T.C.
SAKARYA UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY

DESIGN AND IMPLEMENTATION OF A NEW BLOCKCHAIN ALGORITHM TO INCREASE RELIABILITY, SECURITY AND INTEGRITY

Ph.D. THESIS

A F M Suaib AKHTER

Department	**:**	**COMPUTER AND INFORMATION ENGINEERING**
Supervisor	**:**	**Prof. Dr. Ahmet ZENGİN**

September 2021

T.C.
SAKARYA UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY

DESIGN AND IMPLEMENTATION OF A NEW BLOCKCHAIN ALGORITHM TO INCREASE RELIABILITY, SECURITY AND INTEGRITY

Ph.D. THESIS

A F M Suaib AKHTER

Department : COMPUTER AND INFORMATION ENGINEERING

This thesis has been accepted unanimously / with majority of votes by the examination committee on 20.09.2021

Prof. Dr.
Ahmet ÖZMEN
Jüri Başkanı

Prof. Dr.
Ahmet ZENGİN
Üye

Prof. Dr.
İhsan PEHLİVAN
Üye

Doç. Dr.
Devrim AKGÜN
Üye

Doç. Dr.
Mustafa Zahid YILDIZ
Üye

DECLERATION

I declare that all the data in this thesis was obtained by myself in academic rules, all visual and written information and results were presented in accordance with academic and ethical rules, there is no distortion in the presented data, in case of utilizing other people’s works they were refereed properly to scientific norms, the data presented in this thesis has not been used in any other thesis in this university or in any other university.

A F M Suaib AKHTER
20.09.2021

ACKNOWLEDGEMENT

Firstly, Alhamdulillah for everything as the Almighty Allah has allowed me to perform and finish my Ph.D. thesis.

Secondly, I would like to appreciate the efforts and guidance provided by my supervisor Prof. Dr. Ahmet ZENGİN. His cordial and tremendous support from the beginning to the end of this thesis is priceless. Moreover, I would like to take the opportunity to express my gratitude to the head of the department Prof. Dr. Cemil ÖZ for all kind of support he provides throughout my studentship at Sakarya University. I also appreciate the endeavour provided by Associate Prof. Dr. Ünal ÇAVUŞOĞLU and the jury members.

Furthermore, I am thankful to YTB (Yurtdışı Türkler ve Akraba Topluluklar Başkanlığı) fort he financial support. I would like to thank my mentor Dr. Mohiuddin AHMED who always guided me with great enthusiasm and to all the family members for their unconditional love, prayers, encouragement and support.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SUMMARY

Keywords: Blockchain, Vehicular ad hoc network, Smart contracts, Ad hoc networks, Internet of vehicles, Distributed storage, Intelligent vehicles.

The utilization of blockchain is increasing day by day because of its extra ordinary features including distributed and decentralized storage services. Blockchain can provide flexibility, tamper resistance, immutability, fairness, transparency, and robustness. Moreover, the addition of smart contract provides increases the programmability and management facilities. Although blockchain was first introduced to support cryptocurrency, special facilities make it popular for different fields like e-commerce, global payments, P2P landing, remittance, healthcare, record keeping, voting, logistics, etc.

Smart devices including internet of things (IoT), internet of vehicles (IoV), internet of healthcare (IoH), etc. also start utilizing blockchain for different purposes. However, too much flow of data and duplication increase the scalability problem and there is no efficient solution available to minimize this problem. Thus, in this thesis, we proposed a novel multi-level blockchain structure to minimize the scalability problem. The system is divided into two parts which are global and local blockchain. Local nodes are the member of a local blockchain where all the local service center is a member of the global blockchain. Global blockchain stores information of all the local blockchains’members. Local service centers will provide their support to only the local members and global blockchain will be used to handle the migration process. Because of the proposed structure, local blockchains will not be overloaded and thus able to perform more efficiently and quickly.

To implement the proposed structure, we used Vehicular ad hoc networks (VANET). Smart vehicles while moving around can form a temporary communication with the nearby vehicles to form a VANET to create social networking between them. Blockchain is used by researchers to ensure the security and authenticity of the vehicles, store and analyze traffic events, and also manage and distribute the transmitted messages. However, almost all of them suffered from scalability problem. To minimize this problem, in this thesis, we use blockchain to manage the authenticity and message transmission of both cluster-based and co-operative VANET.

Four different systems have proposed in this thesis and implemented in the ethereum blockchain platform and programmed by using smart contracts. Simulation results and performance analysis shows that the proposed methods provide security, integrity, authenticity, tamper free, robustness as well as outperforms previously available systems.

YENİ BİR GÜVENİLİR, GÜVENLİ ve SAĞLAM BLOK ZINCIR ALGORİTMASININ TASARIM VE UYGULAMASI

ÖZET

Anahtar kelimeler: Blok zinciri, Araçlara özgü ağlar, Akıllı sözleşme, Geçici ağ, Taşıtların interneti, Dağıtık veritabanı, Akıllı taşıtlar.

Dağıtılmış ve merkezi olmayan depolama hizmetlerini de kapsayan üstün özellikleri nedeniyle blok zincirinin kullanımı her geçen gün artmaktadır. Blok zincirin esneklik, art niyetli kullanıma karşı direnç, değişmezlik, açıklık, şeffaflık ve sağlamlık gibi son derece önemli özellikleri vardır. Blok zincir ilk olarak kripto para teknolojisini desteklemek için geliştirilmiş olsa da, son yıllarda yapılan bilimsel çalışmalar onu e-ticaret, küresel ödemeler, P2P landing, havale, sağlık, kayıt, oylama, lojistik vb. gibi farklı alanlar için popüler hale getirmiştir.
Nesnelerin interneti (IoT), araçların interneti (IoV) gibi akıllı cihazlar da farklı amaçlar için blok zinciri kullanmaya başlamıştır. Ancak aşırı veri akışı ve kopyalama, ölçeklenebilirlik sorununu ortaya çıkarır ve bu sorunu en aza indirecek etkin bir çözüm yoktur. Bu nedenle, bu tezde ölçeklenebilirlik problemini en aza indirmek için yeni bir çok seviyeli blok zinciri yapısı önerilmektedir. Geliştirilen sistem küresel ve yerel blok zinciri olmak üzere iki bölüme ayrılmıştır. Küresel blok zinciri, tüm yerel blok zinciri üyelerinin bilgilerini saklar. Yerel hizmet merkezleri, desteklerini yalnızca yerel üyelere sağlayacak ve herhangi bir üye bir yerel alandan başka bir küresel blok zincirine taşındığında, geçiş sürecini yönetmek için kullanılacaktır. Önerilen yapı nedeniyle, yerel blok zincirleri aşırı yüklenmeyecek ve böylece daha verimli ve hızlı bir şekilde çalışabilecektir.

Önerilen yapının uygulanması için araç ad hoc ağları (VANET) kullanılmıştır. Akıllı araçlar hareket halindeyken yakındaki araçlarla geçici bir iletişim kurarak aralarında sosyal bir ağ oluşturmuştur. Blok zinciri, araştırmacılar tarafından araçların güvenliğini ve güvenirliğini sağlamak, trafik olaylarını depolamak ve analiz etmek için kullanılır ve ayrıca iletilen mesajların yönetimini ve dağıtılmasını gerçekleştirir. Ancak, yapılan tez çalışmasında ölçeklenebilirlik sorunu en aza indirmek için, hem kümeleme tabanlı hem de işbirliği yapan araçlardan oluşan bir VANET sistemi blok zincir ile donatılmıştır.

Bu tezde dört farklı sistem önerilmiş, önerilen yöntemler Ethereum blok zinciri platformunda gerçekleştirilmiş ve akıllı sözleşmeler kullanılarak kodlanmıştır. Simülasyon sonuçları ve performans analizi, önerilen yöntemlerin güvenlik, bütünlük, özgünlük, sağlamlık sağladığını ve mevcut sistemlerden daha iyi performans gösterdiğini göstermektedir.

CHAPTER 1. INTRODUCTION

This research is targeted to provide security services to VANETs with the help of blockchain. In this section problem statement, the motivations of the thesis will be presented with the contributions and outcomes.

1.1. Problem Statement and Motivations

With the increment of automated vehicular services, the importance of fully automated VANET services is becoming one of the most appealing research areas. Although, several efficient communication protocols like traditional MAC, clustering, cooperating, etc. protocols can provide the primary needs of communication where security issues like malware attacks, fake vehicles, false notification, etc. may result in fatal accidents. Thus, to ensure the authenticity of the vehicles as well as to manage the communication protocol between them in a secured way are the area that still requires more improvements.

Typically, vehicles use IEEE 802.11 standard to communicate between themselves [1]. The messages transferred between automated vehicles in typical VANET's can be divided into two main categories. Important information, absence or delay or false transmission of those may result in harmful incidence can be classified as safety or emergency or important messages while relatively less important information like weather report, gaming, music services, etc. can be classified as non-safety or general messages. To handle different types of messages several different methods are available where safety messages always get high priority and follow the standard delay requirements of 100ms [2].

Among the previously proposed protocols in this research, a cluster and a cooperative communication protocol are selected to improve their security, integrity, authenticity, attack prevention capabilities with preserving the privacy of the vehicles.

Ensuring authenticity, security of the vehicles is very important as different types of attack can be performed to minimize the performance or sometime result in severe destructions. For example, attackers may perform man-in-the-middle attack by generating false notifications, performing modification, fabrication, etc. [3]. Thus, it requires proper prevention techniques to avoid the destructions.

Security can be provided by many protocols, but extraordinary services such as immutability, distributed and decentralized storage service, powerful management capability, temper resistance, flexibility, fairness, transparency, robustness etc. services make blockchain an efficient solution to perform both authentication of the vehicles as well as message transmission management for VANETs [4,5].

Automated vehicles are considered as light-weight devices and mostly with low computational capability. Because of this, it is required to import additional computational and storage support. It can be possible to use EDGE computing service as well as cloud storage to facilitate, however light weight encryption algorithm may minimize the computational time and increase the throughput of the system.

1.2. Thesis Goals

The thesis is targeted to ensure security, integrity, authenticity, reliability, attack prevention capability of VANET systems by using blockchain. The built-in services of blockchain ensures integrity, immutability, temper resistance, flexibility, fairness, transparency, robustness etc. Additionally, the management services with broadcasting capability help the system handier. However, to minimize the computational cost a light-weight encryption algorithm RSA-1024 is used instead of traditional ECDSA used by blockchains.

A secure message transmission system as well as verification and authentication of vehicles are targeted to implement in the thesis. Additionally, the system is targeted to develop in more efficient way than previously proposed system and can maintain the SDR of 100ms.

1.3. Contribution

These are the contributions of the thesis:

1. A blockchain based message transmission protocol is designed to store, manage and distribute safety messages for cluster based VANETs. The developed system can provide almost all the security aspects with the help of blockchain.
2. The packet structure of the traditional MAC protocol (provided by IEEE-802.11) is updated to provide support to the blockchain based system.
3. To minimize the encryption-decryption cost during communication RSA-1024 is used instead of traditional ECDSA protocol.
4. As proof-of-concept the system was developed by using Ethereum blockchain and emulated in a virtual blockchain named Ganache. Vehicles use metamask wallet to communicate and pay through blockchain.
5. After developing the secured message transmission system an authentication protocol is designed by using blockchain to ensure the authenticity of the vehicles under the clusters. A physical verification is performed during registration and later every time a vehicle wants to join a cluster blockchain is there to ensure the authenticity.
6. To preserve the privacy of the vehicles all the vehicles' real identity is preserved in a secure place and they are able to communication by using their public-private key pairs.

7. Moreover, to minimize the scalability problem of blockchain a multi-level structure is proposed where local blockchains are responsible to handle local vehicles and a global blockchain will store the related information and used while required.
8. Migration from one area to another is also proposed for the multi-level blockchain structure.
9. Additionally, another authentication protocol is proposed to secure another popular message transmission protocol which is cooperative protocol. To do that, traditional MAC packets are updated to provide key transmission and blockchain supports.
10. All the systems are developed by using virtual blockchain simulator and the performance analysis of the authentication protocol is presented which shows that the proposed system can perform more quickly and efficiently than many of the previously proposed system.

1.4. Organization of The Thesis

The thesis is mainly divided into three main parts. Firstly, a blockchain based secured message transmission protocol is presented for cluster based VANETs and accepted as a regular paper in the journal of Computers, Materials & Continua which is a Q1 journal with impact factor of 3.28, is presented in Chapter 2. Secondly, another research paper is published in Sustainability as “A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET”, is presented in Chapter 3. In Chapter 4, the authentication protocol for the cooperative VANET protocol is presented which is also another published paper in the journal of Sensors. Finally, in Chapter 5, the thesis is concluded with the potential future works.

CHAPTER 2. A SECURED MESSAGE TRANSMISSION PROTOCOL FOR VEHICULAR AD HOC NETWORKS

Vehicular Ad hoc Networks (VANETs) become a very crucial addition in the Intelligent Transportation System (ITS). It is challenging for a VANET system to provide security services and parallelly maintain high throughput by utilizing limited resources. To overcome these challenges, we propose a blockchain-based Secured Cluster-based MAC (SCB-MAC) protocol. The nearby vehicles heading towards the same direction will form a cluster and each of the clusters has its blockchain to store and distribute the safety messages. The message which contains emergency information and requires Strict Delay Requirement (SDR) for transmission are called safety messages (SM). Cluster Members (CMs) sign SMs with their private keys while sending them to the blockchain to confirm authentication, integrity, and confidentiality of the message. A Certificate Authority (CA) is responsible for physical verification, key generation, and privacy preservation of the vehicles. We implemented a test scenario as proof of concept and tested the safety message transmission (SMT) protocol in a real-world platform. Computational and storage overhead analysis shows that the proposed protocol for SMT implements security, authentication, integrity, robustness, non-repudiation, etc. while maintaining the SDR. Messages that are less important compared to the SMs are called non-safety messages (NSM) and vehicles use RTS/CTS mechanism for NSM transmission. Numerical studies show that the proposed NSM transmission method maintains 6 times more throughput, 2 times less delay and 125% less Packet Dropping Rate (PDR) than traditional MAC protocols. These results prove that the proposed protocol outperforms the traditional MAC protocols.

2.1. Introduction

Vehicular Ad hoc Networks is an especial type of dynamic wireless network, designed to provide a communication infrastructure between vehicles. Inside a VANETs system each device needed to be well equipped to exchange information (send and receive) with other vehicle’s drivers or vehicles within their reach. The IEEE 802.11-2016 standard [1] provides MAC and physical layer protocols for VANETs.

VANETs are targeted to provide safety, efficiency and Infotainment. Collision warning, safe-distance information, congested road notification, risky vehicle warning, road barrier/ obstacles /block notification, signal/rule violation warning etc. are emergency notifications which are transmitted between vehicles to alert each other by using different VANET protocols. These are called safety messages. Moreover, infotainment can be delivered by incorporating commercial service information, gas station/parking/restaurants/hotel information, media content download, multiplayer games, etc. Those are categorized as the non-safety message. Safety messages always get priority for transmission as fail or delay distribution of those messages may result in severe accidents, traffic jam, etc. Processing all types of messages together will increase the traffic and harm the throughput and overall performance. Because during transmitting, it is required to follow Strict Delay Requirements (SDR) of 100 ms for safety message [2]. Contrastingly, NSM is comparatively less important than safety message and does not require SDR to follow.

To maximize the throughput and minimize transmission delay & PDR Cluster-based (CB) protocols could be a better solution for VANET [2]. The nearby vehicles heading towards the same direction could form a cluster to transfer information among themselves. Although CB systems are easier to manage and simultaneously appropriate for resource utilization and performance enhancement, traditional CB systems are suffering from some shortcomings like hidden node problems, traffic overloading, packet dropping, etc. CB-MAC protocol [2] has overcome the shortcomings of CB systems and proposed a complete solution for VANET. By using their Non-Safety Message Transmissions (NSMT) protocols, it improved the communication quality by increasing the throughput and decreasing transmission delay & Packet Dropping Rate (PDR). Adding the security attributes like confidentiality, authenticity, reliability, transparency, integrity etc. to the CB-MAC system could assure security with good performance.

However, safety messages are very crucial for VANET systems and should be protected from any kind of attacks. Attackers could modify message contents and generate false messages or can provide false replies by using a man-in-the-middle attack [3]. Those security leaks may result in fatal accidents.

Meanwhile, the popularity of blockchain is increasing because of its distributed features and the secured storage service for P2P communication. Blockchain is considered as immutable ledgers and ensures important security services [4], [5]. All data and transactions are stored as chained blocks and it is not possible to edit or delete any information after being stored, which ensures the integrity, immutability and trustworthiness. These features motivate us to employ blockchain in the proposed system to store safety messages. A Public Key Infrastructure (PKI) based digital signature algorithm is used to ensure the authentication of the cluster members and also to provide communication security. Additionally, we propose a Certificate Authority (CA) for physical verification of the vehicles and to generate a public-private key pair for each of the vehicles. In this paper, to increase throughput by ensuring security services, we propose a Secure Cluster-based MAC (SCB-MAC) protocol for vehicular ad-hoc network. The target is to introduce the security features to the SMT of VANET systems. Handling safety and non-safety messages separately, providing signature-based security during cluster joining and communication, blockchain-based decentralized and distributed storage of the messages and vehicles registration and physical verification are the novelty introduced in this paper. As a Proof of Concept (PoC), we implement an Ethereum blockchain in virtual machines with Cluster Members (CMs) and CH to simulate the

SMT. The scenario is tested in a real-world Ethereum test network named Rinkeby test network [6].

The contributions of the paper are the followings:

1. We propose a blockchain-based Secured Cluster-based MAC protocol (SCB-MAC) for VANETs. SCB-MAC defines the formation of the cluster, handshake methods, safety and non-safety message transmission in details. We have modified some of the control packets formats of IEEE 802.11 to allow blockchain and to support those methods.
2. We propose blockchain to store and distributes the safety messages of clusters to provide a decentralized environment while ensuring robustness, tamper resistance, immutability, fairness and transparency of the safety messages. The blockchain is hosted in the cloud and the corresponding CH and CMs will communicate with it by using high-speed internet. All the CMs including CH are considered as the full node and anyone can initiate a transaction on the blockchain to inform a safety message. Blockchain will generate block from each of the safety messages and broadcast it to all the CMs including CH.
3. We have employed a PKI based digital signature method to ensure the authenticity of cluster members as well as to provide communication security. During cluster joining communicating with the blockchain server, digital signature is used to ensure user authentication and integrity, confidentiality, nonrepudiation of the message.
4. We introduce CA to register and verify vehicles. Additionally, it is responsible to generate public-private key pair for each of the vehicles and to ensure the safety, security and preservation of their privacy.

We have discussed some cluster based VANET systems with their performance and security in the related work section (section 2.2). Research paper where blockchain is employed for VANETs is also added in that section. The system structure is demonstrated in section 2.3. The tools used for implementation and experimental setup details are discussed in section 2.4. The performance analysis of the proposed SCB-MAC protocol is demonstrated in section 2.5. Security analysis of the proposed method is presented in section 2.6. In section 2.7 we present the conclusion of the paper with some possible future works.

