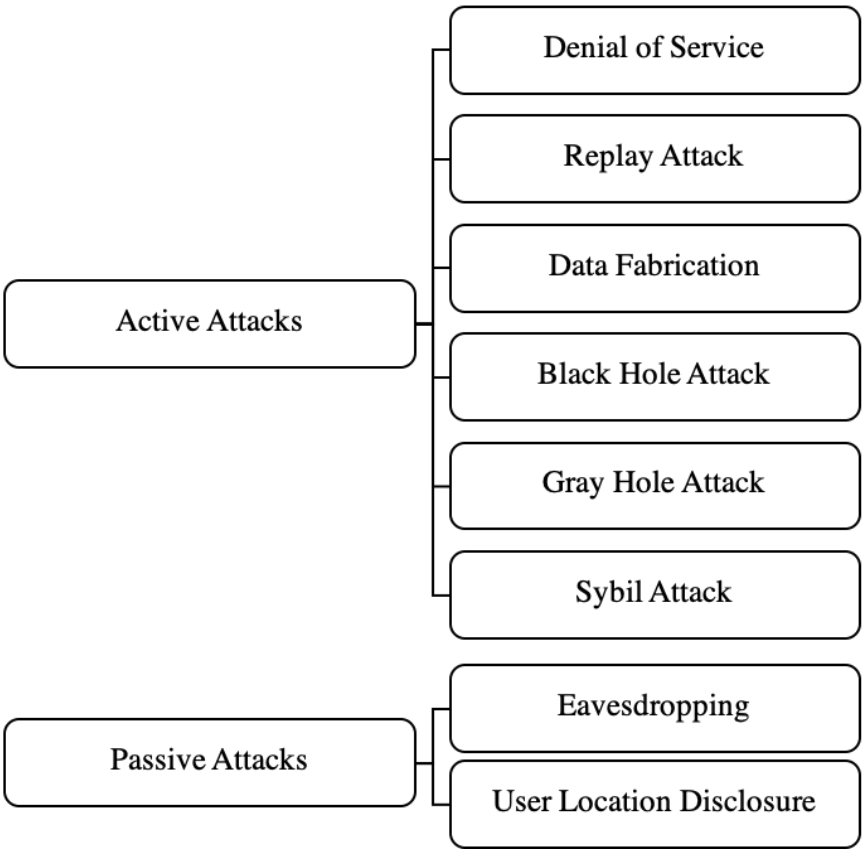

Figure 2.3: Classification of Attacks in VANET (Maria et al., 2016)

2.3.1 Active Attacks

An active attack means an attack initiated by a hacker by exploiting a network in an attempt to make change to the information on the target or the information bound to the route. There are seven attacks namely Denial of Service (DoS), replay attack, data fabrication, user location disclosure, black hole attack, grey hole attack and Sybil attack.

(a) Denial of Service

The most severe attack in VANET system is DoS attack as shown in Figure 2.4. Hackers use this type of attack to stop the legitimate vehicular nodes from accessing the network services, leading them to perform other network attacks. Some of the DoS attack types are jamming, SYN (synchronize) flooding and distributed DoS attack.

i. **Jamming:** This attack is possible when the hacker gets the access to the frequency of the channel and misuses it to deprive communication channel between any two nodes to prevent the flow of a specific or all information.

ii. **SYN Flooding:** Also known as a half-open attack that transmits huge amount of SYN requests to a targeted node in effort to exploit the resources of the server to make the system unresponsive to legitimate traffic information.

iii. **Distributed Denial of Service (DDoS):** Among the three DoS attacks, DDoS is considered the severest attack since it utilizes multiple compromised nodes as a source of attack traffic to ensure the impact is dispersed in the network.

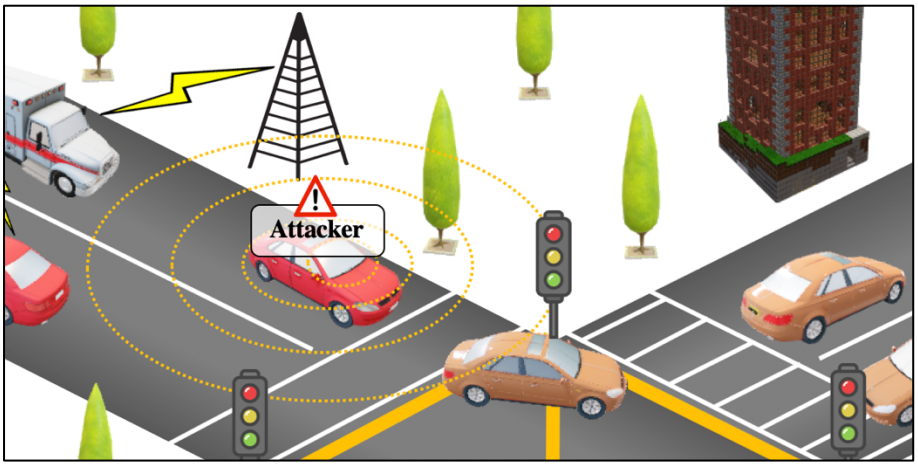

Figure 2.4: DoS Attack in VANET (Khan et al., 2019)

(b) Black Hole Attack

Black hole attack is advertising a malicious node as having an optimum route to the intended node by exploiting the flooding-based routing protocol. This attack is performed by sending a reply to the request from the malicious code right before the actual node replies. Therefore, a false route is generated for that specific communication channel. The attacker node falls out of the black hole that will make all the routes it involves broken down leading to a failure to broadcast message. In this attack, the malicious user known as black node, enters the network to stop forwarding information to the correspondent node.

(c) Grey Hole Attack

A specialized version of black hole attack is known as grey hole attack which indicates the unpredictable behaviour of a malicious node. The node at first acts as though it is an honest node during route recovery process but then changes its state to malicious and vice-versa. Probability distribution is when the system take advantage to drop the data packets or during the Transmission Control Protocol (TCP) packet forwarding. Congestion, overloading and the ability of state-changing makes the identification of this type of attack challenging and dangerous in terms of the ability of broadcasting false information. This attack disrupts the network performance of a system and alters the route discovery process through the malicious node.

(d) Replay Attacks

In order to take advantage of the scenario, the attacker reinjects a previous information at the second of the message sending. No security can be provided against the assault by basic IEEE 802.11pp since it does not come with a unique sequence of numbers or timestamp (La & Cavalli, 2014). The objective of the replay attackers is to escape the hit

and run situation by not exposing the identity of the vehicle. This attack type is also considered a network attack that would maliciously or fraudulently iterate or postpone a valid data transmission (Waghmode, Gonsalves, & Ambawade, 2016). Retransmission of the message with poisoning a node's location table by replaying beacons is the most common assault. Figure 2.5 depicts a replay attack whereby attacker replays an incident that occurred at an earlier time, T1 at a later time, T2. This attack can be prevented by operating VANET in the WAVE framework yet it has to maintain the time accurately to continue protect the system from replay attack.

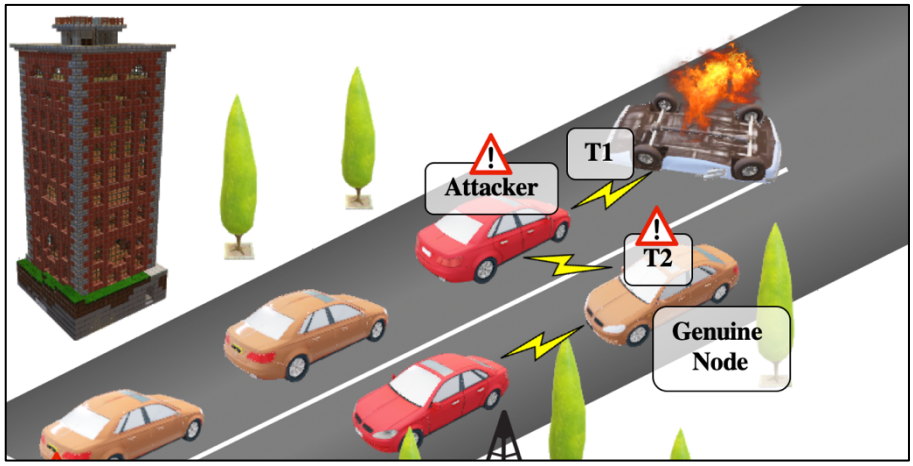

Figure 2.5: Replay Attack in VANET (Khan et al., 2019)

(e) Sybil Attack

This network attack is a forgery action taken by hackers to their advantages. For example, the hacker generates a large number of pseudonyms that creates the system users to believe that there is a traffic congestion. As a result, the users are forced to take an alternative route that becomes a benefit of the hacker for their intended aim. It takes multiple identities to simulate multiple nodes. Figure 2.6 is an example of Sybil attack that is caused

by an attacker who created multiple nodes and communicated the information to the nearest RSU, causing the RSU to interpret and inform other nodes that there is traffic congestion at that particular area. This makes the system dangerous and vulnerable to risks as the bone node gives its various locations at the same time.

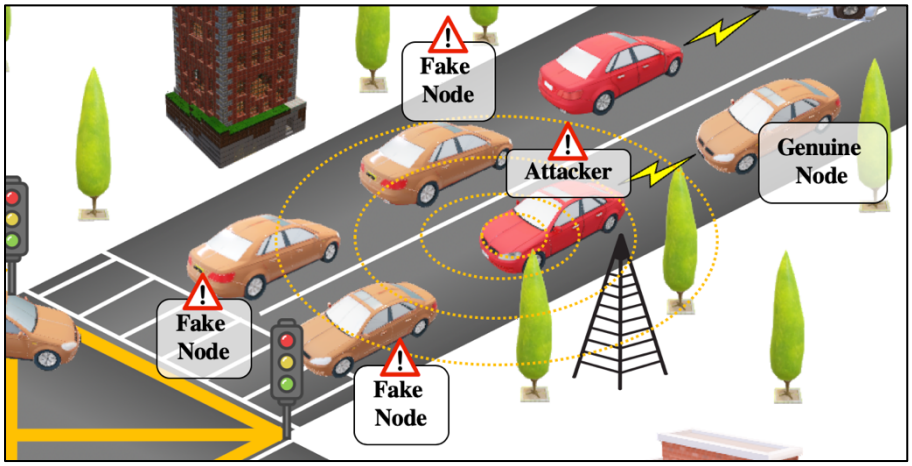

Figure 2.6: Sybil Attack in VANET (Khan et al., 2019)

(f) Data Fabrication

Data fabrication is a network security attack whereby the hacker initiates this assault of sending false information into the system. The information can be either incorrect or the transmitter claims it to be a message from another node. This security breach comprises of message generation, warning, declaration and personalities. In Figure 2.7, it can be seen that an attacker has injected a false information that the vehicle ahead is stalled, causing traffic build up ahead. This message is directly injected into the nearest RSU, warning nearby vehicle on the condition and requesting vehicles to take diversion, clearing the road ahead for the attacker to travel.

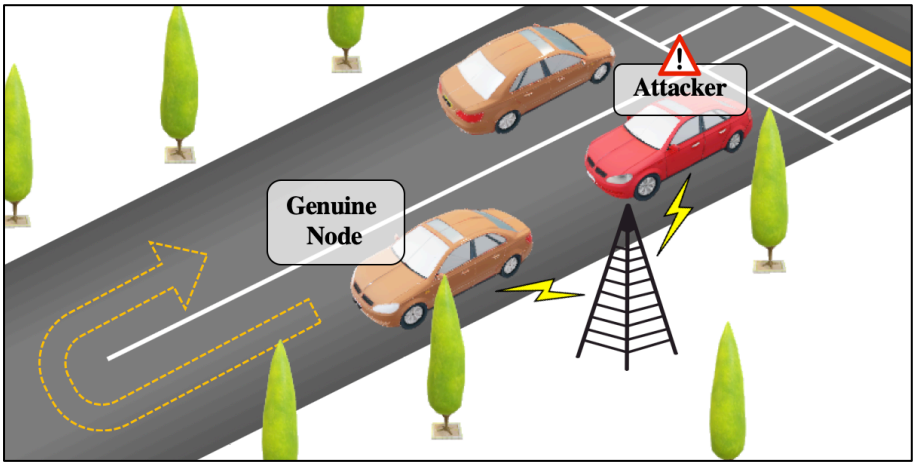

Figure 2.7: Data Fabrication Attack in VANET (Khan et al., 2019)

2.3.2 Passive Attacks

This type of attacks is common when an unauthorized party monitors network and sometimes scans for open ports and vulnerabilities. The focus of this attack is to gain information of the target and no change of information occurs.

(a) User Location Disclosure

Another security threat is the user location disclosure. It is one of the very few passive attacks of a network. This attack is conducted by sending a malicious code to a neighbouring node and attaining all the required information such as user identification and current location of the neighbouring node. This results in the losing of privacy of a vehicular node. Based on Figure 2.8, the location data of a genuine node is being attained by attacker by accessing its GPS system and monitoring the pathways taken by the genuine node.

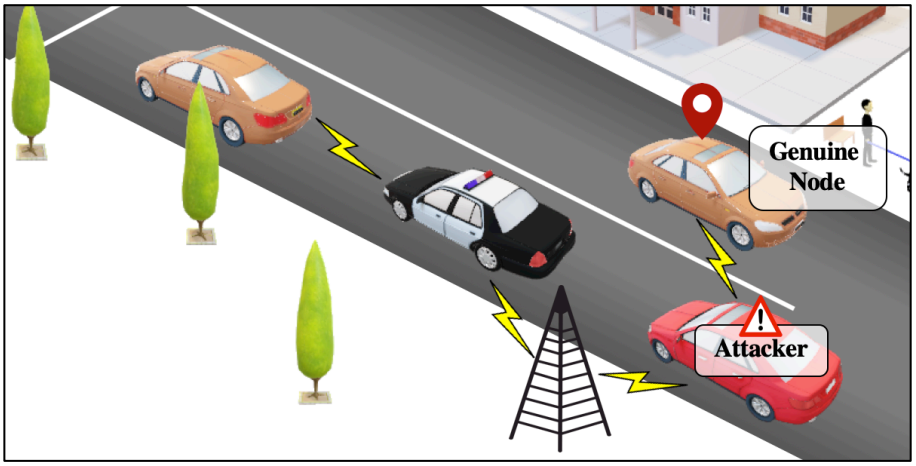

Figure 2.8: User Location Disclosure in VANET (Khan et al., 2019)

(b) Eavesdropping

Eavesdropping is also known as snooping or sniffing which is an unauthorized real-time interception of network traffic such as a phone call, instant message and video-conference or fax transmission. This network security attack is derived from the habit of actually standing under the eaves of a house, listening to discussions inside (Malla & Sahu, 2013). The attacker targets weakened message transmission to listen to message transmission in the network. For instance, in Figure 2.9, an attacker is eavesdropping to the sensitive information that is being exchanged between an RSU and an authority vehicle. That information could later be possibly used for a malicious purpose and the best countermeasure for this attack is by applying a better data encryption.

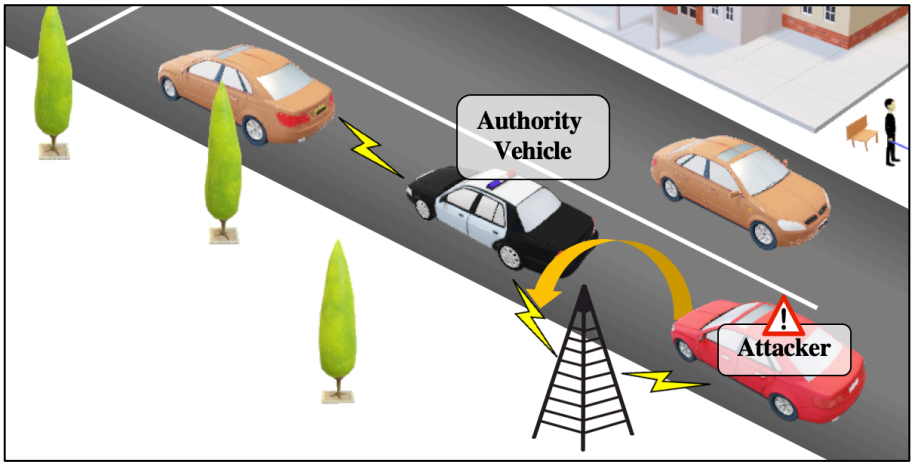

Figure 2.9: Eavesdropping in VANET (Khan et al., 2019)

2.4 Current Approaches to Address Security Issues in VANET

There have been numerous security schemes proposed by various researchers to address the security and privacy issues in VANETs. This section highlights some of the existing approaches that focused similar on problems in VANET.

2.4.1 Anonymous and Lightweight Authentication Based on Smart Card

Ying and Nayak (2017) proposed an anonymous and lightweight authentication scheme based on smart card (ASC) to address privacy-preserving problems such as legitimacy of users and messages transmitted across the network. The authentication of users and message are done using low-cost cryptographic operations. This protocol does not only verify the identity of the users and authenticate messages communicated, but it also guarantees anonymity of users. Anonymity in this scheme is achieved by dynamically generating login identities for users using smart cards to replace users' actual identity; thereby, hiding the real identities of users from attackers. The dynamic login identity is updated periodically to provide anonymous authentication. The researchers also proposed a

dynamic password change without depending on a trusted authority (TA) so that the scheme is resistant to various attacks such as impersonation and offline password guessing attack. The messages in ASC are authenticated using two hash chains to minimize computation complexity. Apart from that, messages are appended with timestamps obtained from GPS devices to validate the freshness of the messages and minimise replay attacks. The performance of ASC was evaluated using VanetMobiSim in terms of communication and computation overheads, end-to-end delay, and average packet loss ratio. From the simulation, ASC was found to perform better and has better efficiency than other baseline protocols. Nevertheless, a major drawback of ASC is the frequent update of login identity and user password which will introduce higher computation cost in the network. Not only that, the frequent update of login identity of many users at a time may increase the chances of network downtime, opening new opportunities for attackers to network launch network attacks.

2.4.2 Lightweight Authentication and Key Agreement Protocol

Wazid et al. (2017) proposed a decentralized lightweight authentication and key agreement protocol (LAKAP) for VANETs, which uses one-way hash functions and bitwise XOR operations. The proposed lightweight protocol highlights several key features such as dynamic addition of RSU in the network after initial deployment and providing key establishment between RSUs for anonymity and untraceability purpose. Apart from that, the solution exhibits three authentication approaches: between vehicles, between vehicle and its respective cluster heads (CHs), and between CHs and their RSUs. The researchers adopted a cluster-based network model to reduce the computation and communication overheads. In this proposed protocol, the CHs are elected based on trust values and strong connectivity.

Only vehicles with high trust values and strong connectivity are selected as the CHs. Each of three authentication approaches also establishes a keypair for the nodes involved. Besides that, a key is also established between neighbouring RSUs to maintain secure communication using the keys. The proposed lightweight authentication scheme uses timestamps to prevent replay attacks in the network. The passwords of each vehicles are updated periodically to improve the security of the user and protect the information such as traffic updates that is exhanged by vehicles in the network. The performance of the proposed scheme was evaluated using Network Simulator 2.35 (NS-2.35) in terms of communication and computation overheads, throughput, end-to-end delay, and PDR. From the analysis, the lightweight authentication and key agreement protocol was found to have a lower communication and computation costs, which indicates that the protocol is efficient. However, in a high-mobility and dynamic environment, it is difficult to select vehicles as CHs due to the high velocity of the vehicles. This could lead to inefficiency as well as unnecessary waste of energy of the nodes. Not only that, the periodic update of vehicles' passwords could also lead to an increased computational overhead in the network as the OBUs need to compute the identity and password of each vehicle before a new password could be passed to the vehicle.

2.4.3 Hybrid Approach for Efficient Privacy-Preserving Authentication

Rajput, Abbas, Eun, and Oh (2017) proposed a hybrid approach for privacy-preserving authentication scheme (HEPPA), which combines features of pseudonym-based approaches and group signature-based approaches, with conditional anonymity. According to the researchers, the real identity of an attacker can be uncovered during the detection of a malicious activity. This hybrid approach uses a simple and lightweight pseudonym which

provides conditional anonymity. The pseudonym provides a trapdoor mechanism to enable the detection of malicious user and subsequently revoke such user from the network. They also introduced a cloud-assisted modular architecture that acts a Certification Authority (CA) which is responsible for vehicle registration and verification of their credentials. Another feature of the hybrid approach is the grouping of vehicles based on regions that are managed by the CA using similar credentials so that attackers cannot differentiate between vehicles in the group. The scheme does not require a vehicle to manage the Certificate Revocation List (CRL) to reduce processing overhead on OBU and bandwidth consumption. The researchers used ECC as the cryptographic tool, in which elliptic curve integrated encryption scheme (ECIES) is used for encryption and ECDSA is used for the signatures of the vehicles. The performance of the proposed hybrid approach was analyzed via simulation using Veins in terms of communication and computation overheads, end-to-end delay, PDR, and packet loss. The simulation results show that the proposed hybrid approach is feasible enough to enhance privacy of users in VANET. Nevertheless, a drawback of this approach is the region-based grouping of vehicles in the highly dynamic and high-speed network. Vehicles enter and leave a region quickly due to their high velocity, therefore, increasing the difficulty in managing the groups by the CA.

2.4.4 Efficient, Scalable, and Privacy-Preserving Authentication Protocol

Tangade & Manvi (2016) proposed an efficient, scalable, and privacy-preserving authentication (ESPA) protocol using hybrid cryptography approach for inter vehicle communications. ESPA is comprised of two phases, which are Phase-I: V2I pre-authentication and Phase-II: V2V authentication. After off-line registration of vehicles and RSUs, the beacon signal of each vehicle is pre-authenticated by RSU during V2I

communication to verify whether the vehicle belongs to any base stations in the network or is an unauthorized vehicle. The pre-authentication is carried out using asymmetric public key infrastructure (PKI). In the second phase, only vehicles that have been pre-authenticated can get involved in the V2V communication. ESPA considers V2V communication covered by the same agents of trusted authority with vehicles having the same secure keys. ESPA was evaluated via simulation using NS-3.23. A two-way highway with two lanes were simulated by integrating traffic simulators to NS-3.23 which are simulation of urban mobility (SUMO) and mobility model generator for vehicular network (MOVE). From the simulation analysis, ESPA was found to reduce transmission and computation overheads and provide better security that meets the privacy properties requirement in VANET.

