6-18-2021

Vehicle Authentication in Vehicular Ad-hoc Network using RSU Based Approach

Steffie Maria Stephen
University of Windsor

Vehicle Authentication in Vehicular Ad-hoc Network using RSU Based Approach

By

Steffie Maria Stephen

A Thesis
Submitted to the Faculty of Graduate Studies
through the School of Computer Science
in Partial Fulfillment of the Requirements for
the Degree of Master of Science
at the University of Windsor

Windsor, Ontario, Canada

2021

Vehicle Authentication in Vehicular Ad-hoc Network using RSU Based Approach

by

Steffie Maria Stephen

APPROVED BY:

N. Zhang
Department of Electrical and Computer Engineering

I. Saini
School of Computer Science

A. Jaekel, Advisor
School of Computer Science

April 29, 2021

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

Vehicular Ad Hoc Network (VANET) is a pervasive network where vehicles communicate with nearby vehicles and infrastructure nodes, such as Road-side unit (RSU). VANET is the subclass of Mobile Ad Hoc Network (MANET) in which nodes move randomly and are connected wirelessly. Information sharing among vehicles is an essential component of an intelligent traffic system (ITS), but security and privacy concerns must be taken into consideration. Security of the network can be improved by granting access only to authenticated vehicles. This research proposes an RSU based approach to authenticate vehicles and notify vehicles about unauthorized messages/vehicles. It helps in preventing other vehicles in the network from being influenced by the malicious vehicle. In this approach, Blockchain has been used to securely maintain the identity of all vehicles in the network. The use of this RSU based approach helps to reduce the computational overhead on the On-board unit (OBU) of individual vehicles and reduces the processing delay.

DEDICATION

I would like to dedicate this thesis to my husband, daughter, parents, in-laws, and my supervisor.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank God, the Almighty, for His blessings to complete my thesis work successfully.

I would like to express my sincere gratitude to my supervisor, Dr.Arunita Jaekel, for her suggestions and assistance throughout my research. Also, I would like to thank my external reader Dr.Ning Zang and internal reader Dr.Ikjot Saini for their feedback and recommendations.

I would like to thank my family and friends for their love, care, and sacrifices. Special thanks to my husband and daughter for understanding and supporting me to complete my research work. I would also like to thank my friends Aekta, Saiteja, and Amanta for their continuous support and help throughout my thesis work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

VANET	Vehicular Ad-hoc Network
MANET	Mobile Ad-hoc Network
DSRC	Dedicated Short Range Communication
WAVE	Wireless Access in Vehicular Environment
CV2X	Cellular Vehicle to Everything
MAC	Medium Access Control
PKI	Public Key Infrastructure
ECDSA	Elliptic Curve Digital Signature Algorithm
DOS	Denial of Service
PBFT	Practical Byzantine Fault Tolerance
BCPPA	Blockchain-based Conditional Privacy-preserving Authentication
CMT	Chronological Merkle Tree
MPT	Merkle Patricia Tree
CRL	Certificate Revocation List
VSS	Verifiable Secret Sharing

CHAPTER 1

Introduction

1.1 An Overview of VANET

At the present time, an increase in the number of vehicles has led to increasing road accidents and congestion. This is a matter of life and death that needs to be addressed. According to senior research scientists, approximately 85% of deaths and 90% of disability are due to road traffic accidents each year in developing countries[1]. The road traffic injuries cause financial losses to both the individual and their families.

The Mobile Ad-hoc Network (MANET) makes it easy to exchange information between mobile devices. This enhanced the automobile industry with the emerging concept of the Vehicular Ad-hoc Network (VANET), where vehicles communicate with each other [2]. The VANET environment comprises Central Authorities (CAs), Roadside units (RSUs), vehicles and their On-board units (OBUs), and other infrastructures like smartphones [3]. The RSUs allow vehicles to disseminate messages within their range and acts as access points in the road network. The OBUs in each vehicle are responsible for transmitting the vehicle's state and collecting the state of other vehicles.

The communication standards used in VANET have Dedicated Short Range Communication (DSRC), Wireless Access in Vehicular Environments (WAVE), IEEE 802.11p, and Cellular-V2X (CV2X). DSRC uses WiFi-based physical layer and Medium Access Control (MAC) layer protocols [4]. The default standard used by the DSRC

technology to define the physical and MAC layers is IEEE 802.11p. WAVE describes the security of exchangeable messages using the IEEE 1609 standards.

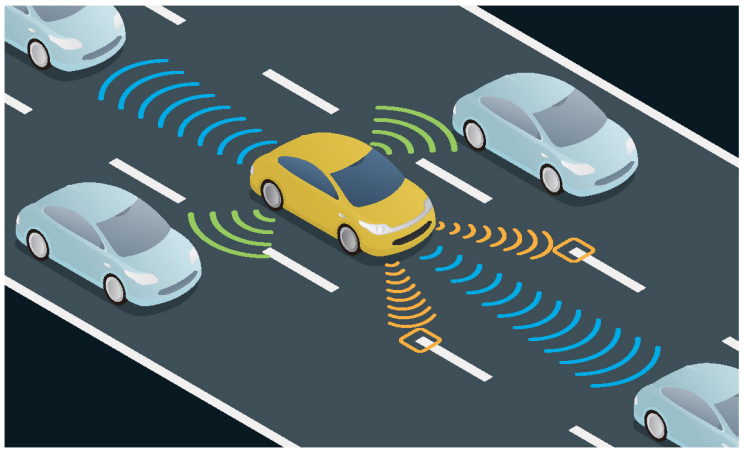

Figure 1.1: Vehicular Ad-hoc Network [5]

The CV2X standard supports network communications and direct communication using a side-link channel in the PC5 interface [4]. Both DSRC and CV2X use 5.9GHz for direct communication between vehicles. In our thesis, we make use of DSRC to transmit and receive messages in the network. The communication technologies ensure security and trust in messages using digital signatures. The possible communication patterns in VANET are Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Infrastructure to Infrastructure (I2I), and Vehicle to other smart devices (V2X) [6].

The different messages transmitted in the network include Basic Safety Message (BSM), Wave Short Message (WSM), and Wave Service Advertisement (WSA). Each vehicle in the network broadcasts 10BSMs per second periodically containing their details like pseudo id, position, and speed. These messages are referred to as periodic safety messages. They also send event-driven messages which are sent when there occurs road accidents, heavy traffic, and ongoing road constructions.

The characteristics of the Vehicular Ad-hoc Network (VANET) are high mobility, rapid change in network topology, and frequent message transmission. Security is one of the important challenges in VANET. As mentioned by [7], the attackers in VANET are classified as:

- Insider vs Outsider - Insider attackers are authenticated users in the network who has knowledge of the network configuration whereas outsider attackers are not authenticated users having limited capability to attack.
- Malicious vs Rational - The malicious attacker's aim is to destroy other vehicles in the network without any personal benefits. And, the rational attackers cause less/no damage to the network for their personal benefits.
- Active vs Passive - Active attackers generate fake messages or alter messages by other vehicles to cause damage in the network while passive attackers only eavesdrop on communication in the network and do not engage in it.
- Local vs. Extended attackers - Local attackers use limited on certain vehicles whereas extended attackers exploit all the resources to control several networks.

Figure 1.2 is an example of a Bogus attack where vehicle C sends a fake message about the traffic ahead of it. And, vehicle D which is unaware of it, changes its route and frees the road. This type of attack can be considered to be done by insider, rational, active, and local attackers. There are various security requirements in VANET to provide a secure and reliable network. In our thesis work, we will be concentrating on Authentication which is to ensure that valid messages are transmitted by authenticated vehicles/users only. To achieve this, we have made use of Blockchain technology which is decentralized, distributed and data is securely stored using cryptography techniques.

1.2 Motivation

To maintain a secure and reliable network, it is necessary to ensure that only legitimate/authenticated users can access and communicate in VANET. The legitimate

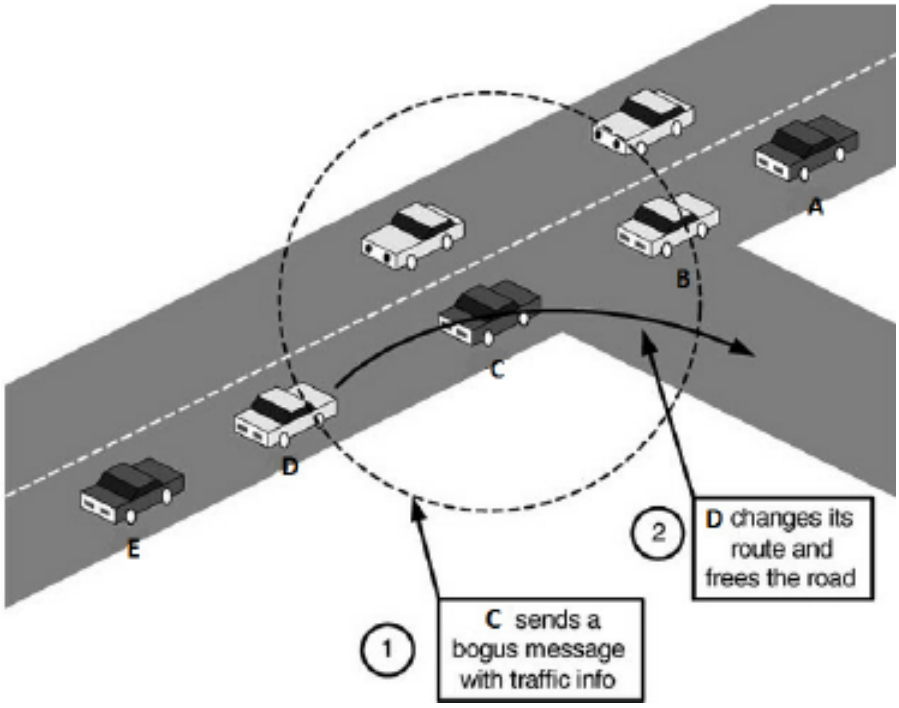

Figure 1.2: Example of an attack [8]

users in the network can be identified by using authenticated schemes. Authentication is an important security requirement in VANET which facilitates accountability for attacks caused by malicious vehicles in the network. These schemes use cryptography techniques such as symmetric or asymmetric cryptography which authenticates the messages by signing and verifying.

The Public Key Infrastructure (PKI) is considered to be the most suitable way for authenticating messages and maintaining a secure network [9]. In this scheme, each vehicle registered in the network will be provided with public and private key pair by the Central Authority (CA). Each message by the vehicles is digitally signed using their private keys before being transmitted. The vehicles are also provided with the public key of CA and a certificate that contains the vehicle's public key. These certificates by the vehicles are digitally signed by the CA using its private key.

After receiving messages, the vehicles will first retrieve the sender's public key by verifying the signature of the certificate using the CA's public key. Then, the digital

signature of the message sent will be verified using the retrieved public key. Since the vehicles send 10BSMs per second, the computational overhead for signing and verifying increases. So, this scheme is not efficient in VANET due to the encryption/decryption delay. It is also necessary to securely maintain the identity of all vehicles in the network.

The main aim of our thesis work is to provide a secure and reliable network by making sure that only authenticated vehicles can transmit/receive messages in the network. The real identity of the vehicles should be securely stored and maintained. This can be achieved using the decentralized and distributed Blockchain network. We also reduce the communication and computational overhead of both the RSU and vehicle's on-board unit using an RSU based approach.

1.3 Problem Statement

The properties of an effective and trustworthy Vehicular Ad-hoc network are [10]:

- Transparency - the activities of the network should be transparent and monitored by all participants.
- Conditional anonymity - the identity of the vehicles should be preserved and maintained anonymously but the authorities should be able to trace the vehicles in case of disputes.
- Efficiency - the authenticity of alert messages should be determined even when the network is congested.
- Robustness - the network should be resistant against attackers who aim to destruct the trustworthiness.

In the Public Key Infrastructure (PKI) authentication scheme, each message received by the vehicle should be verified to authenticate the sender. This process requires

additional computation by the receiving vehicle's on-board units. Hence, the performance of the network is affected due to the delay in encryption/decryption of the messages. Thus, our problem statement is to implement a blockchain-based authentication in VANET that reduces computational overhead on vehicle's OBUs.

Blockchain is a decentralized and distributed system consisting of all transactions in the peer-to-peer network. Each transaction in the distributed ledger is stored as a block. Blockchain technology includes anonymity, transparency, immutability, chronological order which makes it more secure and trustworthy. The data stored in it cannot be altered or deleted since it follows an append-only data structure. In our thesis work, we aim to secure the privacy of vehicle identities by using only Pseudo IDs for communication in the network while the vehicle's real identities are stored in Blockchain. Road Side Units (RSUs) have access to Blockchain and will authenticate senders upon receiving messages. The message signature verification also takes place at the RSU side which reduces both the computational overhead of the vehicle's OBU and delay in the authentication.

1.4 Solution Outline

We have proposed an RSU based approach where the authentication process takes place at the Road Side Unit (RSU) side. This approach includes a two-step authentication of signature verification and vehicle status verification using Blockchain. Here, the vehicle's identities are securely stored in Blockchain and vehicles do not have direct access to it. Each Basic Safety Message (BSM) transmitted will consist of the sender's information like pseudo ID, its public key and, digital signature. To maintain and validate the vehicle's identities we make use of Hyperledger Fabric [11], a permissioned blockchain. The data stored in Blockchain will be tamper-proof as the shared ledger is decentralized and distributed.