2.2. Related Works

Cluster-based systems are proved very useful for VANETs. The quality and performance improvement by using a cluster-based architecture in VANETs can be found in [7]. In [8], Yang et al. proposed a cooperative Clustering-based Medium Access Control (CCB-MAC) protocol to enhance the trustworthiness of emergency message broadcasting by improving their reception rate. In [9], the researchers presented a multi-channel CCB-MAC which also improves the reliability with QoS support with the help of cooperation between the members. The authors in [10] also proposed a cluster-based multichannel MAC protocol where they developed an analytical model to find out suitable window size for the MAC protocol to balance between the delay and the successful delivery rate. A hybrid cluster-based protocol is proposed for safety message transmission by [11] which improves the network stability and increase channel utilization by selecting the cluster head according to the mobility factor of the vehicles. Due to lack of neighboring node, TDMA protocols are not able to utilize all the time slots of a frame. The [8]–[11] do not have efficient resource utilization capability.

In [12], researchers proposed DMMAC, which is also a cluster-based MAC protocol by utilizing Fuzzy logic Inference System (FIS). But their method is applicable only for emergency/safety messages. A multihop-cluster based hybrid architecture is presented for the safety message transmission to minimize the connection overhead and PDR [13]. In [14], the researchers combine the clustering protocol and carry-and-forward schemes for highway VANETs. [14] shows improvement in data download volume and throughput but information about network delay and packet dropping rate is not mentioned.

The strict delay constraint for the safety message transmission is 100ms, but the presented methods do not satisfy this credential. Additionally, [8], [11]–[13] provide solution only for safety messages and does not concern about the general messages or non-safety messages. Thus, in this paper, we propose a cluster-based method where safety and non-safety messages are handled separately according to their importance. Rather than following the traditional MAC protocols, a blockchain-based method is proposed to ensure the SDR for safety message transmission.

In [15], Zhang et al. presented a Data Security sharing and Storage system based on the Consortium Blockchain (DSSCB). They utilize the tamper-proof and security features of blockchain to store authentication information like identity and keys with location, direction, current position and rule violation information of the vehicles. Similarly, Javaid et al. use blockchain to store registration and status information of vehicles in their DrivMan system [16]. To ensure the trust of vehicles, a video storage system was proposed by Xie et al. in [17] where vehicles use their onboard camera to capture video of the surroundings and send it to a blockchain to store. The stored information is used to analyze the behavior of vehicles to find any unwanted or malicious behavior. In [18], Wagner et al. proposed a method to ensure the integrity of the event messages. Blockchain is used to store the reputation score of the vehicles which is updated after each transaction. Zhang et al. utilized blockchain to store important traffic event information like traffic violation and accidents [19]. They use Mobile Edge Computing (MEC) for computational support, but because of MEC, the system is not fully decentralized. Another blockchain-based message dissemination service was proposed in [20], [21]. Blockchain is used to store the verified event information to ensure the security and trust of the system. Another event validation mechanism is proposed in [22] by Yang et al. where RSUs broadcast event messages to the vehicles and vehicles use PoW to verify the trustworthiness of that event. To implement a scalable system, they use local blockchain to provide quick response to the local vehicles and then all the local RSUs synchronized the data into the global blockchain. But the infrastructure cost for RSU and resources are high, thus in most of the cases vehicles have to pay a good amount of money for that [27]. To handle the huge workload of event data, Singh et al. presented branch-based technology with blockchain in [23] where blockchains are divided into branches and each branch is responsible to provide services in different geographical areas. To increase the scalability, some researchers use multiple blockchain to store different information separately [24], [25], [26].

In the above-mentioned research, different types of blockchain are used for different purposes. However, none of them differentiates between message or event types. If all the transmitted messages or event information are stored together in the blockchain with proper security encryption services, the time and storage overhead of the system must be high. It results to decrement of throughput and increment of delay. To minimize the difficulties of consensus and mining [18] minimize the difficulty to 4 leading zeros while [23] set it to 3. Blockchain could be the best solution to provide security, integrity, availability, transparency, robustness etc. But without proper management, the performance could be very low. Thus, we propose a blockchain to store the safety messages. Non-safety messages are not stored in the blockchain as they are less important and consume too much storage.

2.3. System Structure

The nearby vehicles heading towards the same direction will form a cluster. All the vehicles are well equipped with necessary hardware and software resources to send and receive messages including OBU, Sensors, Global Positioning System (GPS) and high-speed internet connection. The vehicles are physically verified by a Certified Authority (CA). CA also generates and assigns a public-private key pair to each vehicle and all the vehicles will be known as their public key. CA is considered as secured enough to preserve the privacy of the vehicles. A graphical representation of clusters is presented in Figure 2.1(a). Among the vehicles, one will be elected as Cluster Head (CH) and others become Cluster Member (CM). By this way, a centralized system is formed where all the NSMTs between CMs will be handled by the CH as an access point. Every cluster owns a blockchain to store the safety messages. All the CMs including CH are considered as a full node and anyone can initiate a transaction in the allocated blockchain to inform about an emergency.

Vehicles will sign the message with their private keys to confirm their identity and to ensure non-repudiation. The blockchain server will check the authentication and then generates block from the message and broadcasts it to all the members. Details of the system model are discussed in the following subsections.

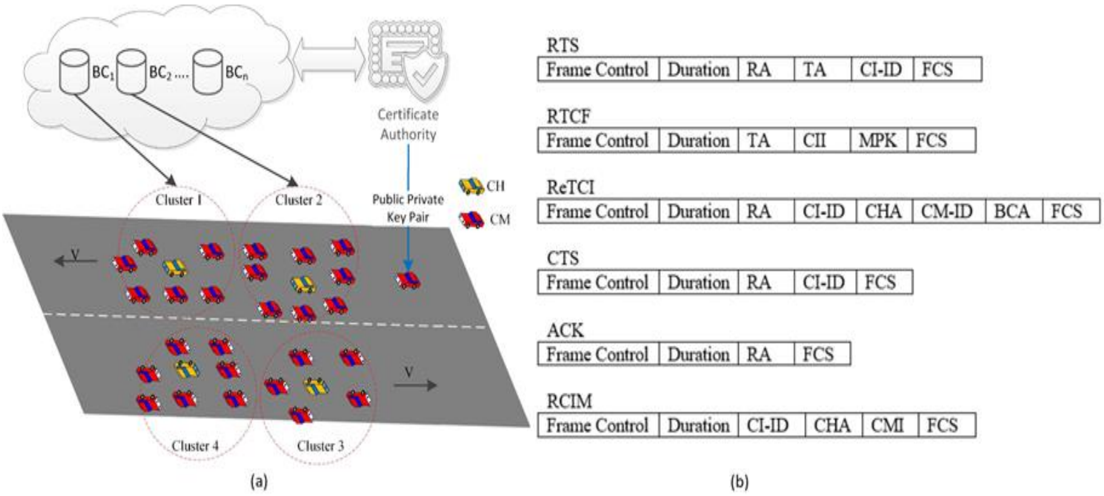

BC$_1$
BC$_2$ ....
BC$_n$
Certificate Authority
Public Private Key Pair
CH
CM
Cluster 1
Cluster 2
Cluster 3
Cluster 4
V
V
(a)
RTS
Frame Control | Duration | RA | TA | CI-ID | FCS
RTCF
Frame Control | Duration | TA | CII | MPK | FCS
ReTCI
Frame Control | Duration | RA | CI-ID | CHA | CM-ID | BCA | FCS
CTS
Frame Control | Duration | RA | CI-ID | FCS
ACK
Frame Control | Duration | RA | FCS
RCIM
Frame Control | Duration | CI-ID | CHA | CMI | FCS
(b)

Figure 2.1. (a) Application scenario, (b) Modified control packet format for SCB-MAC

2.3.1. Formation of SCB-MAC cluster

SCB-MAC is a cluster-based system with some modification from the traditional IEEE802.11 standard (see Figure 2.1. (b)). In this section, we will discuss the details of cluster formation and related details.

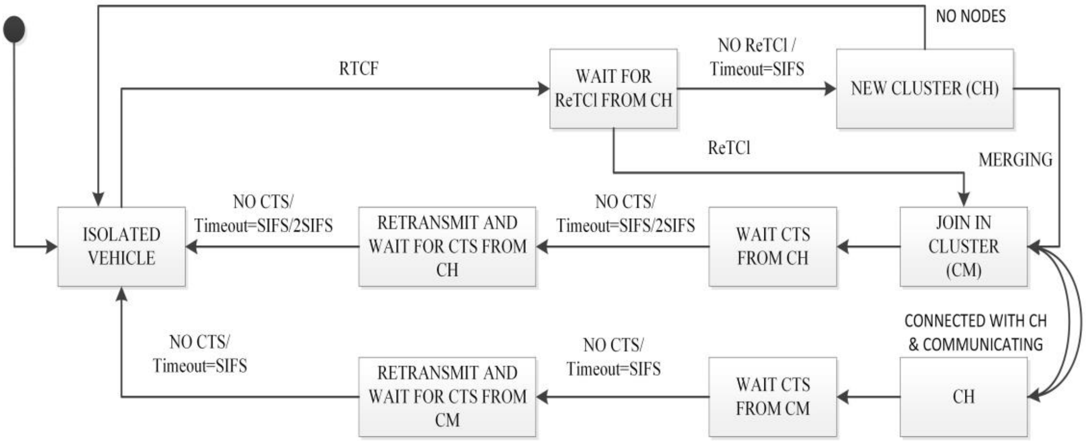


Figure 2.2. Finite state machine of the proposed SCB-MAC protocol

2.3.1.1. Cluster membership

To join a cluster, an isolated vehicle has to broadcast a control message called Request to Cluster Formation (RTCF) in the network. Cluster Information (ClI) and the vehicle’s public key i.e., the Member’s Public Key (MPK) are included in the RTCF. Then, CH of the nearby cluster sends back a (Registration to Cluster) ReTCl packet to the isolated vehicle by informing about the cluster, Public key of CH and the Address of the Blockchain (BCA) assigned to that cluster. The new member id of the vehicle is also included in the ReTCl. To ensure authenticity, CH signs the BCA with its private key. The newly joined member has to decrypt it by using the public key of CH and then registered to the assigned blockchain. A vehicle can receive multiple ReTCl, in that case, the vehicle will calculate the time interval between sending and receiving of the control messages and join the cluster where the delay is minimum. If no cluster is present nearby and the vehicle considers itself as CH and starts a new cluster. Then it can apply to the server to allocate a blockchain for the newly formed cluster. The new CH will broadcast the ClI in the network and wait for some CMs to join. Unified Modelling Language (UML) is used to sketch the FSM of the proposed SCB-MAC protocol (see Figure 2.2).

2.3.1.2. CH election and cluster merging

An active but isolated vehicle will broadcast RTCF and wait for ReTCl to join an existing cluster as a CM. But if it does not receive any ReTCl and SIFS timeout occurs, the vehicle becomes CH to form a new cluster. If multiple CHs come very closer and start using the same channels, CHs will receive control messages from each other. Then all the CHs those who realize the existence of cluster(s) will broadcast a control message called Request to Cluster Merging (RCIM). Inside RCIM, CH includes Cluster’s Member Information (CMI) to inform the number of CMs active under its cluster. After receiving the RCIM, Cluster(s) with a lower number of CMs will join to the cluster with the largest number of CMs. All the CMs including the CH(s) will join as new CM. Newly joined CMs will exchange RTCF and ReTCl with the CH to complete the merging process. CH of the previous cluster will initiate a transaction in the current blockchain to synchronize the valid safety messages from the previous blockchain.

2.3.1.3. Leaving a cluster

For different circumstance, anyone can leave a cluster and then the CMs list is updated dynamically. Cluster leaving may be required in four situations and those are demonstrated in Figure 2.3. While the CH sends RTS to a CM and does not receive any CTS even after retransmission, CM will be considered as out-of-reach (see Figure 2.3(a)). Similarly, while the CH sends RTS on behalf of a sender CM to receiver CM and does not receive any CTS even after retransmission, destination CM will be considered as out-of-reach (see Figure 2.3(d)). If there is no ACK received from a CM after broadcasting and resending a message, that CM will be considered as out-of-reach (see Figure 2.3(b)). If the CH is out of reach and a CM does not receive any CTS even after the retransmission the CM will initiate a cluster leaving process (see Figure 2.3(c)).

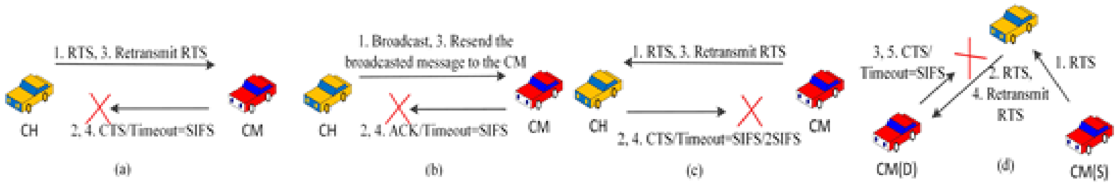

1. RTS, 3. Retransmit RTS
CH
2, 4. CTS/Timeout=SIFS
CM
(a)
1. Broadcast, 3. Resend the broadcasted message to the CM
CH
2, 4. ACK/Timeout=SIFS
CM
(b)
1. RTS, 3. Retransmit RTS
CH
2, 4. CTS/Timeout=SIFS/2SIFS
CM
(c)
3, 5. CTS/ Timeout=SIFS
2. RTS, 4. Retransmit RTS
1. RTS
CM(D)
(d)
CM(S)

Figure 2.3. Cluster leaving processes while (a) no CTS is received from a CM, (b) no ACK is received from a CM, (c) no CTS is received from the CH and (4) No CTS is received from the CM(D).

2.3.2. Safety message transmission (SMT)

Collision warning, safe-distance information, congested road notification, risky vehicle warning, road barrier/ obstacles /block notification, signal/rule violation warning etc. are considered as emergency or safety messages. These types of messages have strict delay requirement which is 100 ms [2]. The safety messages should come from a valid source and stored in such a way that, if one or multiple cluster members (including the CH) leave the cluster, the safety messages should not be lost. Traditional cluster-based systems are managed by a central node and thus the possibility of single point-of-failure is high. Blockchain is a perfect solution for these obligations as it provides data storage and management system in a distributed environment.

When any isolated vehicle become a CH, it will communicate with the server to get the network address of an available blockchain. The server will provide an address where the smart contract for the SMT was previously deployed. If the CH was a member of any previous SMT blockchain, it will copy the related and valid safety messages to the newly created blockchain as transactions. Whenever a CM wants to join the cluster and shares its public key, CH will send the sever credentials of the blockchain by signing it using the CH’s private key. The CM will connect with the blockchain server and then it will synchronize to receive all the existing safety messages of the blockchain. All the CMs including CH are independent nodes in the blockchain and everyone can perform transactions in the blockchain to inform others about a safety message.

Each safety message is generated by a smart contract as a transaction and stored chronologically as a block in the blockchain. After any block is generated, all the CMs will get notification about the newly created safety message in block form. If any CM has validity expired information for a particular safety message, it will request for another transaction in the blockchain to mark the message as invalid. For example, whenever a vehicle changes a lane it will generate a transaction but when the vehicle will move to another lane the previous information become invalid. Thus, it will generate an invalid transaction and the block will be marked as invalid. As the messages consume very small storage, the block will not be removed from the blockchain. However, the information stored in the block could be used by the law enforcement authority to investigate different occurrence like an accident, traffic jam etc.

2.3.3. Non-safety message transmission (NSMT)

The non-safety message transmission will be unicast to and fro a CM or a CH. There are three categories of unicast and corresponding transmission is briefly discussed here. From CH to CM, there is a direct unicast from CH to CM. CH verifies transmission using ACK. The data is routed via CH as a CM cannot send non-safety messages directly to another CM, rather they send it to the CH and CH will be responsible to broadcast messages to the destination CM. On the other hand, CH can transmit non-safety messages to neighbour clusters' CH by using the RTS/CTS mechanism. Figure 2.4(a,b,c) shows the handshaking between the members of the proposed NSMT protocol.

Like traditional MAC protocols, if all the CMs are transmitting messages to each other there will be duplicate message exchanges and hidden node problem is possible to occur. Moreover, with the increment of the number of vehicles a huge flow of messages will be generated which increase the chance of collisions and transmission delay [2]. Thus, in the proposed method, CM has the responsibility to handle the non-safety message communication and rather than broadcasting immediately CH sends to one CM at a time and waits until receiving an ACK from that CM. After the ACK is received it will send the message to another CM. It is possible to set the maximum number of retransmission limit for NSMT, and if an ACK does not receive by the CH within that time, it will retransmit the message until the limit. Figure 2.4(d) shows the flowchart.

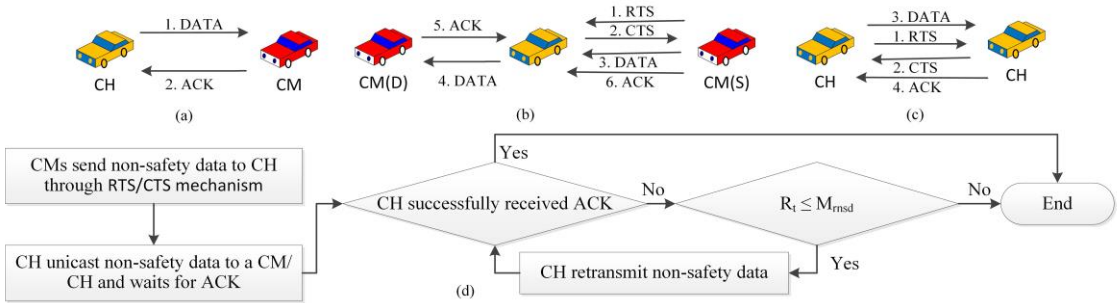

1. DATA
2. ACK
CH
CM
(a)
5. ACK
4. DATA
CM(D)
1. RTS
2. CTS
3. DATA
6. ACK
CM(S)
(b)
3. DATA
1. RTS
2. CTS
4. ACK
CH
CH
(c)
CMs send non-safety data to CH through RTS/CTS mechanism
CH unicast non-safety data to a CM/ CH and waits for ACK
CH successfully received ACK
Yes
No
$R_t \leq M_{rnsd}$
No
Yes
End
CH retransmit non-safety data
(d)

Figure 2.4. (a) Handshake between CH and CM during NSMT, (b) flowchart of the NSMT method

2.4. Implementation

For the proposed SMT of the SCB-MAC protocol, we present a Proof of Concept (PoC) implementation by using the Ethereum blockchain. Generally, the transactions are performed by miners who are also members of the blockchain. But in the proposed system, as the vehicles are the members of the blockchain and many of the vehicles do not have the capability to mine blocks, we have introduced a server which will perform the mining tasks on behalf of the vehicles. Moreover, online computing service providers also maintain a distributed service. Thus, our proposed system is decentralized and distributed as the data are not stored in the server or a specific location rather stored in all the vehicles storage. A Virtual Machine (VM) was configured with Ubuntu-18.04.4-desktop-amd64 to host the Ethereum blockchain and also act as a miner. Two other VM is considered as CH and CM. Registration to the blockchain and message transmission is tested with this setup. We are going to describe the details of the implementation in this section.