2.4.5 Secure Privacy-Preserving Authentication with Cuckoo Filter

Cui, Zhang, Zhong, and Xu (2017) proposed a secure privacy-preserving authentication with Cuckoo Filter (SPACF) scheme for VANET to enhance security and privacy of users as well as to minimise the communication overhead. The researchers proposed to utilise the Cuckoo Filter and binary search methods to achieve higher success rate than other PKI-based and identity-based authentication systems in the verification phase. Additionally, the researchers also proposed a new authentication scheme without bilinear pairings which can result in a heavy computational cost. Cuckoo Filter is a data structure that provides better search accuracy and search time and uses hashing functions. Every time a vehicle moves to a new RSU, it authenticates itself using the TA which will then pass the vehicle's information to verify the identity of the said vehicle. For every message distribution, a vehicle needs to generate a pseudo identity and corresponding signing key to increase the difficulty of attackers tracing the real identity of the users.

Furthermore, RSUs use batch verification approach to verify a set of messages without the bilinear pairings. Apart from that, SPACF also allows for group key generation when vehicles want to form a group as well as group message signing and verification to allow group members to verify the signature of other members without the aid of RSU. The performance of SPACF was analyzed using a simulation software and is evaluated in terms of communication, computation, and transmission overheads. From the analysis, SPACF has lower communication, computation and transmission costs when compared to other security protocols.

2.4.6 Benchmark Protocol Method Comparison

Table 2.1 shows a comparison of methods among the existing approaches discussed in the previous section along with the proposed solution. The existing approaches discussed have been selected as the benchmark protocols for this study as these approaches focus on enhancing security and preserving privacy of users in the network. From the table, it can be seen that the existing approaches have primarily focused on privacy preserving and authentication schemes. However, other security requirements of VANET such as availability, integrity and non-repudiation are not given much attention. This gives a gap for further improvement in VANET security with the consideration of implementing a much newer security-based technology. Thus, the solution proposed in this study attempts to improve the security of VANET by implementing a much up-to-date technology that could address the security requirements as a whole.

Table 2.1: Summary of Benchmark Method Comparison

Author/Year		ASC (2017)	LAKAP (2017)	HEPPA (2017)	ESPA (2016)	SPACF (2017)	Proposed Solution
Technique		User and message authentication using low-cost cryptographic operations and user anonymity using smart card	Multiple authentication and key establishment cluster-based VANET	Hybrid approach of pseudonym and group-signature in region-based VANET	Asymmetric PKI pre-authentication and symmetric hash message authentication code	Cuckoo Filter and binary search methods without bilinear pairing authentication	Dual-factor authentication with blockchain technology to resist network attacks
Simulator		Vanet MobiSim	NS-2.35	Veins	NS-3.23, SUMO, MOVE	C++ based simulator	Veins
Performance Metrics	Communication overhead	Yes	Yes	Yes	No	Yes	No
	Computation overhead	Yes	Yes	Yes	Yes	Yes	No
	Transmission overhead	No	No	No	Yes	Yes	Yes
	PDR	No	Yes	Yes	No	No	Yes
	End-to-end delay	Yes	Yes	Yes	No	No	Yes
	Throughput	No	Yes	No	No	Yes	No
	Packet loss	Yes	No	Yes	No	No	Yes
Security Concerns	Confidentiality	Yes	No	Yes	Yes	Yes	Yes
	Integrity	No	No	No	No	No	Yes
	Availability	No	No	No	No	No	Yes
	Authentication	Yes	Yes	Yes	Yes	Yes	Yes
	Non-repudiation	No	No	No	No	No	Yes

2.5 Blockchain Technology

Blockchain is a technology known for its distributed ledger of all the digital events of a system that have been shared among peers in the network or the participating nodes. The public database that have been shared comprised of definite and verifiable record of every single event ever made. The events in the blockchain database is approved by consensus of multiple nodes in the network.

Blockchain can be divided further into two types as follows: i) public and ii) private blockchains. Anyone within the network of a public blockchain have the rights to join and interact without needing the permission from a central authority. This type of blockchain is also called as an open blockchain. However, private blockchain is all about the access control mechanism. This type of blockchain comes with administration where the administrator is required to control and manage the participants on the network. The administrator has control over whoever joins, views and writes to the blockchain. Besides, the administrator has the ability to create a consensus group where the technology can converge to centralization which can lead to a single point failure vulnerability. On the other hand, single point failure is not an issue to public blockchain as it is completely decentralized and able to withstand malicious attacks. Whenever a new node connects to an existing peer node, the blockchain technology will construct a complete blockchain in the node as a first task.

In the blockchain, the root of the big tree is a genesis block and also the first node to appear in the system. The root node contains all the general information needed by other nodes and can consider as the common origin of all the blocks. Whereas each block consists of information of its preceding block in the record form of cryptographic hash that forms the blockchain. Figure 2.10 depicts the structure of blocks in blockchain. A genesis block leads

the blockchain with a stacked successor blocks as its leaf nodes. Each block contains a previous block hash, nonce, timestamp and Merkle root. Figure 2.11 illustrates the data structure of block hashing. The block starts with a head and followed by records also known as the block body where all blocks comprised of data and pointer information.

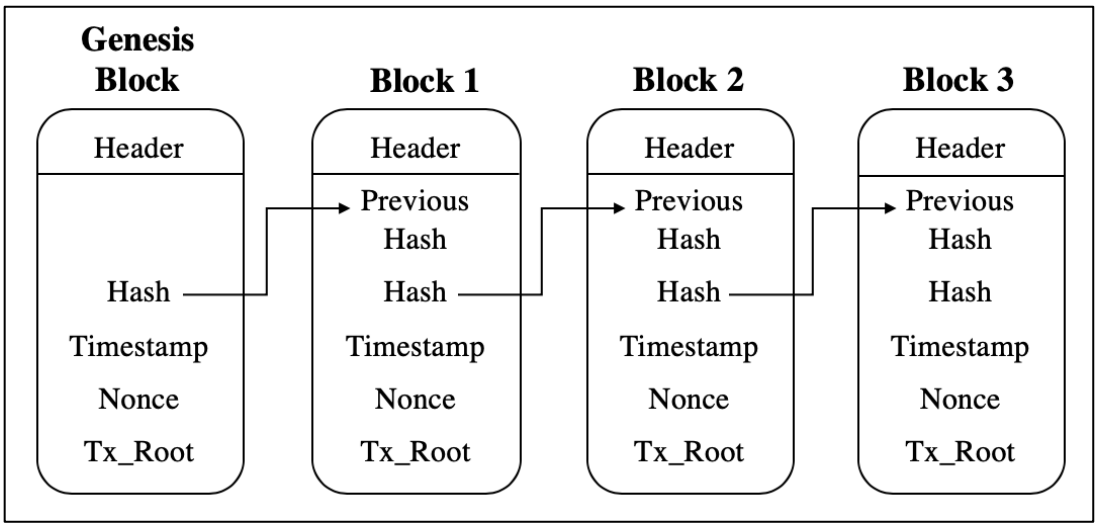

Figure 2.10: Structure of Blocks in Blockchain

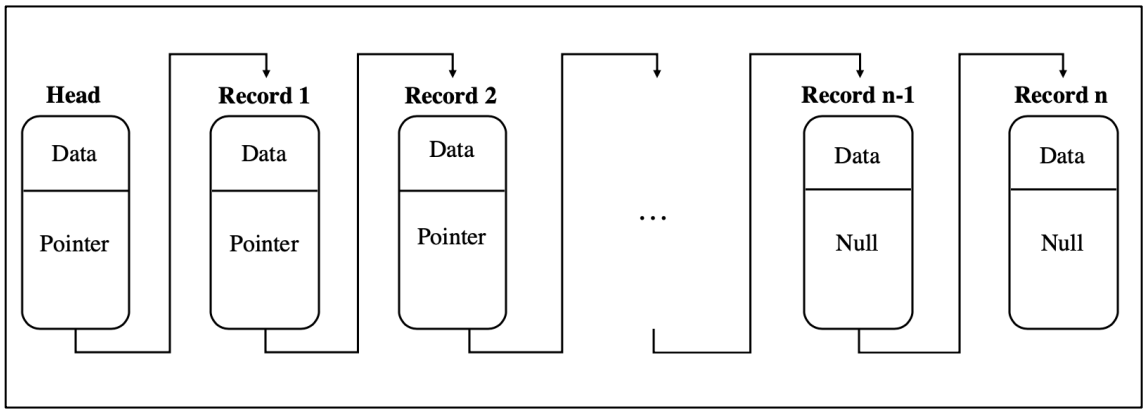

Figure 2.11: Data Structure of Block Hashing

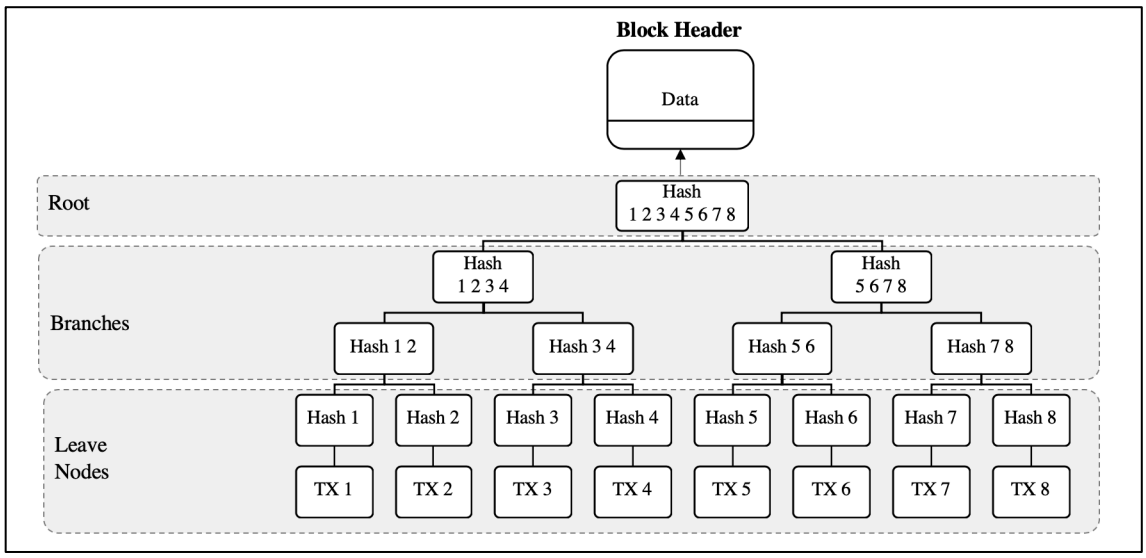

Figure 2.12: Merkle Tree Structure

Figure 2.12 depicts the Merkle tree structure in blockchain. It is a tree of hashes that have leaf node of transactions. Each block body comes with a set of information that such as sender details, receiver details and timestamp. Hash is the data structure of hashes that connects the current block to its preceding block that leads to a chain-like formation. Hash tree is another name for Merkle tree as it hashes all the transactions and links the hashes to one another in a unique root, branch and leave structure, ensuring a secure and efficient way of searching the stored information on blockchain. In 1979, this theory was patented by Ralph Merkle as it was named after him as well.

The Merkle hash is used to hash the transactions and includes the hash into the block header in case of immutability. The cryptographic algorithm used is the Merkle algorithm which is derived from Merkle hash (Merkle, 2000). Merkle algorithm hashes all the contents of the blocks known as leave nodes to a further compact form known as branches. The root of the Merkle tree is responsible for hashing all the branches to one main hash to be appended to the block header. One of the advantages of the Merkle tree is that allows verification and

validation of blockchain as required with just the header part of the blocks. The size of the Merkle hash is not big as compared to the complete set of transactions. Hence, a unique hash value is generated to verify the integrity of the transactions in a block. Due to the security concerns, blockchain is well known for its cryptography feature.

2.5.1 Blockchain Feature

This technology is a leading topic that is beneficial in diverse fields for its useful feature combinations. Some of the basic features of technology are as follows.

2.5.1.1 Immutability

The uniqueness of this technology is that once the information is recoded and endorsed in the blockchain, then it is impossible to overwrite, modify or even delete it from the network. In addition, no information can be tampered. Hence, this is one unique and important feature of blockchain.

2.5.1.2 Trustworthy Distributed Environment

Any of the contents of the blockchain included in the system is distributed among the nodes in the network to synchronize and validate without the help of a central control. This decentralized structure shows that blockchain is a trustworthy environment whereby the entire system will not be affected by a single point failure.

2.5.1.3 Anonymity as a Privacy Concern

Although every transaction is recorded on a public ledger, the blockchain environment never reveals the details of the transactions in a readable format. For example, the verified user information and transactions are encrypted in hash form and linked with

other relevant transaction blocks in the network. In other words, all transaction information is made recorded in a private and confidential manner.

2.5.1.4 Faster Transaction

The transaction speed is remarkably faster as it is effortless to setup in any network environment. A transaction or an event takes approximately from a few seconds to few minutes depending on the task size which is assumedly the fastest transaction of all.

2.5.1.5 Data Accuracy and Reliability

Blockchain is very well known for being an accurate and reliable system. Data in blockchain is always expected to be accurate as blockchain only registers validated information in its public ledger. In terms of reliability, if there were to be a network attack or single point of failure, the network will still be up and running due to its decentralised nature.

2.5.1.6 Transparency

Any transactions or events that takes place in the system will be updated from time to time in the blockchain. So, it is hardly possible to doubt the transparency of the transactions in the network.

2.5.1.7 Elliptic Curve Cryptography

Elliptic curve in cryptography was first used by Lenstra (1987) for his factoring algorithm using elliptic curve. Then, in 1985, Koblitz (1987) and Miller (1986) independently used elliptic curves to develop public-key cryptographic systems. An ECC is a simple encryption method utilised for quicker encryption and decryption (Sathishkumar &

Rajakumar, 2017). The ECC is a public key cryptography method that is based on the algebraic structure of elliptic curves over finite fields (Abdullah, Hakansson, & Moradian, 2017). A major benefit of ECC when compared to other asymmetric cryptography such as RSA is that ECC uses shorter key sizes and system parameters while still providing the same level of security as RSA (Qu, Wu, Wang, & Cho, 2015). A shorter ECC key (ECC-256) is 64,000 times harder to break than a longer RSA key (RSA-2048) (Aitzhan & Svetinovic, 2018), implying a strong authentication security of ECC. Apart from that, ECC also requires lower power usage and reduces storage and transmission requirements (Abdullah, Hakansson, & Moradian, 2017), signifying lower computational overhead. However, a drawback of ECC is that the size of digital signatures is large which can impact authentication and verification (Qu, Wu, Wang, & Cho, 2015). ECDSA is a cryptography algorithm which is based on digital signature algorithm (DSA) and applied to ECC to generate public/private key pair. ECDSA uses a digital signature with hash function and asymmetric cryptography, which provides a much higher authenticity and security in the blockchain system (Mishra, Singh, & Kumar, 2016). Blockchain system uses ECDSA because ECDSA provides an equivalent security level as RSA and DSA but with uses a smaller key size to allow for faster computation in the system (Hanifatunnisa & Rahardjo, 2017).

2.5.2 Blockchain Consensus Mechanism

A consensus mechanism in a blockchain technology is a fault tolerant mechanism. The advantage of having a consensus mechanism is that it can assist to achieve a required agreement based on the information collected from a multi-node system. The agreement is a list of rules and regulations for all the different participating nodes which will be helpful in deciding its contributions eventually. Some criteria are important in decentralized

blockchain network such as the security, efficiency, reliability and real-time information sharing of the publicly shared database to agree upon the participation of a node of a particular consensus and to prove the trustworthiness of the transactions within the network. Consensus mechanism can be categorized based on the blockchain type, either public or private network as shown in Figure 2.13. Each public and private blockchain network category is further divided into four more consensus mechanisms each.

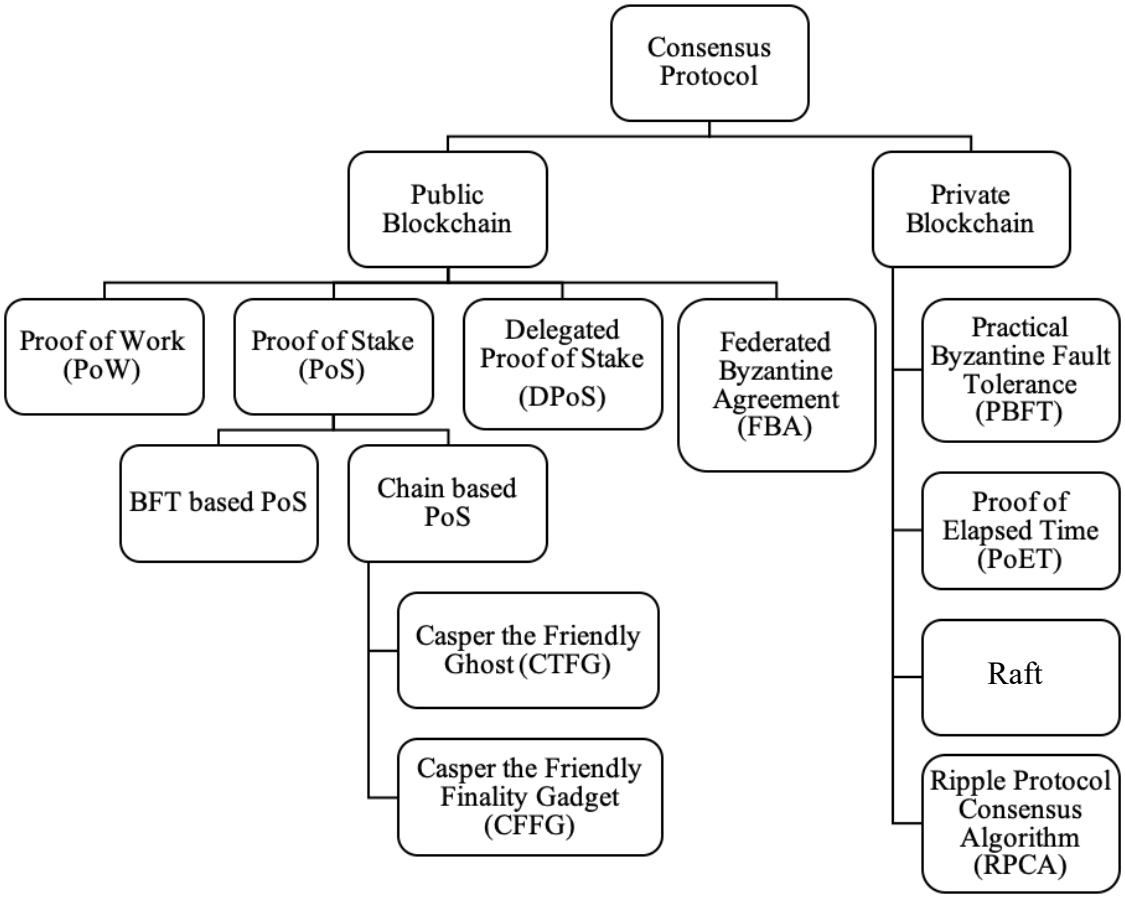

Figure 2.13: Blockchain Consensus Mechanisms

2.5.2.1 Public Blockchain Protocol

Power of Work (PoW), Power of Stake (PoS), Delegated Power of Stake (DPoS) and Federated Byzantine Agreement (FBA) are categories of public blockchain network where PoS can be further classified into Byzantine Fault Tolerance-based PoS (BFT based PoS) and Chain based PoS. Chain based PoS can be either Casper the Friendly Ghost (CTFG) or Casper the Friendly Finality Gadget (CFFG). Brief description of all the consensus algorithms of public blockchain are as follows:

(a) Proof of Work

The value of previous block-header hash in this consensus algorithm is computed by a miner while various nonce values are used iteratively to compute Merkle root of transactions until the difficulty target value is more than the resulting hash value (Antonopoulos, 2014). This consensus algorithm is similar to a difficulty level of cryptographic puzzle but it gets easier when all the inputs are known to be verified by others.

(b) Proof of Stake

Based on the wealth or stake as the name suggests, the new block generated by the miner or validator will be selected by a deterministic way (King & Nadal, 2012). In alternative to approving every single transaction as legitimate, the assets of the miners are needed to be staked out as in coins form to validate the ownership. In return, the transaction fee is transferred to the validators but not all PoS algorithms are equipped with block rewards for this process. This consensus algorithm is also a form of greener distribution and considered inexpensive.

PoS is further classified into BFT-PoS and Chain-based PoS. A multi-round voting process is conducted based on rounds to delegate a validator pseudo-randomly in coming up with a new block (Zhang, 2018). The validator is also responsible in trusting with a complete replica of the blockchain that can be recognized later on with their public keys. Nonetheless, the selected block needs the support of the two third or majority of the validators to sign off in committing and finalising it which can go up to several rounds. This mechanism is also similar to PoW in terms of selecting a validator pseudo-randomly to assign the rights to select a new block. The block of the longest chain in the network will be elected as the previous block to be linked to the new block generated (Moindrot & Bournhonesque, 2017).

Consensus safe is the finalised version of a block whereby no revision can be made after the block generation in the blockchain. A theory of Casper getting inspired by Practical Byzantine Fault Tolerance (PBFT) is brought up the Ethereum blockchain team where propagation of a block in the network requires voting and signing processes by the validators. Casper used a combination of roles in preparing and committing with a single message type called voting. Checkpoints in Casper PoS are the key features where the team decided to come up two different protocols for it, called CTFG and CFFG and the researches led by Vlad Zamfir and Vitalik Buterin respectively (Buterin & Griffith, 2017).

(c) Delegated Power of Stake

This consensus mechanism is targeted to small scale stakeholders as a motivation to participate in the blockchain network more often by delegating or transferring their coins to much bigger stakeholders in the blockchain (Asolo, 2018). The concept is to assign a representative for the small-scale users or stakeholders where the assigned participants are allowed to stake their coins on behalf of them in the network. In return, the small-scale users

or stakeholders holds the rights to receive a reward of certain amount of staking incentive share as per the consensus protocol. In respect to the high return margins for the big scale stakeholders, only a few nodes are assigned as in order to control the majority of the centralized blockchain network.

(d) Federated Byzantine Agreement

In this consensus mechanism, the nodes in the network are given the freedom to elect the trustworthy nodes as the control is decentralized (Mazières, 2015). This mechanism also opens the membership to all and the nodes in the network and does not require an early verification to participate in the public blockchain network. Quorum refers to the number of nodes needed to achieve an agreement within the system. FBA utilizes quorum slice, which is a subset of quorum, that is capable of convincing another specific node to be a part of the agreement. If the quorum slice is believed to be trustworthy, then other nodes can agree to get along with the trusted quorum slice in the network. Hence, a quorum will be in charge to decide on the approval of agreement within the network by identifying the number of trustworthy nodes it requires.