The participants in the network are the Authentication party, Road Side Unit (RSU),

and vehicles. The Authentication party registers the vehicles in the network and generates public-private key pairs for each vehicle. The Central Authorities (CAs) have both read and write access to the Blockchain, whereas RSUs have read-only access to the distributed ledger. When a message is received, the message signature is first verified by RSU and then it queries the Blockchain to authenticate the sender of the message. If the sender is an insider malicious vehicle, RSU notifies other vehicles by transmitting warning messages. This will prevent the legitimate vehicles from being influenced by the malicious vehicle and causing damage to the network. We have conducted performance analysis considering the parameters such as authentication delay and channel busy time. The results obtained indicate that the proposed approach performs better than traditional PKI based approaches, and has reduced computational overhead.

1.5 Thesis Organization

The rest of the thesis work is organized as: Chapter 2 explains the background study of VANET and the related works of Authentication in VANET using various Blockchain methods. In Chapter 3, we discuss our proposed method to securely maintain the vehicle identities using an RSU based approach. Chapter 4 describes the simulation setups, the parameters used for performance analysis, and the results obtained. Lastly, Chapter 5 concludes the thesis work by presenting our contribution towards the problem statement and directions for future work.

CHAPTER 2

Background Review

2.1 VANET

Vehicular Ad-hoc Network (VANET) is a subclass of Mobile Ad-hoc Network (MANET) where vehicles are interconnected and communicate with each other [12]. Vehicles communicate with the nearby vehicles and RSU with the help of an On-board Unit (OBU) installed in it [7]. The main idea of VANET is to frequently exchange road safety information among the vehicles to prevent a collision or any chaos in the network. The three types of applications supported by VANET are as follows [3]:

- Safety-Related Applications - These applications will increase road safety. They provide services like Collision avoidance where an alert/warning message send can prevent a collision. The Cooperative driving service sends lane change warning or curve speed warning to provide uninterrupted safe driving. And the Traffic optimization service informs the driver about accidents or traffic jams which helps them to decide an alternate path.

- User-Based Applications - This provides details like weather forecast and information about nearby locations to access like fuel station, coffee shop, car repair station, restaurants, and parking lots. They also offer peer-to-peer application services for sharing music or video by connecting to the internet or any other smart device.

Figure 2.1 shows the Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication in VANET where vehicles communicate with each other and also with

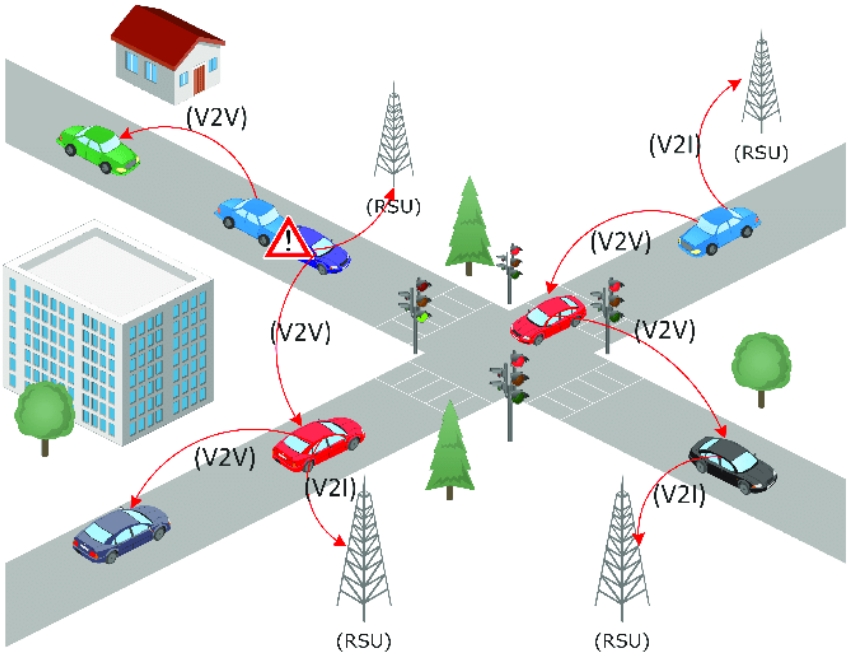

Figure 2.1: V2V and V2I communication [13]

RSUs. The other possible communication patterns in VANET are as follows [6]:

- Vehicle to vehicle (V2V) - Vehicles interact with each other by sending Basic Safety Message (BSM) and exchange information about traffic conditions or road accidents.
- Vehicle to infrastructure (V2I) - Messages are sent/received between vehicles and infrastructures like Road Side Unit (RSU) to improve road safety and traffic flow.
- Infrastructure to Infrastructure (I2I) - Infrastructures communicate with each other to provide various other services to vehicles.
- Vehicle to other smart devices (V2X) - Communication between vehicles to any other internet enables devices such as smartphones for enhancing their connectivity with infotainment systems.

2.1.1 Security in VANET

Security and privacy are two important challenges in VANET. This is because VANET is an open network and any vehicle can join the network and transmit messages. Since the message transmission happens wirelessly, it is possible for any malicious vehicle to either send any false information or alter messages sent by other vehicles [14]. These actions of such malicious vehicles may harm the legitimate vehicles or cause damage to the entire network. The entities concerned with VANET security are the network, vehicles, drivers, third parties, and attackers. The messages should be delivered securely in VANET as the communication medium is through the air and makes it possible for the attackers to enter the network [15]. The various security mechanisms used in VANET involve Public Key Infrastructure (PKI), Elliptic Curve Digital Signature Algorithm (ECDSA), Timed Efficient Stream Loss-Tolerant Authentication (TESLA), Modified version of TESLA (TESLA++), and VANET Authentication using Signatures and TESLA++ (VAST) [16].

The Vehicular Ad-hoc Network (VANET) should satisfy some security requirements to provide a secure, reliable, and trustworthy network. If these requirements are not fulfilled, it may lead to threats or attacks in the network. The various security requirements in VANET are as follows [17] [3]:

- Confidentiality - Messages should be accessed by the designated receivers only and other vehicles in the network should not be able to access the messages not designated to them. This is possible with the help of certificates and shared public keys.
- Integrity - The transmitted messages mustn't be altered/modified during the communication process. Here, the messages by the sender should reach the receiver's side as it is without any changes to it.
- Availability - The network and its resources should be always available to all the vehicles. In some cases, the response time should be quick as a delay in message delivery might make the message worthless.

- Scalability - It should be possible to increase the network size easily in VANET. Adding new vehicles and increasing the network should not affect the functionality, performance, and services provided in the network.

- Authentication - It is required to ensure that messages are sent by valid or legitimate vehicles before reacting to them. This prevents the network from malicious vehicles.

- Privacy - Personal information of vehicles like their ID and private key should be maintained against unauthorized access. So, a pseudo ID is generated for each vehicle that is used for communication in the network.

- Traceability - Although the vehicle's personal information is maintained securely, a trusted authority should be able to obtain the vehicle's real identity in case of some disputes like an accident in the network.

- Non-repudiation - Both the sender and receiver should not deny the transmitted messages. It can be used to interpret the sequence of crash reconstruction.

In our research, we consider the Authentication part of the security requirement where all the messages transmitted over the network are validated to determine if the sender is authenticated or not.

2.1.2 Attacks in VANET

The Vehicular Ad-hoc Network (VANET) is prone to attacks due to the high mobility of vehicles and the rapidly changing network topology. This also makes it difficult to find the suspect vehicles as the communication link between the vehicles break frequently. As mentioned by the authors in [7], [18] and [14], the possible attacks in VANET are categorized as follows:

- Attack on Availability - In this type of attack, the attackers interrupt the network's services and make them unavailable for other vehicles in the network. The lack of availability reduces the efficiency of the network. Examples of this

attack are Denial of Service (DOS) where the attacker jams communication between the vehicles, Malware attack where a virus or worm is sent to the application unit leading to the malfunction of other components in the network. In spamming attacks, lots of spam messages are broadcasted by an attacker to maximize the use of bandwidth while in a Blackhole attack, the attacker receives messages from the network but refuses to participate in the network [19]. Finally, Broadcast Tampering attack is where a malicious vehicle replicates the same message by altering messages or inserting new messages which may result in hiding safety messages to dedicated users.

- Attack on Confidentiality - Eavesdropping, Traffic Analysis attacks, Man-in-the-Middle attacks, and Social attacks are all examples of Confidentiality attacks in VANET. In the eavesdropping attack, unauthenticated users steal legitimate user's personal information like their identity and location by listening to their communication. The Traffic Analysis attack is where the attacker hears the message transmission, analysis its frequency, and extracts maximum useful information about it [17]. In a Man-in-the-Middle attack, the attacker gets access and controls the communication between two vehicles (i.e., V2V) without their knowledge; and in a Social attack, the attacker sends unethical messages to affect the driving experience and performance of the vehicle [19].

- Attack on Authentication - In these attacks, unauthenticated vehicles transmit/receive messages in the network. Examples of this attack are Sybil attack, GPS Spoofing, Impersonation attack, Tunneling attack, and Key/Certificate Replication attack. In a Sybil attack, the attacker creates a vision that there are additional vehicles in the network by using different identities at the same time [19]. In GPS spoofing, the attacker tricks other vehicles by creating false GPS location, whereas in an impersonation attack, the attacker trades the identity of an authenticated vehicle to show that message is sent by a legitimate user [17]. In a tunneling attack, the attackers use an extra communication channel known as a tunnel which helps them to communicate as neighbors even though

they are far-away from each other. In a key/certificate replication attack, the malicious vehicles use the duplicate keys of legitimate vehicles to confuse the Trusted Authorities (TA).

- Attack on Integrity - In this type of attack, the transmitted messages are altered/modified by unauthenticated users. Replay attacks, Message tampering, Masquerading attack, and Illusion attack are examples of Integrity attacks. In a replay attack, a valid message is transmitted fraudulently to produce a malicious effect. In message tampering, the attacker alters/modifies transmitted messages in V2V or V2I communication while in a Masquerading attack, the attacker pretends to be a different user by hiding its real identity to legally obtain unauthorized access. In an illusion attack, the attackers generate traffic warning messages to create an illusion to the nearby vehicles [7].

- Attack on Non-repudiation - In this attack, the attacker denies the message transmission in the network. An example of this attack is the Repudiation attack where the attacker denies engaging in sending and receiving messages in case of any dispute [7].

2.2 Authentication in VANET

To develop trust in vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication, authentication, privacy, and security should be leveraged in VANET. As mentioned in section 2.1.1, Authentication is a security requirement to ensure that only valid/legitimate vehicles join the network and communicate with other participants. This authentication process takes place when a vehicle joins the network or utilizes any services such as communicating with each other. In [7], Sheikh et al. have listed few Authentication requirements which should be satisfied. They are as follows:

- Computational and Communication Overhead - The number of requests sent to authenticate a sender vehicle and the number of computations performed by

vehicles such as cryptographic operations should be minimized.

- Utilization of Bandwidth - The bandwidth of the channel should be utilized in bytes per second (bps) to perform authentication processes such as the secret key exchange.
- Scalability - The authentication process should be able to handle multiple operations ad communications.
- Time Response - The time taken to authenticate the vehicles must be reduced.
- Powerful Authentication - The authentication schemes should be capable of preventing the network from attacks.

Various authentication schemes are being used to ensure secure communication in Vehicular Ad-hoc Network (VANET). These schemes make use of different cryptographic techniques for message signature and verification. The commonly used two schemes for cryptography are Public Key Infrastructure (PKI) and the Symmetric key scheme [20]. The Symmetric cryptography scheme is also known as private key cryptography [7]. The transmitted messages are authenticated/verified using a Message Authentication Code (MAC) in this scheme. Here, the senders generate MAC for each message using a shared secure key. On receiving these messages, the receiver vehicle will verify the attached MAC using the shared key. Since a single secret key is used in this symmetric cryptography scheme, the authentication process will be faster. But, this scheme does not ensure non-repudiation and so it has low level of privacy and reliability [21].

The Public Key Infrastructure (PKI) is considered to be a feasible solution to provide security and privacy through authentication [22]. In this scheme of authentication, the vehicles in VANET should be registered with the Central Authority (CA). The CAs are responsible for issuing public keys, certificates and managing the vehicle's identities those are within their range [23]. Each vehicle registered in the network will receive a private/public key pair and a certificate from the CA. The certificate

will consist of the vehicle's public key, the digital signature of the public key which is signed using the CA's private key and the CA's identity [24].

When sending each Basic Safety Message (BSM), the senders will attach their certificate and digital signature using the private key along with the message. Then, the receiver of the message will first verify the attached certificate using the public key of the CA that was received when keys were issued. After the certificate verification, the public key of the sender will be obtained and used to verify the message's digital signature. The sender of the message is authenticated if both the certificate and message signature verification happens successfully. The main aim of PKI is to achieve message authentication, integrity, and to securely obtain the public key [25].

2.3 Blockchain

Blockchain technology was first introduced as Cryptocurrency by Satoshi Nakamoto in 2008 [26]. It is a decentralized and distributed ledger that allows transparent and trustworthy transactions between participants in the network without the interference of third party [27]. Blockchain is made of a vast number of consistently growing blocks/records which are linked in sequential order using cryptography. The basic components of Blockchain are nodes in the network, the shared ledger, distributed database system, and cryptography [28].