2.4.1. Tools

We implemented the SMT module of the SCB-MAC protocol by using the Truffle framework. It’s a well-known testing framework for Ethereum blockchain which provides all the facilities to manage smart contracts, automated testing of the codes, deploy smart contracts in Ethereum blockchain [28]. To emulate and test the smart contracts into a blockchain, the truffle suite offers Ganache [29], a virtual private Ethereum blockchain. Ganache offers special features to examine the blocks and transactions, blockchain log to analyse the responses and debugging information in the popular platforms like Windows, Mac OS and Linux. The vehicles use metamask wallet [30] to connect with virtual private blockchains. It provides all the wallet facilities to access, control and pay to the blockchain-based applications. Metamask comes in the form of a browser extension and also available for iOS and Android as apps. Not only the main Ethereum network but metamask also provide the facility to connect with different test networks including custom RPC (Remote Procedure Call). A Node Packet Manager (NPM) is used to executes JavaScript in the proposed method [31]. To interact with the smart contract, we developed the client-side in HTML by using Lightweight NPM Server [32].

2.4.2. Experiment

In a typical VANET system, all the vehicles may not have the mining capabilities. Thus, in the proposed system, one or more servers are used to perform mining on behalf of the vehicles. It could be an external EDGE server (like [17], [20], [21]) or an existing blockchain server (like [6], [33]) which is available online. To test our proposed system in both environment we present two different experimental setups. In the first setup, we are considering a dedicated EDGE server as miner (configured in a virtual machine). Moreover, In the second experiment, a real-world platform (Rinkeby test network) is considered as blockchain server to perform mining.

2.4.2.1. Ganache test server

To implement the SMT module we prepared a VM as blockchain server with Ubuntu-18.04.4-desktop-amd64 installed. First, we install ganache and consider it as a blockchain of a particular cluster. Then, we install NPM as it is a prerequisite to rum truffle framework and then install the other dependencies. In the SMT blockchain, there are two types of operations. First one is to store a safety message and the second one is to mark it as invalid when the impact/validity of the message is no longer valid. Thus, we write a smart contract which consists of three functions. One to view the existing blocks, the second one to add a safety message in the blockchain and the third one to mark a safety message as invalid. The SC is written in solidity and deployed into the blockchain by using truffle.

Next, in the CH and CM virtual machines, we install metamask Ethereum wallet extension in the Firefox web browser. In the metamask, we use the custom RPC option to connect the ganache blockchain server which is running in the server VM with a customisable port number. The CM and CH used their public keys to register with the blockchain. We considered that the CM and CH are verified by CA. Thus, the CM and CH have the permission to perform operations in the blockchain. Ganache provides 100 ethers to CM and CH to pay the fees i.e., the gas during a transaction. After testing it in the local VM, we found that all the functions are running fine and ready to deploy in a real-world platform.

2.4.2.2. Rinkeby ethereum testnet

To deploy smart contracts and execute transactions in a real-world platform, we have used Rinkeby [6], which is an Ethereum test network. It is one of the popular test networks used by blockchain developers. By sharing the account information in the social network, we have earned some virtual currency i.e., ether which is usable only for Rinkeby. Although the earned ETHERs for Rinkeby are valueless in the real world, to perform any transaction and smart contract deployment we need those ETHERs to pay the gas price.

We have tested our smart contract in the Remix IDE (integrated Development Environment) which is a platform independent environment [34]. It’s a web-based service which provides different compiler versions to run smart contracts and execute blockchain transaction. After deploying the smart contract and performing some operations in the Rinkeby testnet by using Remix IDE, details report about the blocks and transactions can be found in the etherscan web site [35]. The reports include the timestamp, transaction fee, gas limit, gas fee, block number, hash values of transactions etc.

2.5. Performance Analysis

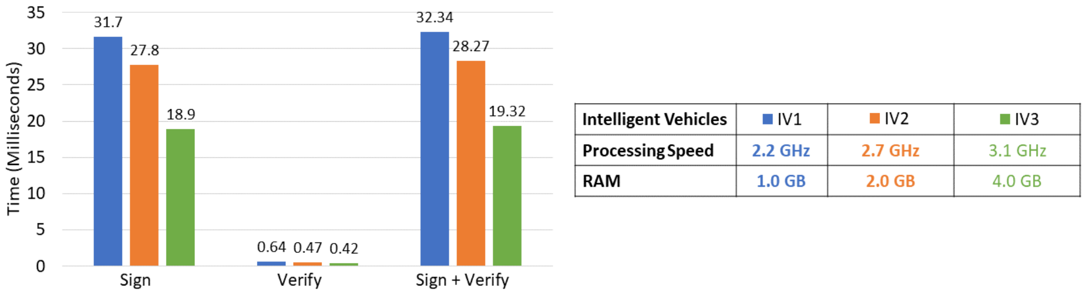
The performance analysis of the proposed SCB-MAC protocol is divided into two parts. Firstly, we will demonstrate the performance of the SMT protocol which includes the computational overhead analysis of the digital signature and key generation algorithm. Storage overhead due to Ethereum blockchain is also presented in that section. Then we will discuss the performance of the NSMT protocol by comparing the throughput, PDR and delay with the traditional MAC protocol.

2.5.1. Performance analysis of the SMT protocol

To ensure security, integrity and authenticity of the transferred message whenever any CM or CH wants to initiate a transaction in the blockchain, it signed the message with its private keys as a proof of authenticity. Similarly, during the first communication with a CM, CH sends BCA inside ReTCl by signing it with CH's private key. In both situations, the system uses RSA-1024 algorithm. The security strength i.e., the difficulty of breaking the key is measured in bits and according to NIST [36], the security strength of RSA-1024 is 80 bits. That means to break the key attacker have to perform at least 280 operations. According to some reports 80-bit security is considered as below standard, but for the system with lower computational power like VANET, IoT, etc. that would be considered secured enough. However, in [37], Singh et al. presented RSA-1024 with the security level equal to the symmetric key size of 112-bit. In SCB-MAC, vehicles use high-speed internet connection to communicate with the blockchain and the propagation delay considered ignorable.

2.5.1.1. Computational overhead

For a computer with more than 1.5GHz clock speed, RSA- 1024 with 80 bits security would take 1.48ms for signing and 0.07ms for verification [38]. So, it is possible to sign and verify a message within 1.55ms. However, to calculate the signature and verification time for RSA-1024 with 112-bit security three intelligent vehicles are considered with different computational resources. Processing speed and RAM of the vehicles are presented with their time required to sign and verify a safety message of 24- bytes are presented in Figure 2.5. For IV1, IV2 and IV3 it requires 32.34, 28.27 and 19.32 milliseconds respectively to complete sign and verification process.



Intelligent Vehicles	🟦 IV1	🟧 IV2	🟩 IV3
Processing Speed	2.2 GHz	2.7 GHz	3.1 GHz
RAM	1.0 GB	2.0 GB	4.0 GB

Figure 2.5. Signature and verification time required for various intelligent vehicles.

As the strict delay constraint for the SMT is 100ms, it is possible to sign and verify at least 64 messages by using RSA-1024 signature method (with 80-bit security). However, while the security strength is considered 112-bit, it is possible to complete 3 to 5 transaction. From the previous works we have found that the average delay for safety messages of [10] is 151ms and in [39] it is also more than 100ms. So, the SMT time is good enough to maintain the SDR. However, it is possible to hire multiple EDGE servers to improve the scalability of the system. During cluster joining i.e., the registration processes the time required for signature and verification is 32.34ms for a low configured vehicle (see Figure 2.5). That means it is possible to register more than 30 low-configured vehicles per second. This is a minimum cost to ensure security, integrity and authenticity. The CA use a key generator to provide public and private key pairs for vehicles. The key generation time for RSA-1024 is 97ms for a computer with a 3.1GHz processor and 4.0 GB of RAM [37]. So, it can generate at least 10 keys per second.

2.5.1.2. Storage overhead

Block header of the Ethereum blockchain is approximately 508 Bytes [40]. In Ethereum, every block consists of a single message. In the worst case, if a safety message block is generated in every 5 seconds (12 in a minute), the storage overhead is 508 x 12 x 60 x 24 = 8.37 MB/Day. Therefore, the proposed method requires a small amount of storage and possible to store them for a long period. However, when there remains no member in a cluster, the server reset the blockchain by archiving all the blocks in a cloud. Thus, too much storage support is not required for the proposed SMT protocol.

2.5.2. Performance of the NSMT protocol

In SCB-MAC safety messages will be transmitted by using high-speed internet which will remove workloads from the internal network which results in an increment of throughput and decrease of PDR and delay during NSMT. In this section, we will present the performance analysis of the NSMT and compare it with the traditional MAC system. A numerical analysis is presented with arbitrarily distributed n number of vehicles which are moving through a multi-lane road. Speed of the vehicles are considered as 100km/h and the width of the road is 5 meters. Vehicles are moving in almost the same speed and their transmission area is 500 meters. If these parameters are changed, performance will be changed too. Details about their impacts are discussed in [41], [42]. Tradition MAC protocols for VANETs are studied in [2], [41], [43]. We used these studies and data to compare our method with the traditional MAC protocols. However, in the context of this paper sensitivity test is not going to add any new value as the comparison will not be fair. More importantly, sensitivity test would have been apt if there were similar blockchain-based MAC protocol for VANET. The analysis is performed in MATLAB and the considered value of parameters are presented in [2].

2.5.2.1. Throughput analysis of the NSMT protocol

The normalised system throughput S for kth cluster can be calculated as:

$$S_K = P_S P_{busy} L \ / \ T_e = P_S P_{busy} L \ / \ P_i T_{slot} + P_{busy} P_S T_S + P_{busy} \ (1\text{-}P_S) \ T_C \qquad (2.1)$$

Here, P_s = Probability of successful transmission, P_{busy} = At least one transmission is in progress, L = Transmitted packet length, P_i = Probability that the channel is idle, T_{slot} = Slot time, T_e = Expected time to spend in a state, T_{span} = Time span of slot, T_s = Time span for successful transmission and T_c = Time span if there is collision.

The throughput of the system would be:

$$S = \sum_{k=1}^{j} S_k \qquad (2.2)$$

Figure 2.6(a) shows that the throughput for SCB-MAC (NSMT) is comparatively higher than traditional MAC-based methods. In traditional MAC, CH broadcasts all the messages immediately which increase collisions and throughput decrease quickly. When the number of vehicles is small, cluster size will be small. A small cluster could not be able to utilise the available radio resources due to an inadequate number of vehicles in the cluster and low traffic demand generated in the cluster [2]. Therefore, throughput is lower than traditional MAC protocol.

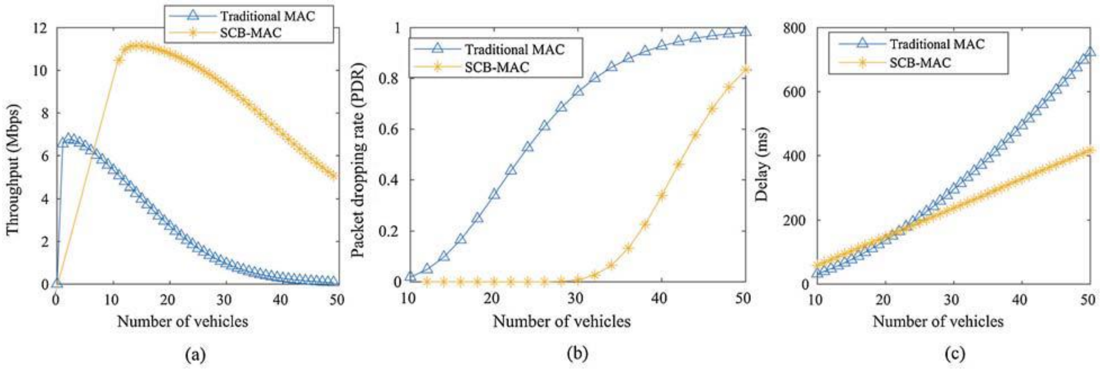


Figure 2.6. (a) Throughput, (b) PDR and (c) delay comparison between SCB-MAC and traditional MAC.

Firstly, as the safety messages are not using the internal network, the load of messages are less. Secondly, rather than broadcasting immediately SCB-MAC uses RTS/CTS to check the existence of the CMs first and then transmits to remove the hidden node problem. Thus, the increment of throughput is significant but with the increment of vehicles, collisions are also increasing which decrease the throughputs gradually for all types of systems. For example, while the number of vehicles reaches to 40, traditional MAC protocol is overloaded and too much collision decreases the throughput to almost 0 while proposed SCB-MAC can maintain a throughput rate near to 6 Mbps. Moreover, the maximum throughput of the SCBMAC protocol is about 12Mbps for NSMT, where previously proposed methods like [11], [14], [7] have achieved 1.1, 1.3 and 11 Mbps respectively.

2.5.2.2. Packet dropping rate of the NSMT protocol

To calculate PDR of the network the following equations are derived in [2]:

$$PDR_{nsd} = (1 - P_S)^{M_{rnsd}} \tag{2.3}$$

where M_{rnsd} are the maximum retransmission limit for NSMT. To ensure the availability of safety messages there is no limit for retransmission, which increase overhead and increment of PDR. In the proposed method, safety messages are not using the internal network which decreases the PDR rate of the network. Thus, PDR is less than traditional MAC in the proposed method although the retransmit limit is the same. Figure 2.6(b) shows that the PDR for the proposed SCB-MAC is near to 0 until the number of vehicles reaches to 30 and after that, it increases but always less than traditional MAC protocols.

2.5.2.3. Delay analysis

In [2], Shah et al. presented the transmission delay of a cluster-based system could be calculated as:

$$E\,[D] = E\,[T_{interval}] - [P_{fdrop} / (1\text{-}P_{fdrop})]\; E[T_{drop}] \tag{2.4}$$

So, delay for non-safety messages will be:

$$E[D_{nsd}] = T_e\,(n - P_{drop} / (1\text{-}P_{drop})\;.\;2 / (1\text{+}CW\text{+}M_{rnsd}\,CW/2)) \tag{2.5}$$

Figure 2.6(c) shows the average packet transmission delay against the number of vehicles. As the proposed method uses RTS/CTS handshake before sending any non-safety messages, initially the transmission delay is a little higher than the traditional MAC protocol. But with the increment of the number of vehicles, the traditional MAC system faces rapid increment of transmission delay because of collisions, while SCB-MAC keeps it manageable.

2.5.2.4. Results and discussions

The cluster-based protocol is based on IEEE802.11 Distributed Coordination Function [DCF]. Performance of the IEEE802.11 can be found in [43]–[49]. NSMT achieved maximum throughput of 12Mbps, while some previously proposed method achieved [11], [14], [7] have achieved 1.1, 1.3 and 11Mbps respectively. Increasing number of messages increases collisions which result to decrement of throughput and increment of PDR and delay. For SCB-MAC the internal network will be available only for non-safety messages because the safety messages will be transmitted by the internet. Therefore, the full network is available only for non-safety messages and that results in throughput increment. Maintain a throughput of 6Mbps for NSMT, while the number of vehicles reaches to 40. In the same state throughput of traditional MAC protocol is close to zero. SCB-MAC is free from hidden node problem as only live nodes could receive non-safety messages which are achieved by RTS/CTS handshaking. By removing hidden node problem SCB-MAC can minimize PDR and transmission delays. When the total number of vehicles is 50, the transmission delay of the MAC protocol reaches to double (800ms) than the proposed protocol.

2.6. Security Analysis

In this section, we will discuss the security features of the SCB-MAC protocol. Blockchain with CA and public key infrastructure provide strong security to the transferred safety messages. The security features are the followings:

2.6.1. Source authentication and non-repudiation

We propose a PKI based digital signature method which is considered as secure until the attacker succeeds to get the private key. Each of the vehicles is physically verified by CA during registration. CA is responsible to ensure the safety and security of identities. To perform a transaction in the blockchain a vehicle has to encrypt the safety messages by using its private key to confirms its identity and nonrepudiation. The blockchain server will verify the vehicle’s identity before creating a block.

2.6.2. Privacy preservation

The real identity of the vehicles is securely stored by CA by mapping it with their public key. The vehicles use to communicate with others by using their public keys to disclose their original identity to the public. Therefore, even if an adversary could get the public-private key pairs it is not possible to guess the real identity of the vehicles. The proposed SCB-MAC ensures the privacy of the vehicles with the help of CA.

2.6.3. Security, integrity and confidentiality of messages

All the SMTs are encrypted by RSA-1024 cryptographic algorithm which ensures security, integrity and confidentiality of the messages. RSA-1024 considered strong enough as the key attacker have to perform at least 280 according to [36] or 2112 according to [37] operations to break the keys. The blockchain server checks for the integrity of the message by matching the hash value by decrypting the message. Any modification affects the hash value and that message will be rejected.

2.6.4. Attack prevention

PKI based digital signature algorithms are considered as secure until an attacker creaks the private key [50]. So, the communication channel used in SCB-MAC is theoretically secured. It also prevents the messages from being modified and fabricates by comparing the hashing value. Even if the adversary got the public-private key pair, it is not possible to get the hash of the former block in the blockchain. So, a fabricated message with wrong hash value will be rejected. So, reply attack from an unknown source similarly rejected. Moreover, the digital signature-based system prevents impersonate attack because it is not possible to generate a valid signature on behalf of a vehicle. However, CA confirms the physical identity of the vehicles and the blockchain server checks the authentication information before block generation. No unauthorized entity, as well as no vehicles with multiple fake identities, could perform any operation in the system. Thus, we can say that the system is free from Sybil attack or unknown source attack.

Additionally, SCB-MAC can prevent DDoS attack as the blockchain never accepts any unauthorized entity to perform any operation and they will be blocked by the server from sending further messages to the blockchain. DDoS, man-in-the-middle attack, Sybil attack, replay attack, etc. are the attacks that can harm a VANET system [51]. By using public-key cryptography based digital signature, SCB-MAC is safe from these attacks. Additionally, proposed signature method does not depend on verifier table, thus the system is safe from stolen verifier table attack.

2.6.5. Others

SCB-MAC utilizes the features of blockchain. It provides a decentralized and distributed environment to store data in a platform-independent and flexible way. Ethereum platform can be accessed by using metamask wallet [30], which could perform operations from any kind of computers and mobile devices using any operating system like Windows, MAC, Linux and any cell phone that uses iOS or Android. All the members have a copy of all the blocks in the blockchain, which prevent the system from single-point-of-failure and provides robustness. The storage structure of blockchain is chronological which is ensured by hashing. It does not allow anyone to change the content even the sequence of blocks which ensures immutability and tamper-free storing of the safety message. All the members in the cluster are equally treated while operating on the blockchain to ensure the fairness of the system. By using smart contracts, a vehicle could disable the safety message which is no more valid. In that case, the message is still stored in the blockchain and every member can see it as an invalid message. Even if any blockchain is reset, data blocks of it are archived in the cloud under the supervision of the CA. It could be used in future for accident investigation, traffic violation, etc. This storing method could help law enforcement authority during the investigation of accidents.