2.5.2.2 Private Blockchain Protocol

Private blockchain network can be classified into Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time (PoET), Raft and Ripple Protocol Consensus Algorithm (RPCA). Among all the private blockchain consensus mechanisms, PBFT is the most frequently and commonly known due to its speed, efficiency and trustworthiness that is decoupled from the resource bearer. Brief description of all the consensus algorithms of private blockchain are as follows:

(a) Practical Byzantine Fault Tolerance

Regardless to some parts of the participating nodes that contains malicious behaviour, this consensus mechanism said to be the advanced version of BFT from public blockchain protocol (Castro & Barbara , 1999). A majority rule is applied in this mechanism to achieve a system agreement on the legitimate node that has been interconnected with all the other nodes in the network. This model works great when the two third of the overall nodes in the network are not the sum of the malicious nodes present in the system. So, the assumption is that the network security will be heightened with the addition of more node participation in PBFT network.

(b) Proof of Elapsed Time

All nodes in this network is required to identify themselves to be able to participate. Since PoET is a private blockchain consensus mechanism, verifying identity of node is crucial and the mechanism gives an equal chance to all the nodes in the network to be chosen among all the participants as it was a fair lottery system. In order for a node to be chosen as the lottery-winning node, it need to complete a certain amount of waiting time and require a short period random time. The fair lottery system is efficient in saving the energy while utilizing resources in a smaller scale.

(c) Raft

This is a consensus algorithm that is good with crash-fault tolerance and was proposed by researchers from Stanford University as a team (Ongaro & Ousterhout, 2014). Raft is organised in a cluster formation where each cluster consist of a few servers in which five servers are commonly placed in a cluster. Each server is entitled to a dynamic status that can be either a follower, candidate or leader. A common scenario for follower server would be to follow all the lead server's command based on client request. Candidate is a state of

the server where it urges the server to elect a new leader. The new leader can be elected by a voting process whereby the majority votes from the cluster will be chosen as the new leader of the consensus mechanism. The leader server takes responsibility for all client requests and leads all the servers to follow its command.

(d) Ripple Protocol Consensus Algorithm

Ripple is the pioneer protocol of consensus algorithm. This protocol comprised of Ripple server, proposer and unique node list (UNL), open and last-closed ledger (Schwartz, Youngs, & Britto, 2014). The Ripple is an important part of RPCA mechanism as it holds the key in retaining the accuracy and agreement every few seconds for all the nodes in the network. As a result of consensus achievement, the recently closed ledger is added into the last-closed ledger. Without the presence of two potential paths splitting in the network, all the last-closed ledgers which are maintained by different nodes in the network will equate to a similar last-closed ledger. Only a total of five validators trusted by each based on a static configuration operated by Ripple could lead to centralization.

2.6 Simulation Tools

In this subsection, several identified existing simulation tools are listed and described in detail. The following are the tools that are identified:

2.6.1 Simulation of Urban Mobility

Simulation of Urban Mobility (SUMO) is an open source, highly portable, microscopic road traffic simulation package designed to handle large road networks. It has several main features including the collision free vehicle movement, different vehicle types, single-vehicle routing, multi-lane streets with lane changing, junction-based right-of-way

rules, hierarchy of junction types, an open Graphical User Interface (GUI), and dynamic routing. Apart from that, large environments can be easily handled by SUMO, i.e., 10 000 streets, and it can import many network formats such as Visum, Vissim, ArcView, or XML-Descriptions. This simulation can be combined with OpenStreetMap and it is possible to simulate traffic in different locations of the globe. Despite the advantages, a serious shortcoming of this simulator is that it generates traces that cannot be directly implemented into available network simulator due to its characteristic of being a pure traffic generator (J. Martinez, Keong Toh, Cano, & Calafate, 2009).

2.6.2 Network Simulator 2

VINT project research group at the University of California at Berkeley is responsible for the Network Simulator 2 (NS-2) development which considered a discrete event simulator. Monarch research group at Carnegie Mellon University continued the simulator extension that includes: (a) node mobility, (b) a realistic physical layer with a radio propagation model, (c) radio network interfaces, and (d) the IEEE 802.11 medium access control (MAC) protocol using the distributed coordination function (DCF).

In terms of communication support, the PHY (physical) is a full-featured generic module and is capable of supporting any single channel frame. The key features include cumulative Signal to Interference plus Noise Ratio (SINR) computation, preamble and Physical Layer Convergence Procedure (PLCP) header processing and capture, and frame body capture. The MAC now accurately models the basic IEEE 802.11 carrier-sense multiple access with collision avoidance (CSMA/CA) mechanism, as required for credible simulation studies (J. Martinez, Keong Toh, Cano, & Calafate, 2009).

2.6.3 Global Mobile Information System Simulator

For wireless and wired network, Global Mobile Information System Simulator (GloMoSim) is a scalable simulation environment. GloMoSim is designed using parallel discrete-event simulation capability which allows the addition of programmable modules in GloMoSim. A layered approach is used to build the simulator similar to the OSI seven-layer protocol model. To connect different simulation layer, a Standard Application Program Interface (API) is used that allows to integrate models developed by different people at different layers rapidly.

2.6.4 OMNeT++

OMNeT++ is an object-oriented modular discrete event network simulator. Component-based design, new features and protocols are present in OMNeT++ and can be supported through modules. This simulator supports both the network and mobility models through the independently developed Mobility Framework and INET Framework modules (Spaho, Barolli, Mino, Xhafa, & Kolici, 2011). Extensions are also made available for real-time simulation, network emulation, alternative programming languages (Java, C #), integration of databases, integration of SystemC, other APIs and functions.

2.6.5 Vehicles in Network Simulation

Vehicles in Network Simulation (Veins) is another simulator that couples a mobility simulator, SUMO with a network simulator, OMNeT++ through a TCP connection. For these two simulators to couple, a manager module is used. The manager module triggers the execution of one-time step of the traffic simulation at regular intervals. For all modules it

initiates which triggers a position update, a resulting mobility trace is received (Martinez, Keong Toh, Cano, & Calafate, 2009).

Table 2.2: Comparison of Simulators for VANET Simulation

Features	**SUMO**	**NS-2**	**GloMoSim**	**OMNeT++**	**Veins**
Supported Language	C++	C++/OTcl	C	C++	C++
License	Open source	Open source	Open source	Open source	Open source
GUI Support	Yes	Yes	Yes	Yes	Yes
Learning time	Moderate	Long	Moderate	Moderate	Moderate
Scalability	High	Low	High	High	High
Network visualization tool	Yes	Yes	Yes	Yes	Yes
Interaction with real system	Yes	Yes	Yes	Yes	Yes
Portable	Yes	Yes	Yes	Yes	Yes
Ease of Use	Easy	Hard	Hard	Easy	Easy
Ease of Setup	Easy	Easy	Easy	Moderate	Moderate

Table 2.2 shows a summary of comparison of simulation tools discussed in this section. From the comparison, it can be seen that Veins simulation tool has many advantages

over the other simulation tools compared and is selected as the most suitable simulation tool for this research. The justification for this selection is highlighted in the following chapter.

2.7 Summary

This chapter provided a brief background knowledge on VANETs in terms of its characteristics, features, security issues, and challenges. Furthermore, this chapter also provided a background to the various network attacks, both active and passive that can possibly bring harm to communication in VANET. Several existing security schemes were reviewed to identify the gap in the field in order to propose an improved solution. From the analysis of the existing approaches, it was found that most of the approaches focused on privacy preserving and authentication technique with lower attention to other security requirements in VANET. Blockchain technology has been discussed in this chapter, highlighting its features, types, and schemes and how it could benefit in terms of providing a much reliable message communication platform. By reviewing this, it will be much clear in the next chapter on how the blockchain technology can be adapted to secure vital information in VANET communication.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter aims to describe the methodology and related activities that are involved in the examination followed by a detailed description of the research activities before the implementation of the proposed solution in VANET. Methodology explains the research question raised during formulation of the problem and why such research question is essential in relation to a research study. It depicts the starting point of the research study, the directions of the research and the possible effects of the research once it is completed. This chapter begins with an overview of research methodology used in this research study, which is followed by a detailed explanation of the research methodology with a flowchart describing the flow of the research methodology and activities. It is then followed by a comprehensive comparison of simulation tools and finally the design of the proposed solution.

3.2 Proposed Blockchain in VANET

Many academicians and researchers are drawn to blockchain technology for its enormous benefits to be gain in vast fields including academics, finance, medicine and banking. Blockchain is technology that technically comprised of unlimited number of blocks that are connected in a sequential order to form a block-chain. As this technology is potentially beneficial to expertise in vast fields, it has also gained the interest of many in resolving critical information dissemination issues in VANETs. Bitcoin cryptocurrency is the underlying support of blockchain technology that emerges decentralisation and

distribution of computing paradigm that has the ability to provide privacy and security in Peer-to-Peer (P2P) networks (Nakamoto, 2008). In VANET environment, this technology is a vital part that helps in managing ground truth of information for automobiles due to the fact that any automobiles in the system can access the past event lists and its information if it is placed in the public blockchain.

The proposal is to generate a scheme whereby the trustworthiness of node and message passing in VANET is guaranteed by placing them in public blockchain to act as a ground truth for other automobiles. For this, event messages will be taking the transaction form. Making the event messages as the transaction is to ensure the suitability of feature to the VANET system in an assurance to providing security for critical information dissemination and resolving the VANET issues. The variation method adapted is adding new blocks based on event messages similar to transactions in bitcoin apart from hashing sequences of blocks to be connected in chronological order to the blockchain.

Many researchers and academicians explore deep into blockchain technology to implement it in geospatial systems due to the benefits and huge demands. A newly issued block of a blockchain supposed to be shared among all the nodes globally in the system as of the scenario involves bitcoins. Conversely in VANET environment, there doesn't exist a necessity to involve sharing of blocks to nodes out of the scope specified. For instance, West Malaysia and East Malaysia are separated geographically from each other regardless to the similar country they share as they do not share any connected roads between them. Hence, the traffic and accident details of a region of Malaysia are entirely not useful to the other region at all times. This suggests that a separate blockchain to be maintained for two different regions in sharing trustworthiness of an automobile and its message passing information that will fall under the geographical category.

This chapter focuses on delivering trustworthy event messages securely by applying blockchain technology in VANETs as one of its objectives. Blockchain technology is implemented for a dual factor authentication purpose to securely deliver trustworthy messages across the network. Furthermore, the proposed solution will integrate a signatureless public key infrastructure to preserve the privacy of the users in the network and timestamp is recorded to maintain the freshness of the message. A simple blockchain would not be suitable for the VANET issue discussed in this thesis. Hence, an improvised type of blockchain mechanism with some feature adaptation is proposed as a solution. Figure 3.1 depicts the improvised packet structure with the integration of blockchain, that will be used for a secure communication by VANET components. In the packet structure, the header will comprise of maximum 3 blocks of information, which is sufficient to create a blockchain. Essential information that each block carries include vehicle identity, V_n, event message, M_n, relative signal strength indicator value, $RSSI_n$, timestamp, t_n, hash value, h_n, and the root transaction value, Tx_Root. This information will act as a medium of trustworthiness for the events that occur in VANET.

Header			Payload	CRC
Block 1	**Block 2**	**Block 3**		
V_A	V_B	V_C		
M_a	M_B	M_C		
$RSSI_A$	$RSSI_B$	$RSSI_C$		
t_A	t_B	t_c		
	h_0	h_1		
h_0	h_1	h_2		
Tx_Root	Tx_Root	Tx_Root		

Figure 3.1: Proposed Packet Structure with Blockchain Integration

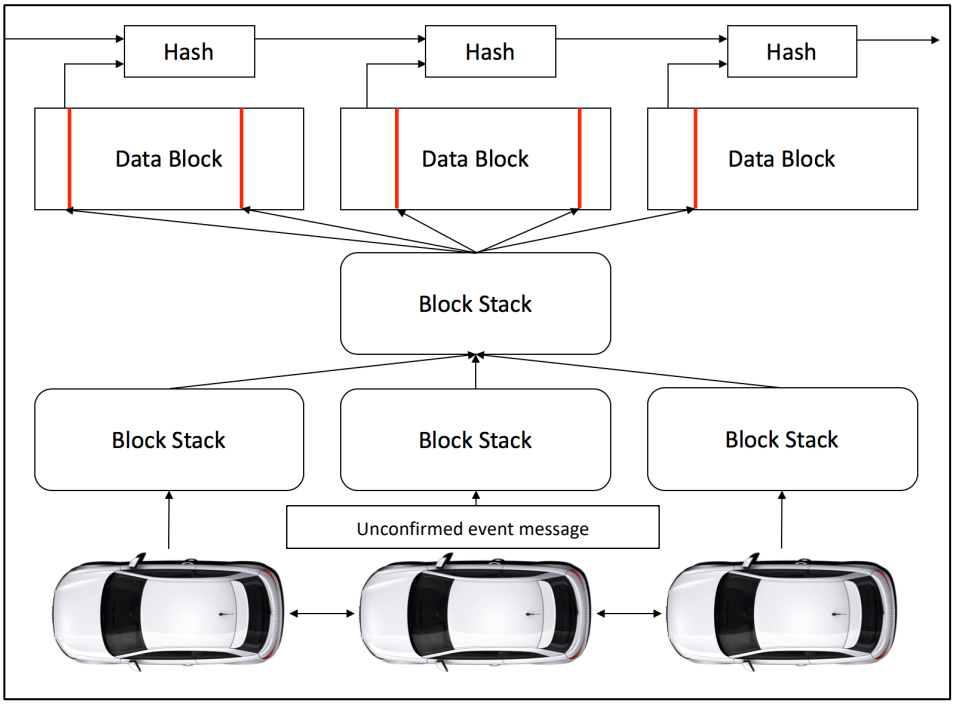

Figure 3.2: Generation of Blockchain from Unconfirmed Event Messages

A new block is mined by all the miners in the independent blockchain which will be sent to the local blockchain network afterwards. The blockchain is the medium to ensure the trustworthiness within the local blockchain network or the country itself as it acts as the global ground truth for the vehicular nodes. To be precise, any automobiles in the network has the possibility to query the trust level of a vehicular node at any times of an event. The unconfirmed event messages were sorted and generate a new block due to aggregation from the message pool. Figure 3.2 shows the blocks with hashes that are chained in a sequential order to build a blockchain. The new blocks are broadcasted after the generation of it where all the automobiles in the network verify and update the chain of the blockchain.

3.2.1 Assumptions

The first assumption about the automobile in the network is that every vehicle able to communicate with other entities either by V2V and V2I communications that can associate with the internet connectivity perfectly (Shanzhi, et al., 2017). Every automobile is assumed to have equipped with three important gadgets called the OBUs, sensors and GPS. It is assumed to be that the number of malicious or harmed RSUs are to be lesser than the number of genuine or unharmed RSUs that are placed alongside the roadway in a network. A genesis block will be able to create and start a blockchain based on local events if it is an RSU that is legitimate and the Certificate authority (CA) is a trusted entity.

Besides, the participating automobiles are assumed to be able to handle high computing power and have a high trust levels which is also considered a complete vehicular node that can take part in the mining process. In addition, the malicious vehicles cannot outnumber genuine vehicles in the network. Another assumption taken into consideration is that Received Signal Strength Indicator (RSSI) is always accurate at any specific geographical location. The unencrypted event messages are also available to other neighbouring automobiles in real time and the timer of all the nodes are synchronized. Lastly, a total of fifteen event messages are required to confirm a new event that is reported to testify as a truthful critical event.

3.2.2 Components of Blockchain Scheme in VANET

There are four components that are vital for the VANET system to perform. The four components are as follows.

3.2.2.1 Road Side Unit (RSU)

This component is responsible for the authentication of an automobile with V2I communication. It also provides a location certificate to the vehicular nodes that are reachable in its communication range. An event or incident that occurs nearby a legitimate RSU will be the starting point to generate a genesis block to kick off a set of blockchain.

3.2.2.2 Automobiles

Automobiles or also known as vehicular nodes or vehicles are the primary constituent of VANET blockchain system as to how an engine is for an automobile. After verification of automobiles, those vehicular nodes are held responsible to produce event messages, mine new blocks and store event messages in the blockchain. Automobiles can be either full node or normal node. If the node has high trustworthiness level based on its previous communication record in the network, then it is a full node that is in authority to mine the blocks. Whereas, a normal node is any nodes that are not full node who are entrusted to assist in message generation during an incident by dispatching and verifying the collected message.

3.2.2.3 VANET Messages

VANET messages are comprised of two categories namely beacon messages and safety messages. Beacon messaging is a type of communication to attain cooperative awareness among the vehicles by transmitting messages involving beacon and safety events. Vehicles on the road and the traffic can be managed efficiently with beacon messaging that broadcast messages periodically to inform driving status and locations of a vehicular node to neighbouring automobiles. However, the broadcasted message during critical event occurrence on the roadway is the safety event messages. For instance, the traffic accidents, road hazards and traffic congestions are some of the critical events where the safety event message transmission will be based on the severity of the emergency in accordance to Level 1, Level 2 and Level 3. Level 1 is the emergency event message broadcasting with highest priority indicating highly critical event occurrence. Safety messages plays a crucial role in saving lives and properties of an automobile owner or the driver through the message transmission. Nonetheless, frequent broadcasting of beacon messages can result in overhead with the signing and authenticating processes of every single beacon messages.

3.2.2.4 Blocks

As per discussed in Section 2.5, a block comprised of a block header with its information stored in the block body. The block header includes the hash of previous block, a nonce, difficulty target, timestamp and a Merkle root. In contrast, the block body consists of a set of safety event messages as a form of transactions of the blockchain.

3.3 Research Methodology and Flowchart

For this study, there are four consecutive stages carried out to complete this research. Each of the stages comprises of one or more substages which need to be conducted consecutively before the research can be completed. The four stages are formulation of problem statement, design of proposed solution, validation of simulation tool and evaluation metrics and simulation and analysis.

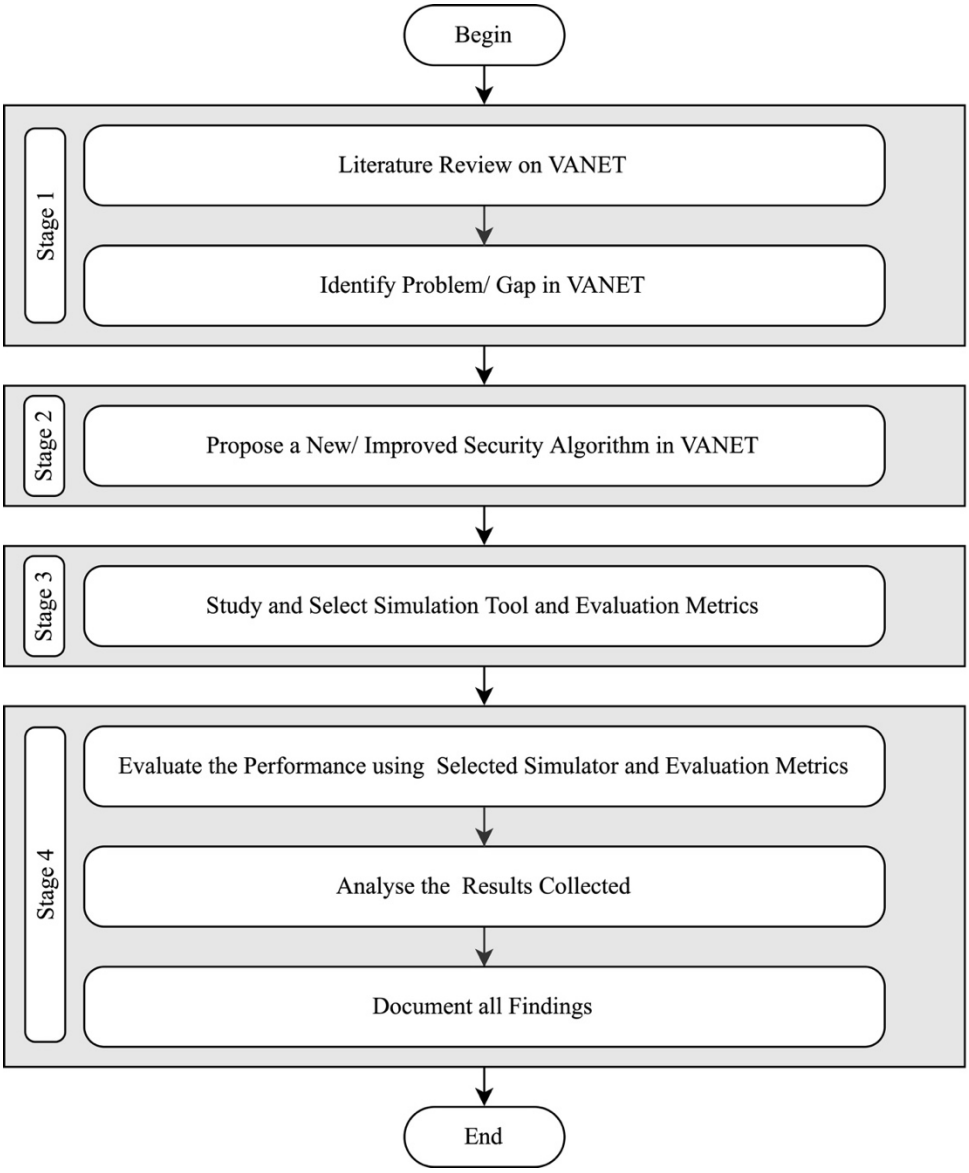

Figure 3.3: Flowchart of Research Methodology

Figure 3.3 shows the flow of the research methodology which begins with the study of past literatures with regards to VANET and followed by the identification of the gap that exists in VANET. From the gap identified, a new solution is proposed to improve the security in VANET. Once the solution has been finalized, an extensive study of various simulation tools along with several performance metrics is conducted. The performance of the proposed solution is then evaluated using selected simulation tool and the results of the simulation are analysed and discussed. All the findings are then finally compiled into a document. All these seven stages are discussed further in the following subsections.

3.3.1 Stage 1: Formulation of Problem Statement

The first stage of the research methodology is concerned with generating problem statements for the current study. This stage is comprised of two sub-stages which are literature review on VANET and identify problem or gap in VANET. An extensive study of current security algorithms and protocols is conducted prior to identifying the problem. In the review of literature, a number of security approaches and performance parameters are identified and validated thoroughly. The benefits and limitations of each of the reviewed techniques are drawn in order to identify the problems that exist in VANET. From the study, it can be concluded that most of the trust-based security protocols employed cryptographic technique, public key infrastructure, and certificate issuance method. Nevertheless, there are other techniques that can be used to improve the security and privacy of the network such as fuzzy solution and reputation-based algorithm.