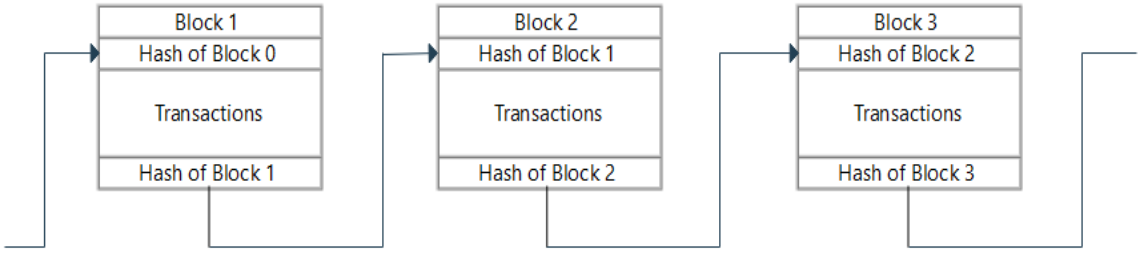

Figure 2.2: Structure of Blockchain

As depicted in Figure 3.2, each block consists of its ID, set of transactions, and the cryptographic hash of both the previous block and the block itself [29]. The hash of each block is generated by performing a hash operation on the transactions and this makes it difficult to retrieve the original data. The blocks also contain the time of block creation as Timestamp which increases the reliability of blockchain [30].

In the blockchain, there is no central node present to verify if the ledgers on the distributed node are all same. So, Consensus algorithms are used to ensure that the new block/record is properly added to the blockchain [31]. These algorithms provide fairness and equality in the network. As mentioned by Sharma et al. in [32], the different consensus algorithms used in blockchain are:

- Proof of Work (PoW) - In this mechanism, participating nodes called miners have to solve mathematical puzzles like calculating a hash function. The node which solves the puzzle and wins will create a block for the transaction and be rewarded. Then, the winning node will broadcast this block to other nodes in the network for its acceptance. The limitation of this algorithm is higher energy consumption and centralization of miners.

- Proof of Stake (PoS) - In the PoS mechanism, the nodes with higher stakes will be selected to add blocks to the network. This reduces the energy consumption compared to PoW. Since the nodes having higher stakes have control over the network, double spending attacks are possible.

- Proof of Activity (PoA) - Instead of the whole block, only the template containing the header information and the miner's address is mined. The nodes having higher stakes are selected as validators to sign the new block. A new group of validators is selected until the same number of signatures are received to add the block to the blockchain.

- Practical Byzantine Fault Tolerance (PBFT) - In PBFT, one node is considered to be a primary/leader node and the other nodes are the secondary nodes. This

mechanism takes place in four phases where the leader node is replaced in each phase. Although this algorithm is energy efficient, it is vulnerable to Sybil attacks and Scaling.

- Proof of Trust (PoT) - The PoT consensus mechanism also functions in four phases. In the first two phases, the leader is selected and the validators are chosen by the leader to validate a transaction. In the next phase, the transaction is validated by the validators using a voting process. And, the validated transaction is added to the blockchain in the last phase. This algorithm has improved scalability, efficiency, and performance [33].

- Proof of Elapsed Time (PoET) - PoET is the algorithm that is used in permissioned blockchain. Here, the miners have to be identified and verified before being added to the blockchain. Each node has to wait for some time, finish the time slot and then create a new block.

2.3.1 Types of blockchain

Blockchain technology is mainly classified into four types as follows [34]:

- Public Blockchain - This is also known as a permissionless distributed ledger system. Any node can join the blockchain network and be an authorized node to access the services. The registered nodes have access to all records, are authorized to verify transactions, and do mining. This type of blockchain will be secure if all the nodes follow the security protocols. Examples of public blockchain are Bitcoin and Ethereum [35].

- Private Blockchain - This is also known as permissioned blockchain where the nodes require permission to join the network. The controlling/central authority will be responsible for enabling authorization, permission, and accessibility to all the nodes. An example of a private blockchain is Hyperledger composer such as Fabric or Sawtooth [11].

- Consortium Blockchain - In this type of blockchain, the network is managed by more than one organization and it is semi-decentralized. The exchange of information and mining is also done by more than one organization. An example of this blockchain is Energy Web Foundation [36].

- Hybrid Blockchain - The hybrid blockchain is a combination of the public and private blockchain. Some of the selected data/records are maintained and managed confidentially while the remaining records are accessed publicly. So, in this type of blockchain, a transaction of a private network is verified within the network and also can be verified in a public blockchain. An example of the hybrid blockchain is Dragonchain [37].

2.3.2 Working of Blockchain

Blockchain consists of three technologies, namely, cryptographic keys, shared ledger, and computations to store records in blockchain network [38]. The cryptographic keys that are the public and private keys are used to perform secure transactions between two nodes. The shared/distributed ledger helps in storing the transaction information at various nodes across the network so that it is not controlled by a single node [39]. The mathematical computations are mainly performed to increase the security and reliability of the transaction and their storage. In this way, blockchain employs cryptography keys to interact over the network and verify the transactions [38].

Figure 2.3 explains the working of a blockchain about how a transaction is created and added to the blockchain network. Initially, a transaction is requested by the node which depends on the purpose of the network. Then, a block is created for the requested transaction and sent to all the nodes in the network to be validated. Based on any one of the consensus mechanisms mentioned in section 2.3, the transaction is validated by the selected validators. If the transaction is considered valid/legitimate by the validator nodes, the block will be added to the existing blockchain and the transaction is said to be complete.

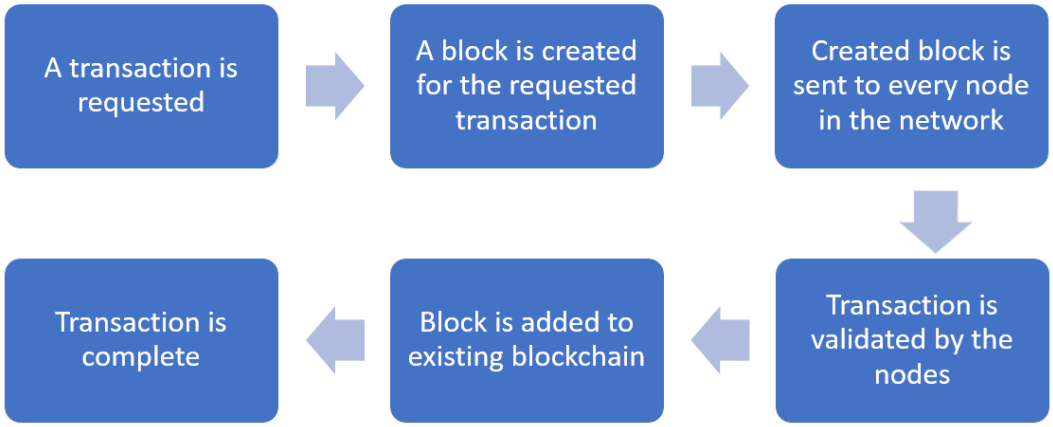

Figure 2.3: Working of Blockchain

2.4 Blockchain in VANET

The number of vehicles and their data gathered in Vehicular Ad-hoc Network (VANET) increases due to high mobility and frequent message transmissions. So, the security of the data is at risk and Blockchain can be used to securely manage these data [40]. The hash functions and the cryptography used in blockchain will make sure that the data stored in VANET are tamper-resistant. This removes the dependency of the network on the central authorities [41].

The four major stages involved in blockchain-based VANET are: blockchain set-up, registration of vehicles, Safety Benefit Maximization (SBM), and blockchain record [42]. In the first stage, the blockchain network is set up based on the nature of the system, i.e., either permissionless or permissioned. Once the network is set-up, the vehicles in VANET are registered to the blockchain network after being validated by the validator nodes. Then, the SBM is leveraged and uploaded to the network to ensure increased security, reliability, and trustworthiness of the VANET. And in the final stage, the transactions that occur within the nodes are stored in the form of blocks/records in the distributed ledger. The usage of blockchain technology and its decentralized nature eliminates single-point failure in VANET [27].

2.5 Literature Review

In recent years, VANET is combined with blockchain technology to authenticate vehicles and for privacy-preserving. Blockchain is an emerging technology that can be implemented as either permissioned or permissionless blockchain. Most of the existing approaches use blockchain to provide secure communication and to convert VANET into a distributed and decentralized network. Few papers which introduced these approaches are reviewed below.

The security of VANET is improved by a proposed security architecture based on blockchain and Mobile Edge Computing (MEC) in [41]. This architecture consists of the perception layer consists of vehicle and RSU, the edge computing layer provides computing resources, and the service layer comprises blockchain and cloud services. The cloud of the service layer is used to store a large amount of data in VANET and blockchain along with MEC is used to ensure the security of data. In [43], a distributed VANET system is proposed by combining Ethereum blockchain, Ciphertext-based Attribute Encryption (CP-ABE), and Inter Planetary File System (IPFS). The blockchain is responsible for managing user identity and all data are maintained through smart contracts. IPFS uses replication proof, provides reliability and availability, and avoids single points of failure. In this approach, the encryption and decryption steps are split by transferring calculation operations to RSU.

In [44], Liu et al. have proposed a Blockchain-based Unlinkable Authentication (BUA) scheme where the attackers are prevented from linking multiple messages and interfering with the vehicle's privacy. Here, the Service Managers (SMs) are used to access vehicular data from the blockchain and verify the legitimacy of vehicles within their coverage area. The SMs are also responsible for the vehicle's registration in the network and conditional traceability. In the authentication phase, the unlinkability of the messages are increased by randomizing them using random number and timestamp. This scheme depends on mutual authentication between the SMs and vehicles in the

network. On receiving a message from vehicles, SMs first decrypts the encrypted address and searches the blockchain. If the address obtained is the same as that in the blockchain, SM authenticates the vehicle to be legal and sends a signature to the vehicle. Then the vehicle authenticates the SM using the signature received and ensures mutual authentication. The drawbacks of this approach are the registration process takes more time than authentication and it cannot resist collusion attacks between SMs.

In [45], Lin et al. have presented a novel Blockchain-based Conditional Privacy-preserving Authentication (BCPPA) to eliminate issues like private key revocation, frequent interactions, and requirement of idea hardware. The communication in Vehicular Ad-hoc Network (VANET) is secured by combining Ethereum based blockchain and a key derivation algorithm for effective certificate management. The ECDSA digital signature scheme is used and it consists of three phases, namely, system initialization, message signing, and message verification. They have implemented an Ethereum test network called Rinkeby where the transactions are recorded. They have also tested the time cost of the algorithms used and evaluated the performance based on the certificate management and authentication in communication. The disadvantage of this approach is that it does not improve the speed of signing and verifying as compared to other approaches.

A traceable and decentralized VANET system based on blockchain technique is proposed in [46] to employ a secure authentication scheme between vehicles and Road-side Units (RSUs). This system provides both a trust communication environment and preserves anonymity without disclosing the user's real identity. The authors have also designed a distributed blockchain-based storage scheme to prevent the distribution of forged messages.They have also evaluated the performance of their approach in terms of privacy, multi-storage, decentralization, compatibility, and accountability.

Table 2.1: Comparison of Authentication Approaches

Papers	**Blockchain Type**	**Authentication Done by**	**Limitations**
Secure Identity Management Framework for Vehicular Ad-hoc Network using Blockchain [47]	Permissioned	Vehicle and RSU	Increase in channel busy time leads to congestion
BUA: A blockchain-based unlinkable authentication in vanets [44]	Permissioned	System Manager	Cannot resist collusion attack between service managers
BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks [45]	Permissionless (Ethereum)	Vehicles	There is no change in performance time (signing and verifying)
A blockchain-based privacy-preserving authentication scheme for vanets [48]	Permissioned	Receivers (Vehicles)	Have not considered the communication overhead
An Anonymous Conditional Privacy-Preserving Authentication Scheme for VANETs [49]	-	Vehicles (On-board Units)	Single point compromise will destruct entire network
Proposed Method	**Permissioned**	**RSU**	**-**

In [47], George et al. have proposed a blockchain-based decentralized authentication approach using a permissioned blockchain, Hyperledger Fabric. They have presented a lightweight authentication that eliminates the certificate verification and the real identities of vehicles can be accessed by authorized entities only. Moreover, the vehicles request Road Side units(RSUs) to authenticate or validate the senders upon receiving each message and if the sender is not authenticated, the message is simply discarded. They have also compared their simulated result to the traditional PKI framework concerning the delay in the authentication. This authentication scheme avoids single-point failure and provides a decentralized and distributed system. The increase in communication overhead and channel busy time leads to congestion in the network.

The authors in [48] have proposed Blockchain-based Privacy-preserving Authentication (BPPA) scheme for VANET. In this approach, they have extended blockchain by combining the Chronological Merkle tree (CMT) and Merkle Patricia tree (MPT). The distributed authentication scheme designed is used to eliminate space and communication overhead in Certificate Revocation List (CRL). The linkability between the certificate and the vehicle's real identity is encrypted and stored in the blockchain which will be revealed only in case of disputes. Their experimental result shows that the delay for issuing and revoking certificates is low. But, they have not considered the communication overhead in their approach.

The security credential management system in [50] uses two types of certificates: enrollment certificate which is issued by Enrollment CA and multiple pseudonym certificates are issued by Pseudonym CA. The enrollment certificates are used to request pseudonym certificates which are considered to be short-term certificates to the vehicles. They also have the misbehavior authority that is responsible for identifying and reporting misbehaviors, revoking the misbehaving vehicle, and adding them to the Certification Revocation List (CRL). In [49], the authors have proposed an anonymous privacy-preserving authentication scheme using Message Authentication Code

(MAC). In the mutual authentication phase, vehicles receive a group key that can be used to generate and verify authenticated messages. This group key is generated using Verifiable Secret Sharing (VSS) to ensure the registration of legitimate vehicles and to provide secure communication between them. The authors have claimed that this approach satisfies the fundamental requirements, has improved computational cost, and reduced communication overhead. However, a single-point compromise can destruct the entire network.