2.7. Conclusion

For VANETs, cluster based VANET systems are performing very well to reduce PDR, increase throughput and maintain hard time constraint for SMT. To keep the performance of the cluster-based system and introduce security features in it, SCB-MAC is proposed. Firstly, an Ethereum blockchain is used to store and distribute the safety messages in a decentralized environment with flexibility, tamper-resistance, immutability, transparency and robustness features. Secondly, a PKI based digital signature algorithm (RSA-1024) is used to ensure the authentication, non-repudiation, integrity and confidentiality of the safety messages. Thirdly, a CA is responsible to generate asymmetric keys for the vehicles and to preserve the privacy of the vehicle’s real identity. The blockchain is implemented and tested in a realistic platform. The results show that it is possible to complete 65 message transmission within SDR of 100ms. Therefore, the introduction of blockchain with digital signature method does not harm the SDR for SMT. Moreover, by using secure vehicles registration process it is possible to register 30 vehicles in every second. SCB-MAC provides source authentication, privacy preservation of the vehicles, attack prevention with the typical facilities of blockchain, digital signature methods. Numerical analysis is presented to check the performance of non-safety message transmission protocol and found that it performs better than the traditional MAC protocol in terms of throughput, delay and PDR. When the transmission rate of the traditional MAC protocols fall down to zero, the proposed NSMT maintain a rate of 7Mbps and when the number of vehicles reaches to 50, transmission delay increases to 800ms for MAC protocols while proposed method faces a delay of 400ms only. Moreover, the PDR of NSMT is zero while the traditional MAC protocols’ PDR reached to almost 60%. In future, we will try to implement a light-weight consensus method for blockchain to ensure the trustworthiness of vehicles. Additionally, we are planning to find a suitable communication protocol to exchange messages between the blockchains from neighbour clusters and also the feasibility of a secured protocol for the non-safety message will be tested in future.

CHAPTER 3. A SECURED PRIVACY-PRESERVING MULTI-LEVEL BLOCKCHAİN FRAMEWORK FOR CLUSTER BASED VANET

Existing research shows that Cluster-based MAC (CB-MAC) protocols perform well to control and manage Vehicular Ad hoc Network (VANET) but requires to ensure improved security and privacy preserving authentication mechanism. To this end, we propose a multi-level blockchain-based privacy-preserving authentication protocol. The formation of the authentication centers, vehicles registration and key generation processes are explained thoroughly in the paper. In the proposed architecture, a Global Authentication Center (GAC) is responsible to store all vehicle information while Local Authentication Center (LAC) maintains a blockchain to enable quick handover between internal clusters of vehicles. To remove the shortcomings of the traditional MAC protocols, we also propose a modified control packet format of IEEE 802.11 standards. Moreover, cluster formation, membership and cluster-head selection, merging and leaving processes are implemented considering the safety and non-safety message transmission to increase the performance. All blockchain communication is performed by using high speed 5G internet while encrypted information is transmitted by using RSA-1024 digital signature algorithm for improved security, integrity, and confidentiality. Our proof-of-concept implements the authentication schema considering multiple virtual machines. With detailed experiments, we show that the proposed method is more efficient in terms of time and storage compared to the existing methods. Besides, numerical analysis shows that the proposed transmission protocols outperform traditional MAC and benchmark methods in terms of throughput, delay and packet dropping rate.

3.1. Introduction

Vehicular Ad hoc Network (VANET) is a temporary wireless network which can be formed to exchange important information between vehicles. To become a part of VANET, vehicles need to be equipped with necessary hardware for information exchange for example On Board Unit (OBU), sensors, GPS and most importantly high-speed internet connection. IEEE 802.11-2016 [52] provides standards for VANET communication and recent improvement of internet speed because of 5G technology the opportunities and application of VANETs are in acceleration.

VANET provides an opportunity to create Vehicular Social Networking (VSN) betwecen vehicles. Generally, the transmitted messages can be categorized into two categories those are safety messages (SM) and general purpose or non-safety messages (NSM). In Table 3.1, examples of safety and non-safety messages are cited. To inform about any emergency situation vehicles could transmit or broadcast SMs. Because of the high importance of SMs, it is required to provide high priority during safety message transmission (SMT). In [2], it is mentioned that Strict Delay Requirement (SDR) of 100ms is required to maintain for SMT to ensure real time availability. On the other hand, there are some information which does not have any impact on the safety or security but beneficial are called NSMs. The NSM transmission (NSMT) does not require to maintain SDR like SMT protocol.

Table 3.1. Examples of Safety (SM) and Non Safety Messages (NSM)

Safety Messages (SMs)	Non-Safety Messages (NSMs)
Lane change	Information about gas station, parking, hotel, restaurants, etc.
Collision warning	Gaming
Safe distance information	Browsing
Congested road notification	Distribution of contents
Warning about risky vehicles	Advertisements
Barriers, obstacles, road block notification	GPS update

To ensure better management and performance efficiency of VANET systems, several protocols are proposed. Among them cluster based systems are performing better than others [2]. In a typical cluster based (CB) system, vehicles from nearby areas can form a cluster and one of the vehicles is selected as Cluster Head (CH) to manage internal and external communication. Typical CB systems suffer from traffic overloading, packet dropping and hidden node problem. But by minimizing or removing shortcomings it is possible to increase their efficiency. In [2], Shah et al. proposed a cluster based method where they made some changes in the MAC protocol and packet structures to remove hidden node problem and increase efficiency by minimizing delay and Packet Dropping Rate (PDR). Moreover, the proposed method handles SMs and NSMs separately and ensure SDR of 100ms for SMs. Thus, it can be considered a pretty successful protocol for VSN. For the communication purpose, we are going to use the proposed ACB-MAC protocol for internal communications.

With the increment of Intelligent Transport System (ITS), the importance and application of related systems like VANETs are also increasing. A number of researches have been found which are targeted to increase the performance of the VANETs. As vehicles are moving at high speed it is challenging to maintain good communication speed, high throughput, low PDR, etc. However, ensuring security and privacy of the vehicles were less important issues. Though, VANETs has to face Authentication, identification, confidentiality, Integrity and availability related threads and attacks [53,54]. Vehicle authentication is the most important security feature a VANET system must ensure. In spite of high mobility and low configured computation support real time authentication is required to maintain for VANETs.

Typically a secure authentication system is based on Public Key Infrastructure (PKI), where a vehicle can prove it's identity by sending an encrypted identification to the Local Authentication Center (LAC). LAC will decrypt the information and matched it with the authorized vehicles list i.e. database and take a decision (accepts or rejects). Though the PKI based systems provide effective security, it is time consuming and mostly stored in the centralized server which has single point-of-failure problem. Time consumption of encryption and decryption increases with the level of security. Moreover, because of high mobility each time the vehicles move from one cluster to another one encryption overhead increases. Frequent encryption/decryption will increase traffic overhead which decreases efficiency. Additionally, vehicles with lower computational support require more time for authentication and thus face more difficulties during authentication. If any critical traffic information is missed by any vehicle because of authentication delay, it may result in fatal accidents. Thus, a lightweight authentication mechanism is still a big challenge for VANET security.

Blockchain is a distributed storage platform which provides additional security, immutability, tamper-resistance, traceability, transparency, robustness etc. Although blockchain was invented to store public ledger related information but because of its varieties of security and other features it becomes popular to store different types of information in various applications [4,5,55]. Blockchain stores information as blocks which are chained together and it is not possible to update or delete any information from the blocks, thus it is called tamper-resistance storage. Moreover, new blocks can only be added at the end of the chain which makes the blockchain immutable and robust. However, the most important feature of blockchain is, it does not require any third party involvement to verify transactions as all the members store a copy of the whole blockchain and after a new block is added every member updates their database. This ensures transparency, third-party independence and traceability of the blockchain. In this paper, we are going to use blockchain to store authentication related information of the vehicles which help us to during registration and inter-cluster handover.

In this paper, we have proposed a blockchain based authentication schema for cluster based VANET system. LACs are responsible to register vehicles inside an area (for example state) and generate PKI keys for them. LACs maintain a local blockchain (LABC) where all the locally registered vehicles' public keys are stored and all the CHs are the member of that blockchain. Inside a state, whenever a vehicle moves from one cluster to another one, rather than traditional encryption/decryption or sign/verification the CH will search the list of public keys and verify the vehicles. Additionally, all the LACs are the members of a Global Authentication Blockchain (GABC) where all the registered vehicles of a larger area (for example country) are stored with their LAC name. If any vehicle moves from one state to another one, it has to apply to the destination LAC for temporary registration with an expected time period. LAC will verify the identity of the requested vehicle from GABC and added in the local tree so that all the local CHs can give easy access to the visiting vehicles. By this way, a simple and quick handover method is implemented with the help of multi-level blockchains. The proposed system removes the dependency of expensive infrastructures (for example roadside units) for VANET by utilizing high speed 5G internet.

To ensure faster authentication services to the emergency service provider vehicles, vehicles are divided into two categories general vehicles (GVs) and Emergency Vehicles (EVs). Vehicles like Ambulance, emergency medical services, fire service and civil defence, etc. are registered as EVs. Whenever an EV authenticated in a cluster, the corresponding CH will immediately broadcast an SM by informing the existence of an EV so that all the vehicles can provide a free passage for the EV.

As a Proof of Concept (PoC), we implement a multi-level blockchain by using virtual machines (VMs) to simulate both inter-cluster and inter-LAC authentication. Computational and storage overheads are presented to prove that the proposed authentication protocol can performs faster than some of the previously proposed methods. As well as numerical analysis is presented to demonstrate the throughput, PDR and transmission delay for the proposed VSN protocol which show that ACB-MAC outperforms the traditional MAC and some of the other previously proposed protocol.

The contributions of the paper can be summarized as follows:

1. We propose a blockchain-based secured, decentralized and distributed authentication protocol for Cluster-based MAC (ACB-MAC) for VANETs.

Inside this paper, the formation of the authentication centers, vehicles registration and key generation processes are explained with the secure and faster authenticating methods.

2. To increase the scalability, faster authentication service with decentralized and distributed storage support we propose a multi-level blockchain. In the top level a global authentication center (GAC) is responsible to store all the vehicles information in a blockchain where all the LAC are the members. However, to manage the vehicles internally LACs also manage a blockchain called LABC, which enable quick handover between internal clusters. All the CHs are the member of the LABC.
3. To remove the shortcomings like hidden node problem, packet overloading, packet dropping, etc. of the traditional MAC protocols, we propose a modified control packet format of IEEE 802.11 standards. Cluster formation, membership details, CH election, cluster merging and leaving processes are discussed with the safety and non-safety message transmission are proposed to increase the performance of the ACB-MAC system.
4. To preserve the privacy of the vehicles the original identity of them are securely stored in the LAC and only the public keys are shared between the CHs. Vehicles have to register to LAC to get physical verification. Moreover, RSA-1024 PKI is used by the LAC to generate public-private key pairs for the vehicles during registration and to ensure security, integrity, confidentiality of the transmitted messages.

In section 3.2 we discuss some of the previously proposed cluster based systems as well as some blockchain based authentication protocols. The complete cluster structure, authentication details and the message transmission protocols are demonstrated in section 3.3. The express services proposed for the EVs are described in section 3.4. Implementation tools with the experiment details are presented in section 3.5. Performance analysis of the authentication protocol and the VSN protocols are available in section 3.6. Section 3.7 is there to present the security analysis of the proposed method. Finally, in section 3.8 we conclude the paper with potential future works.

3.2. Related Works

3.2.1. Cluster based VANET systems

The advantages of cluster based systems in terms of performance and management is available in [56]. A cooperative Clustering-based Medium Access Control (CCB-MAC) protocol is proposed by Yang et al. to increase the reception rate and ensure trustworthiness of broadcasted message [8]. In another paper, Yang et. al. proposed a multi-channel cluster based method targeted to ensure the reliability of the transmitted message with additional QoS support [9]. Su et al. [10] presented a multi-channel MAC protocol to improve the delivery rate by decreasing the delay. Gao et al. presented a hybrid cluster based system where the mobility factor is considered to elect the cluster head [11]. Their proposed method performs well to increase network stability and channel utilisation. All the above mentioned are based on Time Division Multiple Access (TDMA) but TDMA based protocols suffer from the hidden node terminal problem. For a hidden node, the system requires multiple retransmission, which increases the traffic and results to delay as well as decrement of throughput. Due to lack of neighbouring node, TDMA protocols are not able to utilize all the time slots of a frame. Thus, we can say that, above mentioned [8, 9, 10, 11] TDMA based protocols do not have efficient resource utilization capability. In [12], Hafeez et al. proposed Distributed multichannel and mobility-aware cluster-based protocol in short DMMAC which utilizes Fuzzy-logic Inference System for safety message transmission. Another safety message transmission method is proposed by Ucar et al. targeted to minimize packet dropping rate and also connection overheads but only for safety messages transmissions [13]. In [14], Zhang et al. proposed a method for highway VANET by combining the cluster with carry-and-forward schemes. Although their proposed method improves throughput and data download speed but network delay and PDR information are not provided.

In the IEEE 802.11 and the cluster-based system, Clear to Send (CTS) transmission from each of the member node is required after each broadcast. This is one of the main reason for packet drooping and therefore throughput reduction. So the above-mentioned methods are not free from these problems. However, for safety message transmission it is required to maintain the SDR of 100ms which did not satisfy by the above mentioned papers. However, some of them (for example [9,11,12,13]) provide solutions only for emergency message transmission and others does not differentiate between messages which reduce the importance of the emergency messages.

3.2.2. Blockchain based authentication

Authentication of vehicles are primary requirement for VANET. Blockchain is utilized to store the registration information of the vehicles by Javaid et al. in their proposed method called DrivMan [16]. To ensure fast authentication and handover Li et al. proposed a method called SEBGMM [24]. In SEBGMM, three blockchains are used by three components of VANET (Vehicles, Routers and control mobility database) and they share information for authentication during handover. In [57], Malik et al. also use blockchain to store the authentication information and ensure the privacy of the vehicles. Ali et al. presented a method to ensure integrity and trust of vehicles where a blockchain is used to stores the identity of the authorized vehicles and another to store the unauthorized or revoked vehicles [3]. In [20,21] researchers proposed a privacy-preserving trust model to provides security features including transparency, conditional anonymity, efficiency and robustness. They used two blockchains to store the identity of the certified vehicles, revoked vehicles. Another blockchain is also used to store the messages which are transferred between vehicles. In [58], Kulathunge et al. presented an automated cashless Intelligent Payment System (ITP). Blockchain is used to store authentication and trust information of drivers and infrastructures i.e. RSU. Blockchain will share the trustworthiness of drivers and RSU between each other before the transaction. Moreover, blockchain also stores the details of each transaction. A consortium blockchain is proposed by Zhang et al. in [23], where they store the authentication information with location, position, direction and rule violation information of vehicles to ensure security and tamper-resistance of those information.

The previously proposed methods utilize blockchain for different purpose including authentication. Most of them use complex authentication method which consumes much time. Moreover, all the methods are dependent on Road Side Unites (RSUs) where the infrastructure costs are high [27]. In some previously proposed method like [59, 60, 61, 62] the computational overhead higher where some other method like [61, 63] suffers from high storage overhead. Additionally, all the vehicles including emergency vehicles considered similar which means the emergency service provider vehicles will not get any extra facilities from the proposed methods. Thus in this paper we proposed a lightweight and faster authentication protocol by utilizing cluster based system which is free from extra infrastructural costs. Moreover, special services are provided to the emergency vehicles during authentication and priority passage allocation in the proposed method.

3.2.3. Motivations

Firstly, it requires expensive infrastructures to implement RSU based VANETs and to remove the extra expanses CB systems are the best solution. Thus we introduce a CB system by modifying IEEE 802.11 packet structures.

Secondly, several types of messages are transmitted between vehicles and in most of the cases, all of them are treated equally. In that case, sometimes the flow of unwanted, irrelevant and less important messages become a barrier to the emergency information transmission. To ensure priorities to the emergency i.e., safety messages we divide the messages to safety and non-safety messages and proposed two different transmission protocol for them. We also ensure the SDR of 100ms for safety message transmissions. Together with this, the proposed method is targeted to increase system throughput and minimize the delay and PDR.

Thirdly, in the previously proposed VANET protocols all the vehicles are considered equal which means there are no especial facility for the emergency vehicles. To ensure priority to the EVs like Ambulance, emergency medical services, fire service and civil defence, etc. we categorized vehicles into GVs and EVs. In the proposed method, EVs get faster authentication services and a free lane while passing through inside clusters.

Fourthly, some of the previously CB methods are based on TDMA which is time-consuming and suffers from hidden node problems. To remove these shortcomings we introduce RTS/CTS handshaking in the proposed method.

Fifthly, privacy-preserving authentication is a principal requirement for VANETs to ensure security, confidentiality, trustability, etc. But to ensure high performance i.e., increased throughput, lower PDR and delay sometimes the security is compromised in the previously proposed VANET systems. Lacking of proper authentication protocols may allow malicious entities to enter and cause severe accidents inside a VANET. Moreover, lack of security, confidentiality and encrypted communication may offer attackers to perform different types of attack like information theft, Sybil attack, fabrication, modification, man-in-the-middle, DDoS, etc. To ensure security requirements like authenticity, non-repudiation, privacy preservation, confidentiality, integrity and attack prevention we propose a PKI digital signature algorithm which is RSA-1024.

Sixthly, to ensure flexible, immutable, transparent and robust authentication in a decentralized environment blockchain-based light-weight authentication system for vehicles are introduced. Typical certificate oriented authentication protocols are not capable to provide all these facilities as well as signature generation and verification have higher computational overhead [3, 16, 24, 25, 57]. Additionally, the proposed method is also targeted to minimize the transmission delay, computational and storage overhead for authentication.

3.3. System Structure

In this paper, we proposed a tree structure where a GAC is considered as the root of the tree (see Figure 3.1). All the LAC are in the second level where all of them are connected to a blockchain called GABC. GABC stores all the information about the vehicles of a large area. LACs are consist of several numbers of clusters which comes in the third level of the tree. Each of the clusters is maintained by a CH and all the CHs under the same LAC are the member of another blockchain called LABC which stores all the local vehicles public keys. Whenever a vehicle comes to join in a cluster the corresponding CH check it's the entry in the LABC to authenticate. In the fourth level, there are vehicles connected to their corresponding clusters. All the communications between vehicles are handled by the CH under the cluster.

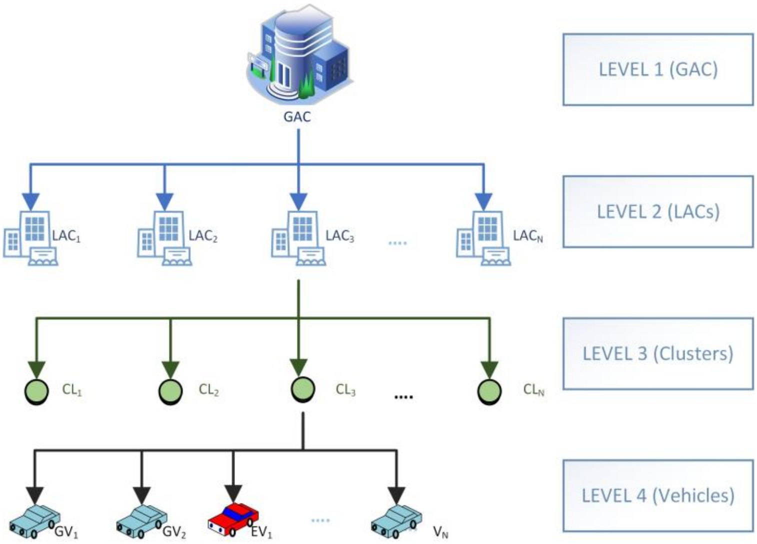


Figure 3.1. Tree structure of the proposed method

3.3.1. Cluster formation

All the vehicles moving through same direction will form a cluster. All the vehicles are equipped with On Board Unit (OBU), Global Positioning System (GPS), etc. with high speed 5G internet connection and communication capability. Figure 3.2 (a) illustrates the finite state machine (FSM) the cluster formation for GV. A GV is selected as CH and other become CMs. EVs will not participate in the process of becoming a CH, rather wait to join in a cluster as CM. CH is responsible to manage all the communication between the vehicles i.e., the CH acts as the center of VSN. CH is also responsible to communicate with the LABC and also with the neighbour CHs. To support cluster based system and to increase the efficiency of the message transmission specially to ensure SDR for the SMs we have proposed some changes in the IEEE 802.11 standard packet format and added some new packets. New Packets are: Registration To Cluster (ReTCl), Request To Cluster Formation (RTCF) and Request To Cluster Merging (RClM). The changes are presented in Figure 3.2(b).