3.3.2 Stage 2: Design of Proposed Solution

After discovering the limitations of the existing privacy preserving protocols, the following step is to design a new solution that can address the problems and limitations identified in Stage 1. This research proposes an implementation of a reliable, sophisticated, and evolving technology in the field of computer and communication security, which is the blockchain technology.

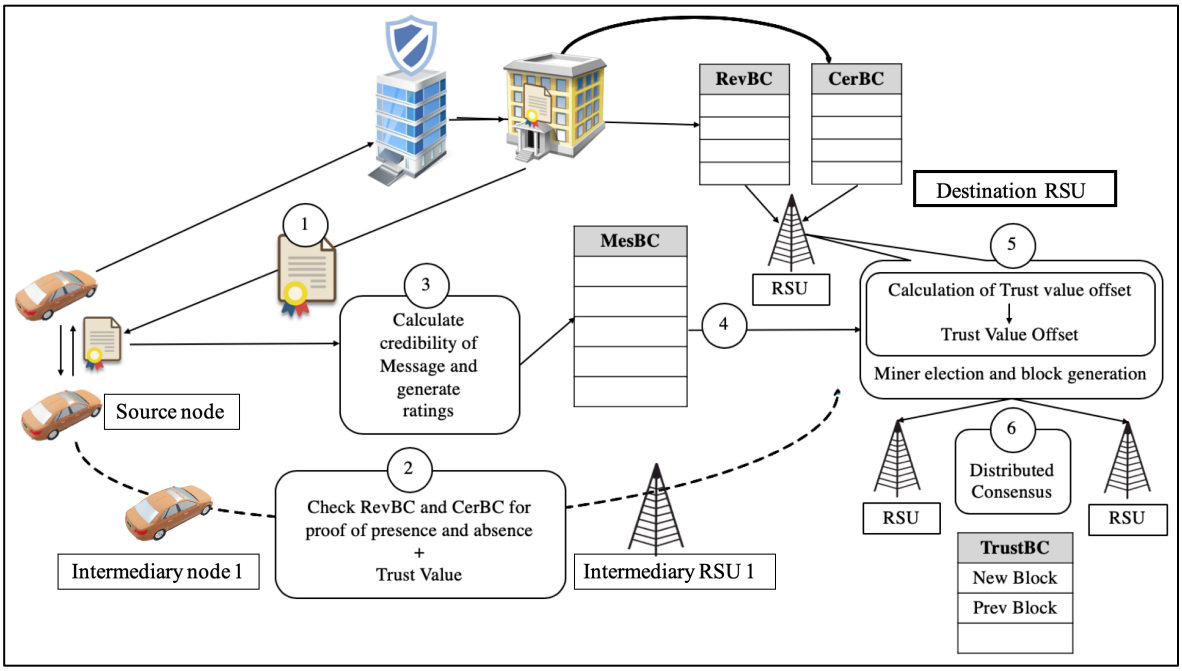

Figure 3.4: System Design of Proposed Solution

Figure 3.4 shows the system design of the proposed solution in which a communication occurs between two vehicles. In this study, four different blockchains are considered for the system design, which are the certificate blockchain (CertBC), revocation blockchain (RevBC), message blockchain (MesBC), and trust blockchain (TrustBC). All of these blockchains are administered by government agencies such as the law enforcement

agency (LEA) and certification authority (CA) because the proposed solution may require legal actions and legal usage of data for investigation. The standard submission regulation is to be set by the government agencies and it is to be adhered by the respective automakers registered in the country for the participation of their vehicles in the VANET.

3.3.2.1 Overall Flow of Proposed Solution

Figure 3.5 shows the overall flowchart of the proposed solution which consists of six phases. The phases are system initialisation, system authentication, message rating generation, trust value offset calculation, miner election and block generation, and distributed consensus accordingly. Each phase has a significant purpose in this model.

The first phase of the proposed solution begins with a system initialisation. This phase is responsible to validate the identity of the nodes and issue certificate to them when nodes move into a network. The subsequent phase is system authentication which act as a security layer to authenticate nodes via dual factor authentication before the nodes can begin communicating with each other in the network. Next, message rating generation is concerned with providing a rating on the messages sent by the communicating nodes to ensure their trustworthiness. Following this, the fourth phase is trust value offset calculation that is required to calculate the trustworthiness of each node in the network. Then after, the system conducts a miner election and block generation which implements the blockchain technology for an efficient tracking of the nodes in the system. The last phase of the proposed solution is the distribution of consensus that acts a ledger that is spread around the network. The following subsection gives a detailed insight of the six phases with a flow chart and a sequence diagram to support the phases. The diagrams are demonstrated for a scenario of two nodes in a system. Table 3.1 shows a list of notations and their respective explanation.

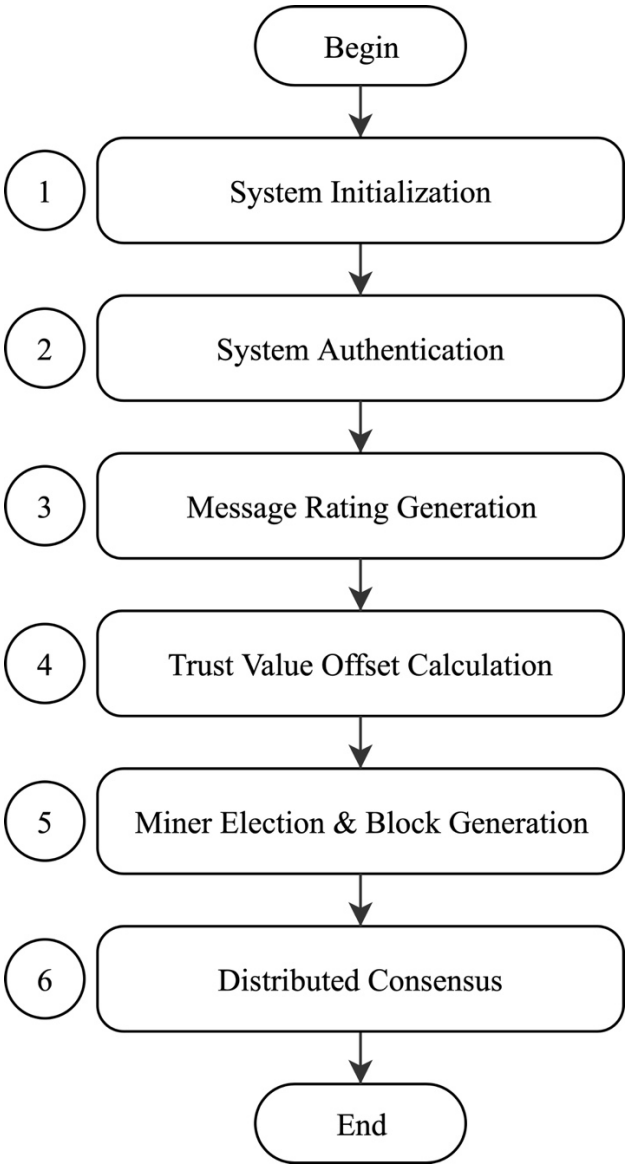

Figure 3.5: Flowchart of Proposed Solution

Table 3.1: List of Notations and Description Used

Notation	Description
V_A	Vehicle A
PU_A	Public Key of V_A
PR_A	Private Key of V_A
LEA	Law Enforcement Authority
CA	Certificate Authority
C_A	Certificate of V_A
V_B	Vehicle B
CertBC	Certificate Blockchain
RevBC	Revocation Blockchain
RSU	Road Side Unit
ID_B	Identity of V_B
M_A	Message A from Vehicle A
M_B	Message B from Vehicle B
TrustBC	Trust Blockchain
P(e/C)	Probability of event *e*
MesBC	Message Blockchain
RSU *r*	Destination RSU
O_r	Set of offsets of RSU *r*
S_r	Hash Threshold of RSU *r*
BC	Blockchain

3.2.2.2 Phases of the Proposed Solution

The proposed solution is comprised of six subsequent phases, which are system initialization, system authentication, message rating generation, trust value offset calculation, miner election and block generation, and finally, distribution of consensus. This sub-section presents the phases in a more detailed manner.

(a) Phase 1: System Initialization

A node enters VANET, known as Vehicle A and is denoted as V_A. As V_A enters the network, the first measure of initialisation is the generation of its public and private keys, PU_A and PR_A, respectively. The generated PU_A along with a set of private information of V_A is then submitted to LEA for verification. If the verification of the materials by LEA are valid, LEA then issues a warrant to the CA for certification of V_A. When CA receives the warrant from LEA, it sends a valid certificate to V_A, known as C_A. However, if the materials are not verified by LEA as valid, then LEA rejects V_A. Once V_A is verified and receives C_A, V_A enters the second phase, that is system authentication as shown in Figure 3.6.

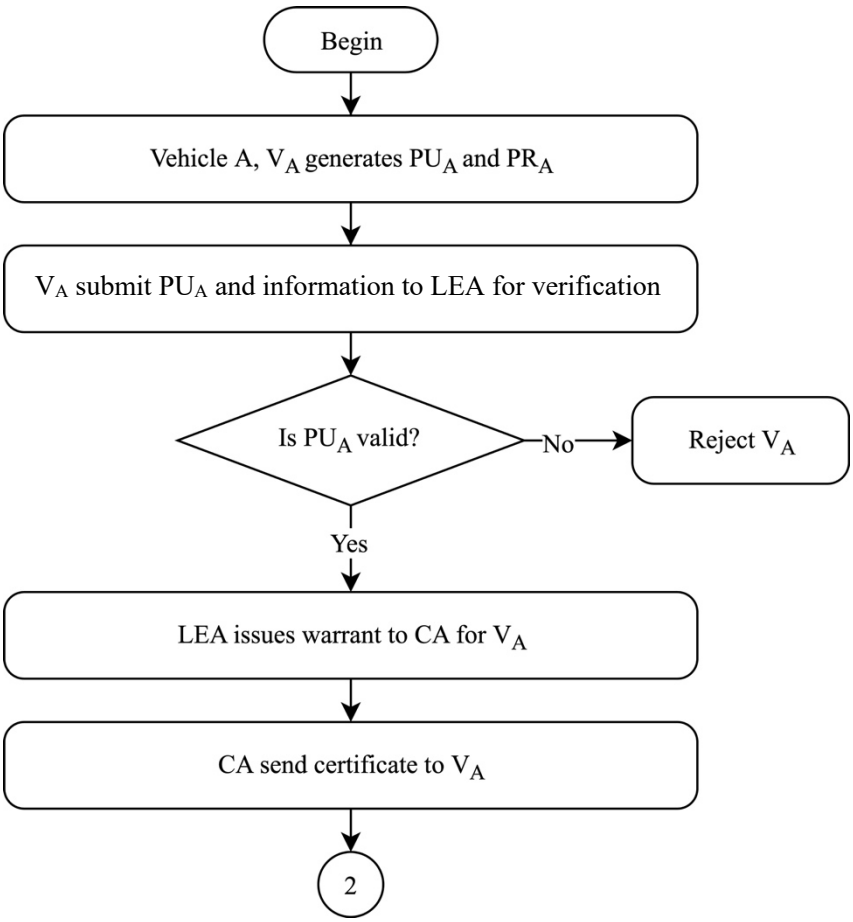

Figure 3.6: System Initialization of Proposed Solution

(b) Phase 2: System Authentication

The second phase is crucial to authenticate the vehicles in the network via dual factor authentication prior to communicating and exchanging data with each other. Assuming there is now another vehicle, Vehicle B, in the same network, known as V_B with which V_A wishes to communicate. This phase begins with V_A sending its C_A to V_B to authenticate the identity of V_A. When V_B receives the certificate from V_A, V_B checks whether the C_A delivered is valid as of the delivery date and time. The certificate would contain the public key and signature of V_A as well as the expiration date of C_A. In order to authenticate V_A, V_B checks the expiration of C_A. If C_A has not expired, C_A is still valid. Then, V_B checks CertBC to see if C_A is present in the blockchain. If C_A is present in CertBC, then V_B proceeds to check RevBC to see if the PU_A is absent in the blockchain.

If all these three conditions are fulfilled, only then the communication between V_A and V_B will take place. Failure of any of the three conditions would indicate that either the C_A has expired and is invalid or the PU_A is invalid. Hence, the authentication process will be halted immediately. When the identity of V_A is authenticated, V_B then sends a query to the nearest RSU to obtain the current trust value of V_A. Initially, RSU checks the identity of V_B using the ID of V_B, ID_B. If the ID_B is valid, RSU then obtains the trust value of V_A from TrustBC and sends the trust value to V_B. However, V_B is rejected if the ID_B is found to be not true. Once the trust value is calculated, V_B will receive the details of V_A and proceeds to the third phase as shown in Figure 3.7.

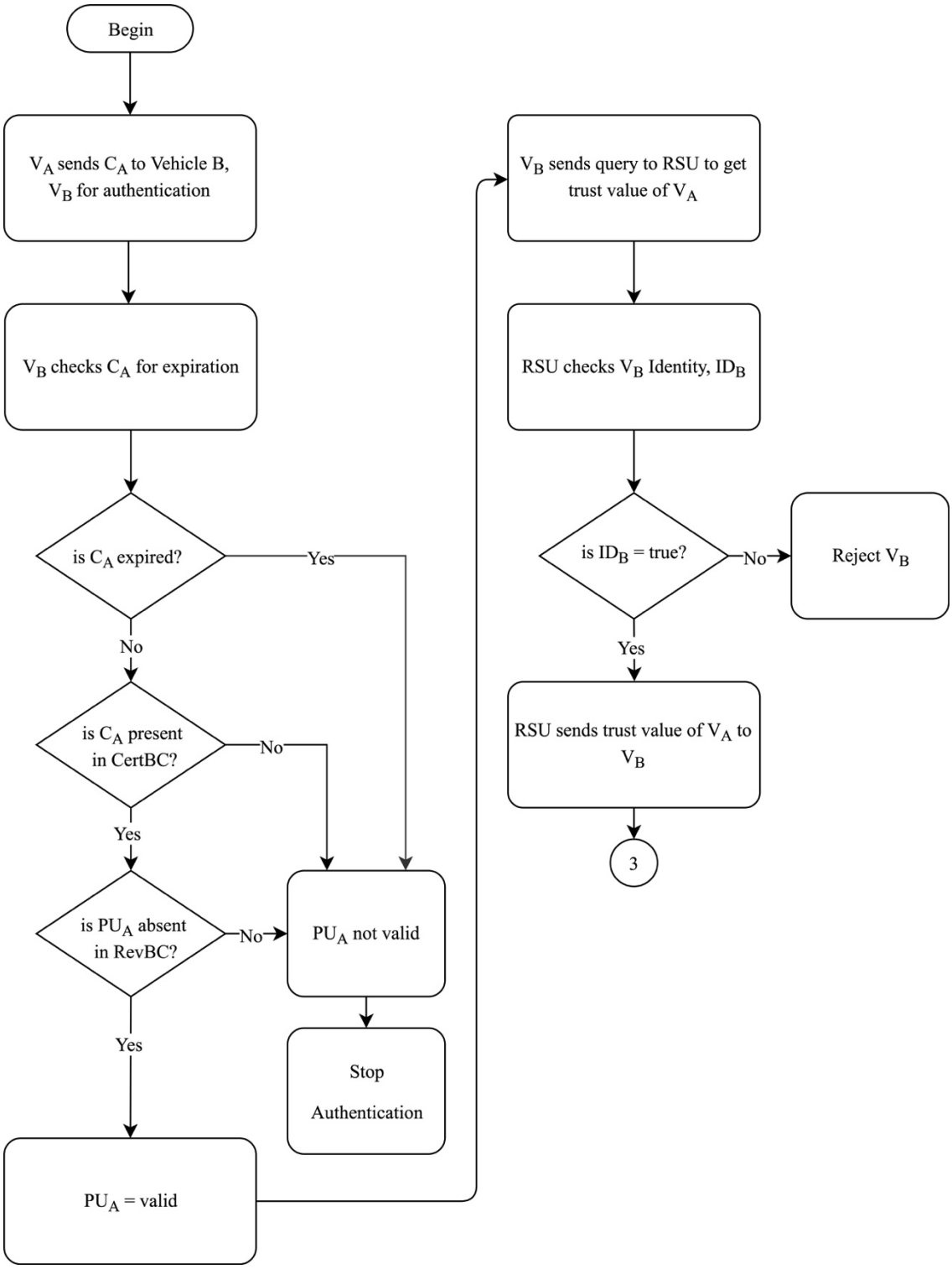

Figure 3.7: System Authentication of Proposed Solution

(c) Phase 3: Message Rating Generation

Once the identities of the communicating vehicles are authenticated, the vehicles can now exchange data between them. Message rating generation is the third phase that will officially initiate communication between the nodes. When V_A sends a message of a particular event, M_A, to V_B, V_B calculates the trust of M_A to determine the trustworthiness of the message. Messages that report similar incidents or events are recorded in the MesBC. Therefore, for every vehicle that reports similar events occurrence in the network, the trust of the events is calculated and stored in a trust set. Next, the probability of such events, occurring, P(e/C) is calculated using the trust set.

$$P(e/C) = \frac{P(e) \cdot P(c_A/e)}{P(e) \cdot P(c_A/e) + P(\bar{e}) \cdot P(c_A/\bar{e})} \qquad \text{Equation 3.1}$$

Based on Equation 3.1, c_A refers to the credibility of message sent by V_A. Based on the credibility set C, the receiver is able to calculate the aggregated credibility of event e, where ē is complementary of event e. If the calculated P(e/C) is greater than the existing threshold value, then M_A will be reported as true. However, if P(e/C) does not exceed the threshold, then M_A will be reported as a false report. When M_A is true, V_B generates a positive rating on the message received from V_A. If otherwise, V_B generates a negative rating on that message. Then, V_B stores the messages received in the MesBC blockchain. The MesBC along with the ratings given on each message will be then uploaded periodically to a nearby RSU by V_B before proceeding to the next phase as shown in Figure 3.8. The message ratings will indirectly reflect the trustworthiness of the source vehicle, which in this case is V_A.

Therefore, if a vehicle has more positive ratings, the vehicle can be identified as a trustworthy vehicle in the network. On the contrary, if a vehicle is found to have more negative ratings, the certificate and public key of the vehicle will be revoked by the LEA. This algorithm can mitigate false data injection attack as the ratings will help users in the network to identify and differentiate between trustworthy vehicles and untrustworthy vehicles.

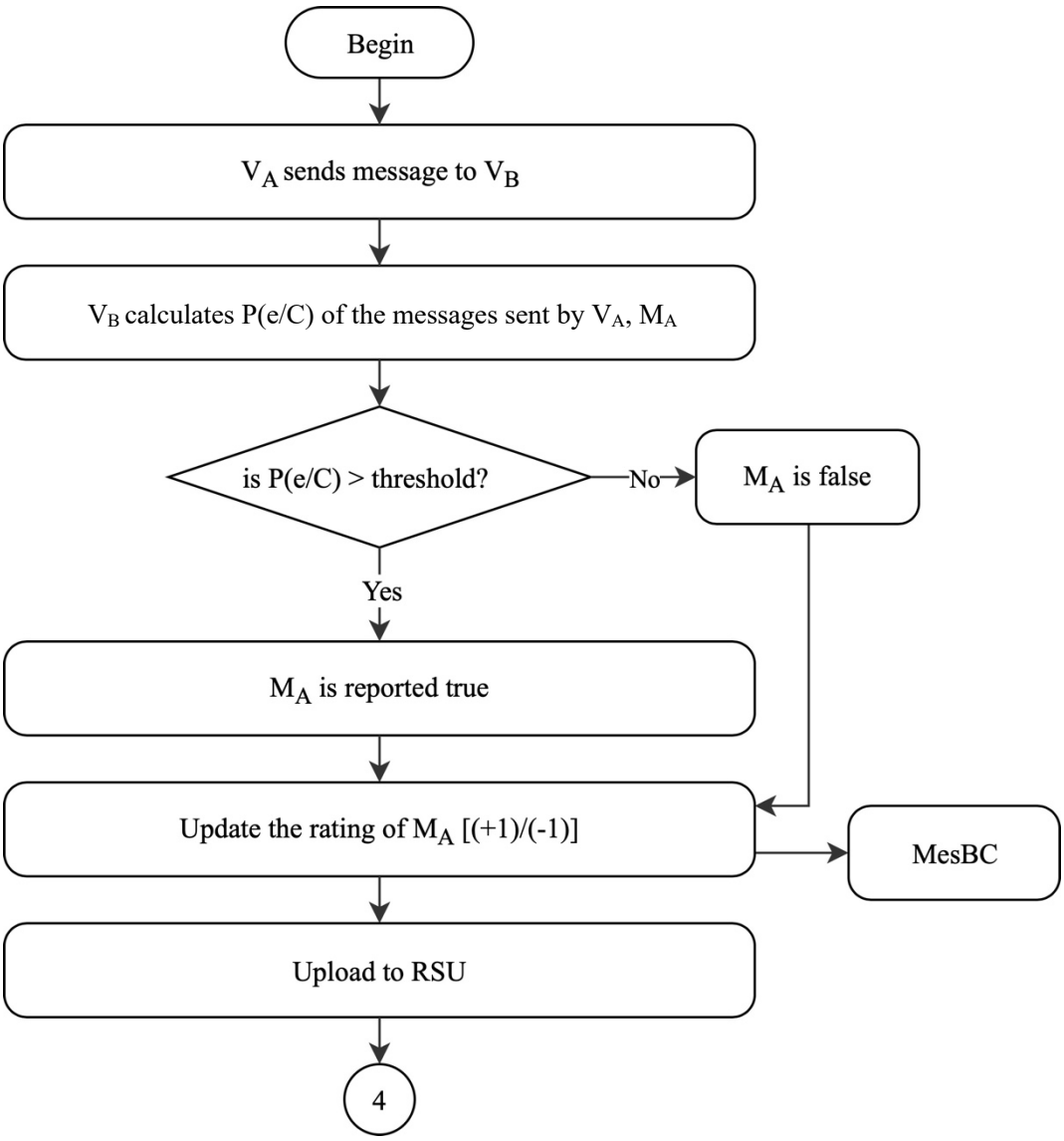

Figure 3.8: Message Rating Generation of Proposed Solution

(d) Phase 4: Trust Value Offset Calculation

The fourth phase of the proposed solution begins as the RSU receives MesBC from V_B as illustrated in Figure 3.9. This phase calculates the trust value offset of each vehicle (in this case, V_A) in the network. Once the RSU receives MesBC, it first checks if MesBC is updated from the previous uploads. If MesBC is not updated, the trust value of V_A remains the same. However, if MesBC is updated, RSU begins calculating the trust offset for V_A.