Table 2.1 shows the comparison of different existing approaches and our proposed method. Most of the approaches have used either permissioned or permissionless blockchain. And the authentication takes place at the vehicle's On-board Unit (OBU) or any third parties such as System Manager (SM) in [44]. All these approaches have various limitations like channel busy time, computational and communication overhead, collusion attack, single-point compromise, and increased authentication delay. To overcome some of these drawbacks, we propose an RSU based approach where the vehicle's real identity is known only to Central Authorities. The vehicles communicate with each other using their pseudo ids that are generated when they register in the network. We also use Hyperledger Fabric, a permissioned blockchain to store and manage the identity of all vehicles registered in the network.

CHAPTER 3

Blockchain Based Vehicle Authentication

3.1 Introduction

To provide secure and reliable communication in Vehicular Ad-hoc Network (VANET), it is required to ensure that only authenticated vehicles can communicate and be a part of the network. The efficiency of the network can be leveraged by securely maintaining the identities of the vehicles and by reducing the computational overhead of the vehicles and it's On-board units (OBUs). So, we aim to implement a blockchain-based authentication scheme in VANET that reduces computational overhead on vehicle's OBUs. We also securely store and manage the real identities of vehicles by using their pseudo IDs only to communicate in the network.

Our proposed method is an RSU based approach that includes a two-step authentication. The first step of authentication is signature verification and the second step is the vehicle status verification using blockchain. Both the authentication step takes place at the RSU (Road-side Unit) side. In this approach, we securely store the vehicle's identities in Hyperledger Fabric, a permissioned blockchain. The vehicles communicate with each other using their pseudo id and so their real identity is not revealed to any other nodes in the network. The vehicles in the network are not connected to the blockchain and do not have access to it.

All the vehicles in the network periodically broadcast the vehicle's details such as position and traffic details to neighboring vehicles and infrastructure. The Basic Safety Messages (BSMs) transmitted by the vehicles consist of its Pseudo ID, public key, digital signature, and other information about the sender vehicle. Each BSM will be digitally signed by the sender using its private key before transmission. On receiving the BSMs, the RSU verifies the message's signature using the public key of the sender. After the first step of signature verification, the RSU looks up at the blockchain to check if the sender's pseudo ID is present in it. This two-step verification authenticates the user to be a valid participant in the network.

3.2 Proposed Architecture

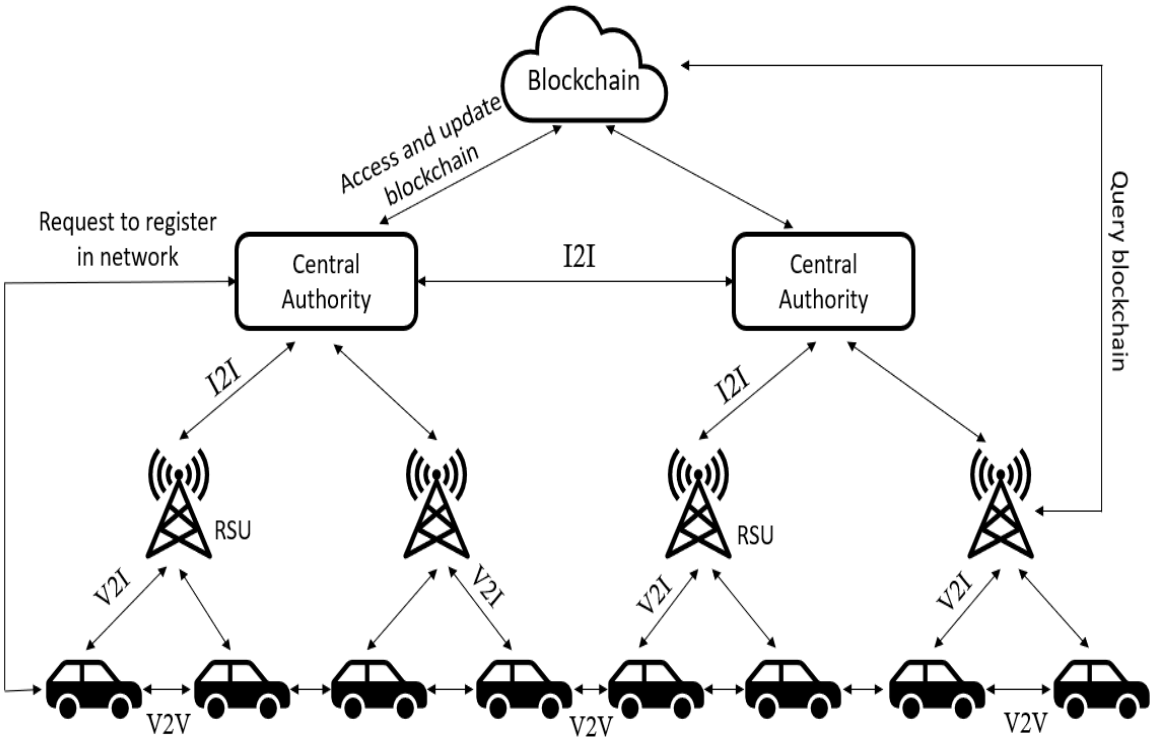

Figure 3.1: Proposed Architecture

Our proposed architecture consists of Blockchain, Central Authority (CA), Road-side Unit (RSU), and vehicles in the network. The blockchain that we use is the Hyperledger Fabric, a permissioned blockchain that provides a distributed and decentralized

Vehicular Ad-hoc Network (VANET). As shown in Figure 3.1, the RSUs and central Authorities have access to the blockchain whereas the vehicles are not connected to it. The vehicles register to the network by requesting the CA and the RSUs are connected to the nearest central authority. The CA updates the blockchain upon adding a new vehicle to the network and assigns a pseudo id, public key, and private key to each vehicle.

3.2.1 Participants in the network

The main participants in our proposed architecture are the vehicles, Road-side Unit (RSU), and the Central Authority (CA). The CA has both read and write access control over the blockchain whereas, RSU has only read access. And, the vehicles do not have any access control on the blockchain. The functionalities and operations of these participants are as follows:

- Vehicles - All the vehicles registered in the network have their public and private key with which they sign each message before sending them. The main operation of the vehicles is to transmit Basic Safety Messages (BSM) to broadcast the vehicle's information such as its speed and position, traffic details and to notify other vehicles about road accidents or ongoing construction works.

- RSU - The function of RSU is to hear all messages transmitted in the network and verify the sender of the messages. The sender is validated by RSU using message signature verification and by querying the blockchain to check if the sender ID is the same as stored in it. Another function of RSU is to broadcast warning messages whenever a message is received from insider malicious/attacker vehicles.

- Central Authority (CA) - When a vehicle requests to register in the network, the CA validates and approves its request. While registering the vehicle to the network, the function of CA is to generate a pair of public and private keys for each vehicle which is further used by them to communicate securely. The CA is

also responsible to update the blockchain for every newly added vehicle in the network.

3.2.2 Assumptions

In this thesis, our focus is specifically on compromised/misbehaving vehicles, since these are the most vulnerable components of the proposed architecture. It is also possible for RSUs and CAs to be compromised, although this is much less common. Techniques to address compromised RSUs/CAs are available in [51], but are out of the scope of this thesis. Therefore, we have made the following assumptions in terms of the different components:

- We assume that the Road-side Unit (RSU) cannot be compromised by an attacker and will be resistant to both the collusion and single-point attacks.
- We assume that there is always an RSU within the transmission range of any vehicle in the network.
- We also assume that the RSUs have sufficient computational power to verify the messages transmitted and to validate the sender of all messages.
- Also, we assume that the Central Authority (CA) which registers vehicles to the network will not be compromised by any malicious node.

3.2.3 Hyperledger Fabric Blockchain

We use Hyperledger Fabric to create the blockchain network which consists of decentralized and distributed ledgers. The Hyperledger Composer is a development toolset and framework that is used to develop and support Hyperledger fabric. It is used to create a network definition comprising of a model file, script file, access control file, and query file [52]. These files include the declaration of participants in the network, transactions between them, their functions, access control rules, and the query definitions. These files are exported as an archive file which can be deployed anywhere

later and accessed by the participants with appropriate credentials.

The Hyperledger fabric network consists of the following components [53]:

- Assets - Assets in Hyperledger Fabric constitute key-value pairs and have state and ownership. In our approach, the vehicles are the assets of the network.
- Shared ledger - The ledger consists of the world state which is the state of the ledger at that particular time and records all transactions.
- Smart contract - Smart contract is also known as chaincode that defines the assets and their related transactions. This chaincode could be written in either Golang or Node.js.

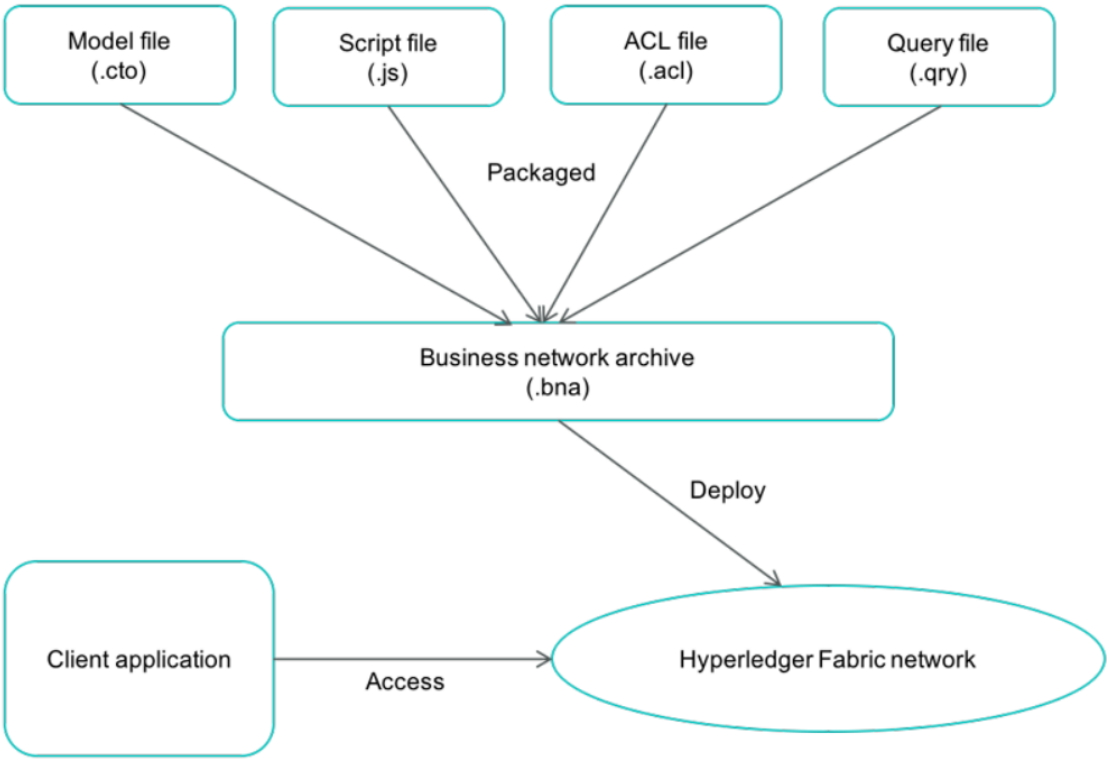

Figure 3.2: Components of Blockchain [54]

The three components of hyperledger composer are the business network archive (.bna) file, hyperledger composer playground and REST API [54]. The data in the ledger are encrypted and only those who are permitted to see the data can access

them. This reduces the risk of the vehicle's credentials being stolen or misused. The permissioned blockchain provides secure communication and manages a decentralized network. The use of hyperledger fabric increases the performance level, privacy, and protection in VANET [55].

As shown in Figure 3.2, blockchain in our approach is made up of the Business network archive (.bna) file which is a package consisting of the model, script, access control, and query files. This .bna file is then deployed as a hyperledger fabric network (i.e., Blockchain network) and can be accessed by the client application. The assets in our blockchain network are the vehicles, the participants include Road-side Unit (RSU) and Central Authority, and transactions are the messages transmitted between them.

3.3 Proposed Authentication Method

In our proposed architecture, the blockchain network is created initially and then linked to VANET using the REST API. The participants of the blockchain are RSU and the Central Authority (CA) who have access to it. Firstly, the vehicle requests the CA to register them in the network as shown in Figure 3.3. Upon receiving this request from the vehicle, CA analyzes it and decides if the vehicle can be registered to the network or not. If the vehicle's request is approved, the CA registers it to the network and assigns its pseudo ID (PID) which will be used while communicating. It also generates a pair of public and private keys for each registered vehicle.

The successfully registered vehicle's personal information is then added and securely stored in the blockchain by CA. Data stored in the blockchain includes the real identity of the vehicle, its pseudo id, public key, and status of the vehicle. The ordering service in Hyperledger Fabric can be either SOLO used for development purposes or Kafka, for production. The consensus mechanism used in our approach is SOLO where a single node is used to endorse, order, and validate each transaction in the

blockchain network.