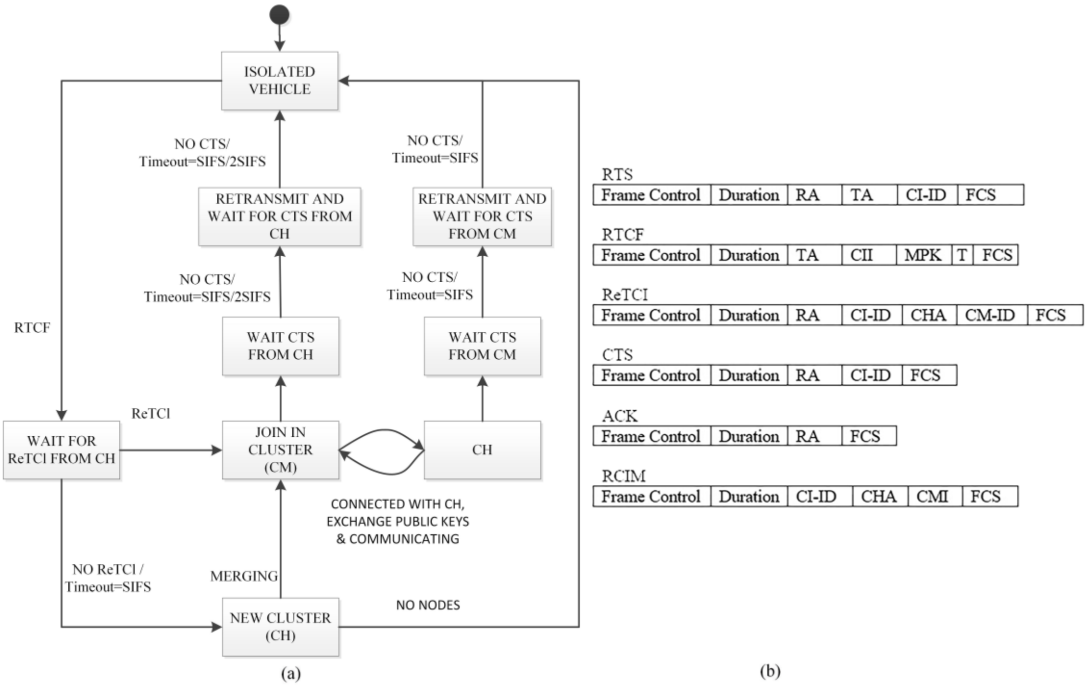

ISOLATED VEHICLE
NO CTS/ Timeout=SIFS/2SIFS
NO CTS/ Timeout=SIFS
RETRANSMIT AND WAIT FOR CTS FROM CH
RETRANSMIT AND WAIT FOR CTS FROM CM
NO CTS/ Timeout=SIFS/2SIFS
NO CTS/ Timeout=SIFS
RTCF
WAIT CTS FROM CH
WAIT CTS FROM CM
ReTCl
WAIT FOR ReTCl FROM CH
JOIN IN CLUSTER (CM)
CH
CONNECTED WITH CH, EXCHANGE PUBLIC KEYS & COMMUNICATING
NO ReTCl / Timeout=SIFS
MERGING
NO NODES
NEW CLUSTER (CH)
(a)
RTS
Frame Control | Duration | RA | TA | CI-ID | FCS
RTCF
Frame Control | Duration | TA | CII | MPK | T | FCS
ReTCI
Frame Control | Duration | RA | CI-ID | CHA | CM-ID | FCS
CTS
Frame Control | Duration | RA | CI-ID | FCS
ACK
Frame Control | Duration | RA | FCS
RCIM
Frame Control | Duration | CI-ID | CHA | CMI | FCS
(b)

Figure 3.2. (a)FSM and (b) updated packet structure of the proposed method

3.3.2. Cluster membership

All the inactive i.e., parked vehicles are the member of the inactive cluster. Whenever a vehicle becomes active it broadcast RTCF by including cluster information, public key, type, etc. in the network. The nearby CH(s) will check the authenticity of the vehicle with the help of LABC and after getting positive feedback from the database send(s) back ReTCl with the cluster-ID (Cl-ID), Cluster Head Address (CHA) and the assigned cluster member ID (CM-ID). Multiple CHs may return with ReTCl. In that case, the vehicle will join to the cluster whose response came first. After joining the cluster, corresponding CH will update the cluster list and the newly joined member will move from inactive cluster to the new cluster as a child or CM. If a GV will not found any cluster to join after short inter-frame space (SIFS) timeout it will create a new cluster and become CH of the cluster. But the

EVs will not form a cluster or become a CH, rather continue moving until receive any ReTCl.

3.3.3. Authentication center

The proposed blockchain-based authentication system can be represented as a tree. In the top-level GAC is there to store all the vehicles' information in a blockchain called GABC. GABC stores the real identity, driver information, vehicle type, public and private key, etc. information of the vehicles. All the vehicles have to register to the LAC before getting road permit. LAC is responsible to physically verify and generate a public-private key pair for each of the vehicles. Then it creates a transaction in the GABC by entering the required information. By this way, all the LACs get the information about a new vehicle's entry. GABC usually stores vehicles of a large area and it is time consuming to retrieve information of a particular vehicle. Thus to increase the scalability all the LAC maintain a blockchain called LABC by storing information of the locally registered vehicles only. This is the second level of the tree structure where not all but only the public key and the vehicles' types are stored during registration.

All the CHs under same state are the members of the LABC (as the third level of the tree) and thus got the list of all the locally registered vehicles. So whenever a new vehicle comes nearby and requests to join into the cluster, CH can verify the authenticity of the vehicle. By this way, secure authentication is performed by the CHs with the help of LABC. LAC maintains a tree where all the CHs are the child nodes and vehicles are children of the CHs. Similarly, visiting vehicles from another LAC can be verified by the destination LAC with the help of GABC. In Figure 3.3 the application scenario is demonstrated.

3.3.4. Blockchain based authentication

For vehicles authentication during cluster joining, we have changed a control packet named RTCF. Two fields named Member's Public Key (MPK) and type (T) is added in the RTCF to send the public key and the type of the requested vehicle within the control packet. The type field is used which require only 1 bit where 0 and 1 represent GV and EV respectably. Rather than searching for all the vehicles from the blockchain, the system will search according to the category which increases the efficiency of searching. If there are 10% of the vehicles are EV, it is possible to get 10 times faster authentication than a system where all the vehicles are considered as same. After receiving the RTCF, CH will generate a transaction in the LABC to search for the received MPK. Reply will come in form of 0 and 1 to represent valid and invalid respectively. To sign and verify only 1 bit data the computation time can be considered as ignorable. Whenever an EV become a member of a cluster, the CH immediately broadcasts a safety message by informing that an EV is there, so that the vehicles can clear the left lane (or right lane for right hand driving countries) and give free passage to the EV. By this way, the cluster based system provides a clear channel to the EVs. A flow chart in Figure 3.4(a) shows the inter cluster authentication method.

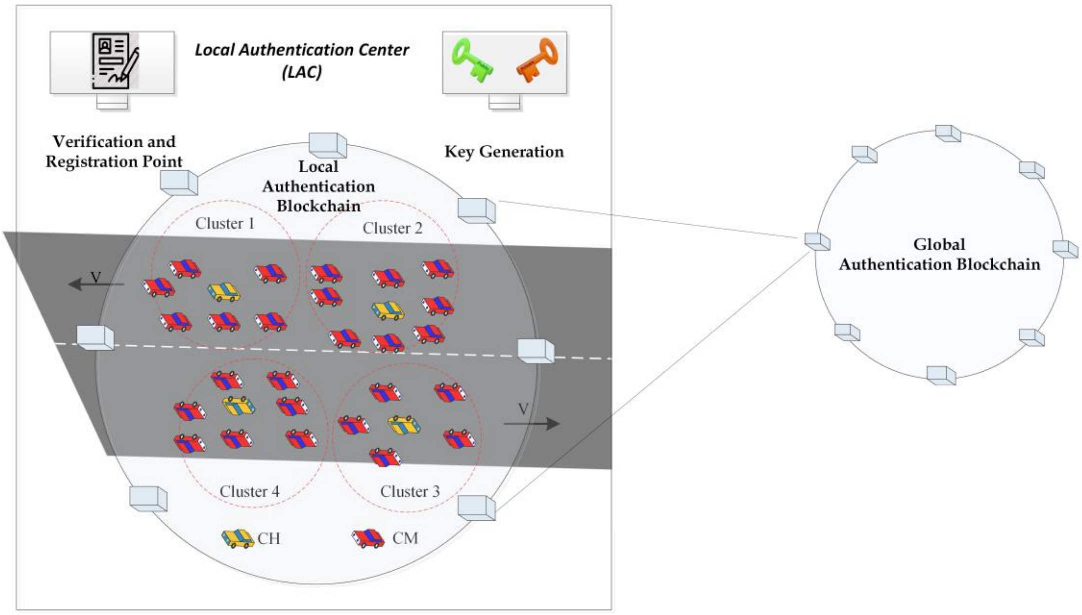

Local Authentication Center (LAC)
Verification and Registration Point
Key Generation
Local Authentication Blockchain
Cluster 1
Cluster 2
Cluster 3
Cluster 4
V
V
CH
CM
Global Authentication Blockchain

Figure 3.3. Application scenario with local and global authentication center

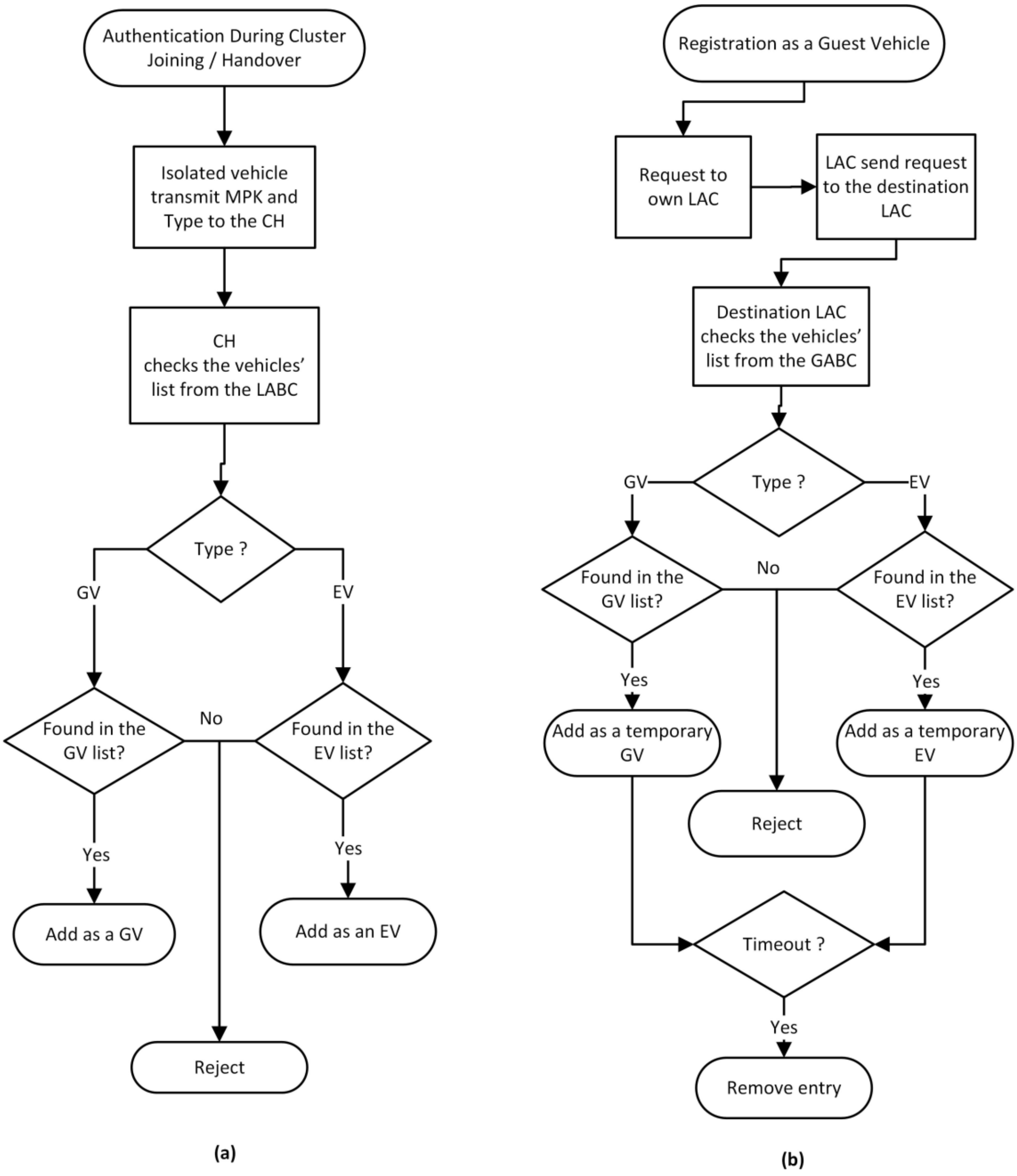

Authentication During Cluster Joining / Handover
Isolated vehicle transmit MPK and Type to the CH
CH checks the vehicles' list from the LABC
Type ?
GV
EV
Found in the GV list?
No
Found in the EV list?
Yes
Yes
Add as a GV
Add as an EV
Reject
(a)
Registration as a Guest Vehicle
Request to own LAC
LAC send request to the destination LAC
Destination LAC checks the vehicles' list from the GABC
Type ?
GV
EV
Found in the GV list?
No
Found in the EV list?
Yes
Yes
Add as a temporary GV
Add as a temporary EV
Reject
Timeout ?
Yes
Remove entry
(b)

Figure 3.4. Flow chart demonstrates vehicle authentication during (a) cluster joining and (b) guest vehicles' registration

Similarly, for inter LAC authentication, whenever a vehicle requires temporary access to another LAC, it has to register to that destination LAC. For the vehicle's point-of-view the process is not time consuming at all, because it is required to apply to its own LAC. Local LAC will send a request to the destination LAC with the vehicle type and required time period i.e., a timestamp. Destination LAC will check the existence of the requested vehicle's public key in the GABC blockchain by performing a search operation. If the existence of the requested vehicle is found, the public key of that vehicle will be added temporarily to the LABC with its type. After the requested time period, LAC will automatically disable the entity from the LABC by using smart contract. As all the CHs store the LABC, disabling temporary public keys will reduce the storage requirements and also reduce download time for the new CH while copying the LABC’s transactions. The flow chart (see Figure 3.4 (b)) describes the authentication details.

3.3.5. CH election and cluster merging

A cluster is formed by the isolated vehicle if any of the following conditions are satisfied: (i). If ReTCl is not received by any of the isolated vehicle, or (ii) after the broadcasting of the RTCF messages, the SIFS interval timeout occurs. In such scenarios, the vehicles will be attributed as CH by itself. For the scenario where the isolated vehicles receive ReTCI and there exists a cluster, the role of the vehicle will be CM because of the presence of the CH for a pre-existing cluster. The question may arise what will happen when two or more CHs joins the same network? In such cases, the CHs will merge if they join the same network coverage. A step by step procedure is outlined below:

1. The existence of multiple CH is often realized when any individual CH receives control messages from another peer CH.
2. The CH which realized the existence of multiple CHs will broadcast RCIM. The structure of the RCIM control packet includes critical information like cluster member information (CMI).
3. CMI includes the list of CMs for that particular cluster.
4. Once the RCIM from the first CH is received by other existing CHs, they will broadcast their own RCIM.
5. At this point, it will be accounted for the number of CMs for each CH. The merging of CH happens based on the maximum number of CMs. The CH who owns the highest number of CMs gets the priority to be selected as CH.

During this transformation, the remaining CHs then join as CMs and the existing role of CMs remain the same.

6. Once the process is finalized, the merging updates are broadcasted to all CMs by the new CH.

3.3.6. Leaving a cluster

In this section, we discuss the procedure of leaving a cluster. To this end, the process is observed by maintaining the list of CMs. This list is dynamically updated when a new vehicle joins or leaves. Both type of vehicles, i.e., CH and CMs can leave the cluster if they need to. The detailed process is presented in Figure 3.5. The figure has four parts: (i) Figure 3.5(a) shows the process where any vehicle leaves the cluster. In this case, at first, CH communicates with CM through RTS. The process continues until CH receives CTS and it stops upon SIFS timeout. During this waiting period, until SIFS timeout happens, a new RTS is transmitted if no CTS is received by that time. In a case when CM is out of transmission range, it is obvious that the CTS will not be received within the allocated SIFS time interval. Hence, the CM list is updated by removing that CM.

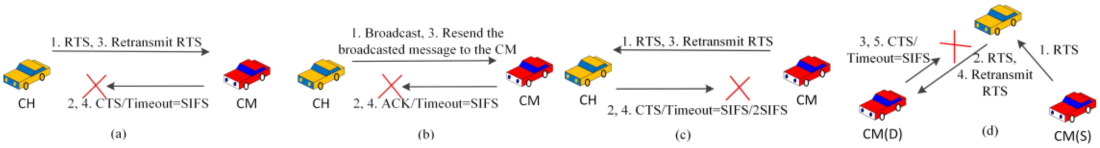

1. RTS, 3. Retransmit RTS
CH
2, 4. CTS/Timeout=SIFS
CM
(a)
1. Broadcast, 3. Resend the broadcasted message to the CM
CH
2, 4. ACK/Timeout=SIFS
CM
(b)
1. RTS, 3. Retransmit RTS
CH
2, 4. CTS/Timeout=SIFS/2SIFS
CM
(c)
3, 5. CTS/ Timeout=SIFS
2. RTS, 4. Retransmit RTS
1. RTS
CM(D)
(d)
CM(S)

Figure 3.5. Cluster leaving processes in different situations.

In the second part of the figure, a broadcasting based cluster leaving process is explained. Here, in the initial step, the CH broadcasts messages within the cluster so that it is available to all CMs. Upon successful receiving of the messages, the acknowledgement (ACK) message is sent to the CH by all existing CMs. The success of the ACK message receipt will validate the existence of any CM for that particular cluster. For those cases where ACK is not received by the CH, the CH will consider that the CM is not within the transmission range and the list is updated.

Please note, for information integrity and availability, the message is retransmitted after a failed transmission and at the same time, the SIFS timeout is also monitored. The whole process is summarized in Figure 3.5(b).