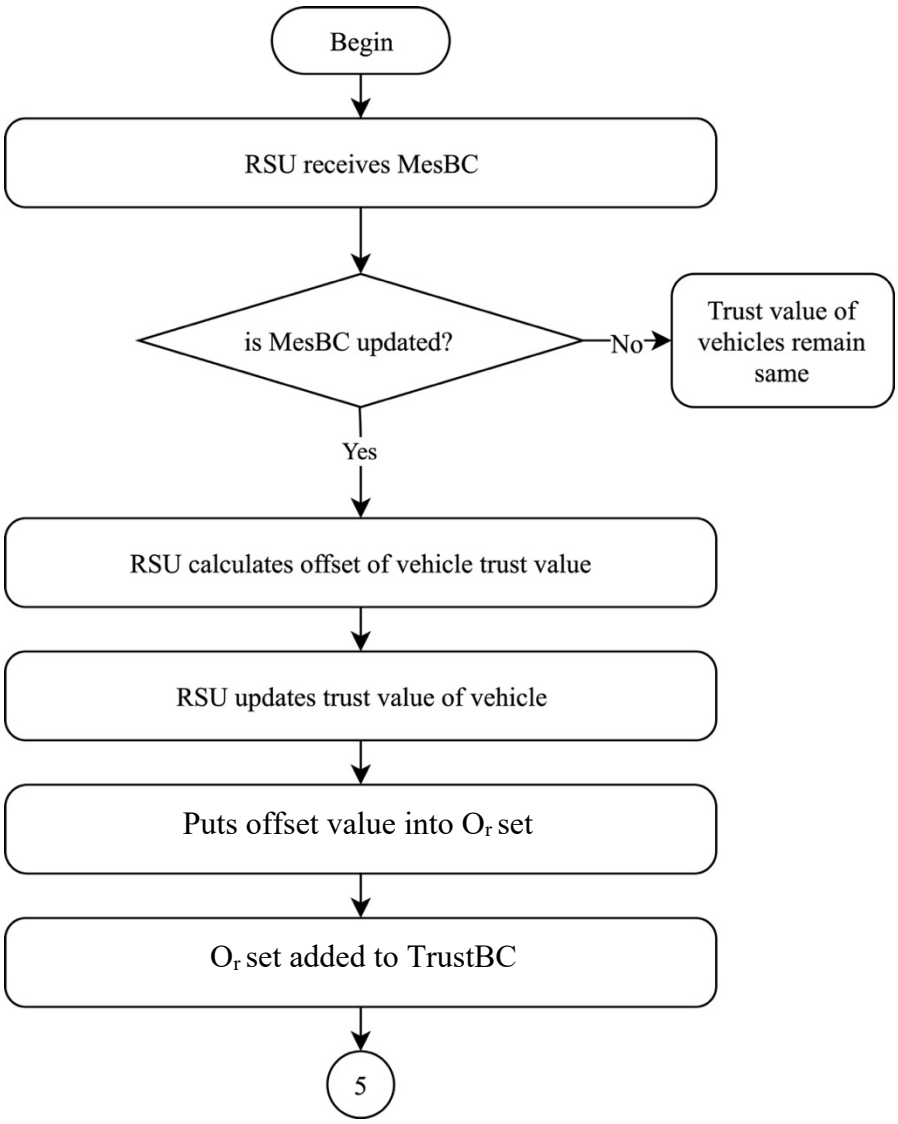

Figure 3.9: Trust Value Offset Calculation of Proposed Solution

If V_A has not sent any message to V_B prior to the latest upload of MesBC, then the trust value of V_A remains the same as it was in the previous upload. If V_A did, indeed, send a message to V_B, then RSU obtains the updated rating of V_A. Then, RSU calculates the offset of vehicle trust value. Next, RSU updates the trust value of V_A in the network. RSU also updates the offset of trust value into a set of trust offset, known as O_r, which is then uploaded into TrustBC before moving to the next phase in the proposed solution.

(e) Phase 5: Miner Election and Block Generation

Following trust value offset calculation in phase four, the proposed solution then moves into phase five which is concerned with miner election and block generation. The fifth phase is the shortest phase among the other phases; however, it has the most significance to the efficiency of the proposed solution as it implements blockchain technology in the network. Each RSU in the network registers its timestamp and calculates the hash value. If the calculated hash value of RSU *r* is lower than S_r, then RSU *r* crosschecks its sum of absolute values of trust offset with the maximum sum of absolute values.

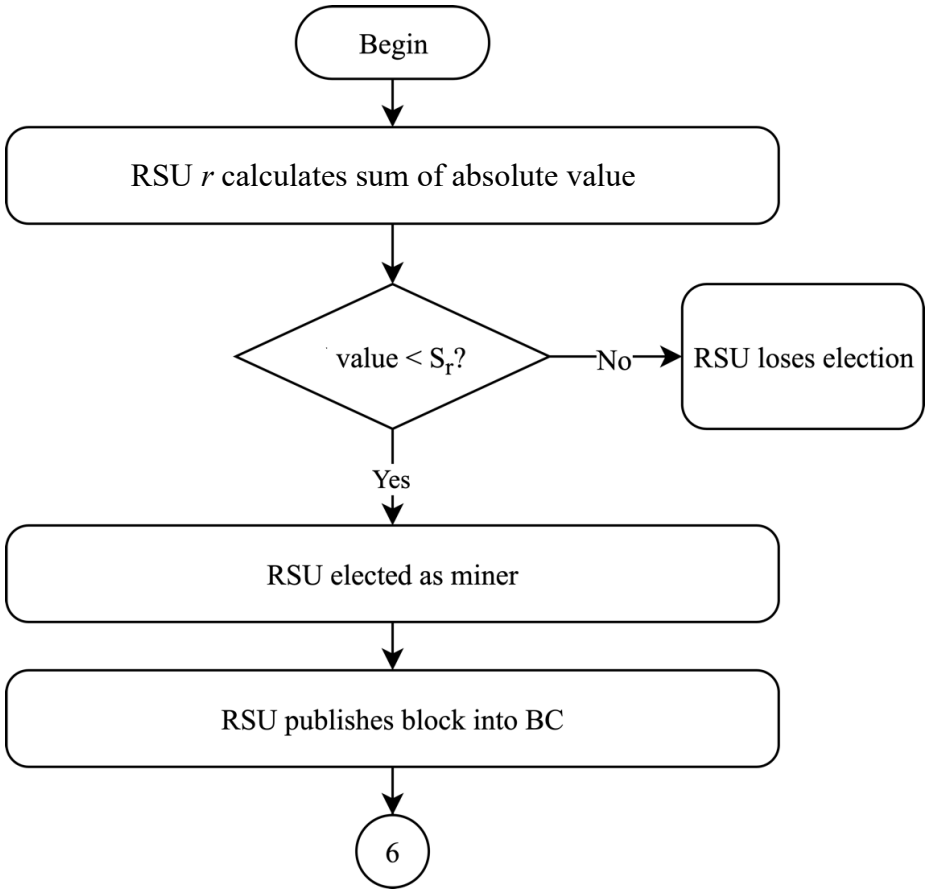

Figure 3.10: Miner Election and Block Generation of Proposed Solution

If the sum of absolute values of RSU is lower than the S_r, then RSU is elected as the miner. If RSU fails any of these two conditions, then RSU loses the election. The election of miner RSU moves to the next RSU in the network and repeats the steps mentioned. When miner RSU is elected, the miner publishes its block into blockchain. The flow of the fifth phase is shown in Figure 3.10. A miner RSU is elected periodically in the network to manage the blockchain. The election of miner RSU ensures the update of data in the blockchain in a timely manner.

(f) Phase 6: Distributed Consensus

The last phase of the proposed solution is the distribution of consensus. This phase begins with RSU receiving a block that has been published by the miner RSU from the previous phase. The RSU which received the block then checks the validity of the timestamp of the block. If it is valid, then the RSU adds its block to the block received from miner RSU. Else, the block is rejected immediately. Should the RSU receive more than one block from the miner RSU, the blockchain begins to split to two potential paths in the network, known as forking. Therefore, in such scenario, the RSU must choose a fork to add its block. The RSU checks the validity of the fork and adds the its block to the fork if the fork is valid. If not, the fork is rejected by the RSU. Eventually, the fork in the blockchain network that is highly acknowledged by other RSUs will grow longer and faster, which then becomes the distributed consensus whereas other forks are discarded. When other forks are discarded, RSUs gather their respective blocks from the discarded forks and add them to the distributed consensus as illustrated in Figure 3.11. The sixth phase ensures that all RSUs in the network have the same blockchain which results in the consistency of data.

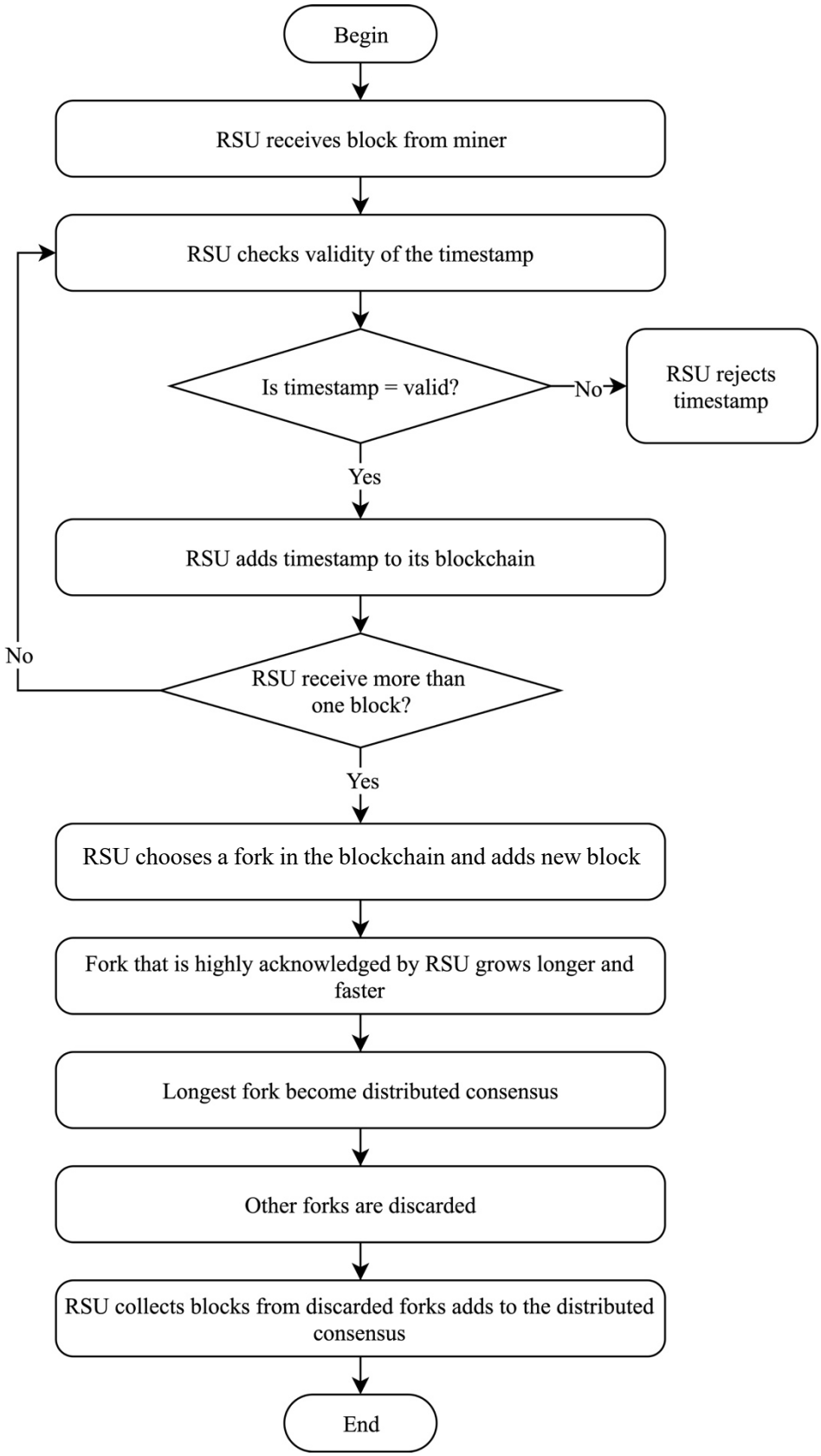

Figure 3.11: Distributed Consensus of Proposed Solution

3.3.3 Stage 3: Validation of Simulation Tool and Evaluation Metrics

The Stage 3 in the research methodology is the selection of a suitable simulation tool for the performance evaluation of the proposed solution. Based on the review of existing simulation tools in Chapter 2, the features of each tool are compared. The most suitable simulation tool identified will be used to ease the evaluation process in the final stage.

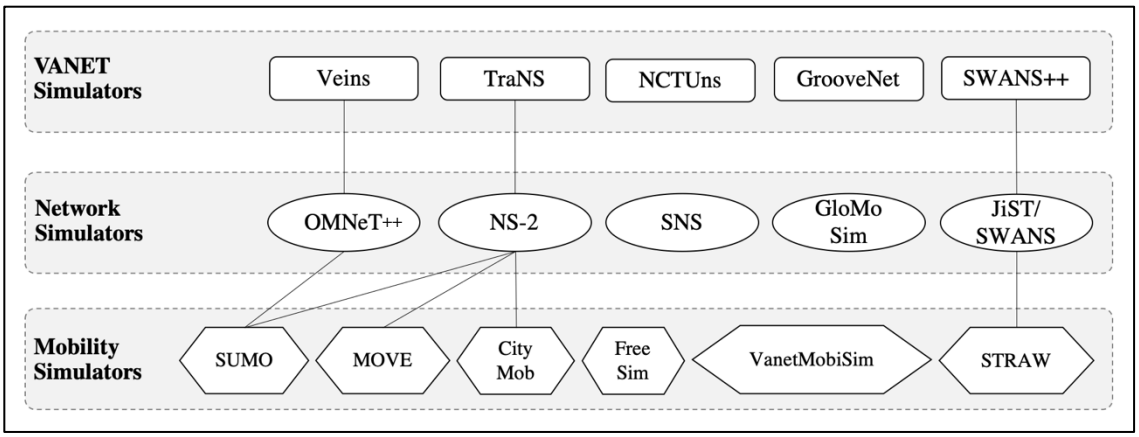

Figure 3.12: Classification of Various Simulators

Accomplishment of new protocols, scenarios and wireless technology in large testbed becomes highly challenged due to the high expenses and complexity. Therefore, most researchers resort to simulation of VANETs as an alternative solution to identify the potentiality of system and latest approaches. 2 types of simulation components are needed for a VANET simulation, namely network and mobility simulations. Figure 3.12 illustrates existing VANET simulators with the classification as per the components in discussion (Noori, 2012). Majority of the simulations are performed with separate network and mobility components. Nonetheless, there are several simulators that are readily available in the market for the purpose of VANET simulation that can provide traffic and network simulation or a combined version for both.

3.3.3.1 Veins as the Chosen Simulation Tool

The selection of a network and mobility simulator is highly crucial to efficiently transmit several messages per second when simulating a VANETs environment with large number of vehicles. Parameters such as user friendliness, scalability, and the interconnect ability of road traffic and network communication simulators are important when choosing a suitable simulator.

The simulator that has been chosen for this simulation is Veins due to the following features: Online re-configuration and re-routing of vehicles in reaction to network simulator, fully-detailed models of IEEE 802.11p and IEEE 1609.4 DSRC/WAVE network layers, supporting the realistic map and traffic scenario, user friendliness and the ability to interconnect. Veins is capable of running two simulators in parallel, connected via a TCP socket. The framework of Veins has been developed based on MiXiM, which is a framework for simulating wireless channels to provide a precisely detailed models of wireless channels; connectivity, mobility and with a MAC layer protocols for OMNeT++. Moreover, (Simulation of Urban Mobility) SUMO is an open source microscopic simulator which enables researchers to develop a continuous road traffic simulation to handle large road networks. In addition, SUMO accepts different type of map formats from multiple platform. The most commonly used map platforms are OpenStreetMap (OSM) and Java OpenStreetMap (JOSM) as an interface and editor for OSM maps.

Veins is chosen in order to achieve the bidirectional coupled simulation while benefits from state-of-the-art simulation techniques of both the network simulation and the road traffic microscopic simulation domains. In Veins, OMNeT++ works as the network simulator and SUMO in the other hand acts as the road traffic simulator. Traffic control

interface (TraCI) integrates both SUMO and OMNeT++ to provide a TCP connection between the simulators. A real time communication between network simulation module and road traffic simulation module can be generated in Veins.

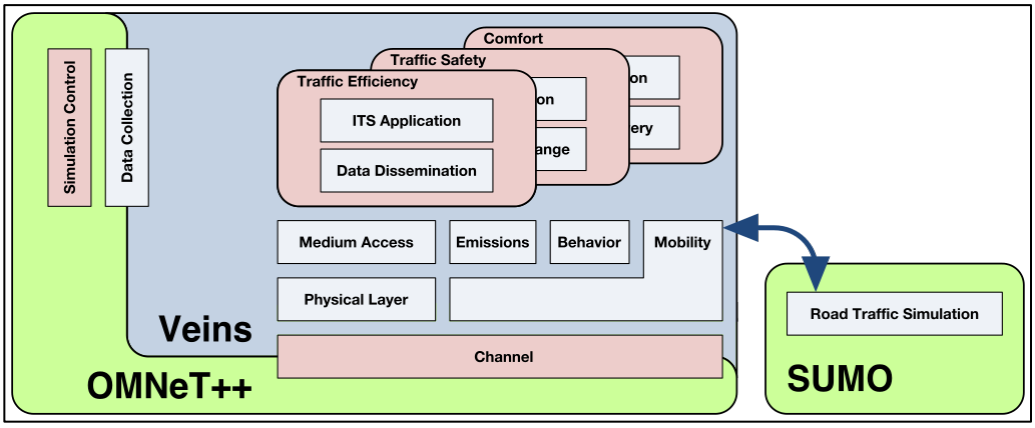

Figure 3.13: Veins Simulator (Sommer, 2018)

Figure 3.13 depicts the structure of the Veins simulator (Sommer, 2018). As shown in the figure, OMNeT++ is an event-based simulator that handles mobility by scheduling node movements at consistent intervals (Toutouh, Garcia-Nieto, & Alba, 2012). The approach of SUMO fits perfectly as it advances simulation time in discrete steps. At the defined intervals, a synchronous execution is guaranteed for every command buffer arriving in-between timestep which is enabled by the control modules integrated with OMNeT++ and SUMO. At each timestep, OMNeT++ would then send all buffered commands to SUMO and trigger the corresponding timestep of the road traffic simulation. Upon completion of the road traffic simulation timestep, SUMO would send a series of commands and the position of all instantiated vehicles back to the OMNeT++ module. This allows OMNeT++ to react to the received mobility trace by introducing new nodes into the network, removing old nodes that had reached their destination, and moving nodes according to their road traffic

simulation counterpart. After processing all received commands and moving all nodes according to the mobility information, OMNeT++ would then advance the simulation until the next scheduled timestep and allows nodes to react to altered environmental conditions.

3.3.3.2 Simulation Environment Setup

The environmental conditions are set at default settings for the simulation of traffic scenario. Figure 3.14 illustrates the interface of basic simulator set up using Veins.

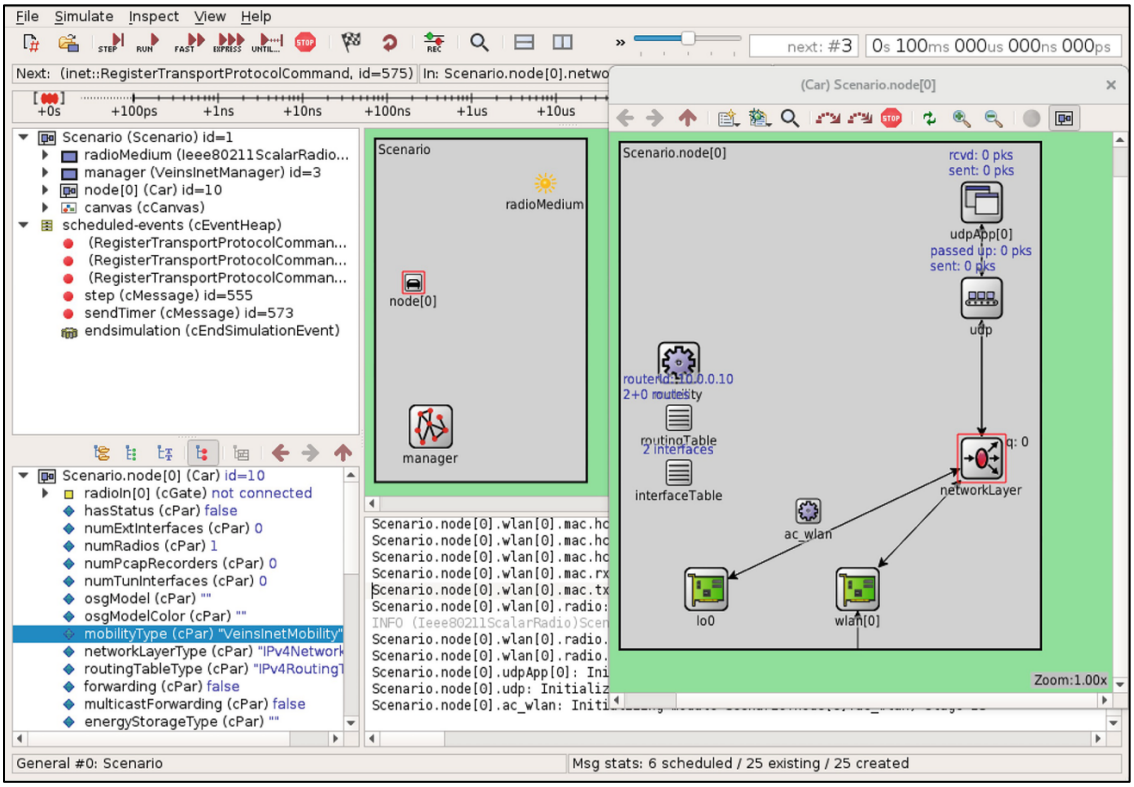

Figure 3.14: Veins Simulator Set up

The parameter and values set for SUMO simulator is as shown in Table 3.2. The parameters set fixed are as follows: number of nodes, maximum vehicle speed, maximum acceleration, maximum deceleration, vehicle length, vehicle width and driver imperfection.