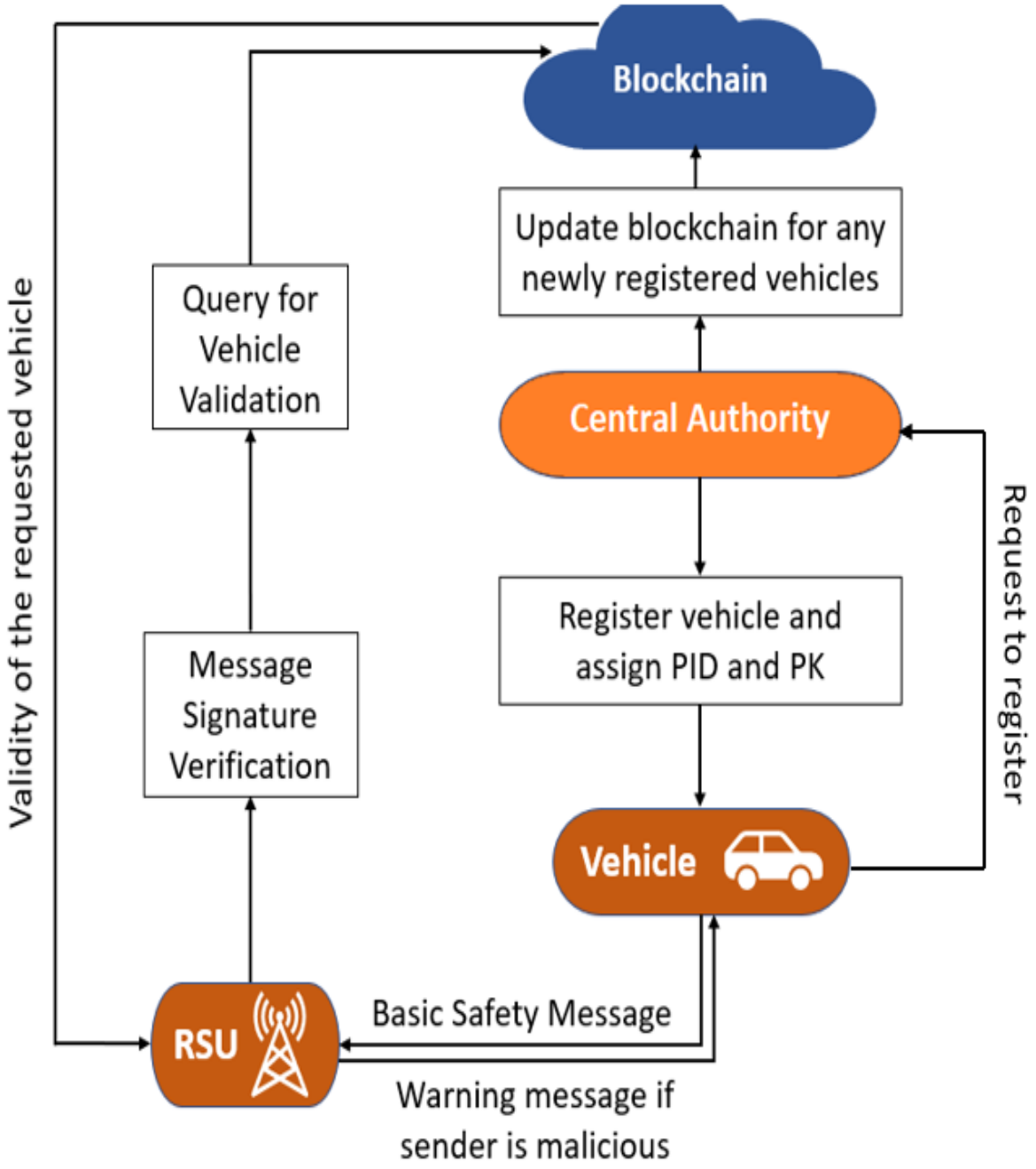

Figure 3.3: Proposed Architecture for Authentication

After being registered to the network, the vehicle can now transmit messages to other vehicles within its range. The Basic Safety Messages (BSM) sent by the vehicle are digitally signed using their private key. The average BSM packet size is considered

to be between 350 bytes and 800 bytes based on the security-related overheads [56]. As shown in Figure 3.5, the BSM packet size in our approach is 171 bytes which consists of the sender's information (42 bytes), the message signature (64 bytes), and the sender's public key (65 bytes) [47] [57]. In our approach, we use the cryptographic technique, Elliptic Curve Digital Signature Algorithm (ECDSA) to digitally sign the messages before sending. The ECDSA uses cryptographic hash functions like SHA-256 to calculate the hash of the message and sign them with the sender's private key.

On receiving the messages, the RSU verifies the message signature and it is the first step of authentication. This is done using the sender's public key that was transmitted along with the BSM sent. If the message signature is verified successfully, the second step of authentication is performed where the RSU queries the blockchain to check if the sender's PID is present in the blockchain. The vehicles that pass both steps of authentication is considered to be a valid or legitimate vehicle.

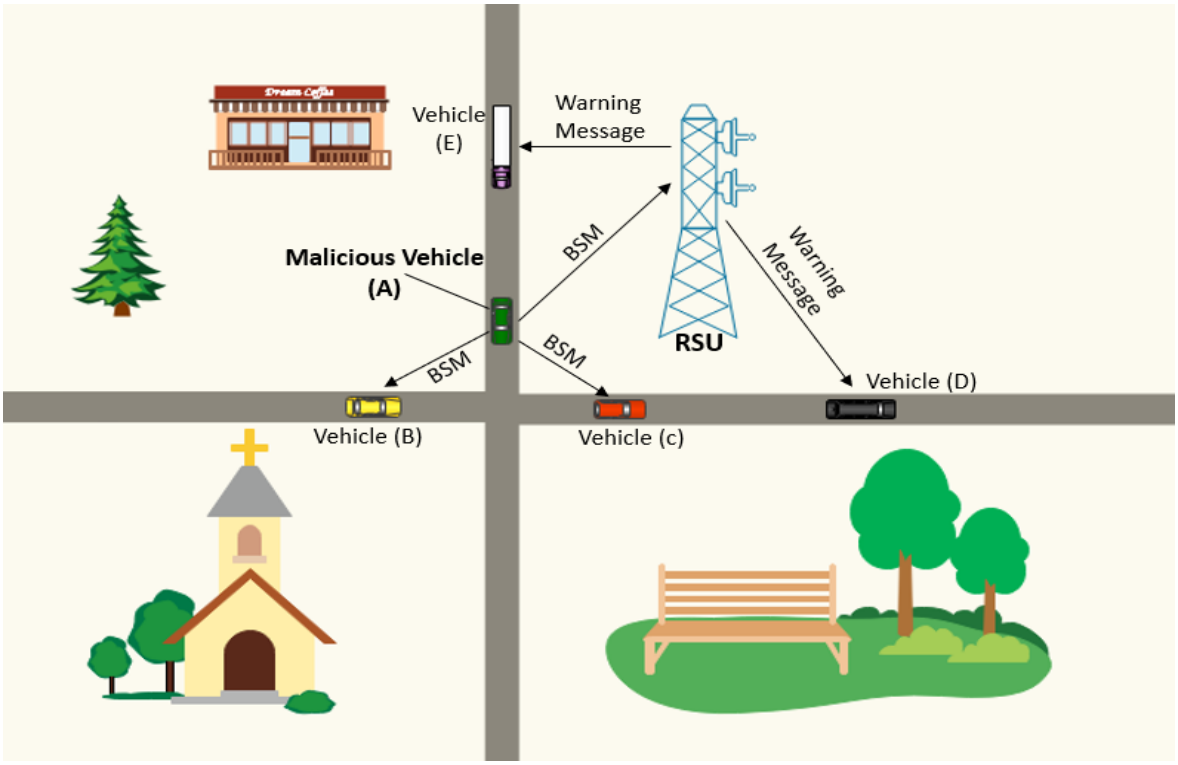

Figure 3.4: Warning Messages by RSU

If the message received is from an invalid or malicious vehicle, then the RSU sends a warning message to all the vehicles within its range. As shown in Figure 3.4, the malicious vehicle 'A' transmits BSM and on receiving it, the RSU validates the message and sends warning messages to all nearby vehicles. This prevents valid vehicles from being influenced by the insider malicious vehicle's messages and causing damage to the network. However, the RSU does not send any messages if the sender is valid, which reduces the channel congestion and prioritizes the transmission of important or emergency messages.

All vehicles in the network communicate with each other using their assigned PID only. So, the participants in the network do not have access to the personal details of each other. The CA can access the real identities of vehicles in case of any dispute or accident to trace the attacker. Also, the data stored in blockchain are tamper-proof as it is decentralized and consists of a distributed ledger. This preserves the privacy of vehicles and increases the reliability of the network.

3.3.1 Communication Mechanism in Proposed Approach

The communication pattern in our proposed approach includes Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communications as shown in Figure 3.1. In V2V communication, the vehicles transmit BSMs periodically to all the other vehicles in their range. These BSMs consist of the sender's pseudo id, the public key, the message signature, and the sender vehicle's related data as shown in Figure 3.5.

Figure 3.5: BSM Packet Frame [47]

The V2I communication happens between the vehicles and the RSU that is within

each vehicle's range. Here, the vehicles send BSMs and the RSUs send warning messages whenever it receives a message from an insider malicious vehicle. Figure 3.7 depicts that the warning messages consist of the malicious sender's pseudo id and its validity which indicates if the sender is malicious or not.

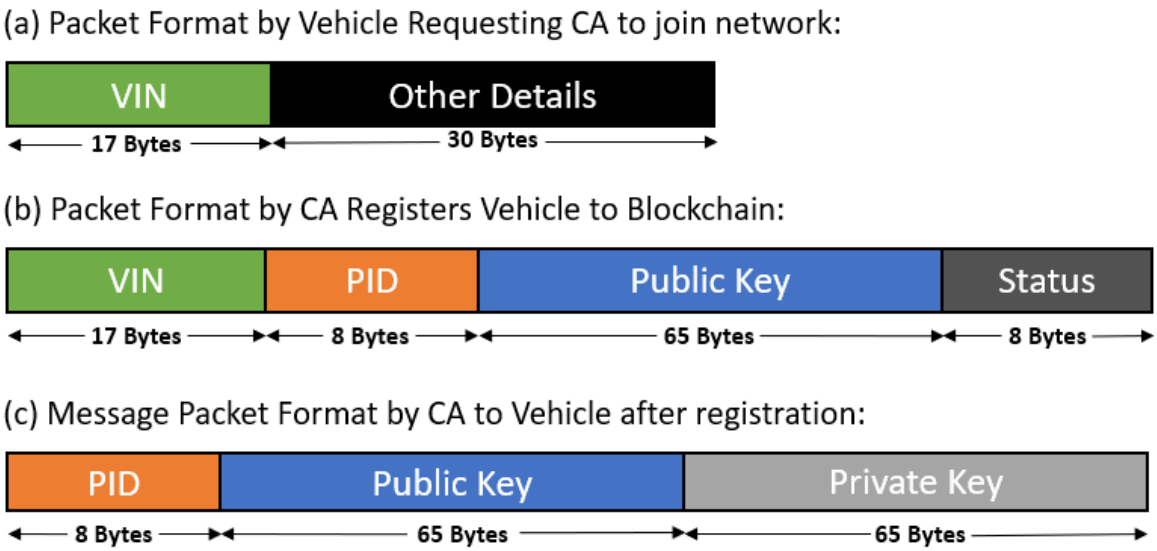

Figure 3.6: Packet Frame of Other Messages

In V2I, the vehicles also send requests to Central Authorities (CAs) when they want to register to the network. As shown in Figure 3.6(a), these requests comprise the Vehicle Identification Number (VIN) which won't be visible to other vehicles in the network and other details including speed and position of the sender. Upon accepting the request, CA sends a pseudo id, a public key, and a private key to each registered vehicle like in Figure 3.6(c). In our proposed approach, we assume that the message sent by CA to the requesting vehicle after registration is tamper-proof.

Figure 3.7: Warning Message Packet Frame

In I2I, communication occurs between the infrastructures such as RSUs and CAs.

Figure 3.1 depicts that the CAs are linked to each other which ensures that the same vehicle is not registered again with other CAs. After registration, the CA updates the blockchain with the new vehicle's details like VIN, pseudo id, its public key, and status as shown in Figure 3.6(b). The RSUs in the network are directly connected to the nearby CA. As the RSU has read-only access to the blockchain, it reports to the CA in case of any dispute and then the CA updates the blockchain.

3.3.2 Difference between Proposed Approach and Existing Approaches

In most of the existing blockchain-based methods, the authentication part of the network is done by either vehicles, Road-side Units (RSU) or other third-party participants such as System Managers (SM) in [44]. This increases the computational overhead of the On-board Units installed in the vehicles. The registration time of vehicles takes more time than authentication in [44] and cannot resist collusion attack between SMs because of the unlinkability in their approach. Some works have decreased computational cost but the communication overhead increases leading to channel congestion. The authentication scheme in [49] is vulnerable to single-point compromise that will destruct the entire network.

Our approach is especially based on the work of George et al. [47] where blockchain is used to store and manage the vehicle's identity. In this method, the vehicles request the RSU to validate the sender of the messages they receive and the OBUs are responsible for the message signature verification. Based on the vehicle's request, the RSU looks-up at the blockchain and sends the validity of the sender vehicle to the requested vehicle. This authentication scheme increases the computational overhead on OBUs and the communication overhead between the vehicles and RSU.

Whereas, in our proposed approach, the vehicles do not request the RSU to validate the sender of each message they receive. The RSU itself keeps track of all the

messages being transmitted in the network and validates the sender by our two-step authentication scheme. If the sender is valid, the RSU does not notify the vehicles. However, if the sender is invalid and a malicious vehicle, the RSU sends a warning message to all the vehicles within its range. This reduces the computational and communication overhead of both RSU and the vehicle's OBUs compared to [47].

We do not use certificates for message verification and so our approach is certificate-less. Whereas the traditional PKI and some of the other approaches include both message signature verification and certificate verification [45] [48]. The use of blockchain and query to the blockchain using REST API in our proposed method eliminates the purpose of certificates. It reduces the communication overhead as the certificates are not attached to each Basic Safety Message (BSM) [47] and also reduces the BSM packet size compared to the traditional PKI approach.