In the last two parts of Figure 3.4 (c and d), we have adopted the notion S and D that demotes the sender and destination, respectively. In those figures, during the cluster leaving process, a CM transmits data as a sender (S) to all D (that includes both CH and CM). After sending the RTS, the sender will be waiting for CTS. This waiting time is related to the SIFS time out. In our modelling, if S sends RTS to CH then the timeout happens after SIFS interval. However, if S sends RTS t another CM, the timeout happens for 2SIFS interval. Within the waiting time, if no CTS is received by the CM, RTS message is retransmitted. While Figure 3.5(c) shows the case when CM retransmits the RTS while Figure 3.5(d) shows the case when CH retransmits the RTS.

3.3.7. Safety message transmission (SMT)

Safety message transmission is one of the critical aspects of the proposed model. Safety related messages include accident prevention information, emergency brake signalling, emergency cautionary, etc. These messages are critical and needs to be satisfied strict time requirements. These safety messages are reliably transmitted from CMs to CH by using the RTS or CTS mechanism. The usages of RTS and CTS helps to reduce the packet collisions during a large scale broadcasting of the safety messages among CMs and CH. The safety message broadcasting procedure is summarized as below:

1. At the first step, CH broadcasts the safety related messages.
2. Upon successful receiving of the messages, the CMs follow up ACK messages.
3. The process is considered successful if ACK messages are received from all CMs.

4. For those scenarios where ACK message is not received, the possibility of transmission failure is evaluated by checking whether the number of retransmission (Rt) is less than or equal to the maximum retransmission limit for safety messages (Mrsm) [2]. In those cases, the safety messages are retransmitted for the missing ACK cases.

The ACK of the safety messages plays an important role in reliable message transfer. The complete process of the proposed safety message transfer protocol is illustrated in Figure 3.6(a) and the handshaking between the vehicles during SMT in Figure 3.6 (b and c).

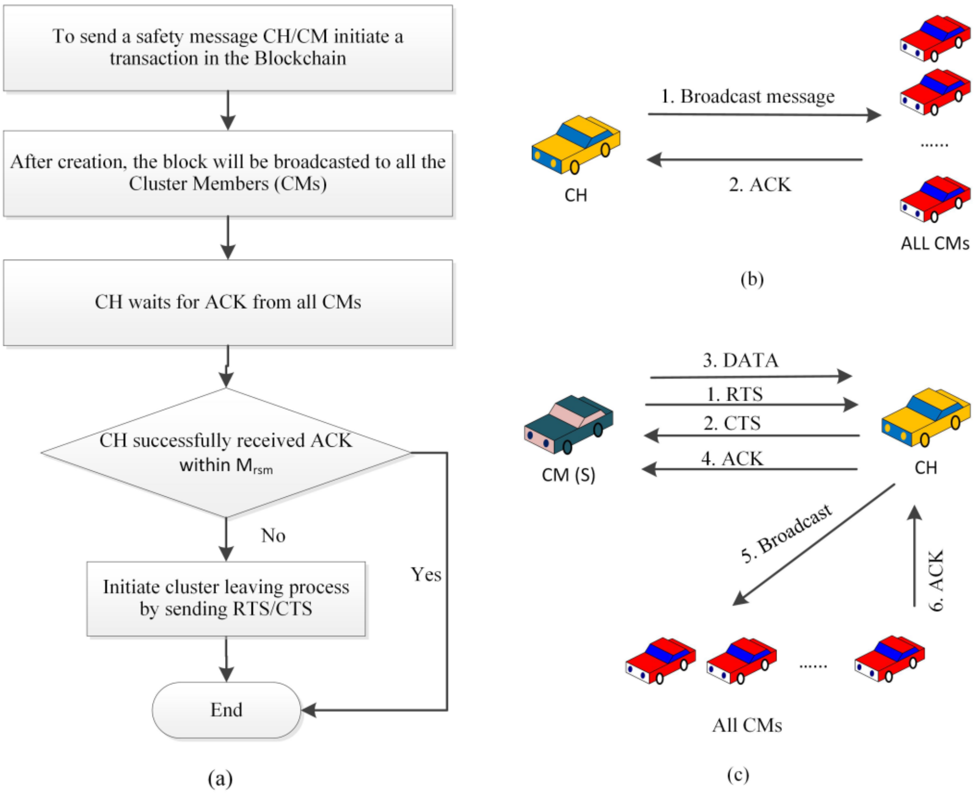

To send a safety message CH/CM initiate a transaction in the Blockchain
After creation, the block will be broadcasted to all the Cluster Members (CMs)
CH waits for ACK from all CMs
CH successfully received ACK within M_{rsm}
No
Yes
Initiate cluster leaving process by sending RTS/CTS
End
(a)
1. Broadcast message
2. ACK
CH
......
ALL CMs
(b)
3. DATA
1. RTS
2. CTS
4. ACK
CM (S)
CH
5. Broadcast
6. ACK
......
All CMs
(c)

Figure 3.6. (a) Flow chart demonstrates safety message transmission and (b, c) handshake between vehicles during SMT

3.3.8. Non-safety message transmission (NSMT)

Similar to the safety message transmission discussed in the previous section, our proposed VANET model also propose non-safety message transmission protocol to exchange general purpose messages. The non-safety messages include map download and updates, audio and media file transfer, web browsing, etc. The process of non-safety message transmission is supported by the unicast message broadcasting. In this setup, The sender (S) sends messages to the destination (D). Both CH and CM acts like a S or D. Based on the roles, one CH can send messages to a single CM. In this scenario, the effectiveness of the successful message transmission is observed by realizing the message acknowledgement (ACK). In another setup, one CH can send messages to another CH. In the last option, CMs can communicate among themselves via CH. In this setup, the communication happened between CMs and CH using RTS or CTS mechanism. Once the receiver CM receives the messages, it sends an ACK message to the intermediate CH and then CH forwards it to the sender CM. Throughout the process, the RTS/CTS ensures reliable message communication that avoids packet collisions. Those cases where ACKs are not received are considered as unsuccessful message transmission. The retransmission of the non-safety messages happens if the number of retransmission (Rt) for the failure transmission is less than or equal to the maximum retransmission limit for the non-safety message (Mrnsm) [2]. The whole concept of non-safety message transmission is summarized in Figure 3.7(a) and the handshake between the vehicles durinf NSMT are illustrated in Figure 3.7(b, c, d).

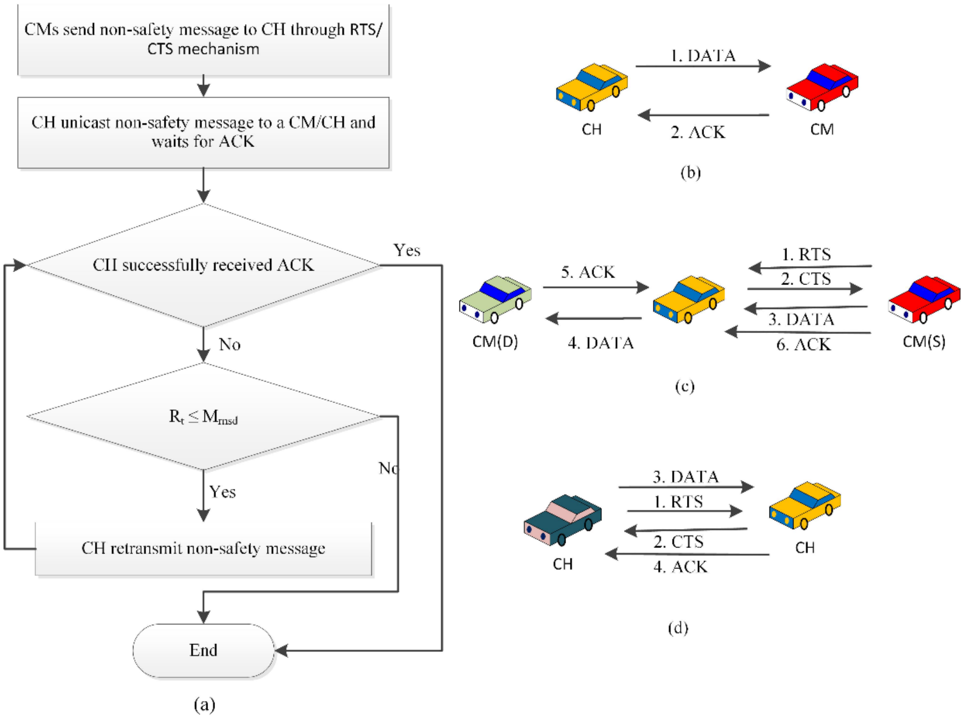

CMs send non-safety message to CH through RTS/ CTS mechanism
CH unicast non-safety message to a CM/CH and waits for ACK
CH successfully received ACK
Yes
No
$R_t \leq M_{msd}$
Yes
No
CH retransmit non-safety message
End
(a)
1. DATA
2. ACK
CH
CM
(b)
5. ACK
4. DATA
1. RTS
2. CTS
3. DATA
6. ACK
CM(D)
CM(S)
(c)
3. DATA
1. RTS
2. CTS
4. ACK
CH
CH
(d)

Figure 3.7. (a) Flow chart demonstrates Non-safety message transmission and (b, c, d) handshake between vehicles during NSMT

3.4. Emergency Vehicle Management

The proposed method ensures especial support for EVs. Firstly, the vehicles are divided into two parts to keep the EVs separate from the general vehicles. This will increase the searching speed during authentication. If all the vehicles are stored without type information for n number of vehicles in the worst case the search complexity will be O(n) but because of separate type if there are 10% EV, the search complexity will become O(n/10). By this way, the proposed authentication method for EV become 10 times faster than a method where all the vehicles are together.

On the other hand, during inter-cluster handover after completing the authentication process the CH immediacy broadcast an SM to all its member to inform about the presence of an EV. After receiving the SM all the vehicles will clear the left lane so that the EV will get the clearance to move forward quickly. From the best of our knowledge, this is the first time where special vehicles get real time treatment during authentication and road clearance.

3.5. Implementation

We present a PoC implementation of the proposed ACB-MAC by using the ethereum blockchain. Multiple VMs are used to represent a random GABC, an LABC which is also a member of the GABC and a CH which is a member of the LABC. Bothe inter-cluster and inter-LAC authentication are simulated with the setup. Implementation details with the tools used are described in this section.

3.5.1. Tools

3.5.2. Truffle framework

Truffle framework is a well-known framework to test transaction and other functions of ethereum blockchain. It is possible to deploy and test codes written in smart contract by using this framework. Additionally, it provides network management, scripting and client-side development services [28].

3.5.2.1. Ganache emulator

Ganache is a virtual ethereum blockchain emulator [29]. It can be used as real blockchain as it provides all the facilities to develop and test Decentralized Application (DApp). Moreover, it supports blocks and transactions detail examination, log analysis and debugging. It is possible to create users and customize the attributes of the users and other configurations of blockchain. Ganache is platform independent and two variants (UI and CLI) are available. UI version is used for this implementation.

3.5.2.2. Metamask ethereum wallet

In this implementation, metamask wallet [30] for currency management in ethereum blockchain. To connect and perform transactions in the blockchain all the members will use metamask. It can be used from both computer or mobile devices. It is possible to connect with custom Remote Procedure Call (RPCs) by using metamask. We utilized this facility to connect it with the local blockchain.

3.5.2.3. Node packet manager (NPM)

Both of the blockchains are hosted on the web for easy access. NPM [31] provides that facility by executing JavaScripts. In the truffle framework, we installed NPM with some dependencies to interact with the smart contract. A Lightweight Node Server [32] is used to develop the client-side in HTML.

3.5.3. Experiment

To present the tree structured authenticating system we use a VM by using Oracle VM VirtualBox 6.1 to host the GABC named GABC-VM. After installing the truffle framework we install ganache which will act as the GABC. NPM with other dependencies is also installed to provide web based services. All the LABC are members of this blockchain. All the machines are using Ubuntu-18.04.4-desktop-amd64 operating system and connected each other by using internet connections. Parameters are available in Table 3.2.

Table 3.2. Configuration of the experimental setup.

Machine	No of CPU	Memory	storage	OS
GABC-VM	2	3GB	40GB	Ubuntu-18.04.4-desktop-amd64
LABC-VM	2	3GB	30GB	Ubuntu-18.04.4-desktop-amd64
CH-VM1	1	2GB	20GB	Ubuntu-18.04.4-desktop-amd64
CH-VM2	1	2GB	20GB	Windows 7 Ultimate (64 Bit)

Another VM is configured with the same programs and considered as an LABC-VM. The LABC-VM is a member node of the GABC and it is able to perform transactions on the GABC by using metamask wallet installed in the Firefox web browser. By using RPC metamask is connected to the virtual private blockchain hosted in the VM. During new vehicle's registration, two transactions are generated by LAC for two different blockchain, one to store the details of the vehicle in the GABC and another to store public keys and types of the vehicle in the LABC.

All the local CHs are the members of the LABC. To represent the CHs, two more VMs with two different OSs are configured. As a member CH will download all the contents of the LABC. During vehicle registration in the cluster, these CH-VMs use metamask wallet to perform search operations in the LABC. Whenever a vehicle become CH, it becomes a member of the LABC and will download all the transactions i.e., local vehicles' public keys and types. All the necessary programmings for vehicle authentication during cluster joining and temporary access permission are written by using solidity which is a popular language to write smart contracts. The program for the GABC consists of two functions, first one to add a new vehicle in the blockchain, second to view or search the existing public keys from the database. All the LACs are connected to the servers through high speed 5G internet connection.

For LABC, three functions are used by the LAC, one to store the public key and type information of vehicles (during registration) the second one to add vehicles from another LAC (temporarily) and the third one to view or search for the public keys. CHs are the members of the LABC with view permission only. CHs also use the search function to check the authentication of the vehicles during cluster joining process. There is another function which performs automatically when a timeout occurs. Whenever a visitor vehicle joins another LAC, it requests a required time period. After the timeout, the disabling function runs automatically which generates a transaction to disable the entry of the visitor vehicle. This one is used to reduce the storage requirement and all the members (LAC and all the CHs) updated their storage accordingly.

During cluster joining, after receiving the public key and type of the requested vehicle, the CH generates a transaction to search for the public key in the LABC. The LABC is hosted in the LABC-VM, which performs the searching and provides the result. If the public key is found, the CH will store the key in the CM list and starts communicating as a member.

For temporary access permission, vehicle’s own LAC sends a request with the vehicles public key, type and requested time period. After receiving the request, the destination LAC will generate a search transaction in the GABC and temporarily registers the public key in the LABC. The smart contract is written in such a way that after the requested time period a transaction will automatically generate which disables the entity from the LABC.

3.6. Performance Analysis

3.6.1. Performance analysis of the authentication protocol

To ensure secured authentication whenever a vehicle wants to join in a cluster, the CH will check the validity of the requested vehicle’s public key from the LABC. The communication between the CH and the blockchain server is secured by RSA-1024 PKI algorithm. Before sending the public key of the requested vehicle, the CH digitally sign that by using its private key and send a search request to the blockchain server. The server decrypts the message, perform a search in the blockchain and sends results by signing it with its own private key. The result will be only 1 bit to confirm the authentication where 0 and 1 represent not found and found respectively. For faster authentication RSA-1024 digital signature algorithm is used as it lightweight and provide comparatively strong security. RSA-1024 has a security strength of 80-bits which signify that it is required at least 280 operations to guess the private key [37]. In the proposed ACB-MAC method vehicles use high-speed 5G internet connection and thus it required ignorable time. We can say that because of 5G technologies the proposed method performs authentication in real-time. Moreover, some proposed method use Road Side Unites (RSUs) to handle the authentication but those infrastructures are too much costly.

3.6.1.1. Computational overhead

For the ACB-MAC system its require 1.48ms to sign and 0.07ms (total 1.55ms) to verify a signature generated by RSA-1024 digital signature algorithm for a 1.5GHz processor [38]. In [59], Zhang et al. used Elliptic Curve Digital Signature Algorithm (ECDSA) where the average computational time required for the server is 2.5ms and for the client it is 0.37ms. Lin et al. also used ECDSA where their proposed method has an average computational latency of 3.6ms for sign and 7.2ms for verification (total 10.8ms) [60]. Li et al. presented a blockchain based key management schema where they used the Elliptic Curve Integrated Encryption Scheme (ECIES) which also provides 80-bit security. They calculated the signing and verification time as 0.51ms and 1.10ms respectably (total 1.6ms) in a machine configured with Core i5 and 8GB of RAM [61]. However, in [62], Wang et al. proposed two different methods which are authenticated during joining and handover. It took an average of 10ms and 20ms for initial and handover authentication respectably. The proposed method performs better than [59,60,61,62]. Figure 3.8(a) shows the comparison between different previously proposed methods.

During registration, the LAC is responsible to generate keys for the vehicles. A computer with a 3.1GHz processor and 4GB memory will require only 97ms to generate keys for a vehicle [37] which means it is possible to generate at least 10 keys in every second. To search for a vehicle during authentication for a dedicated blockchain server and then to encrypt one bit of data before sending the response are require a few milliseconds. Moreover, to reduce the searching time we have used vehicle type so that if there is a query for an emergency vehicle (type 1) the search engine will not search for vehicle type 0. Thus if there are 10% EV exists in a database, the search for the EV will become 10 times faster than a database where all the vehicles are not classified. By this way, proposed method ensures faster authentication for both vehicle types.

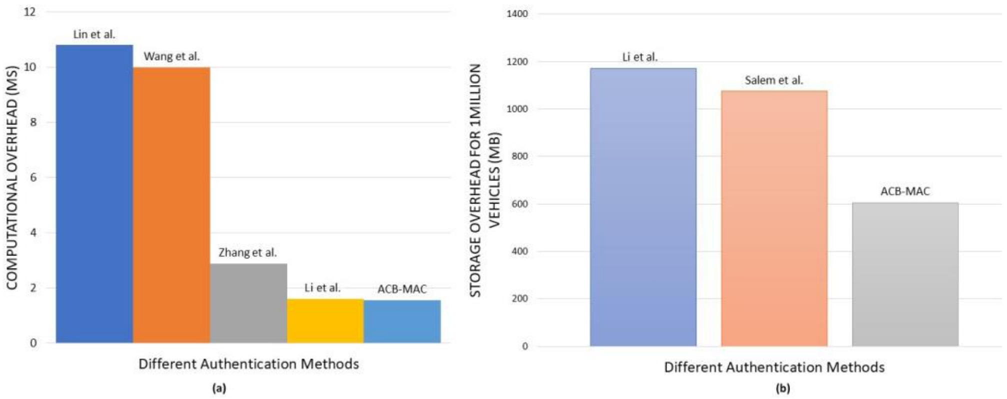


Figure 3.8. (a) Computational and (b) storage overhead comparison with the proposed ACB-MAC protocol

3.6.1.2. Storage overhead

In the ethereum platform, a typical blockchain header is approximately 508 Bytes [40] and each of the blocks can store one transaction. Thus to store one public key (generated by RSA-1024) of a vehicle it requires approximately 636 bytes (508byte header + 128byte public key). Thus for a LAC with 1 Million vehicles require only 606MB of storage. Similarly CHs have to store the same information thus they also require similar storage. In [61], it require 1172.3MB to store 1 Million identity information of the vehicles and 810.3MB for data total 1982.6MB. While in the proposed method of Salem et al. it requires 1126 bytes for vehicle authentication i.e., 1.05GB of storage required which is double than our proposed method [63]. Figure 3.8(b) shows the comparison between different previously proposed methods. Thus a vehicle may require at least 606MB of storage to become a member of a LACB which is a very small amount to ensure security, authenticity, privacy etc. of vehicles and it is minimum than the mentioned methods.