As for the number nodes in the network, 20 nodes are introduced initially in the simulator and gradually increased the nodes by 20 up to a maximum of 100 nodes. Table 3.3 shows the fixed variables set up for OMNeT++ simulator with a set of parameters as follows: Sim-time-limit, Mac.queuelength, Mac.maxTxAttempts, Mac.txpower, Mac.bitrate, Mac.contentionWindow, Mac.slotduration, Phy.sensitivity and UpdateInterval.

Table 3.2: Default Parameters Set for SUMO Simulation

Parameter	Values
Maximum vehicle speed (m/s)	33.0
Maximum acceleration (m/s^2)	2.6
Maximum deceleration (m/s^2)	4.5
Vehicle length m	5.0
Vehicle width m	3.5
Driver imperfection	0.5

Table 3.3: Default Parameters Set for OMNeT++ Simulation

Parameter	Values
Sim-time-limit (s)	6000.0
Mac.queuelength	5.0
Mac.maxTxAttempts	14.0
Mac.bitrate (Mbps)	11.0
Mac.txpower (mW)	100.0
Mac.contentionWindow	20.0
Mac.slotduration (ms)	40.0
Phy.sensitivity (dBm)	-80.0
UpdateInterval (s)	0.1

3.3.4 Stage 4: Simulation and Analysis

Once the simulation tool has been tested with the default parameters, the proposed algorithm was added in the simulation via the blockchain API which was integrated to the simulator. NETwork Attacks (NETA) framework was added to OMNeT++ to simulate DoS attack. During the simulation, packet delivery ratio (PDR), end to end delay, packet loss and transmission overhead are collected, plotted and presented using gnuplot to show the efficiency and the effectiveness of the proposed solution with and without network attack.

3.4 Summary

This chapter highlighted the research methodology used in executing this research. The research methodology is categorized into four consecutive stages: i) Formulation of Problem Statement; ii) Design of Proposed Solution; iii) Validation of Simulation Tool and Evaluation Metrics; and iv) Simulation and Analysis. Each of these stages are described in detail to provide a strong basis in the execution of this research work. In order to overcome the issue of security attacks and privacy, a new solution that is based on blockchain technology and signatureless public key infrastructure. From the comparison study of simulation tools, Veins is chosen as the most suitable simulation tool to evaluate the performance of the proposed solution. Veins is chosen because of its capability of running network and mobility simulators simultaneously, which are OMNeT++ and SUMO. In the next chapter, the extracted results from the simulation experiments will be discussed and the analysis is based on several different criteria to evaluate the performance of the proposed solution using Veins.

CHAPTER 4

PERFORMANCE ANALYSIS

4.1 Introduction

This chapter includes a brief overview of performance evaluation of the proposed blockchain based privacy preserving algorithm implemented on VANET and the performance metrics that are used to measure the performance of the proposed solution in different network environment and set-up. Besides that, this chapter also discusses the basic simulation set-up applied in the experiments as well as the experimental outcomes of the simulations in terms of the observed parameters. The observed parameters are namely packet delivery ratio (PDR), end to end delay, packet loss and transmission overhead. These four parameters are measured and tested over a range of number of nodes both with and without network attack.

4.2 System Development

The first phase is depicted in Algorithm 1 which is the system initialization in which each entity in the vehicular network generates a pair of public and private keys. Vehicle A submits its original public key and materials containing the vehicle's private information to the Law Enforcement Authority (LEA) to prove its legitimate identity when A enters the network. If the materials are proven valid, the LEA then issues a warrant to the CA. Based on the signed warrant received, the CA then sends an initial certificate to the vehicle.

Algorithm 1 System initialization

Require: PU_A generated by vehicle *A*; *A* submits PU_A to LEA

```
if (PU_A == true) then
        LEA warrant → CA
        CA certificate → A
else reject A
end if
```

Algorithm 2 is for the second phase which shows the vehicle authentication process dual factor authentication during communication between vehicles. If Vehicle A wants to communicate with Vehicle B, Vehicle A sends its certificate, C_A issued by the CA to Vehicle B for authentication. As Vehicle B receives C_A, it inspects if the certificate has expired. If C_A is not expired, Vehicle B then crosschecks with the Certificate Blockchain (CertBC) to ensure that the C_A is present in the blockchain. If the C_A is not present in the CertBC, then the public key of Vehicle A is invalid and the authentication process stops. Next, Vehicle B checks the Revocation Blockchain (RevBC) for the absence of Vehicle A's public key. If the public key of Vehicle A is present in RevBC, this implies that the public key has been revoked by the CA and the authentication process stops. Therefore, for a V2V communication to take place, the C_A must be present in the CertBC and the public key must be absent in the RevBC. Both of these blockchains are stored in the RSUs. Besides checking for proof of presence and proof of absence in the CertBC and RevBC respectively, Vehicle B can check with the miner for the trust value of Vehicle A.

Algorithm 2 Authentication process

Require: Valid C_A; *A* sends C_A to *B*; C_A contains PU and Sig of CA, PU and Sig of LEA, PU of *A*, and T_A expiration date

```
if (T_A > current time) then
        if (C_A present in CertBC) then
                if (C_A absent in RevBC) then
                        PU_A == 1
                else
                        PU_A == 0
                        stop authentication
                end if
        else
                PU_A == 0
                stop authentication
        end if
else    PU_A == 0
        stop authentication
end if
```

Require: Request query from *B* to RSU

```
if (ID_B = true) then
        trust value → B
else
        reject B
end if
```

The third phase is shown in Algorithm 3 is message rating generation, which takes place after the authentication process. After Vehicle A has been authenticated by Vehicle B, Vehicle A can now send messages to Vehicle B. Since messages can be untrustworthy, the messages must be checked for trust and rated. All the messages sent by vehicles in the network are stored in the Message Blockchain (MesBC) for message rating and uploading

purposes. When an event occurs, every message broadcasted by vehicles must be calculated for its trust. Once the frequency of event occurrence exceeds the predefined threshold in which this case is 15 confirmed messages, the receiving vehicle assumes that the event is true and produces a positive rating on the messages. After the message has been evaluated for trust and rated, it will be stored in the MesBC which will then be sent to the nearest RSU.

Algorithm 3 Message rating generation

Require: M_j: Message group reporting event e_j broadcasted by Vehicle V_i (i = 1, 2, …n); T^j_i: Trust of M_j as reported by V_i; T^j {}: trust set for event e_j; P(e/C): probability of event e; *Thr*: threshold of event frequency = 15 ; R'_i: current rating of V_i

Ensure: R_i: Updated rating of V_i

```
if (i = 0) then
        Tj_i = 0
else
        for each V_i do
                calculate Tj_i
                T^j {} ← Tj_i
        end for
        calculate P(e/C) using T^j {}
        if (P(e/C) > Thr) then
                for each (M_j = true) do
                        R_i ← R'_i + 1
                end for
        else
                for each (M_j = false) do
                        R_i ← R'_i – 1
                end for
        end if
end if
```

The fourth phase comprises Algorithm 4 that is trust value offset calculation when an RSU receives MesBC from vehicles. This MesBC may contain contradictory ratings for any specific messages. Therefore, the RSU weighs the positive and negative ratings to get the offset of trust value. After calculating the offset values of the ratings, the RSU then adds it into the blockchain.

Algorithm 4 Trust value offset calculation

Require: R_i: Updated rating of V_i; T'_i: current trust value of V_i; O_r {}: RSU r set of offsets

Ensure: T_i: Updated trust value of V_i

```
if (i = 0) then
        T_i ← T'_i + 0
else
        for each V_i do
                get R_i
                calculate offset
                T_i ← T'_i
                O_r {} ← T_i
        end for
```

The fifth phase runs Algorithm 5 which involves miner election and block generation. In order to manage the blockchain, there is a need for a central node. Hence, a miner from all the RSUs in the network is periodically selected to create new offset blocks. All RSUs in the network constantly change the nonce and calculate the hash values. Eventually, the RSU with a hash value lower than the threshold value set by the RSU r is selected as a miner. The miner RSU can then add the offset value obtained in Phase 4 into the blockchain and publish its block to other RSUs.

Algorithm 5 Miner Election and Block Generation

Require: S_r: Hash threshold of RSU r; F_r: sum of absolute values of trust value offsets; F_{max}: upper bound of F_r; O_r {}: set of offsets of RSU r; calculate hash

```
if (hash < S_r) then
        if (F_0 < F_r < F_max) then
                miner = RSU r
        else
                reject RSU r
        end if
else
        reject RSU r
end if
BC ← blocks from miner RSU r
miner RSU r clears O_r {}
```

The sixth phase is where the consensus is distributed among the rest of the RSUs as shown in Algorithm 6. When other RSUs receive a block from the miner, the RSUs evaluate the validity of the timestamp and add it to their block. In cases where the RSUs receive more than one block at a given time, the blockchain will fork. To handle this issue, a distributed consensus approach is used. Using this approach, each RSU can choose a fork and add a new block. Over time, the fork acknowledged by most RSUs becomes the longest and is then used the distributed consensus of the network, as the Trust Blockchain (TrustBC).

Algorithm 6 Distributed Consensus

Require: Blocks from miner RSU *r*; Add into RSU blockchain

```
if (timestamp = true) then
        RSU ← BC from miner RSU r
else reject block
end if
if (BC > 1) & (timestamp = true) then
        Fork_n ← BC from miner RSU r
else reject block
end if
if (Fork_n > Fork) then
        Fork_n = D_c
else Discard Fork_n
end if
```

4.3 Performance Analysis

This section presents and discusses the experimental analysis of the efficiency of the proposed method. The proposed method is evaluated in terms of performance during the absence as well as the presence of a network attack. PDR, end-to-end delay and packet loss is compared with the first three existing methods namely anonymous and lightweight authentication scheme based on smart card (ASC), lightweight authentication and key agreement protocol (LAKAP) and privacy-preserving authentication scheme (HEPPA). The performances of these three methods were evaluated and results were published based on PDR, end-to-end delay and packet loss. Finally, transmission overhead result is compared with efficient, scalable and privacy-preserving authentication (ESPA) and secure privacy-preserving authentication with Cuckoo Filter (SPACF) methods as these two methods were evaluated and results were published based on transmission overhead.

Each performance analysis is run 10 times at random in the simulator using default parameters. A statistical analysis is performed by averaging the values obtained to be compared with the benchmark protocols. These values are finally calculated for standard deviation (SD) and the confidence interval (CI) and tabulated. The results obtained at the presence of 100 nodes in the simulator are compared and discussed the next section.

4.3.1 Packet Delivery Ratio

PDR is obtained by determining the ratio of total number of packets received, P_r, to the total number of packets sent, P_s, in the network as shown in Equation 4.1.

$$PDR = \frac{P_r}{P_s} \qquad \text{Equation 4.1}$$

Figure 4.1 illustrates the result of PDR when the attacker or malicious user is non-existent. Table 4.1 shows that the proposed solution incurs higher PDR with a difference of 0.08, 0.10 and 0.02 as opposed to ASC, LAKAP and HEPPA correspondingly. The PDR of the proposed solution is higher because the proposed solution involves a lower computationally intense operation using hash function in order to execute the algorithm. The decentralized nature of blockchain also causes a decrease in the delay of packet transmission, resulting in higher PDR. Similarly, it can be seen from Table 4.2 that the proposed solution maintains PDR at a tolerable level with a ratio difference of 0.22, 0.18 and 0.18 as opposed to ASC, LAKAP and HEPPA correspondingly when a DoS attack is executed in the network. The PDRs of the benchmark protocols are much lower than the proposed solution because the algorithms are not able to protect network from DoS attack properly, resulting in higher loss of packet.

Table 4.1: Packet Delivery Ratio without Network Attack

No. of Nodes	Protocols					
	ASC	LAKAP	HEPPA	Proposed Protocol		
				Avg.	SD	CI (95%)
20	0.95	0.90	0.95	0.98	0.013166	0.022483
40	0.93	0.88	0.95	0.97	0.018529	0.017523
60	0.92	0.86	0.94	0.96	0.027889	0.011779
80	0.88	0.85	0.92	0.94	0.030111	0.011286
100	0.86	0.84	0.92	0.94	0.033483	0.019504

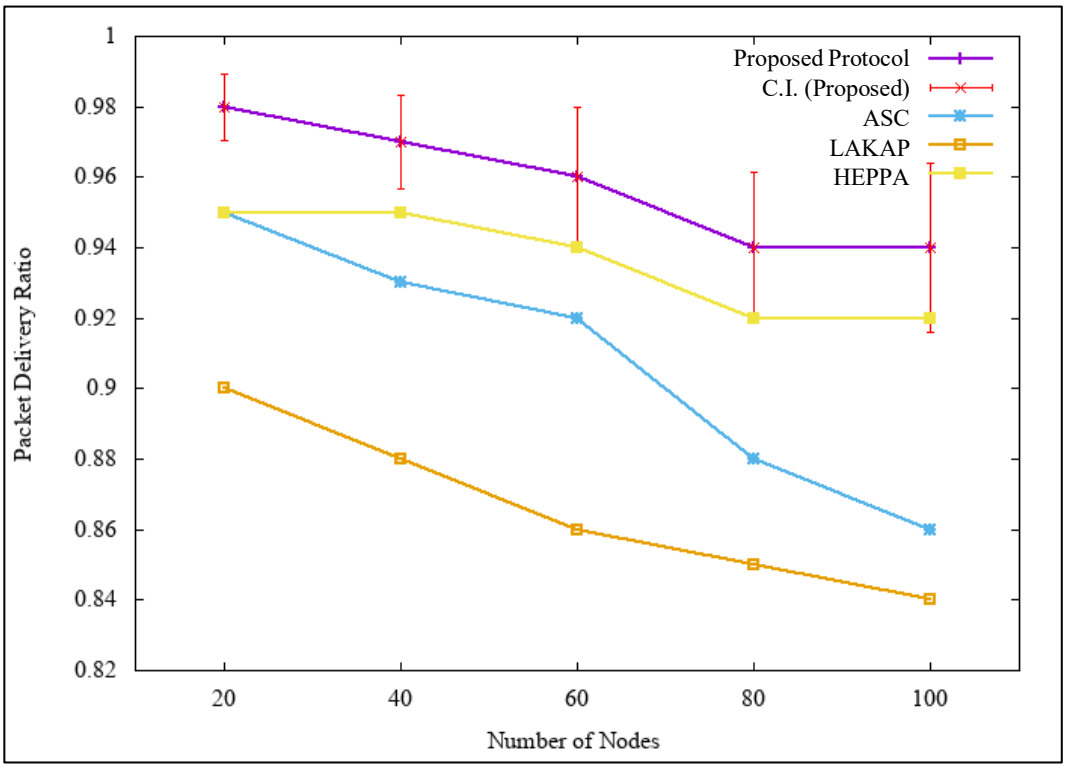

Figure 4.1: Packet Delivery Ratio without Network Attack

Table 4.2: Packet Delivery Ratio with Network Attack

No. of Nodes	Protocols					
	ASC	LAKAP	HEPPA	Proposed Protocol		
				Avg.	SD	CI (95%)
20	0.76	0.70	0.84	0.94	0.031429	0.009418
40	0.63	0.68	0.73	0.86	0.024495	0.013255
60	0.58	0.64	0.70	0.81	0.016465	0.019952
80	0.57	0.64	0.67	0.79	0.015776	0.021543
100	0.53	0.57	0.57	0.75	0.027264	0.023952

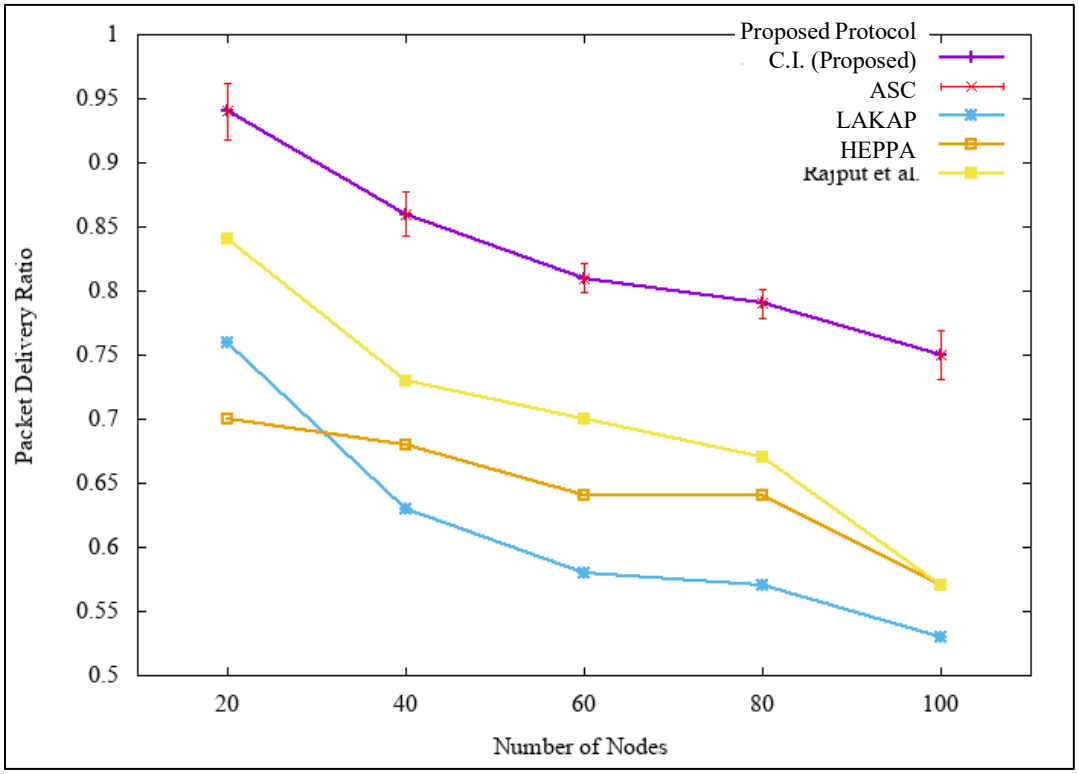

Figure 4.2: Packet Delivery Ratio with Network Attack

4.3.2 End to End Delay

End to end delay is defined as the time taken for a packet to arrive at destination from the source (Shorfuzzaman, Masud, & Rahman, 2016; Pukale & Gupta, 2016). PDR is significantly impacted by the end to end delay experienced by the network. Equation 4.2 shows the formula for end to end delay calculation, where EED denotes end to end delay, T_A denotes arrival time of a packet, and T_S denotes sent time of a packet.

$$EED = \sum T_A - T_S \qquad \text{Equation 4.2}$$

Figure 4.3 shows the simulation results of end to end delay incurred by the network when there is no attack executed. Table 4.3 shows that the proposed solution incurs a steady, lower end to end delay with a difference of 0.12 seconds, 0.30 seconds, 0.08 seconds as compared to ASC, LAKAP and HEPPA correspondingly. LAKAP shows a significant hike in end to end delay when the number of nodes is increased from 60 to 80 compared to the rest of the three solutions. Overall, the proposed solution incurs a lower and steady end to end delay because of the lightweight hashing technique which relies only on single permutation. This implies that the data packets are processed in a shorter time. This finding corroborates the results found in Section 4.3.1. Similarly, it can be seen from Table 4.4 that the proposed solution maintains a steady yet minor end to end delay time, with the difference of 0.22 seconds, 0.39 seconds and 0.34 seconds as opposed to ASC, LAKAP and HEPPA correspondingly when denial of service attack is executed in the network. The values are achievable due to the lightweight blockchain format in the proposed solution, linked via previous hash of message blocks, which also stands as a challenge for attackers to execute denial of service attack and modify data packets.