CHAPTER 4

Simluation and Results

4.1 Simulation Tools

We made use of several tools to simulate the road network and to obtain the values of various parameters related to the vehicles. These tools include OMNET++ 5.3, SUMO 0.32.0, Veins 4.7.1, and Hyperledger Composer. The Objective Modular Network Testbed (OMNET++) is the network simulator that is widely used and supported by the researchers [58]. The properties of OMNET++ are scalability, hierarchical architecture, minimal simulation runtime, and memory consumption, accurate simulation of MAC and physical layers.

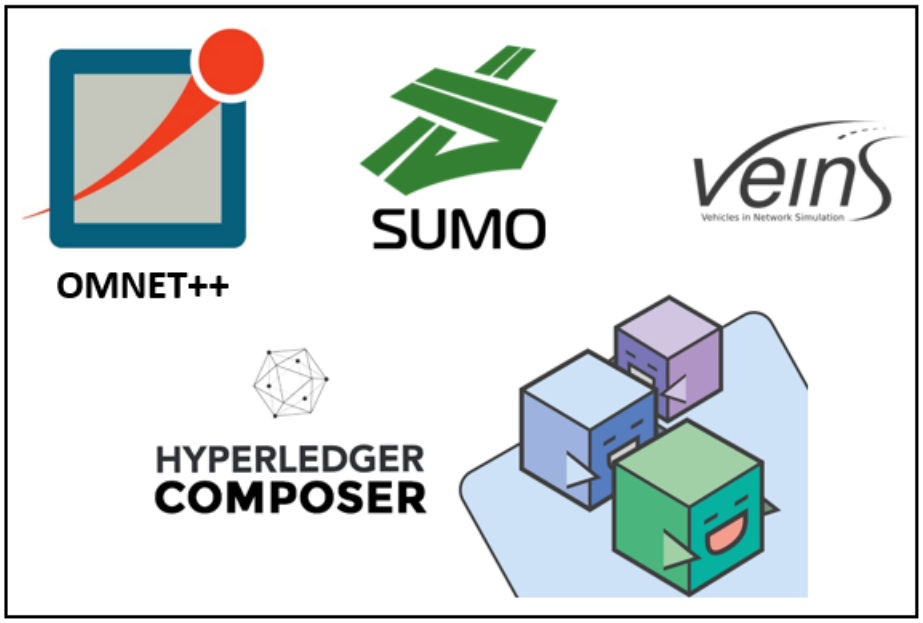

Figure 4.1: Simulation Tools Used

Simulation of Urban Mobility (SUMO) is an open-source framework that has been used for road traffic simulations that support importing real-world maps consisting of buildings, traffic signs, and lanes [58]. The Vehicles in Network Simulation (VEINS) is also an open-source framework that connects both the simulators, OMNET++, and SUMO to provide vehicular communication. It can also provide re-routing and re-configuration of vehicles concerning the network simulator [58].

Hyperledger Fabric which is supported by Hyperledger Composer has been used to implement the permissioned blockchain network in our research work. Hyperledger Composer is a framework that helps in developing blockchain applications [55]. The composer supports defining the network using a modeling language and then deploys the network to Hyperledger Fabric. We have connected the OMNET++ network simulator to the Hyperledger Composer's REST API using the external library, cpprestsdk [59].

4.1.1 Simulation Setup

The .ini file in OMNET++ consists of the simulation parameters that are mentioned in Table 4.2. These parameters indicate the total simulation time, data transmission rate, and other simulation-related details. The SUMO route file which is included within OMNET++ contains the information about the number of vehicles that take part in the simulation, their speed, source and destination of the vehicles, and the time between each vehicle's entry.

Table 4.1: Experimentation Setup

Parameters	**Value**
Operating System	Windows 10
Processor	Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
RAM	7.89 GB

The vehicles in our proposed approach are generated every 2 seconds and their maximum speed is set to 50km/hr. The map which we have used for our simulation runs is the University of Erlangen-Nuremberg, Germany, the default map in Veins. All the vehicles are generated at the same point and travel straight through the road until they reach the destination. The finish() function is called when the simulation time ends or if all the vehicles that took part in the simulation reached the destination. We simulated our approach for 50, 100, 150, and 200 vehicles with total simulation times of 200, 300, 400, and 500 seconds, respectively. The results reported in the following sections are the based on the average of 3 runs.

Table 4.2: Simulation Parameters

Parameters	**Value**
Simulation Time	200s-500s
Number of Vehicles	50-200
Data Rate	6Mbps
Transmission Power	20mW
Thermal Noise	-110dBm
Sensitivity	-89dBm
Route Length	3400m
Maximum Vehicle Speed	50km/hr
BSM Size	171 Bytes
Transmission Rate	1Hz (1 BSM per second)

4.2 Results for Proposed Approach

In our proposed approach, we analyze the results of each simulation based on the delay in the authentication. We also consider the number of warning messages send by the RSU, which is dependent on the number of attackers in each simulation.

4.2.1 Warning Messages

As discussed in Chapter 3, warning messages are sent by RSU whenever it receives BSM from a malicious vehicle. The number of warning messages in each simulation depends on the number of malicious vehicles in the network. For each simulation time, we recorded the total number of warning messages sent by the RSU for different attacker densities.

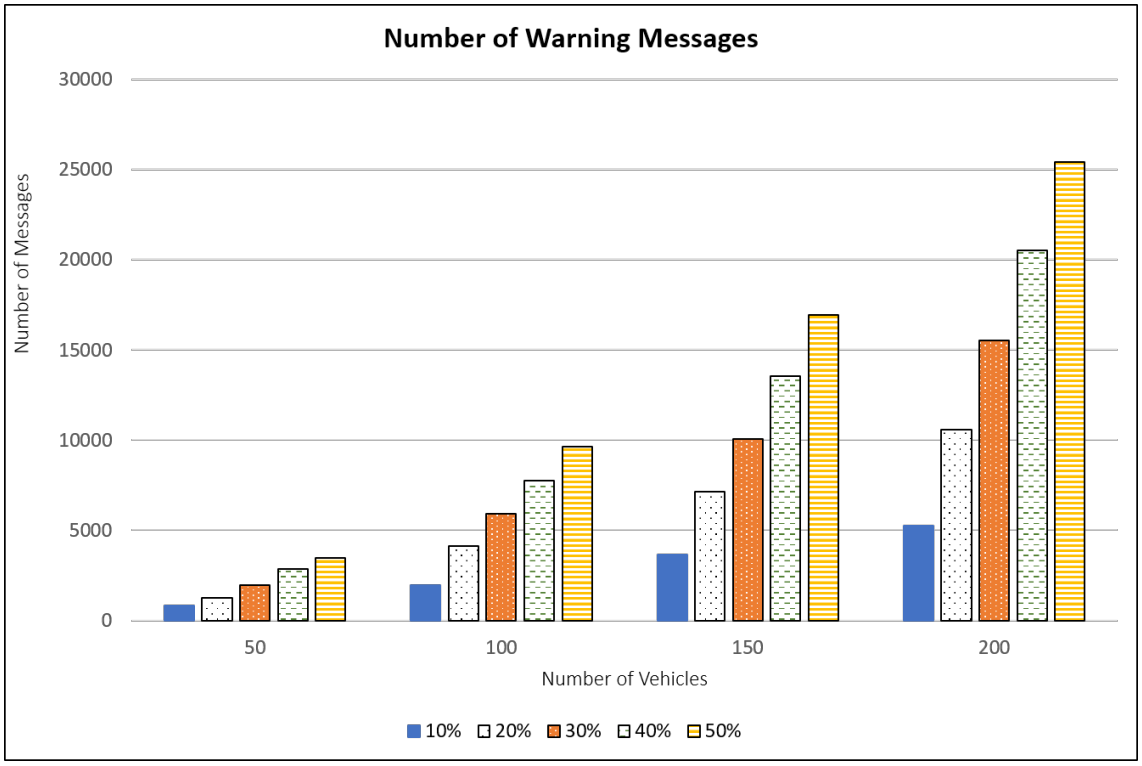

Figure 4.2: Number of Warning Messages with respect to Attackers

The graph in Figure 4.2 shows how the number of warning messages send by the RSU varies with the attacker densities for different values of total number of vehicles. For each vehicle density, we varied the attacker density from 10% - 50%. As expected number of warning messages increases with the number of vehicles and malicious vehicles in the network increases. We have increased the simulation time also depending on the number of vehicles so that there is enough time for all vehicles to enter and spend time in the network.

4.2.2 Authentication Delay

The delay in authentication is the time taken by RSU to authenticate each BSM transmitted in the network and send a warning message if the BSM is from a malicious vehicle. In our approach, we calculate the delay in authentication and the delay by RSU to transmit warning messages. The average delay in authentication per BSM is computed by dividing the summation of authentication delay for all BSMs by the total number of BSMs received.

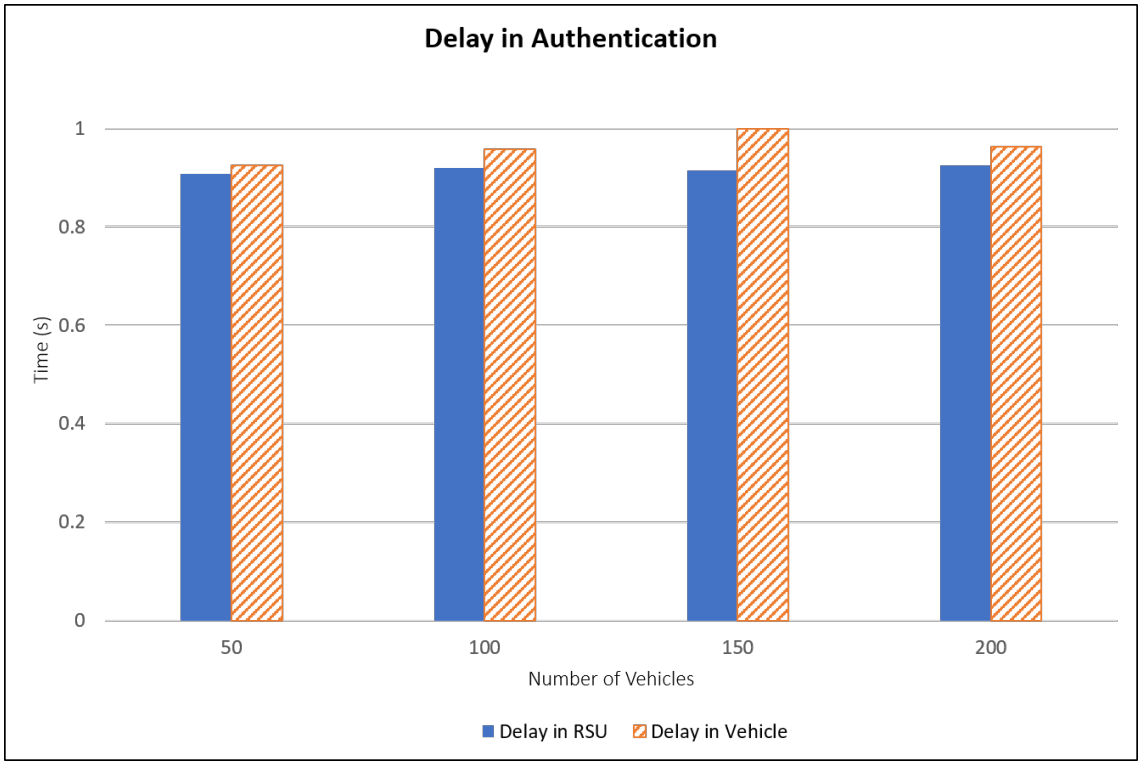

Figure 4.3: Delays in Authentication

Figure 4.3 shows the variation of both the average delay in RSU ($Delay_{rsu}$) and average delay observed by the vehicles ($Delay_v$) to receive warning messages from the RSU. The delay in RSU is the time taken to confirm if a BSM is from a legitimate or malicious vehicle by checking the blockchain and is given in equation (1). The delay at the vehicle is the time from when a BSM is received by a vehicle to when it receives a warning message for that BSM. for the vehicles to receive the response messages from RSU as shown in equation (2).

$$Delay_{rsu} = \frac{\sum_i (TA_i - TR_i)}{N_{rsu}} \tag{1}$$

$$Delay_v = \frac{\sum (TWM_{v,i} - TR_{v,i})}{N_v} \tag{2}$$

Where,

- TR_i is the time when BSM i received at the RSU
- TA_i is the time when status of BSM i is confirmed through the blockchain
- N_{rsu} is the total number of BSMs received by the RSU
- $TWM_{v,i}$ is the time when a warning message is received for BSM i at vehicle v
- $TR_{v,i}$ is the time when a malicious BSM i is received at vehicle v
- N_v is the number of malicious BSMs received at vehicle v

The graph in Figure 4.3 illustrates that we have plotted the delays when attacker density is 50% for different number of total vehicles. We observed that the delay did not vary significantly with the number of vehicles or the attacker density. Therefore, we have not included the results for the other attacker densities, which followed a very similar pattern. We note that we have calculated the delays using the clock() function defined in the ctime library. These values will depend on the resources allocated to the process and can vary with each processor or operating system. Therefore, we have reported *normalized* values, as we are mainly interested the relative values of delay components and how they change with the number of vehicles, rather than the actual numerical values.

4.3 Results Comparison with Existing Approaches

In this section, we compare the results of our proposed approach to the results obtained from the existing approaches, Secure Identity Framework using blockchain [47]

and the traditional PKI Framework. In addition to the delay in authentication and the number of warning messages, we also compare the Channel Busy Time (CBT).