3.6.1.3. Propagation delay

The enhancement of internet speed in the 5G technology enables faster communication between vehicles and infrastructures. To transmit an ethereum block it will not even take a millisecond. However, when a vehicle becomes CH, it has to download the registered vehicles information as a member of the LABC. To download data for 1 million vehicles i.e., 606MB of data it will require less than 5 seconds with a download speed of only 1 Gbit/second.

3.6.2. Performance analysis of VSN

To analyze the performance of safety and non-safety messages we considered n number of vehicles moving through a multi-lane road. In this section, we are going to present throughout, PDR and delay of the transmitted messages and compare them with traditional MAC protocols. All the required equations are derived previously in [2].

3.6.2.1. Throughput analysis

To calculate the throughput of the safety and non-safety messages we have considered S as the normalized throughput and presented by the following equation (derived in [2]).

$$S_K = P_S P_{busy} L / T_e = P_S P_{busy} L / P_i T_{slot} + P_{busy} P_S T_S + P_{busy} \, (1\text{-}P_S) \, T_C \tag{3.1}$$

Here, P_s = Probability of successful transmission, P_{busy} = At least one transmission is in progress, L = Transmitted packet length, P_i = Probability that the channel is idle, T_{slot} = Slot time, T_e = Expected time to spend in a state, Tspan = Time span of slot, T_s = Time span for successful transmission and T_e = Time span if there is a collision. From this equation normalized throughput for SMT for kth cluster can be presented as:

$$S_{ksm} = \frac{(x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)}L}{(1-P_{(t-cl)})^{(x-1)}T_{slot}+(x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)}T_{s-sm}+[(1-(1-P_{(t-cl)})^{(x-1)})-((x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)})]T_c} \tag{3.2}$$

And for NSMT it can be presented as:

$$S_{knsm} = \frac{(x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)}L}{(1-P_{(t-cl)})^{(x-1)}T_{slot}+(x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)}T_{s-nsm}+[(1-(1-P_{(t-cl)})^{(x-1)})-((x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)})]T_c} \tag{3.3}$$

From these equation we can calculate the normalize system throughput of the system can be presented as:

$$S = \sum_{k=1}^{j} S_k \tag{3.4}$$

3.6.2.2. PDR analysis

PDR is dependent on the maximum retransmission limit. Thus for SM if M_{rsm} is the maximum retransmission limit then PDR of SMT will be:

$$PDR_{sm} = (1 - P_S)^{M_{rsm}} \tag{3.5}$$

And if M_{rnsm} is the maximum retransmission limit then PDR of NSMT will be:

$$PDR_{nsm} = (1 - P_S)^{M_{rnsm}} \tag{3.6}$$

3.6.2.3. Delay analysis

The time required to transmit a message successfully is considered as delay. However, the unsuccessful transmission's i.e., packet drops or collisions times are not considered for calculating the average delay. The average delay E[D] can be presented as:

$$E\,[D] = E\,[T_{interval}] – [P_{fdrop} / (1-P_{fdrop})]\,E[T_{drop}] \tag{3.7}$$

Here, $T_{interval}$ = average time interval between two successfully received packet P_{fdrop}= possibility of packet drop $E[T_{drop}]$ = average time of a dropped packet

From this equation we can present the mean packet delay for SM as:

$$E[D_{nsm}] = T_e\,(n – P_{drop} / (1-P_{drop})\,.\,2 / (1+CW+M_{rnsm}\,CW/2)) \tag{3.8}$$

And the mean packet delay for non-safety messages can be presented as:

$$E[D_{nsm}] = T_e \, (n – P_{drop} / (1-P_{drop}) \, . \, 2 / (1+CW+M_{rnsm} \, CW/2)) \quad (3.9)$$

3.6.2.4. Numerical analysis and discussions

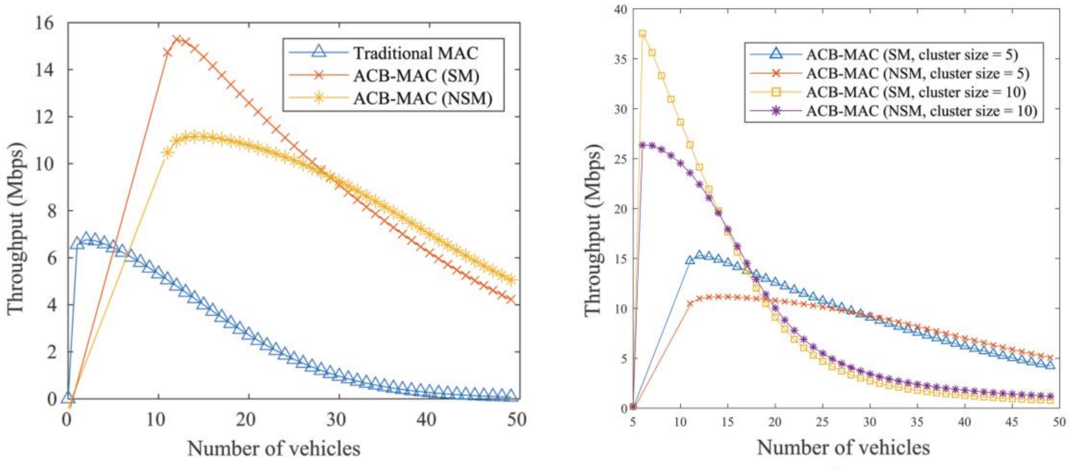
To present the performance of the ACB-MAC protocol a numerical analysis is performed by using MATLAB. numerical research is performed. Where each road width is 5 m, a VANET of randomly distributed cars driving thru a two-lane road is considered. In a cluster, we assume that all the vehicle are moving with a speed of 100 km/h. The performance of traditional MAC protocol according to IEEE 802.11 standard is also included in the numerical analysis to compare it with the proposed method. Besides, a quantitative comparison is described with previous methods based on clusters. The value of variables used in numerical analysis is given in Table 3.3.

Table 3.3. Data used for numerical analysis.

Parameter	Symbol	Value
Slot time	Tslot	20 (μs)
Propagation delay	Tdelay	1 (μs)
DCF & Short Inter-frame space	DIFS, SIFS	50, 10 (μs)
Size of the packet	Lh, L	50, 512 (bytes)
Control messages	RTS, CTS, ACK	27, 12, 14 (bytes)
Control messages	RTCF, ReTCl	26, 28 (bytes)
Transmission range, arrival rate	Rc, Rd, λ	1, 11, 0.5 (Mbps)
Maximum retransmit limit	Mr, Mrnsd	7, 7
Number of vehicles	n	50
CW size	W	64
Transmission range	R (m)	500
Traffic density	DT	0.5 (veh/m)
Vehicles velocity	v	100 km/h
Average inter-vehicle distance	β	10 (m)

Figures 3.9(a) and 3.9(b) display the changes in the system throughput with the increment of the number of vehicles and also with the with different cluster sizes,

respectively. The cluster size in Figure 3.9(a) is 5. It is evident that in the ACB-MAC protocol for both SM and NSM, there is a substantial improvement in throughput. Although the number of vehicles increases within a certain range, since it does not create many collisions, the throughput improves. However, as the number of vehicles continues to increase, extra packets can fight for transmission, causing more collisions and deteriorating throughput.



(a) (b)

Figure 3.9. (a) Comparison of throughput against number of vehicles and (b) throughput of the proposed method under different cluster sizes

In addition, figure 3.9(b) indicates that the throughput depends on the cluster size also. For the clusters with big amount of vehicles, the probability of packet collision is high which will minimize the throughput. On the other hand, for a cluster with small amount of vehicles are not able to utilize the available bandwidth. Since CH transmits the urgent notification to all CMs instantly without channel contention via the control channel (CCH) and there is no need to send RTS, so awaiting for CTS is not necessary. NSM is, however, targeted for a CM, not for all CMs. NSM would, therefore, not be broadcast. After RTS and CTS delivery, NSM will be transmitted to the intended CM to prevent hidden node issues and to confirm that the CM is still in the cluster.

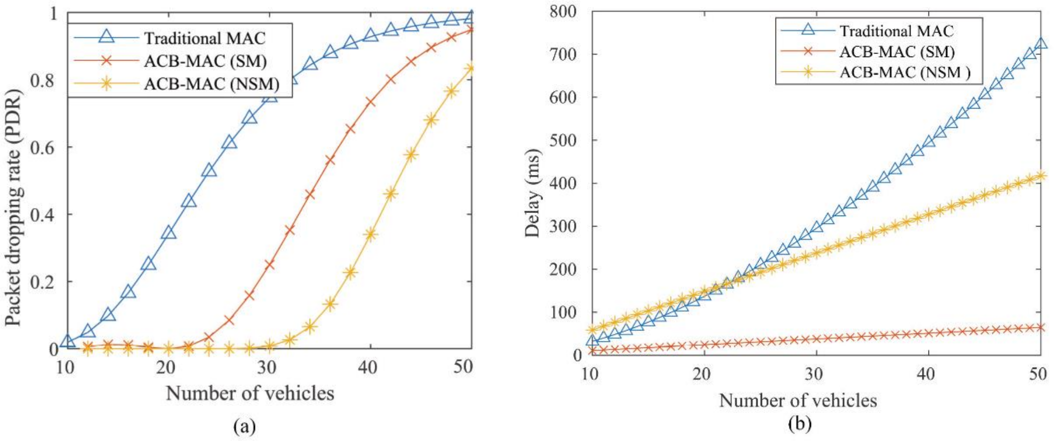


Figure 3.10. (a)PDR and (b) Delay of the proposed method against number of vehicles

The PDR against the number of vehicles is displayed in figure 3.10(a). The PDR of NSM is considerably less than the conventional MAC for the same retransmission number. Although the PDR of SM is smaller than the traditional MAC that is more than NSM since the retransmission threshold for NSM is lower, and without RTS / CTS delivery, SM is transmitted instantly. While PDR of SM are larger than NSM, until all ACKs are obtained, SM can be retransmitted. The average delay of the packet versus the number of vehicles is shown in Figure 3.10(b). As the number of vehicles increases, the average packet delay increases significantly. The risk of collision as well as PDR and delay increases with the increment in the number of vehicles. When the traffic is less, delay of NSMT is little higher because of RTS/CTS, but the delay becomes less than traditional MAC as traffic rises. The latency for transmission of SM is lower than traditional MAC, however, and the ACB-MAC protocol reaches the 100 ms latency requirement for SM.

In the same network model, the overall throughput attained against the number of vehicles in developed cluster-based schemes is approximately 1.1 Mbps, 1.3 Mbps and 11 Mbps, respectively, for [11,14,56]. In the CB-MAC protocol, on the other hand, the maximum throughput is about 15 Mbps. In [10], the latency for SM is 151 ms that is more than the requirement of latency of SM. The average delay is larger than the SDR [13]. It is clear that the proposed method continuously maintain high throughput as well as the SDR of 100 ms for SMT.

3.6.3. Discussions

The proposed method successfully utilize a light weight digital signature method to ensure security services like authenticity, non-repudiation, privacy preservation, confidentiality, integrity and attack prevention (discussed in the next section). Additionally, the computational overhead of the proposed authentication method is only 1.55ms which outperforms some of the previously proposed methods ([59,60,61,62]). Moreover, the storage requirements for the proposed method is smaller than [61,63]. To increase the authentication efficiency the proposed method divided the vehicles into two types which increase the authentication speed by 10 times for EVs and 2 times for GV than the method where all the vehicles are together and 10% among them are EVs. This is a novel part of the proposed method and the efficiency will increase with the number of EVs. All the vehicles are using 5G high-speed internet connection thus the propagation delay during authentication is ignorable.

To remove the huge expanses of the RSU based VANETs, in this paper we proposed cluster-based VANET protocol for VSN by modifying some of the packet structures of the traditional MAC protocols. The proposed method divides the transmitted messages into two types to give priorities to the safety message transmissions. The updated packet formats and the quick broadcasting algorithm of the SMT ensures the SDR of 100ms. Additionally, RTS/CTS supported NSMT protocol removes the shortcomings of the hidden node problems to increase the throughput and to decrease the delay and PDR. With the help of numerical analysis, we also proved that Both the transmission protocols perform better than the traditional MAC protocols. Additionally, the proposed method provides maximum throughput of 15 Mbps which is better than some of the previously proposed methods for example [11,14,56].

3.7. Security Analysis

The security services provided by the proposed ACB-MAC protocol is discussed in this section. The security services provided by public key based digital signature method with the blockchain are the followings:

3.7.1. Authentication and non-repudiation

PKI based digital signature algorithm ensures the authenticity of the sender. Thus the identity of the sender during registration, cluster joining and guest permission process are authenticated. However, blockchain based storage system verify the authenticated vehicles. During any transaction in any of the blockchain, the vehicles and the LAC confirms its authenticity and non-repudiation by signing the messages using their private keys.

3.7.2. Preserving the privacy of the vehicles

All the vehicles are known by their public keys and their original identity including public keys is securely stored in their LAC. By this way, the real identities of the vehicles are preserved by LAC and it is safe until adversaries get access to the LAC. Moreover, the identity information is stored in encrypted form, thus the privacy of the vehicles are preserved strongly. Additionally, it is not possible to get the real identity even if attackers got the public-private key pairs of a particular vehicle.

3.7.3. Security, confidentiality and integrity of the transactions

All the transaction in the proposed ACB-MAC protocol is signed by the senders to ensures security, confidentiality and integrity of the information. RSA-1024 is used as the digital signature method which has a security strength of 80-bits which means at least 280 number of operations are required to break the keys [36]. All the transaction are checked by the hash value to ensure the integrity of the transactions.

3.7.4. Attack prevention

1. RSA-1024 digital signature algorithm is considered secured until the primary key is broken by the attacker [50]. So, the communication between the vehicles and LAC are theoretically secured in the proposed ACB-MAC protocol.
2. LAC ensures the physical identity and the blockchain is there for verification. This combination keeps the system safe from unauthorized or fake vehicles which protect the system from Sybil and other unknown source attacks.
3. The Proposed digital signature algorithm use hash value to confirm the integrity of the transactions thus any fabrication is the original content get caught and rejected. This feature keeps the proposed method safe from reply attack as well as from man-in-the-middle attack.
4. ACB-MAC is free from DDoS attack as no unauthorized vehicles can perform any transaction. Both physical and public key verification is required to become a member of a cluster.

3.7.5. Others

1. In the proposed ACB-MAC method blockchain is used to store authentication information in a decentralized and distributed environment. Additionally, blockchain stores data in a flexible way.
2. Ethereum is a platform independent and accessible by using metamask wallet [30] from Windows, MAC, Linux, etc. as well as from cellphone operating systems like iOS and Android.
3. All the vehicles information details are stored in a blockchain thus the information is free from single-point-of-failure and together ensure their robustness.
4. Blockchain is also famous for its hash based chronological storage technique which ensures tamper resistance and immutability of the authentication information of the vehicles.

5. All the members are treated equally by the blockchain to ensure fairness between the members. To provide additional and faster facilities to the EVs we have used other techniques outside the blockchain.
6. Smart contract is utilized to allow guest vehicles temporarily. It also allows removing the guest vehicles from the LABC automatically after the requested time period.

3.8. Conclusions

A cluster based method is presented in this paper to manage VSN where one of the vehicle become CH to manage the communication as well to check the authenticity of the vehicles during cluster joining process. For VSN, transmitted messages are divided into two categories, important information is considered as SM which must be delivered within SDR of 100ms where other general information messages i.e., the NSM get less priority than SM. To manage these types of messages two different transmission protocol are presented named SMT and NSMT protocols. Additionally, a multi-level vehicle authentication model is also proposed by using two blockchains. One of the blockchain is used to store the details information of the vehicles during registration called GABC and another to store minimum information to check the authenticity of the vehicles called LABC. Vehicles of a state are registered to their local authentication centers and a public-private key pair is assigned to them. During cluster joining and visiting outside the local area, the public key will be used as their identity. All the LACs are the member of the GABC and all the CHs under an LAC are the members of the LABC. Thus CHs are able to store the authenticated vehicles' information in their local storage to ensure faster member authentication. In the proposed method, to provide priority services to the EVs like ambulances, fire trucks, emergency medicine, etc. the vehicles are divided into two types which are general (GV) and Emergency (EV). This will help to increase the authentication speed by 10 times for EV and 2 times for GV than the method where all the vehicles are together and 10% among them are EV. In addition, whenever an EV joins a cluster immediately the corresponding CH generates an SM to inform all the members to clear the left lane and give free passage to the EV. By this way, EVs get faster treatment during authentication and movement. The communication between the blockchains and their members are encrypted by utilizing RSA-1024 digital signature algorithm to ensure the safety, security, integrity, confidentiality, etc. of the communication between vehicles and the blockchains. Additionally, blockchain provides robust, decentralized and distributes database service including security, flexibility, tamper-resistance, immutability, transparency, etc. We have tested the proposed authentication protocols by implementing them in VMs as a proof-of-concept and showed the computational, storage and propagation overhead by the authentication process. Results show that it requires 1.55ms time for the authentication process which is better than [59,60,61,62]. However, to store 1 Million vehicles' authentication information it requires 606MB which is minimum and less than the proposed method like [61] and [63]. Because of high speed 5G internet the proposed method requires ignorable propagation time. Moreover, internet based communication removes the high infrastructures' expanses. Mathematical and numerical analysis of the proposed message transmission protocols were also presented which shows the proposed method provides better throughput, lower delay and lower PDR from the traditional MAC protocols and other previously proposed method like [11], [14] and [56]. In future, we are planning to collect abnormal behaviours of the vehicles from their neighbour vehicles to perform behaviour analysis and to take actions against the vehicles with malicious or abnormal behaviours.

CHAPTER 4. A BLOCKCHAIN-BASED AUTHENTICATION PROTOCOL FOR COOPERATİVE VEHICULAR AD HOC NETWORK

The efficiency of cooperative communication protocols to increase the reliability and range of transmission for Vehicular Ad hoc Network (VANET) is proven, but identity verification and communication security are required to be ensured. Though it is difficult to maintain strong network connections between vehicles because of there high mobility, with the help of cooperative communication, it is possible to increase the communication efficiency, minimise delay, packet loss, and Packet Dropping Rate (PDR). However, cooperating with unknown or unauthorized vehicles could result in information theft, privacy leakage, vulnerable to different security attacks, etc. In this paper, a blockchain based secure and privacy preserving authentication protocol is proposed for the Internet of Vehicles (IoV). Blockchain is utilized to store and manage the authentication information in a distributed and decentralized environment and developed on the Ethereum platform that uses a digital signature algorithm to ensure confidentiality, non-repudiation, integrity, and preserving the privacy of the IoVs. For optimized communication, transmitted services are categorized into emergency and optional services. Similarly, to optimize the performance of the authentication process, IoVs are categorized as emergency and general IoVs. The proposed cooperative protocol is validated by numerical analyses which show that the protocol successfully increases the system throughput and decreases PDR and delay. On the other hand, the authentication protocol requires minimum storage as well as generates low computational overhead that is suitable for the IoVs with limited computer resources.