Table 4.3: End to End Delay without Network Attack

No. of Nodes	Protocols					
	ASC (s)	LAKAP (s)	HEPPA (s)	Proposed Protocol		
				Avg. (s)	SD	CI (95%)
20	0.10	0.09	0.18	0.09	0.015239	0.010901
40	0.15	0.15	0.15	0.10	0.016364	0.011706
60	0.19	0.22	0.16	0.11	0.016997	0.012159
80	0.24	0.35	0.18	0.12	0.013703	0.009803
100	0.25	0.43	0.21	0.13	0.018738	0.013404

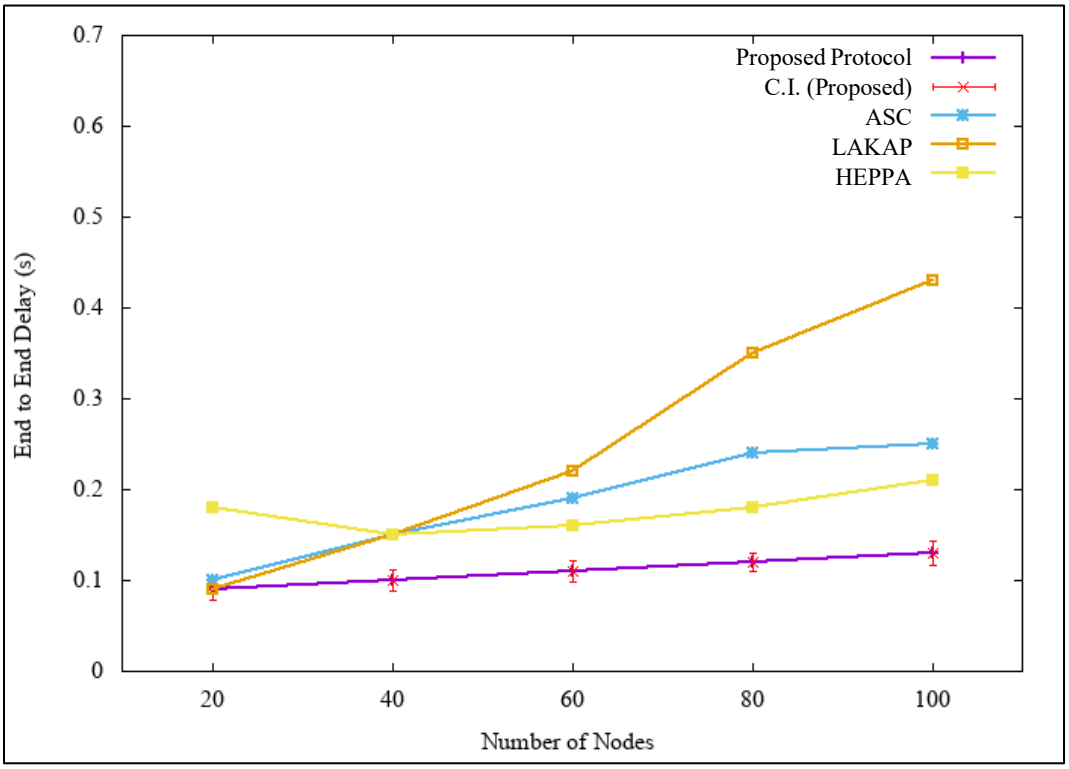

Figure 4.3: End to End Delay without Network Attack

Table 4.4: End to End Delay with Network Attack

No. of Nodes	Protocols					
	ASC (s)	LAKAP (s)	HEPPA (s)	Proposed Protocol		
				Avg. (s)	SD	CI (95%)
20	0.13	0.12	0.28	0.09	0.018886	0.01351
40	0.21	0.17	0.29	0.11	0.012517	0.008954
60	0.24	0.27	0.33	0.12	0.011547	0.008261
80	0.32	0.37	0.43	0.13	0.021602	0.015453
100	0.35	0.52	0.47	0.13	0.017638	0.012618

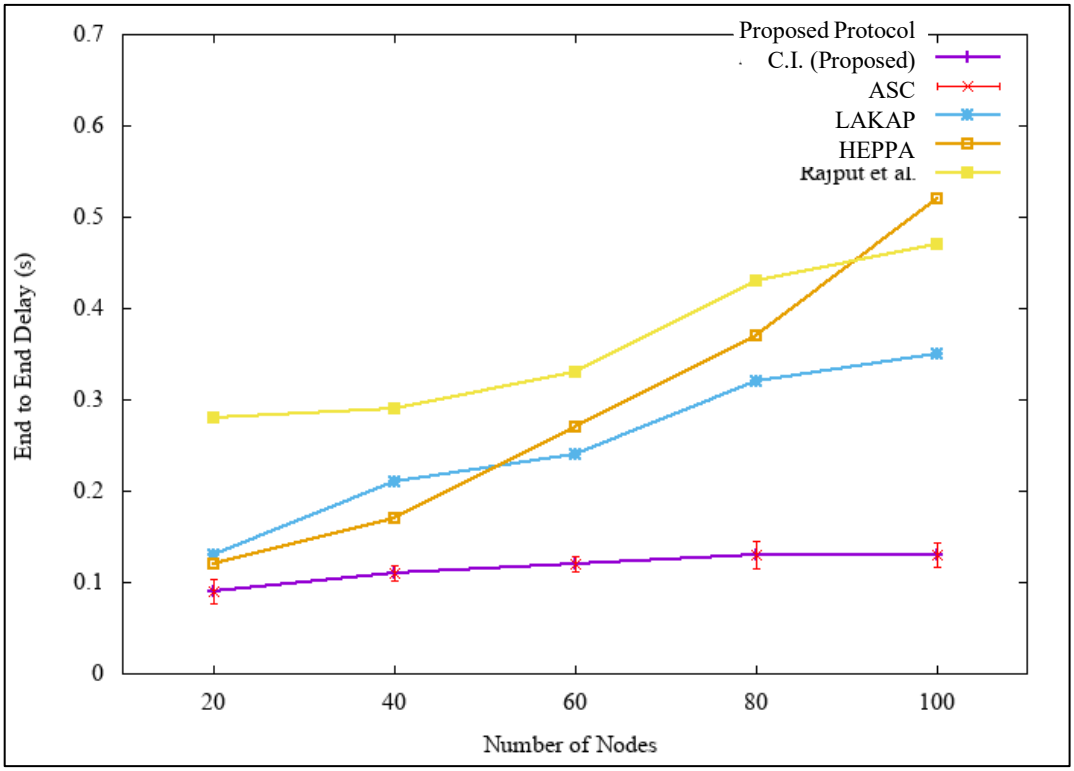

Figure 4.4: End to End Delay with Network Attack

4.3.3 Packet Loss

Packet loss, PL is obtained by determining the ratio of total number of packets lost, P_l, to the total number of packets sent, P_s, multiplied by 100 percent in the network as shown in Equation 4.3.

$$PL = \frac{P_l}{P_s} \times 100\% \qquad \text{Equation 4.3}$$

Figure 4.5 illustrates the results on packet loss when the attacker or malicious user is non-existent. Table 4.5 shows that the proposed solution incurs lower packet loss with a difference of 8.0%, 10.0% and 2.4% as opposed to ASC, LAKAP and HEPPA correspondingly. As for the average reading at 100 nodes, the value is 6.0%, which is the lowest among the three benchmarks. The packet loss of the proposed solution is lower because the proposed solution involves a lower computationally intense operation in order to execute the algorithm. This causes a decrease in the delay of packet transmission, resulting in lower packet loss. Similarly, it can be seen from Table 4.6 that the proposed solution maintains packet loss at a tolerable level with a difference of 21.5%, 17.7% and 17.5% as opposed to ASC, LAKAP and HEPPA correspondingly when a DoS attack is executed in the network. The packet loss of the benchmark protocols is much higher than the proposed solution because the algorithms are not able to protect network from DoS attack properly, resulting in higher number of packet drops as shown in Figure 4.6.

Table 4.5: Packet Loss without Network Attack

No. of Nodes	Protocols					
	ASC (%)	LAKAP (%)	HEPPA (%)	Proposed Protocol		
				Avg. (%)	SD	CI (95%)
20	5.0	10.0	5.0	2.0	0.942809	1.274445
40	7.1	12.1	5.1	3.0	1.763834	1.261771
60	8.3	13.9	5.9	4.0	2.788867	1.295035
80	12.4	15.3	8.0	5.5	2.173067	1.254519
100	14.1	15.7	8.4	6.0	3.299832	1.300557

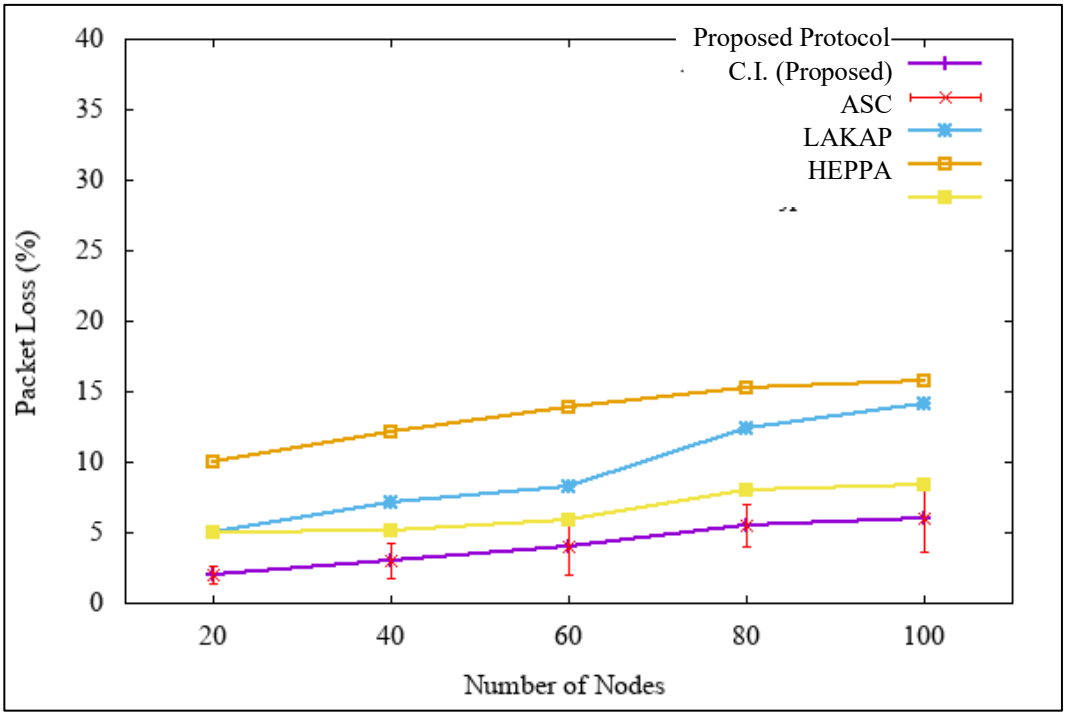

Figure 4.5: Packet Loss Ratio without Network Attack

Table 4.6: Packet Loss with Network Attack

No. of Nodes	Protocols					
	ASC (%)	LAKAP (%)	HEPPA (%)	Proposed Protocol		
				Avg. (%)	SD	CI (95%)
20	24.1	30.0	16.1	5.8	2.740641	1.960536
40	37.2	32.0	26.9	13.8	2.097618	1.500545
60	41.8	36.0	30.3	19.3	1.251666	1.895388
80	43.2	36.0	32.8	20.4	1.577621	1.128562
100	47.1	43.2	43.3	25.5	2.321398	1.660628

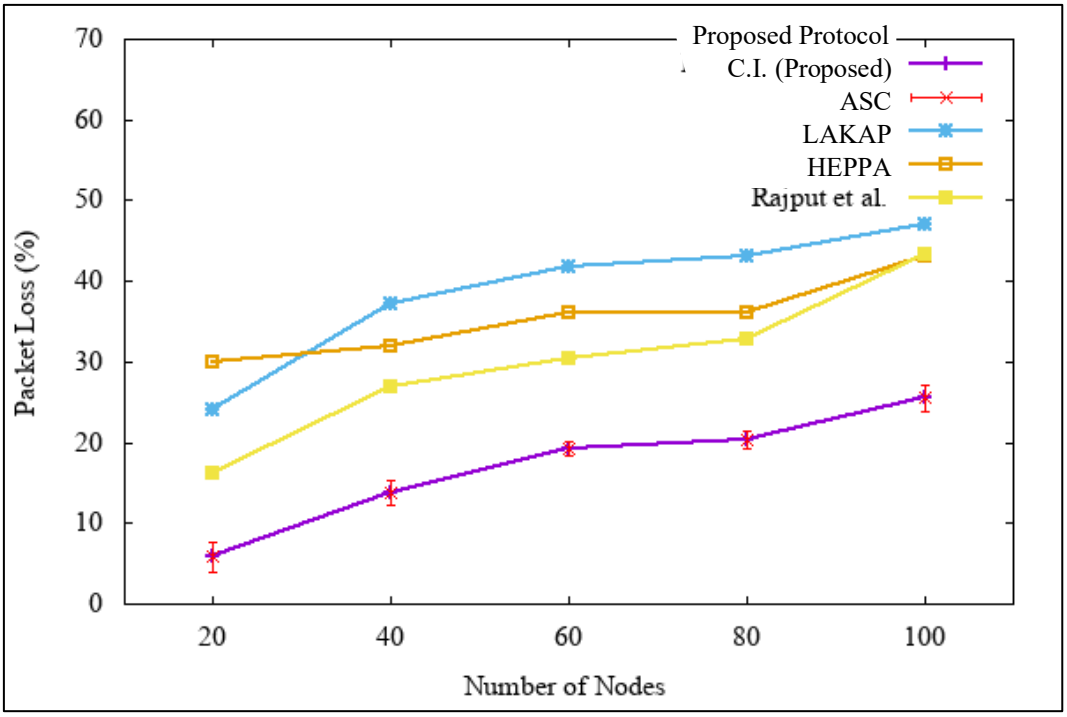

Figure 4.6: Packet Loss Ratio with Network Attack

4.3.4 Transmission Overhead

Transmission overhead refers to the number of overhead bytes divided by the total number of bytes in a packet transmission multiplied by one hundred percent. In other words, transmission overhead is the header packet and acknowledgement packets which determines the length and weight of a data packet. Longer data packets will be heavier as they have to carry more data in a packet, resulting in higher transmission overhead.

$$O_T = \frac{bytes_{overhead}}{bytes_{total}} \times 100\% \qquad \text{Equation 4.4}$$

Equation 4.4 shows the formula of transmission overhead calculation, where O_T denotes transmission overhead, $bytes_{overhead}$ denotes overhead bytes, and $bytes_{total}$ denotes the total number of bytes in a transmission. The results of transmission overhead when the attacker or malicious user is non-existent are illustrated in Figure 4.7, which clearly shows that the transmission overhead increases with increase in the number of nodes. Table 4.7 shows that the proposed solution incurs lower transmission overhead with a of 0.60% and 0.51% as opposed to ESPA and SPACF correspondingly. In other words, as the number of packets increases, the transmission overhead increases. Similarly, when an there is an attack as shown in Figure 4.8, the proposed solution incurs a steady increase in transmission overhead as compared to ESPA and SPACF. In Table 4.8, it can be seen that ESPA and SPACF is suffering a drastic increase of transmission overhead, with a difference of 0.16 and 0.08 respectively. The proposed solution incurs a lower transmission overhead compared to the benchmark protocols because of its implementation of signatureless public key infrastructure authentication technique to maintain a lighter and shorter packet header.

Table 4.7: Transmission Overhead without Network Attack

No. of Nodes	Protocols				
	ESPA (%)	SPACF (%)	Proposed Protocol		
			Avg. (%)	SD	CI (95%)
20	2.1	1.8	1.6	0.131656	0.094181
40	4.2	3.5	2.3	0.131656	0.094181
60	6.3	5.7	2.7	0.133749	0.095679
80	8.4	7.2	3.4	0.139841	0.100036
100	10.5	9.6	4.5	0.149443	0.106905

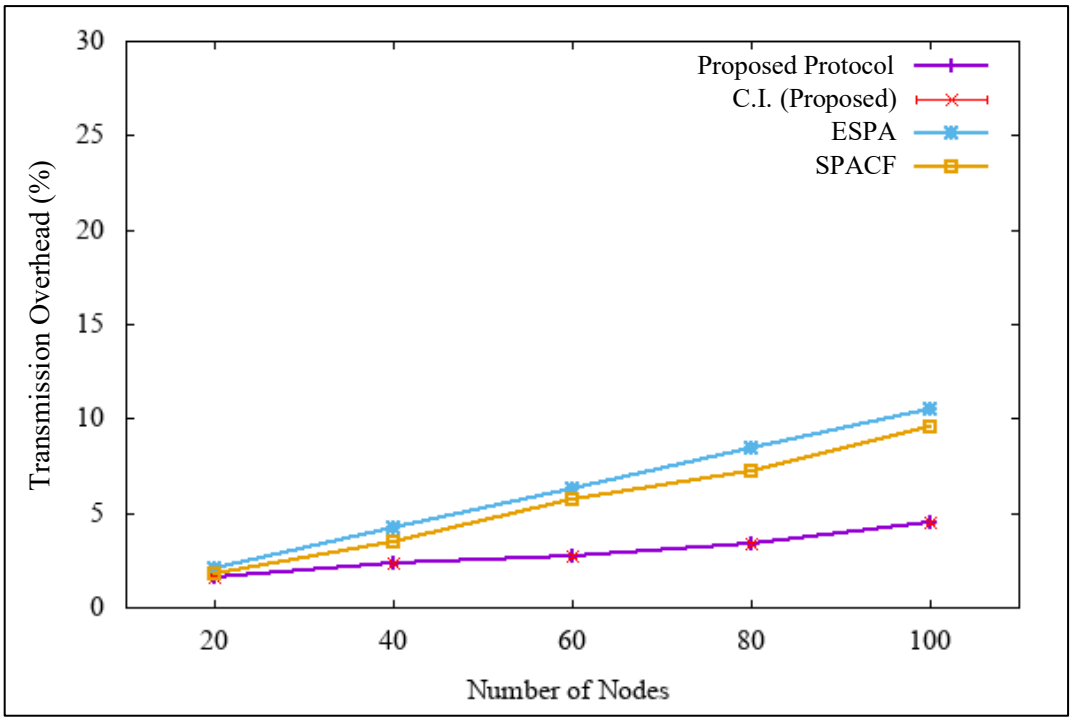

Figure 4.7: Transmission Overhead without Network Attack

Table 4.8: Transmission Overhead with Network Attack

No. of Nodes	Protocols				
	ESPA (%)	SPACF (%)	Proposed Protocol		
			Avg. (%)	SD	CI (95%)
20	3.4	3.1	1.8	0.154919	0.110823
40	6.2	5.5	2.7	0.168655	0.120648
60	10.3	7.3	3.2	0.185293	0.13255
80	15.4	8.5	3.7	0.193218	0.13822
100	20.5	12.6	5.0	0.207913	0.148722

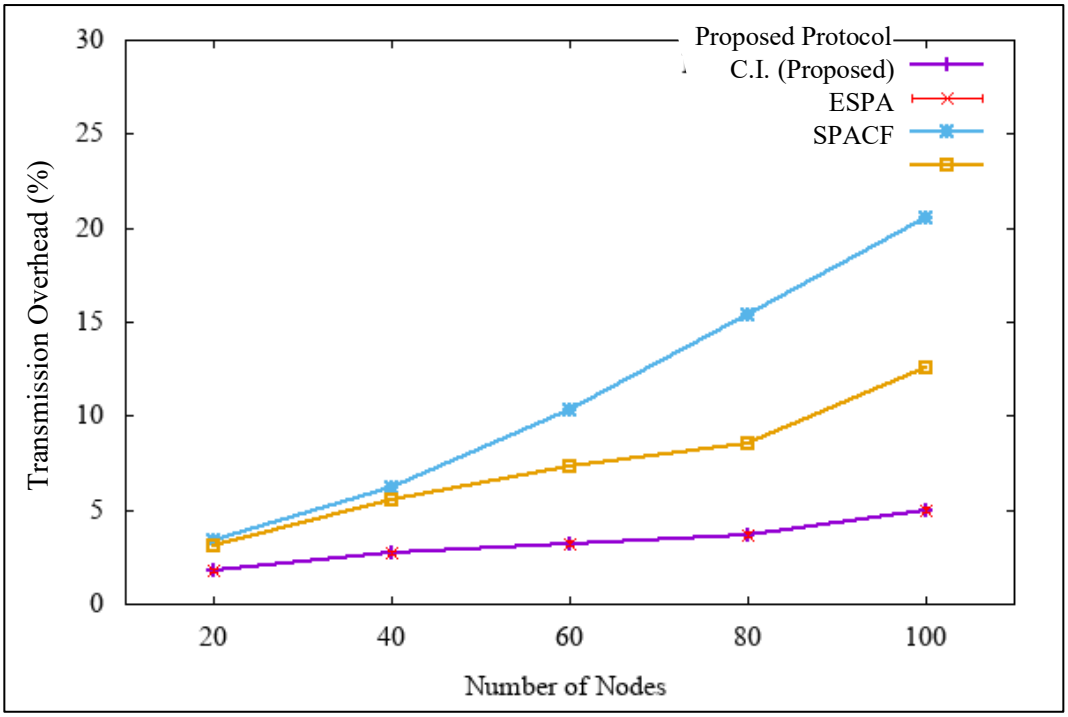

Figure 4.8: Transmission Overhead with Network Attack

4.4 Summary

This chapter presented the system development of the proposed solution to address the existing trust management and privacy protection issues in VANET. The proposed solution integrates a dual factor authentication technique and a fairly new technique which is blockchain technology implementation into a communication network. The dual factor authentication consists of PKI and timestamps of vehicles communicating in VANET. The proposed solution employs a dual factor authentication technique to improve the security and privacy of the data exchanged between vehicles. Furthermore, blockchain technology is implemented in the proposed solution to prevent the tampering of data by malicious nodes and to maintain the freshness of the communicated data. Each block is linked with the previous hash hence all communications are linked. As communication occurs, a node is authenticated when it has the private key correspondent to the output public key of the sender. Each communication has the sender's digital signature hence the sender cannot deny the sending the packet nor the receiver cannot deny receiving the packet since all transactions are kept in a public ledger.

In this chapter, the efficiency of the proposed solution is evaluated via simulation using Veins simulation tool. The performance analysis demonstrated a significant performance of the proposed solution in terms of PDR, end to end delay, percentage of packet loss and transmission overhead as compared to the benchmark security protocols. From the simulation results, it can be deduced that the proposed solution provides a better security against DoS attack which mostly lead to other active network attacks such as message fabrication, replay attacks, impersonation attacks as well as sybil attacks.

CHAPTER 5

CONCLUSION AND FUTURE WORKS

5.1 Introduction

This thesis depicted the issues of security and privacy loophole of VANET components namely nodes and RSUs that can result in various network attacks carried out by malicious users in the network. The main aim of the current study is to address the issues that arise in VANET, which is an open communication network in nature. Therefore, this research made an attempt to reduce the probability of security and privacy attacks such as impersonation, message fabrication, denial of service, replay and Sybil attacks. This chapter concludes the current study with a summary of contributions in fulfilling the main aim and research objectives. Moreover, some potential future works for other researchers in the field are also highlighted in this chapter.

5.2 Significance of Research

VANETs have received an enormous amount of attention from both researchers and vehicular industry due to their potential in delivering information to provide safety and infotainment messages to drivers and passengers. However, due to the high mobility of nodes and dynamic network topology, VANETs are vulnerable to network attacks such as message fabrication, impersonation, DoS, and Sybil attacks. All of these network attacks are capable of bringing catastrophic impacts on the safety of drivers and passengers in VANET. Apart from that, a lack of strong authentication of VANET users can lead to an increase in fake users with malicious intent to harm the network. Eventually, this can result in an increased dissemination of fake messages and unavailability of resources across the network. To

address these problems, many researchers have proposed security protocols to enhance security and privacy of users in VANET. Unfortunately, trust management for vehicles are still an open issue in VANETs. Other than that, most existing privacy preserving solutions are focused on mitigating only one network attack at any given time, leaving opportunities for other attack to occur in the network. In order to solve the issues mentioned, this research proposed a secure trust-based algorithm using blockchain technology to effectively mitigate several network attacks while preserving the privacy and security of the users in VANET.

The proposed solution is developed to mitigate networks attacks primarily DoS attack and other attacks that follow such as message fabrication, impersonation, and Sybil attacks, while maintaining the privacy of the users in VANET. The blockchain technology in the proposed solution uses timestamps and hashing techniques to maintain the freshness of the messages delivered. These techniques minimize message fabrication or modification attacks as the timestamps record the time a message is delivered while hashing secures the message against tampering by malicious users. Furthermore, the proposed solution also uses a message rating and trust approach via the blockchain technology. The message rating and trust approach ensures the trust management among vehicles during information exchange in VANET. Any vehicle that communicates fake messages to other vehicles in the network will be rated with low values, decreasing its trust. Vehicles with a lower trust value than the threshold value will be rejected from the network and their vehicle certificates will be revoked. Moreover, the proposed solution also uses a dual factor authentication method to verify the identity of the users in the network. This approach reduces Sybil attacks as the dual factor authentication allows only verified and authenticated users in the network.

The performance of the proposed solution was evaluated via simulation using Veins simulation tool under two settings, which were without network attacks and with network attacks. From the simulation, the proposed solution was found to perform better than the benchmark algorithms in terms of the PDR against increasing number of nodes in the network. The simulations showed that the proposed solution experienced up to 98% of PDR when there were no attacks launched in the network while during an attack, the proposed solution incurred up to 94% of PDR. Interestingly, the proposed solution experienced a delay of 0.130 seconds over increasing number of vehicles in the network with and without network attacks. Apart from that, the simulation results also showed that the proposed solution incurred a lower transmission overhead compared to the benchmark protocols due to the implementation of signatureless public key infrastructure authentication technique. The results of the simulation have achieved the third objective of this research.