4.3.1 Number of RSU Response Messages

In our proposed approach the RSU transmits *warning messages*, whenever it encounters a BSM from a malicious vehicle in the network. Whereas, in the Secure Identity Management Framework, the RSU sends *status messages* upon receiving BSM validation requests from the receiver vehicles in the network. These response messages are sent for both legitimate and malicious vehicles. The PKI Framework does not include any such transmission of warning messages, and each vehicle is responsible for authenticating every BSM based on the attached certificate. So, here, we compare the number of RSU response messages transmitted for the proposed approach and the Secure Identity Management in [47] only.

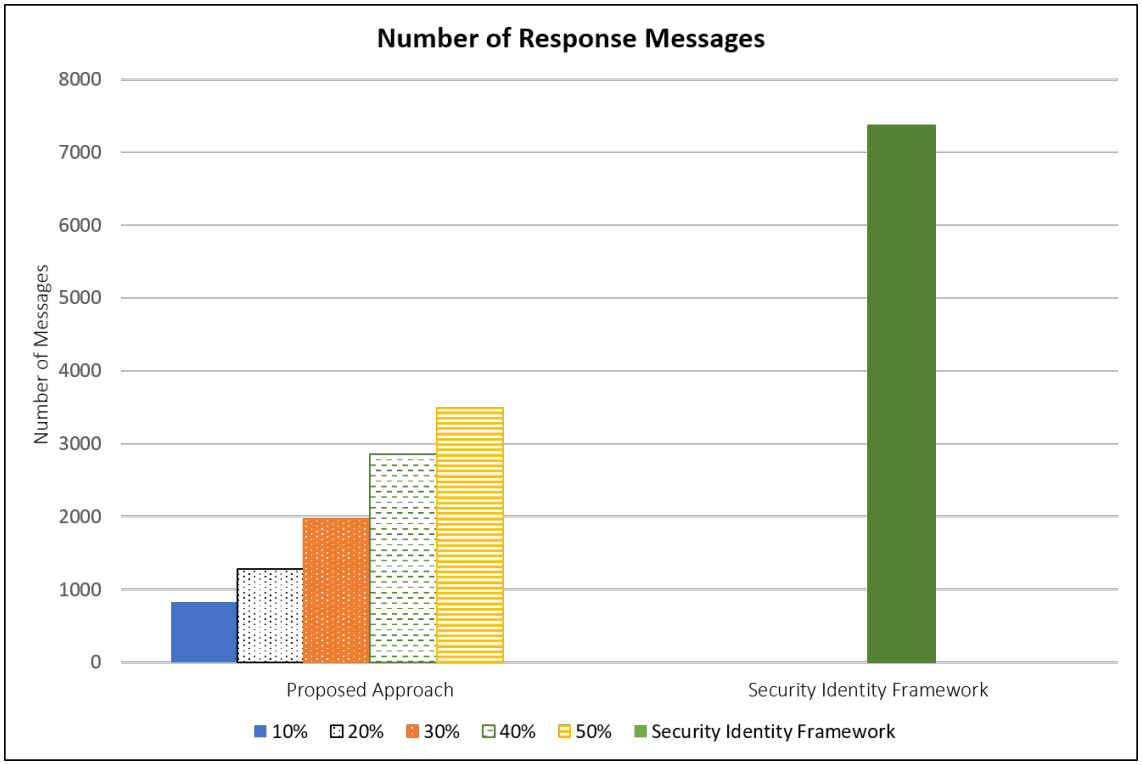

Figure 4.4: RSU Response Messages for 50 Vehicles

Figure 4.4 shows a comparison of the number of RSU response messages for the two

approaches, with a total of 50 vehicles in the simulation. In the proposed approach, the number of responses depends on number of malicious vehicles. This is shown on the left in Figure 4.4. For the Secure Identity Framework, it is independent of the number of attackers, as messages are sent for all vehicles - both legitimate and malicious. This is represented by a single bar on the right. It is evident that the number of warning messages transmitted in the Secure Identity Framework is significantly higher than the proposed approach, even with a high (50%) attacker density.

In Figure 4.5, for our proposed method, we have recorded the response messages sent in each simulation with a number of vehicles ranging from 50 to 200 and higher attacker density (i.e., 50%).When comparing these results to the Secure Identity Framework, we can see that the number of responses sent in our method increases gradually, while the Secure Identity Framework shows a rapid increase. We also observed that the Secure Identity Framework generates 70% - 90% more response messages than our proposed approach.

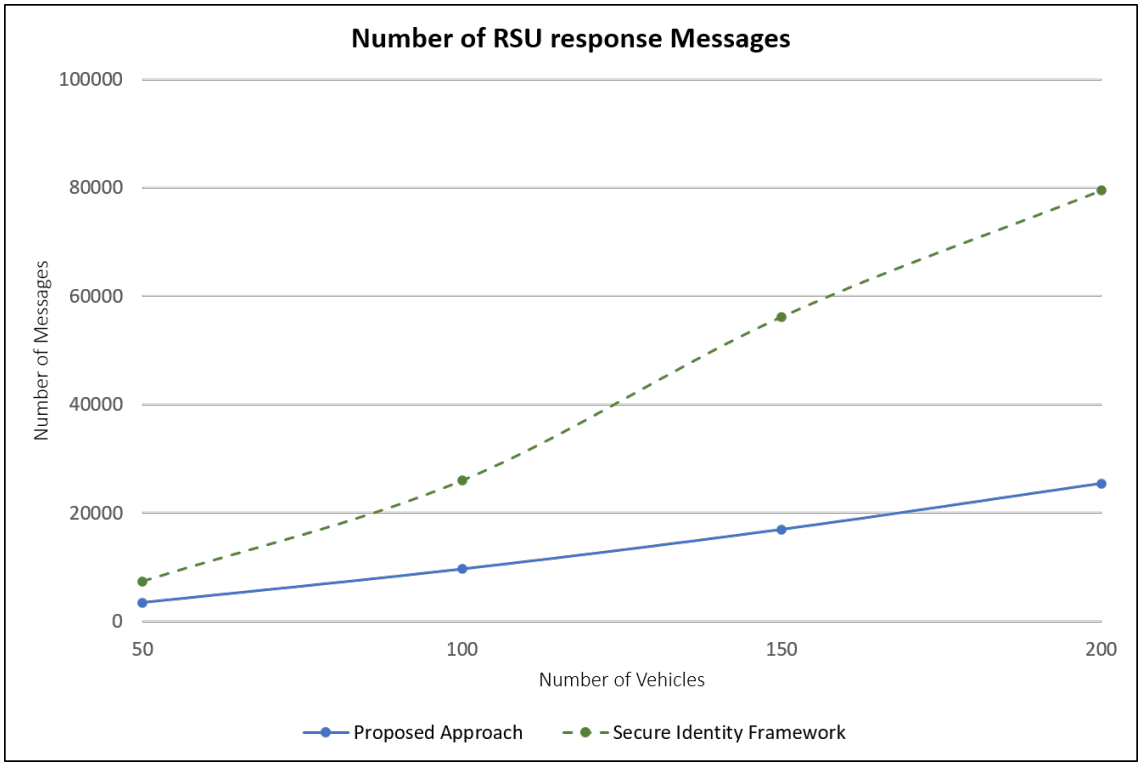

Figure 4.5: Total RSU response messages for different vehicle densities

4.3.2 Comparison of Delay in Authentication

Authentication delay in our proposed approach includes both the RSU and vehicle delays as discussed in section 4.2.2. For the purpose of comparison, we take into account the delay at the vehicle, which includes the time taken to receive BSMs, the time it takes for RSU to authenticate, the time it takes for response messages to be sent, and the time it takes for response messages to be received by vehicles. The authentication delay in the Security Identity Management Framework is the time it takes each vehicle to receive BSM and authenticate the sender by requesting the RSU. The time required by vehicles to validate the certificate attached to the received BSM and authenticate the message signature is the authentication delay in the PKI Framework.

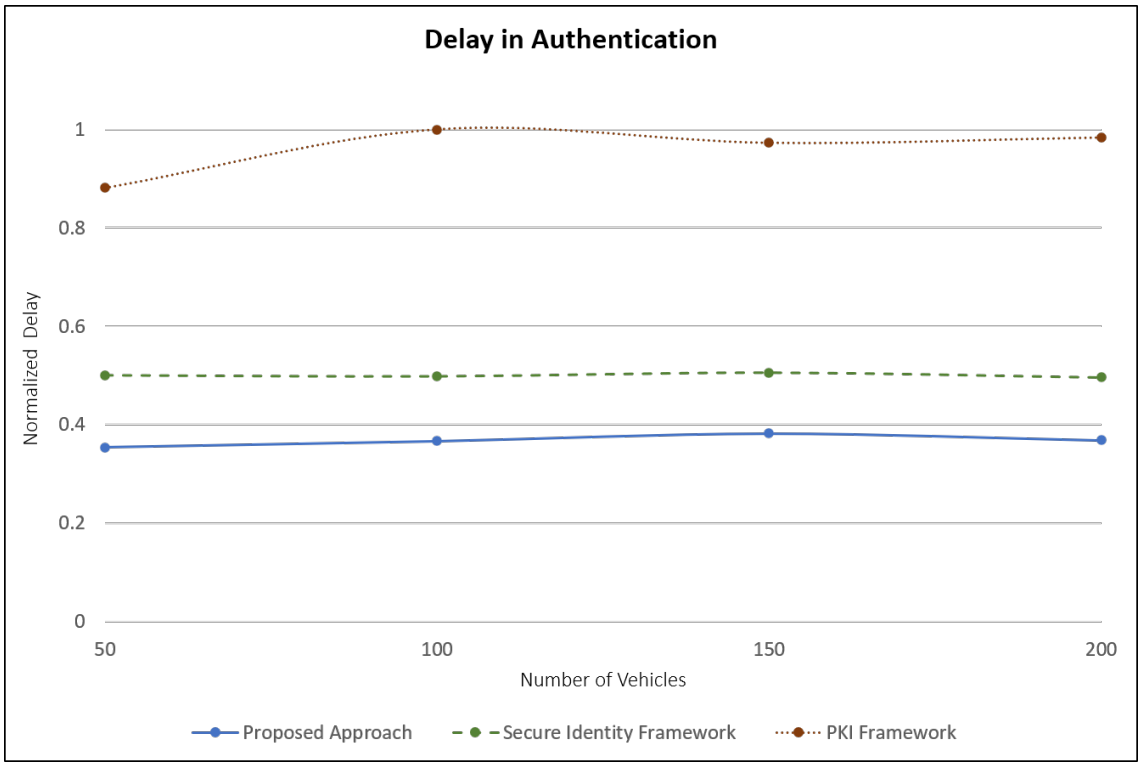

Figure 4.6: Total Delay in Authentication

The line graph in Figure 4.6 shows the normalized delays per BSM for the 3 approaches. We see that the delay in each approach does not vary significantly with the number of vehicles or the simulation time. According to our findings, PKI Framework

takes longer to authenticate than Secure Identity Framework because it comprises both the message signature and certificate verification. Furthermore, the proposed solution has a 35% and 85% lower authentication latency on average compared to the Secure Identity Framework and the PKI Framework respectively.

4.3.3 Channel Busy Time

The channel busy time (CBT) is the amount of time that the communication medium, the MAC layer, is in use. The CBT value is calculated by dividing the cumulative busy time of all network participants by the total simulation time in seconds. These values depend on the number of vehicles in the sender's range and its message transmission rate.

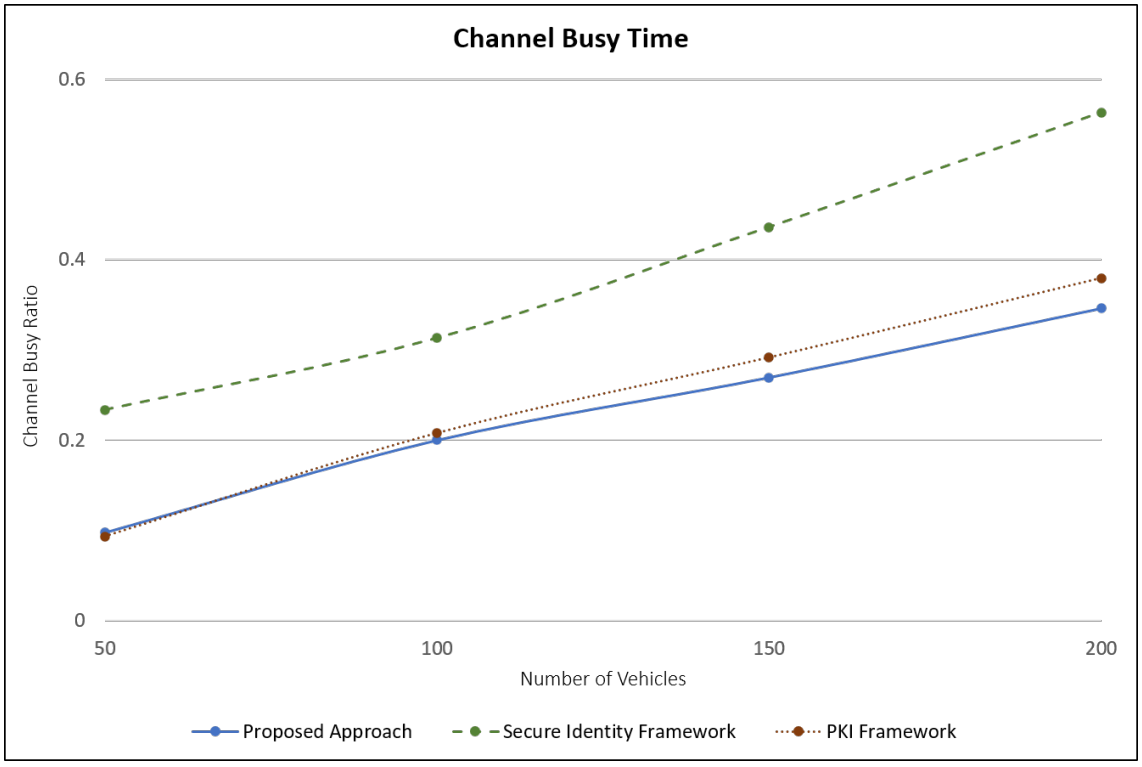

Figure 4.7: Channel Busy Time

Figure 4.7 shows a comparison of our proposed solution, Security Identity Framework, and PKI Framework in terms of channel busy time. For the less number of

vehicles, the CBT values are very similar, for both the proposed approach and the PKI Framework. As the number of vehicles increases, the PKI Framework, on the other hand, sees a slight increase. However, because of the requests sent by vehicles and the answer messages from RSU, the Secure Identity Framework has a higher CBT than the proposed approach and the PKI Framework. For the proposed approach, CBT values are slightly higher than PKI, but still remains well below that of the Secure Identity Framework approach. Therefore, we feel the proposed approach offers a suitable trade-off between the authentication delay and CBT.