5.3 Research Contributions

The motivation of this research work is to enhance the security and privacy of users and shared information between vehicles in VANET by reducing the occurrence of network attacks by malicious users. A new and secure trust-based algorithm is proposed in this research. The proposed solution offers a light-weight algorithm with the integration of blockchain technology to increase the trust level among the vehicles and users on a highway road in VANET. The blockchain technology allows the delivery of trustworthy messages among the vehicles across the network. Besides using blockchain technology, the proposed solution also uses a dual factor authentication method to authenticate the user as well as to safeguard the user privacy. This section highlights the important contributions made by the research work, which are as follows:

(a) Dual Factor Authentication

The proposed solution provides a dual factor authentication and integration of blockchain technology into the communication network. The dual factor authentication comprises of two authenticating factors which are signature-less PKI and timestamp. This dual factor authentication approach is responsible for a successful handshake between the nodes to securely communicate messages and exchange data packets in the network and maintain its freshness. Once a message is shared, the message blockchain will be refreshed periodically. The performance of the proposed solution in the network has been evaluated using simulation via Veins simulation tool. The simulation analyzes and compares existing methods against the proposed method. From the simulation, it has been shown that the proposed method performs well when an attack is induced in the network. Introducing blockchain technology instead of the conventional centralized security protocols, the proposed method reduces the occurrences of attacks against the privacy and the integrity of the messages that is being exchanged over VANET. Having timestamps in every message communicated, it maintains the freshness of the message and mitigates replay attack meanwhile the existing hashing feature in the blockchain technology mitigates impersonation and sybil attack within the network. Moreover, blockchain adapts a decentralized structure, where the occurrence of DoS attacks can be prevented and maintain the availability of services and communication channel in the network. This means that even if a DoS attack were to happen in VANET, the availability of the network to the users is not significantly affected.

(b) Effectiveness of Proposed Solution

In Chapter 4, performance of the proposed solution was evaluated using Veins simulation tool against several benchmark protocols that have similar techniques as the proposed solution. Two experiments were carried out to determine the effectiveness of the proposed solution, which were: (i) without network attack, and (ii) with network attack. The simulation results showed that without the network attack, the proposed solution incurred up to 98% PDR over increasing number of vehicles as compared to benchmark algorithms. Similarly, with network attack, the proposed solution has a high PDR of up to 94.2% which is relatively higher than the benchmark protocols.

The simulation results also demonstrated that the proposed solution experienced a lower end to end delay of 0.130 seconds at the peak number of nodes in the network compared to the benchmark methods. During a network attack, the proposed solution maintained the end to end delay as in the network without attack whereas all the benchmark methods experienced much higher delays, signifying the effectiveness and efficiency of the proposed method. The simulation results in Chapter 4 displayed that the proposed method can effectively prevent as well as reduce the occurrence of network attacks without imposing higher transmission overhead as well. From the simulation results, it can be deduced that the proposed secure trust-based algorithm offers security, privacy, and trust to the users in VANET.

5.4 Future Works

From the proposed solution described in this thesis, several future works can be carried out to further enhance the security and privacy in VANET. These future works are described as follows:

(a) Deployment in Autonomous Vehicles

In this research work, the proposed solution focused on vehicles equipped with advanced sensors which detect changes in the traffic or road conditions and send the information to the OBUs which interpret the data for drivers to make decisions. A possible future work for the proposed solution would be to implement the proposed solution in autonomous vehicles which are defined as self-driving vehicles which requires no control from humans to operate the vehicles safely (Union of Concerned Scientists, 2018). Since autonomous vehicles are connected to each other via a wireless medium, they, too, are vulnerable to malicious network attacks. Therefore, implementing the proposed solution into autonomous vehicles can help the vehicles to make much better decisions for safe driving. Nonetheless, various scenarios in which network attacks can occur in the network must be systematically modelled and tested prior to implementing in such vehicles in order to guarantee the safety of users and to minimize the costs (Rosique, Navarro, Fernández, & Padilla, 2019).

(b) Deployment in Multi-Junction Road Network

The current scope of this research is focused on highways with straight roads. Another future work is to deploy the proposed solution in a multi-junction road network since most actual routing decisions are made at multi-junctions (Zahedi, Zahedi, & Ismail, 2019; Tsiachris, Koltsidas, & Pavlidou, 2013). This implies that multi-junctions are often subjected to a high density of vehicles at any given time which can lead to nodes not being able to access the wireless medium due to the busy condition of the junctions (Acarman, Yaman, Peksen, & Peker, 2015). This situation opens up a new opportunity for adverse users to launch malicious attacks in the network, causing traffic jams and harming the lives of

drivers. Nevertheless, higher number of junctions have been found to offer better vehicle localisation, resulting in higher throughput and lower end to end delay (Sheet, et al., 2017). Therefore, it would be interesting to observe the effectiveness of the proposed solution when implemented in a multi-junction road network. The proposed solution may offer higher security and privacy to the users while efficiently reducing network attacks due to the integration of blockchain technology in the network.

(c) Introducing Cloud Server for Cloud Computing

Cloud computing in VANET is a fairly recent research interest for many researchers since it is a new technology capable of integrating VANET and mobile cloud computing. Vehicles using cloud (VuC) offers traditional cloud services such as network as a service (NaaS) and computing as a service (COaaS) via the Internet (Aliyu, et al., 2017). Cloud computing has the potential to enhance traffic safety and offer computational services to road users (Bitam, Mellouk, & Zeadally, 2015). Therefore, the blockchains used in the proposed solution can be uploaded into cloud server to enable easy access and light-weight computation which can then be delivered to the vehicles, thereby, further reducing transmission overhead of the proposed solution. Furthermore, by integrating 5G technologies with the cloud services can help the computational processes to be much faster, reducing the end to end delay encountered by the proposed solution.

5.5 Summary

In conclusion, a secure trust-based algorithm is proposed to improve the security, privacy, and trust level of vehicles in VANET. The proposed solution uses a dual factor authentication to ensure the privacy of the users and safe transmission of messages between vehicles. Moreover, the proposed solution is also integrated with blockchain technology to minimize the occurrence of network attacks such as message fabrication, impersonation, DoS, and Sybil attacks. Simulation of the proposed solution using Veins has shown that the proposed solution can mitigate the network attacks while ensuring the security and privacy of the users.

REFERENCES

Abbasi, I. A., & Khan, A. S. (2018). A Review of Vehicle to Vehicle Communication Protocols for VANETs in the Urban Environment. *Future Internet 2018, 10*(2), 14. doi:10.3390/fi10020014

Abdullah, N., Hakansson, A., & Moradian, E. (2017). Blockchain based approach to enhance big data authentication in distributed environment. *2017 Ninth International Conference on Ubiquitous and Future Networks* (pp. 887-892). Milan, Italy: IEEE. doi:10.1109/ICUFN.2017.7993927

Acarman, T., Yaman, Ç., Peksen, Y., & Peker, A. U. (2015). Intersection based routing in urban VANETs. *2015 IEEE 18th International Conference on Intelligent Transportation Systems* (pp. 1087-1092). Las Palmas, Spain: IEEE. doi:10.1109/ITSC.2015.180

Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing, 15*(5), 840-852. doi:10.1109/TDSC.2016.2616861

Aliyu, A., Abdullah, A. H., Kaiwartya, O., Cao, Y., Usman, M. J., Kumar, S., . . . Raw, R. S. (2017). Cloud computing in VANETs: Architecture, taxonomy, and challenges. *IETE Technical Review, 35*(5), 523-547. doi:10.1080/02564602.2017.1342572

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* In: M. Loukides, & A. MacDonald (Eds.) United States of America: O'Reilly Media Inc.

Asolo, B. (1 November, 2018). *Delegated Proof-of-Stake (DPoS) Explained*. Retrieved from MYCRYPTOPEDIA: https://www.mycryptopedia.com/delegated-proof-stake-dpos-explain ed/

Azees, M., Vijayakumar, P., & Deborah, L. J. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems, 10*(6), 379-388. doi:10.1049/iet-its.2015.0072

Begum, R., Raziuddin, S., & Prasad, K. (2016). A survey on VANETs applications and its challenges. *International Conference on Advanced Computer Science & Software Engineering*, (pp. 1-7). Hyderabad, India.

Bhoi, S. K., Khilar, P. M., Singh, M., Sahoo, R. R., & Swain, R. R. (2018). A routing protocol for urban vehicular ad hoc networks to support non-safety applications. *Digital Communications and Networks, 4*(3), 189-199. doi:https://doi.org/10.1016/j.dcan.2017.08.003

Bitam, S., Mellouk, A., & Zeadally, S. (2015). VANET-cloud: A generic cloud computing model for vehicular ad hoc networks. *IEEE Wireless Communications, 22*(1), 96-102. doi:10.1109/MWC.2015.7054724

Buterin, V., & Griffith, V. (2017). Casper the friendly finality Gadget. 1-15. Retrieved from arXiv:1710.09437

Castro, M., & Barbara , L. (1999). Practical Byzantine fault tolerance. *OSDI, 99*, 173-186.

Chaubey, N. K. (2016). Security analysis of vehicular ad hoc networks (VANETs): A comprehensive study. *International Journal of Security and Its Applications, 10*(5), 261-274. doi:http://dx.doi.org/10.14257/ijsia.2016.10.5.25

Choi, Y. H., Rajkumar, R., Mudalige, P., & Bai, F. (2009). Adaptive Location Division Multiple Access for reliable safety message dissemination in VANETs. *2009 6th International Symposium on Wireless Communication Systems* (pp. 565-569). Tuscany, Italy : IEEE. doi:10.1109/ISWCS.2009.5285227

Cui, J., Zhang, J., Zhong, H., & Xu, Y. (2017). SPACF: A secure privacy-preserving authentication scheme for VANET with Cuckoo Filter. *IEEE Transactions on Vehicular Technology, 66*(11), 10283-10295. doi:10.1109/TVT.2017.2718101

Dak, A. Y., Yahya, S., & Kassim, M. (2012). A literature survey on security challenges in VANETs. *International Journal of Computer Theory and Engineering, 4*(6), 1007-1010.

Defrawy, K. E., & Tsudik, G. (2011). ALARM: Anonymous location-aided routing in suspicious MANETs. *IEEE Transactions on Mobile Computing, 10*(9), 1354-1358. doi:10.1109/TMC.2010.256

Engoulou, R. G., Bellaïche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. *Computer Communications, 44*, 1-13. doi:https://doi.org/10.1016/j.comcom.2014.02.020

Florian, M., Finster, S., & Baumgart, I. (2014). Privacy-preserving cooperative route planning. *IEEE Internet of Things Journal, 1*(6), 590-599. doi:10.1109/JIOT.2014.2361016

Ghaleb, F. A., Razzaque, M. A., & Zainal, A. (2014). Mobility pattern based misbehavior detection in vehicular adhoc networks to enhance safety. *2014 International Conference on Connected Vehicles and Expo.* Vienna, Austria: IEEE. doi:10.1109/ICCVE.2014.7297684

Ghori, M. R., Zamli, K. Z., Quosthoni, N., Hisyam, M., & Montaser, M. (2018). Vehicular ad-hoc network (VANET): A review. *2018 IEEE International Conference on Innovative Research and Development.* Bangkok, Thailand: IEEE. doi:10.1109/ICIRD.2018.8376311

Gillani, S., Shahzad, F., Qayyum, A., & Mehmood, R. (2013). A survey on security in vehicular ad hoc networks. In: M. Berbineau, M. Jonsson, J.-M. Bonnin, S. Cherkaoui, M. Aguado, C. Rico-Garcia, . . . A. Vinel (Eds.), *Communication Technologies for Vehicles. Nets4Cars/Nets4Trains 2013. Lecture Notes in Computer Science* (Vol. 7865, pp. 59-74). Berlin, Heidelberg: Springer. doi:https://doi.org/10.1007/978-3-642-37974-1_5

Hanifatunnisa, R., & Rahardjo, B. (2017). Blockchain based e-voting recording system design. *2017 11th International Conference on Telecommunication Systems Services and Applications.* Lombok, Indonesia: IEEE. doi:10.1109/TSSA.2017.8272896

Hasrouny, H., Bassil, C., Samhat, A. E., & Laouti, A. (2015). Group-based authentication in V2V communications. *2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)* (pp. 173-177). Beirut, Lebanon: IEEE. doi:10.1109/DICTAP.2015.7113193

Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANet security challenges and solutions: A survey. *Vehicular Communications, 7*, 7-20. doi: https://doi.org/10.1016/j. vehcom.2017.01.002

Jindal, V., & Bedi, P. (2016). Vehicular ad-hoc networks: Introduction, standards, routing protocols and challenges. *International Journal of Computer Science Issues, 13*(2), 44-55. doi:http://dx.doi.org/10.20943/01201602.4455

Junaid, M. A., Syed, A. A., Warip, M. N., Azir, K. N., & Romli, N. H. (2018). Classification of security attacks in VANET: A review of requirements and perspectives. *MATEC Web of Conferences. 150*, pp. 1-7. Penang, Malaysia: EDP Sciences. doi:10.1051/matecconf/ 201815006038

Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors*, *19*(22), 4954. doi:10.3390/s19224954

King, S., & Nadal, S. (19 August, 2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 6. Retrieved from https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf

Kolte, S. R., & Madankar, M. S. (2014). Adaptive congestion control for transmission of safety messages in VANET. *International Conference for Convergence of Technology - 2014* (pp. 1-5). Pune, India : IEEE. doi:10.1109/I2CT.2014.7092177

La, V. H., & Cavalli, A. R. (April, 2014). Security attacks and solutions in Vehicular Ad Hoc Networks : a survey. *International Journal on AdHoc Networking Systems, 4*(2), 1-20. doi:10.5121/ijans.2014.4201

Lai, C., Zhang, K., Cheng, N., Li, H., & Shen, X. (2017). SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs. *IEEE Transactions on Intelligent Transportation Systems, 18*(6), 1559-1574. doi:10.1109/TITS.2016.2612233

Li, J., Lu, H., & Guizani, M. (2014). ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Transactions on Parallel and Distributed Systems, 26*(4), 938-948. doi:10.1109/TPDS.2014.2308215

Lim, K., & D., M. (2016). An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. *Vehicular Communications, 4*, 30-37. Elsevier. Retrieved from https://doi.org/10.1016/j.vehcom.2016.03.001

Lisk Academy. (n.d.). *Hashing*. Retrieved 4 June, 2019, from Lisk: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-hashing

Lu, Z., Qu, G., & Liu, Z. (2019). A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems, 20*(2), 760-776. doi:10.1109/TITS.2018.2818888

Malik, N., Nanda, P., Arora, A., He, X., & Puthal, D. (2018). Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering* (pp. 674-679). New York, USA: IEEE. doi:10.1109/TrustCom/BigDataSE. 2018.00099

Malla, A. M., & Sahu, R. K. (2013). Security Attacks with an Effective Solution forDOS Attacks in VANET. *International Journal of Computer Applications, 66*(22), 45-49.

Mazières, D. (2015). The Stellar Consensus Protocol:A Federated Model for Internet-level Consensus. *Stellar Development Foundation*, 1-45.

Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications, 1*(2), 53-66. doi:https://doi.org/10.1016/j.vehcom.2014.05.001

Merkle, R. C. (2000). A Digital Signature Based on a Conventional Encryption Function. *CRYPTO 1987: Advances in Cryptology '87. 293*, pp. 369-378. Springer, Berlin, Heidelberg. doi:https://doi.org/10.1007/3-540-48184-2_32

Mishra, R., Singh, A., & Kumar, R. (2016). VANET security: Issues, challenges and solutions. *International Conference on Electrical, Electronics, and Optimization*

Techniques (pp. 1050-1055). Chennai, India: IEEE. doi:10.1109/ICEEOT.2016.7754846

Moindrot, O., & Bournhonesque, C. (2017). Proof of Stake Made Simple with Casper. *CS244b: Distributed Systems, Autumn 2017*, 1-7.

Nakamoto, S. (31 October, 2008). Bitcoin:A Peer-to-Peer Electronic Cash System. Retrieved from http://www.academia.edu/download/54517945/Bitcoin_paper_Original_2.pdf

Ongaro, D., & Ousterhout, J. (2014). In search of an understandable consensus algorithm. *2014 {USENIX} Annual Technical Conference*, 305-319.

Patel, N. J., & Jhaveri, R. H. (2015). Trust based approaches for secure routing in VANET: A survey. *Procedia Computer Science, 45*, 592-601. doi:10.1016/j.procs.2015.03.112

Qu, F., Wu, Z., Wang, F.-Y., & Cho, W. (2015). A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems, 16*(6), 2985-2996. doi:10.1109/TITS. 2015.2439292

Rabieh, K., Mahmoud, M. M., & Younis, M. (2017). Privacy-preserving route reporting schemes for traffic management systems. *IEEE Transactions on Vehicular Technology, 66*(3), 2703-2713. doi:10.1109/TVT.2016.2583466

Rabieh, K., Mahmoud, M. M., Guo, T. N., & Younis, M. (2015). Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs. *2015 IEEE International Conference on Communications.* London, UK: IEEE. doi:10.1109/ICC.2015.7249492

Rajput, U., Abbas, F., Eun, H., & Oh, H. (2017). A hybrid approach for efficient privacy-preserving authentication in VANET. *IEEE Access*, 12014-12030. doi:10.1109/ACCESS.2017.271 7999

Raya, M., Jungels, D., Papadimitratos, P., Aad, I., & Hubaux, J.-P. (2006). *Certificate Revocation in Vehicular Networks.* School of Computer and Communication Sciences, Laboratory for computer Communications and Applications (LCA), EPFL, Switzerland.

Rosique, F., Navarro, P. J., Fernández, C., & Padilla, A. (2019). A systematic review of perception system and simulators for autonomous vehicles research. *Sensors, 19*(3), 648. doi: https://doi.org/10.3390/s19030648

Sathishkumar, N., & Rajakumar, K. (2017). A study on vehicle to vehicle collision prevention using fog, cloud, big data and Elliptic curve security based on threshold energy efficient protocol in wireless sensor network. *2017 Second International Conference on Recent Trends and Challenges in Computational Models* (pp. 275-280). Tindivanam, India: IEEE. doi:10.1109/ICRTCCM.2017.32

Schwartz, D., Youngs, N., & Britto, A. (2014). The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper, 5*(8), 1-10.

Shanzhi, C., Hu, J., Shi, Y., Peng, Y., Fang, J., Zhao, R., & Zhao, L. (2017). Cite. *IEEE Communications Standards Magazine, 1*(2), 70-76.

Sheet, D. K., Kaiwartya, O., Abdullah, A. H., Cao, Y., Hassan, A. N., & Kumar, S. (2017). Location information verification using transferable belief model for geographic routing in vehicular ad hoc networks. *IET Intelligent Transport Systems, 11*(2), 53-60. doi:10.1049/iet-its.2015.0228

Tamraparni, D., Kanza, Y., & Srivastava, D. (2018). Unchain your blockchain. *Proc. Symposium on Foundations and Applications of Blockchain, 1*, 16-23.

Tangade, S., & Manvi, S. S. (2016). Scalable and privacy-preserving authentication protocol for secure vehicular communications. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems.* Bangalore, India: IEEE. doi:10.1109/ANTS. 2016.7947800

Tippenhauer, N. O., Popper, C., Rasmusssen, K. B., & Capkun, S. (2011). On the requirements for successful GPS spoofing attacks. *Proceedings of the 18th ACM conference on Computer and communications security* (pp. 75-86). ACM.

Tsiachris, S., Koltsidas, G., & Pavlidou, F.-N. (2013). Junction-based geographic routing algorithm for vehicular ad hoc networks. *Wireless Personal Communications, 71*(2), 955-973. doi:https://doi.org/10.1007/s11277-012-0854-5

Union of Concerned Scientists. (21 February, 2018). *Self-driving cars explained*. Retrieved from ucsusa.org: https://www.ucsusa.org/clean-vehicles/how-self-driving-cars-work

Waghmode, R., Gonsalves, R., & Ambawade, D. (2016). Security enhancement in group based authentication for VANET. *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology* (pp. 1436-1441). Bangalore, India: IEEE. doi:10.1109/RTEICT.2016.7808069

Wazid, M., Das, A. K., Kumar, N., Odelu, V., Reddy, A. G., Park, K., & Park, Y. (2017). Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. *IEEE Access, 5*, 14966-14980. doi:10.1109/ACCESS.2017.2723265

Wu, Q., Liu, Q., Zhang, L., & Zhang, Z. (September, 2014). A trusted routing protocol based on GeoDTN+Nav in VANET. *China Communications, 11*(14), 166-174. doi:10.1109/CC.2014. 7085617

Xi, Y., Sha, K., Shi, W., Schwiebert, L., & Zhang, T. (2007). Enforcing privacy using symmetric random key-set in vehicular networks. *Eighth International Symposium on Autonomous Decentralized Systems.* Arizona, USA: IEEE. doi:10.1109/ISADS.2007.37

Ying, B., & Nayak, A. (2017). Anonymous and lightweight authentication for secure vehicular networks. *IEEE Transactions on Vehicular Technology, 66*(12), 10626-10636. doi:10.1109/TVT.2017.2744182

Zahedi, K., Zahedi, Y., & Ismail, A. S. (2019). CJBR: Connected junction-based routing protocol for city scenarios of VANETs. *Telecommunication Systems*, 1-12. doi:https://doi.org/ 10.1007/s11235-019-00590-8

Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommunication Systems, 50*(4), 217-241. doi:https://doi.org/10.1007/s11235-010-9400-5

Zhang, E. (2018). A Byzantine Fault Tolerance Algorithm for Blockchain (White Paper). Retrieved from https://docs.neo.org/en-us/basic/consensus/whitepaper.html#top

Zhang, Y., Zheng, D., & Deng, R. H. (2018). Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE Internet of Things Journal, 5*(3), 2130-2145. doi:10.1109/JIOT.2018.2825289

APPENDIX

Publications

1. Balan, K., Abdulrazak, L. F., Khan, A. S., Julaihi, A. A., Tarmizi, S., Pillay, K. S., & Sallehudin, H. (2018). RSSI and public key infrastructure based secure communication in autonomous vehicular networks. *International Journal of Advanced Computer Science and Applications*, *9*(12), 298-304. doi: 10.14569/IJACSA.2018.091243

2. Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors*, *19*(22), 4954. doi:10.3390/s19224954