CHAPTER 5

Conclusion and Future Work

5.1 Conclusion

In this thesis, we have used Blockchain to securely maintain the vehicle's real identities and to ensure that only legitimate or authenticated vehicles can access and communicate in VANET. This approach extends the work of George et al. in [47] and reduces the communication and computational overhead of on-board units by eliminating the requests send by vehicles to validate the BSM's sender. In our approach, the RSU listens to all network messages and sends warning messages if they receive a BSM from an insider malicious vehicle. RSU authenticates the received BSMs by looking up the status of the sender in the Blockchain.

In comparison to PKI and Secure Identity Framework, the proposed method achieves a substantial reduction in authentication delay, while still maintaining a low CBT that is comparable to PKI. The BSM packet frame size in our approach is smaller than the traditional PKI Framework, since we do not include digital certificates with BSMs for validation. Additionally, since we use RSU-based authentication for validating messages and their sender, the computational overhead of on-board units has been reduced. The use of Blockchain technology provides a distributed and decentralized network that prevents single-point failures.

5.2 Future Work

Future work of our proposed approach includes improvement in the consensus mechanism of Blockchain. There are various fast and fault-tolerant consensus mechanisms that can be used in our approach for better performance. Also, more research is required to detect the malicious or attacker vehicles and revoke them from the network.

REFERENCES

[1] Vinand M Nantulya and Michael R Reich. "The neglected epidemic: road traffic injuries in developing countries". In: *Bmj* 324.7346 (2002), pp. 1139–1141.

[2] VV Ziyadinov and MV Tereshonok. "Analytical Survey on MANET and VANET Clusterisation Algorithms". In: *2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*. IEEE. 2020, pp. 1–5.

[3] M Newlin Rajkumar, M Nithya, and P HemaLatha. "Overview of VANETs with its features and security attacks". In: *International Research Journal of Engineering and Technology* 3.1 (2016).

[4] Sherali Zeadally, Muhammad Awais Javed, and Elyes Ben Hamida. "Vehicular communications for ITS: standardization and challenges". In: *IEEE Communications Standards Magazine* 4.1 (2020), pp. 11–17.

[5] *Autonomous Vehicles on the Map*. [Accessed: 2021-02-09]. URL: `https://www.govtech.com/Autonomous-Vehicles-on-the-Map.html`.

[6] Ryma Abassi. "VANET security and forensics: Challenges and opportunities". In: *Wiley Interdisciplinary Reviews: Forensic Science* 1.2 (2019), e1324.

[7] Muhammad Sameer Sheikh, Jun Liang, and Wensong Wang. "A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)". In: *Sensors* 19.16 (2019), p. 3589.

[8] Vinh Hoa La and Ana Rosa Cavalli. "Security attacks and solutions in vehicular ad hoc networks: a survey". In: *International journal on AdHoc networking systems (IJANS)* 4.2 (2014), pp. 1–20.

[9] Xiaonan Liu, Zhiyi Fang, and Lijun Shi. "Securing vehicular ad hoc networks". In: *2007 2nd International Conference on Pervasive Computing and Applications*. IEEE. 2007, pp. 424–429.

[10] Jonathan Petit et al. "Pseudonym schemes in vehicular networks: A survey". In: *IEEE communications surveys & tutorials* 17.1 (2014), pp. 228–255.

[11] Elli Androulaki et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains". In: *Proceedings of the thirteenth EuroSys conference*. 2018, pp. 1–15.

[12] Muhammad Rizwan Ghori et al. "Vehicular ad-hoc network (VANET)". In: *2018 IEEE international conference on innovative research and development (ICIRD)*. IEEE. 2018, pp. 1–6.

[13] Syed Sarmad Shah et al. "Time barrier-based emergency message dissemination in vehicular ad-hoc networks". In: *IEEE Access* 7 (2019), pp. 16494–16503.

[14] Nitika Phull and Parminder Singh. "A Review on Security Issues in VANETs". In: *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE. 2019, pp. 1084–1088.

[15] Mohammed Ali Hezam et al. "Classification of security attacks in VANET: A review of requirements and perspectives". In: (2018).

[16] Amit Kumar Goyal, Arun Kumar Tripathi, and Gaurav Agarwal. "Security Attacks, Requirements and Authentication Schemes in VANET". In: *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*. Vol. 1. IEEE. 2019, pp. 1–5.

[17] Rajdeep Kaur, Tejinder Pal Singh, and Vinayak Khajuria. "Security issues in vehicular ad-hoc network (VANET)". In: *2018 2nd International conference on trends in Electronics and Informatics (ICOEI)*. IEEE. 2018, pp. 884–889.

[18] Ajay Kumar, Manu Bansal, et al. "A review on VANET security attacks and their countermeasure". In: *2017 4th international conference on signal processing, computing and control (ISPCC)*. IEEE. 2017, pp. 580–585.

[19] Shrikant S Tangade and Sunilkumar S Manvi. "A survey on attacks, security and trust management solutions in VANETs". In: *2013 Fourth international conference on computing, communications and networking technologies (ICCCNT)*. IEEE. 2013, pp. 1–6.

[20] Safi Ibrahim and Mohamed Hamdy. "A comparison on VANET authentication schemes: Public Key vs. Symmetric Key". In: *2015 Tenth International Conference on Computer Engineering & Systems (ICCES)*. IEEE. 2015, pp. 341–345.

[21] Shrikant Tangade, Sunilkumar S Manvi, and Pascal Lorenz. "Decentralized and scalable privacy-preserving authentication scheme in VANETs". In: *IEEE Transactions on Vehicular Technology* 67.9 (2018), pp. 8647–8655.

[22] Miraj Asghar, Robin Ram Mohan Doss, and Lei Pan. "A scalable and efficient PKI based authentication protocol for VANETs". In: *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE. 2018, pp. 1–3.

[23] Sumegha C Sakhreliya and Neha H Pandya. "PKI-SC: Public key infrastructure using symmetric key cryptography for authentication in VANETs". In: *2014 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE. 2014, pp. 1–6.

[24] Maxim Raya and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks". In: *Journal of computer security* 15.1 (2007), pp. 39–68.

[25] Yu Zhang and Xiangyu Bai. "Comparative Analysis of VANET Authentication Architecture and Scheme". In: *2019 12th International Symposium on Computational Intelligence and Design (ISCID)*. IEEE. 2019, pp. 89–93.

[26] Rishav Chatterjee and Rajdeep Chatterjee. "An overview of the emerging technology: Blockchain". In: *2017 3rd International Conference on Computational Intelligence and Networks (CINE)*. IEEE. 2017, pp. 126–127.

[27] Soha Yousuf and Davor Svetinovic. "Blockchain Technology in Supply Chain Management: Preliminary Study". In: *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE. 2019, pp. 537–538.

[28] Madhusudan Singh, Abhiraj Singh, and Shiho Kim. "Blockchain: A game changer for securing IoT data". In: *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. IEEE. 2018, pp. 51–55.

[29] Arvind Narayanan et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[30] Julija Golosova and Andrejs Romanovs. "Overview of the blockchain technology cases". In: *2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*. IEEE. 2018, pp. 1–6.

[31] S Velliangiri and P Karthikeyan Karunya. "Blockchain Technology: Challenges and Security issues in Consensus algorithm". In: *2020 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE. 2020, pp. 1–8.

[32] Kapil Sharma and Deepakshi Jain. "Consensus algorithms in blockchain technology: A survey". In: *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE. 2019, pp. 1–7.

[33] Jun Zou et al. "A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services". In: *IEEE Transactions on Services Computing* 12.3 (2018), pp. 429–445.

[34] D Team. "Types of blockchains-decide which one is better for your investment needs". In: *URL https://data-flair. training/blogs/types-of-blockchain* (2020).

[35] *Blockchain - Wikipedia*. `https://en.wikipedia.org/wiki/Blockchain#Public_blockchains`. (Accessed on 02/24/2021).

[36] Sam Hartnett et al. "The Energy Web Chain: Accelerating the Energy Transition with an Open-Source, Decentralized Blockchain Platform". In: *Energy Web Foundation* (2018).

[37] AKM Haque and Mahbubur Rahman. "Blockchain Technology: Methodology, Application and Security Issues". In: *arXiv preprint arXiv:2012.13366* (2020).

[38] *What is Blockchain Technology and How Does It Work?* `https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology`. (Accessed on 02/24/2021).

[39] *What Different Types of Blockchains are There? - Dragonchain*. `https://dragonchain.com/blog/differences-between-public-private-blockchains`. (Accessed on 02/24/2021).

[40] Qalab E Abbas and Jang Sung-Bong. "A survey of blockchain and its applications". In: *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE. 2019, pp. 001–003.

[41] XiaoDong Zhang, Ru Li, and Bo Cui. "A security architecture of VANET based on blockchain and mobile edge computing". In: *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. IEEE. 2018, pp. 258–259.

[42] Hui Li et al. "Blockchain meets vanet: An architecture for identity and location privacy protection in vanet". In: *Peer-to-Peer Networking and Applications* 12.5 (2019), pp. 1178–1193.

[43] Hui Li et al. "FADB: A fine-grained access control scheme for VANET data based on blockchain". In: *IEEE Access* 8 (2020), pp. 85190–85203.

[44] Jiao Liu et al. "Bua: A blockchain-based unlinkable authentication in vanets". In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

[45] Chao Lin et al. "BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks". In: *IEEE Transactions on Intelligent Transportation Systems* (2020).

[46] Dong Zheng et al. "A traceable blockchain-based access authentication system with privacy preservation in VANETs". In: *IEEE Access* 7 (2019), pp. 117716–117726.

[47] Sonia Alice George, Arunita Jaekel, and Ikjot Saini. "Secure Identity Management Framework for Vehicular Ad-hoc Network using Blockchain". In: *2020 IEEE Symposium on Computers and Communications (ISCC)*. IEEE. 2020, pp. 1–6.

[48] Zhaojun Lu et al. "A blockchain-based privacy-preserving authentication scheme for vanets". In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 27.12 (2019), pp. 2792–2801.

[49] Xincheng Li, Yali Liu, and Xinchun Yin. "An anonymous conditional privacy-preserving authentication scheme for VANETs". In: *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE. 2019, pp. 1763–1770.

[50] William Whyte et al. "A security credential management system for V2V communications". In: *2013 IEEE Vehicular Networking Conference*. IEEE. 2013, pp. 1–8.

[51] Mohamed Nidhal Mejri and Jalel Ben-Othman. "GDVAN: a new greedy behavior attack detection algorithm for VANETs". In: *IEEE Transactions on Mobile Computing* 16.3 (2016), pp. 759–771.

[52] *Introduction — Hyperledger Composer*. `https://hyperledger.github.io/composer/latest/introduction/introduction.html`. (Accessed on 03/02/2021).

[53] *Blockchain basics: Hyperledger Fabric – IBM Developer*. https://developer.ibm.com/technologies/blockchain/articles/blockchain-basics-hyperledger-fabric/. (Accessed on 03/17/2021).

[54] *Build your own Blockchain network with Hyperledger Fabric & Composer. Part II. — by Eli Elad Elrom — Blockchain-Developer — Medium*. https://medium.com/blockchain-developer/build-your-own-blockchain-network-with-hyperledger-fabric-composer-part-ii-35897bf9e7ab. (Accessed on 03/02/2021).

[55] Vance Morris et al. *Developing a Blockchain Business Network with Hyperledger Composer using the IBM Blockchain Platform Starter Plan*. IBM Redbooks, 2018.

[56] Xiaofeng Liu and Arunita Jaekel. "Congestion control in V2V safety communication: Problem, analysis, approaches". In: *Electronics* 8.5 (2019), p. 540.

[57] Abdallah Dabboussi et al. "Dependability overview for autonomous vehicles and reliability analysis for basic safety messages". In: *2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC)*. IEEE. 2018, pp. 86–91.

[58] Sofian Ali Ben Mussa et al. "Simulation tools for vehicular ad hoc networks: A comparison study and future perspectives". In: *2015 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE. 2015, pp. 1–8.

[59] *GitHub - microsoft/cpprestsdk: The C++ REST SDK is a Microsoft project for cloud-based client-server communication in native code using a modern asynchronous C++ API design. This project aims to help C++ developers connect to and interact with services.* https://github.com/microsoft/cpprestsdk. (Accessed on 04/05/2021).

VITA AUCTORIS

NAME:	Steffie Maria Stephen
PLACE OF BIRTH:	Nagercoil, TamilNadu, India
EDUCATION:	B.E. Computer Engineering, Arunachala College of Engineering for Women, Kanyakumari, TamilNadu, India, 2017
	M.Sc. Computer Science, University of Windsor, Windsor, Ontario, Canada, 2021