4.1. Introduction

Internet of Vehicles (IoV) is a revolutionary addition in the field of Intelligent Transportation Systems (ITS). Typical intelligent vehicles are equipped with On Board Unit (OBU), sensors, GPS, etc. where the IoVs have communication capabilities through high-speed internet (5G/6G). Initialization of internet facility with the vehicles could be utilized to increase communication efficiency as well to increase security requirements. Vehicular Ad hoc Network (VANET) could be formed by the nearby IoVs to share information with the neighbours. IoVs could pass emergency messages (EM) which include lane change information, collision warning, congested road information, accident prevention warnings, traffic signal violation, barriers, obstacles, safe distance warning, etc. and also general messages (GM) which include different types of web services, gaming services, information of nearby gas stations, parking, restaurants, hotels, advertisements, etc. The IEEE 802.11p standard provides the Control Channel (CCH) and Service Channels (SCHs) to enable the Vehicular Social Networking (VSN) between the nearby vehicles.

Because of high mobility, it is difficult to maintain a stable connection for the IoVs during communication which results in packet drop, link blockage, and delay. Thus, to improve the communication quality at present, most of the ITS communication protocols are available to increase the efficiency of communication while the authentication, reputation, privacy, and security are getting less importance. However, in today's world, security is an essential part of communications and establishes communication with un-authenticated IoVs are nothing but opening the path to accepting all types of security attacks. Thus, in this paper, a blockchain based authentication protocol is proposed which provides a digital signature facility to ensure confidentiality, integrity, and attack prevention supports so that IoVs can verify the authenticity of the neighbour IoVs before initiating a communication with them. Blockchain provides security services like encryption, signature, hashing, etc. Special features like decentralization, distribution, flexibility, robustness, temper-resistance, immutability, transparency, fairness, etc. help blockchain to become a prevalent tool to store various types of information for different types of applications

[4,5]. By default, Ethereum blockchain uses a Elliptic Curve Digital Signature Algorithm (ECDSA), but, in the proposed method, the RSA-1024 algorithm is used because it requires a comparatively smaller time.

Managing the communication by increasing the transmission rate and decreasing the link breakage, delay and packet dropping rate (PDR) are primary challenges for VANET researchers. Several protocols are proposed by the researchers for many years to achieve better solutions. Some of the protocols are there where the IoVs get services from Road Side Units (RSUs) which require expansive infrastructural expanses [27]. IoVs could get similar services (provided by RSUs) by using the internet. On the other hand, by utilizing the bandwidth provided by IEEE802.11p, it is possible to create VSN with the neighbour IoVs and the communication areas could be increased with the help of cooperative neighbouring nodes. In this paper, a cooperative protocol is proposed to increase the communication quality. The concept of the cooperative or helping nodes is while the service provider is far from a potential receiver i.e., does not have enough signal strength to receive services from the server/sender could relay that service/information on behalf of the server. Although some overhead is created during cooperation but still the throughput provided by the cooperative node is better than typical protocols' throughput. The proposed protocol take special care of the EMs so that it could be delivered to the receivers before 100 ms to maintain the Standard Delay Requirements (SDR) for EMs [2].

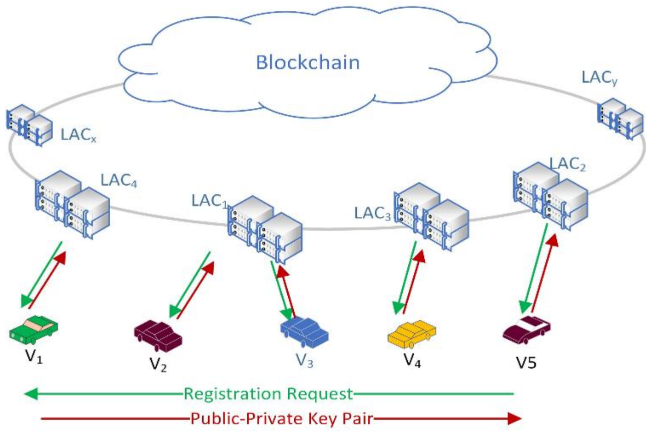


Figure 4.1. System structure and the registration process.

In the current novel coronavirus (COVID-19) pandemic, the busyness of the ambulance, medicine suppliers, and other related emergency IoVs become very high and thus it requires special support while providing emergency supports. Thus, in this paper, the IoVs are classified into two categories where all the emergency service providers are categorized as Emergency IoVs (EV) while the other IoVs are considered as General IoVs. This will make the authentication process of EVs faster; in addition, by utilizing VSN, it is possible to alert the neighbouring nodes so that they can provide a free passage to the EVs. All the IoVs are required to register in the Local Authentication Centers (LAC) to get the public-private key pairs which will become their identity for future communication with the blockchain. It will also help to preserve the original identity of the IoVs. All the LACs from a state are connected together as members of the blockchain and all the IoVs' registration information are stored as transactions. By this way, all the LACs have the information of all the registered IoVs in a state. The registration process is illustrated in Figure 4.1.

The contribution of the paper are as follows:

1. A blockchain based authentication schema is proposed so that, before accepting any information or service from any other source, IoVs will check the authenticity of the sender by sending a request to the blockchain. Blockchain is responsible for storing authentication information of the IoVs in a distributed fashion and supports digital signature based cryptography to ensure additional security services. IoVs have to register to their LACs to get key pairs. The public key of an IoV will be their identity during communication to preserve the privacy, and a private key will be used to send a request to the blockchain. The blockchain server will provide the reply in the form of 1 and 0, which means authentic and not-authentic, respectively.
2. To increase the range as well as the quality of communication, a cooperative communication protocol is proposed where IoVs can become helper nodes to relay a message or service on behalf of the original sender to those IoVs who do not have a strong communication link with the sender. All the receiver

IoVs will check the authenticity of the service providers as well as the helper node before accepting any message or service. An optimization algorithm is also proposed to select the best helper node.

3. To increase the authentication speed, IoVs are divided into two types where emergency service providers are considered as EVs. Moreover, transmitted messages or services are also divided into two types and important information is considered as EMs and get priorities during transmissions and are delivered before 100 ms. To remove congested traffic for the EVs, EMs are broadcasted so that the nearby IoVs can give free passage to the EVs.

Previous research works related to authentication protocols for VANETs and cooperative VANET methods are presented with the motivation of the proposed method in Section 4.2. In Section 4.3, the structure of the blockchain based authentication schema is presented with the cooperative model of VANET. Section 4.4 provides the implementation details and, in Section 4.5, performance and security analysis of the proposed protocols are explained. Section 4.6 discusses the pros and cons of the proposed protocols and, finally, in Section 4.7, the paper is concluded by mentioning some of the possible future works.

4.2. Previous Works

The exclusive set of features available in the blockchain makes the researchers interested in utilizing it in various fields. For example, blockchain is utilized by industry 4.0 [64,65], Internet of Things (IoT) [66], Smart grid [55], transportation services like smart airports [67], smart medical [68], etc. to increase security, decentralization, trust, etc. Similarly, by collaborating with EDGE computing, cloud storage, and other mobile services, the efficiency, availability, and reliability of blockchain based systems are increased. Utilization of blockchain in ITS is also increasing to get similar advantages to provide source authentication [69], trust and reputation management [70], event and message exchange management [21], intelligent payment [58], traffic investigation [71], etc.

To ensure the authenticity of IoVs or IoVs, several authentication methods were proposed previously. Some of the researchers proposed Certificate Authority (CA) to authenticate IoVs where some of them utilize blockchain for authentication. For example, to increase the efficiency of the authentication and handover process, Lai et al. proposed SEBGMM, where blockchain is used to share information between vehicles, routers, and control databases [24]. In [3], Ali et al. use a couple of blockchains to store authorized and unauthorized vehicles information separately. However, to remove the overhead of certificate based system, Ali et al. proposed a certificate-less authentication protocol. Similarly, in [25,26], two different blockchains store certified and revoked vehicles' information where another blockchain is there to store the transmitted messages between vehicles. Not only the vehicles but also the infrastructure's trust information are stored in a blockchain to develop an intelligent payment system in [58]. Before any transaction, both the cash counter and the driver check the authenticity of each other, and the transaction information is also stored in the blockchain.

In [16], Javaid et al. use CA for authentication and blockchain to store the authentication information, but did not mention the sign and verification overhead. In [15], Zhang et al. proposed a blockchain based storage system where authentication information is stored with their position, location, and direction information. Additionally, to store the reputation information, all the rule violations are also added in the blockchain. However, the certificate generation, sign, and verification create high overhead.

Storing authentication information and preserving the privacy of the vehicles' blockchain are used in [57]. To increase the security services, the method generates high computational overhead. Similarly, several other protocols like [15, 61, 86, 87, 88, 89] require a lot of time to complete their authentication process. In addition, storing the authentication information of the vehicles with a proposed method by Li et al. and Salem et al. requires a lot of storage space [61, 63]. All of the above mentioned protocols depending on the RSU demands expensive infrastructural supports [27]. However, typical certificate based protocols create higher overhead where the blockchain based system with light-weight encryption generates less overhead and additionally provides extra facilities of typical blockchain [69].

To increase the reliability of communication and enhance the VSN area, the efficiency of cooperation is already proven [72]. Several types of cooperation protocols are presented by the researchers to improve the performance of VANETs. In [73], a cooperative method is proposed for cluster based VANET, which is suitable only for Emergency Message Transmission (EMT). However, cooperation can be formed only if the channel is free. Woo et al. proposed a cooperative protocol applicable for EMT only, and the effect of mobility is not considered [73]. The proposed method by Taghizadeh et al. is also for EM only but unable to fulfil the SDR of 100 ms [71]. Similarly, the concurrent transmission based MAC protocol by Zhang et al. also does not fulfil the SDR and is suitable only for GMTs [75].

In [35], Zhou et al. presented a cooperative schema by using Request to Send/ Clear to Send (RTS/CTS) mechanism, but it creates additional overhead in the channel, and the possibility of collision is increased. However, the RTS/CTS based method is not suitable for EMT. In [77], a cooperative downloading protocol was presented and, in [78], a relay broadcasting is presented to increase the availability of resources but none of them discloses the delay of their transmission protocol.

The proposed cooperation method by Bharati et al. is based on Time Division Multiple Access (TDMA) which supports point-to-point (P2P) communication only [79]. Therefore, it is not possible to broadcast EMs and communication will be stopped while there is no available time slot. However, an enhancement of the proposed method in [79] is presented in [80], where the time slots are utilized more efficiently. Similarly, Zhang et al. presented cooperation where TDMA is used with central supervision [81] and, in [82], Omar et al. presented a method called VeMAC that is also based on TDMA. However, because of mobility, VANETs are in a dynamic nature and thus TDMA protocol are not able to manage radio resources efficiently, which results in additional delay and minimized throughput [72].

Thus, a protocol that can manage both emergency and general messages, and will be efficient in terms of throughput, and have minimum delay and PDR is required. Proper resource utilization and fulfilling the SDR is also required to be considered while managing VANETs. On the other hand, to utilize cooperation efficiently, proposed management is required and cooperation should only be used when it is necessary.

4.2.1. Problem statements and motivations

1. Avoiding malicious or bad intended vehicles involved in the VANET authentication of the vehicles is required. To ensure the authentication of vehicles for VANETs, several methods were presented, but blockchain based systems could be a better option with additional features like decentralization, distribution, flexibility, robustness, temper-resistance, immutability, transparency, fairness, etc. Regular certificate based protocols are not able to provide all these features together.
2. To ensure the security of the communication, an encryption method is crucial, but blockchains usually use strong digital signature methods for encryption, which required a good amount of computational time to perform. For example, ECDSA is used by a Ethereum blockchain which required nearly 10 ms to perform one signature and verification [42]. To minimize that a light-weight encryption algorithm like RSA-1024 could be used will provide a security strength of 80 bits and require one-third the time of ECDSA [68].
3. Preserving the privacy of the vehicles is required because identity theft could be performed by malicious entities to perform illegal activities by using it. Hiding the original identity of the IoVs' could use public keys that can be assigned by the registration centers during registration. The real identities should be mapped with the respective public key and stored in a secured place will preserving the privacy of the IoVs.
4. All of the transmitted messages are not the same in terms of importance. Thus, it requires to handle EMs separately by giving high priorities.

Moreover, the performance of the GMT is also important in order to maintain by minimizing the delay, collision, and PDR.

5. In the previously proposed papers, all the vehicles get equal priority, and there is no special priority for the emergency service provider vehicles. Classification of vehicles will add extra optimization, and ensuring priorities for the emergency IoVs during authentication and driving as well as classification of message or service types also provides priorities to the emergency messages during transmissions. Handling EVs separately by giving them preference while driving can help with performing emergency tasks quickly.
6. As cooperation can increase the reliability and range of communication, it could be used for VSN. A cooperation protocol is required to be well managed to increase the throughput by minimizing the delay and PDR. Moreover, it requires handling both the general and emergency messages separately and to ensure SDR for EMs.
7. Many of the previously proposed protocols utilize RSU for various support like computational, storage, management, etc. However, it requires additional infrastructural cost to construct RSU and maintain. On the other hand, ITS with internet facility could remove the expansive infrastructural cost of RSU by using EDGE computing services or from servers situated anywhere in the world.

These are the motivations of this research work and all the mentioned points are addressed in the proposed method and proved their efficiency in terms of performance and security.

4.3. System Structure

Intelligent vehicles with internet connectivity i.e., IoV from the nearby area, could form a VSN between themselves by performing direct or cooperative communication (when required). For the proposed method, it has been considered that all the IoVs are equipped with an OBU with data processing and wireless communication facilities, GPS, sensors, and internet connection facilities. These are the basic requirements and, without these, vehicles can not use the facilities offered by the proposed protocol.

There are four main components of the proposed system. In the first part, the registration process is discussed. Whenever an IoV requires a road permit, it has to register with the LACs. LAC then add details of the registered IoVs as blockchain transactions so that all the member LACs can get the authentication information of the IoVs. The second component is the blockchain based authentication process. The cooperative communication protocol is the third component of the system and discussed how, when, and in which situation the cooperation is required. As the fourth component, details of the VSN with the classification are explained.

4.3.1. Registration and classification of IoVs

All of the IoVs register to their Local Authentication Centers to participate in the VANETs. LACs are responsible to generate public-private key pairs for them and to preserve their privacy, IoVs will use their public keys as the identity for all types of communications. LACs will register IoVs with all required information and generate a blockchain transaction to store those in the database. All of the LACs of a state or country will get the information immediately as a member of the blockchain. All the LACs preserve a copy of all registered IoVs' information to form a distributed and decentralized system. The registration process is illustrated in Figure 4.1.

In VANET, typically all the IoVs are treated equally. However, in real-world emergency service, providers need priorities to ensure quick and efficient services. For example, in these pandemic situations, ambulances together with emergency medicine, face masks, sanitation products, COVID-19 test kits and equipment suppliers require priority services while moving. This is why the classification of IoVs is presented to give priority to the EVs. During registration or later by submitting proper documents, an IoV can be recognized as EV. To implement this, a field called type is added in the database. Other emergency service providers like fire services, civil defence, police, and VIPs could also be considered as EVs.

While driving, the EVs continuously broadcast EMs by informing the nearby IoVs that there is an existence of an EV nearby and therefore please clear the left lane and give free passage to the EV. After receiving the EM, the neighbour IoVs will clear the lane for the EVs and perform their emergency services.

4.3.2. Authentication process

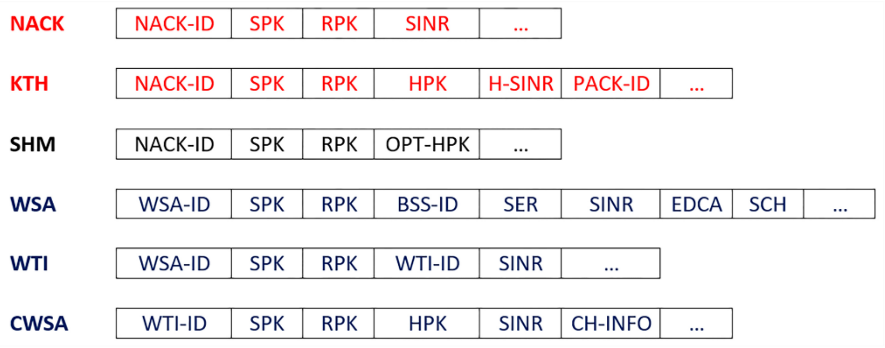
In the proposed method, there are two ways (direct and cooperative) to participate in a VSN. While driving, an IoV may receive a message or service advertisement from another source (vehicle, infrastructure, etc.). Before establishing a communication with the sender to check the authenticity of the sender, the receiver will request from the nearby LAC by sending the sender's public key (SPK) and type (T). The server will perform a search operation in the blockchain to check the existence of the SPK in the database and send a response with the requested SPK and 0 or 1 to inform the authenticity. The receiver will take action after getting the confirmation from the server. Similarly, while getting cooperation requests or any other requests, the IoVs must check the reliability of the sender. As a decentralized system, an IoV can get the authentication checking service from all over the country and the LACs can provide instant replies within some milliseconds by just performing a lookup operation for their local storage. Optimizing the authentication process sender will check the authenticity of only the optimal helper. Details of the authentication will be explained in Section 3.4 with the cooperation details.

By default, in the Ethereum blockchain, all the communications between the blockchain server and the members are encrypted by using ECDSA [83]. However, in the proposed system, it has been replaced by a lightweight digital signature algorithm RSA-1024 which provides 80-bit security and is pretty good for light-weight devices [37].

4.3.3. Cooperation details

By utilizing the IEEE 802.11p, IoVs can create or participate in a VSN. However because of the high velocity of the IoVs, it is always a challenge to maintain a stable network connection while communicating. By using cooperation, it is possible to increase link reliability and the efficiency of the communication [84]. However, cooperation naturally creates extra overhead, duplication, etc., thus it requires proper management to get the best from the cooperation [72]. In this paper, a mixed protocol is presented by combining direct and cooperative communication together. The dynamic nature of VANET supports both of the protocols. For random access, according to IEEE 802.11p, the CSMA/CA approach is utilized to avoid packet collisions.

To support cooperative communication protocol, some new control packets are introduced, those are NACK, KTH, SHM, WSA, WTI, and CWSA. The detail packet structure is illustrated in Figure 4.2 and will discuss details of it in Section 4.3.4.



NACK	NACK-ID	SPK	RPK	SINR	...				
KTH	NACK-ID	SPK	RPK	HPK	H-SINR	PACK-ID	...		
SHM	NACK-ID	SPK	RPK	OPT-HPK	...				
WSA	WSA-ID	SPK	RPK	BSS-ID	SER	SINR	EDCA	SCH	...
WTI	WSA-ID	SPK	RPK	WTI-ID	SINR	...			
CWSA	WTI-ID	SPK	RPK	HPK	SINR	CH-INFO	...		

Figure 4.2. Proposed packet structure for cooperative communication.

4.3.4. Direct or cooperative communication?

When direct communication (DC) is possible, cooperative communication (CoC) is a waste of resource, time, etc. However, when DC is not possible because of distance or weak network connections, a helper node who has good link connections between the sender (S) and the receiver (R) could make the communication smooth and reliable. Thus, deciding to use DC or CoC is the first challenge. EMs are important and, if an IoV senses that there is an EM broadcasted in the network and somehow it could not receive it, it will initiate cooperation by broadcasting NACK. Neighbour node(s) who has a better communication link between the S and R can become a helper node to relay the EM to the receiver. In the case of GMs, if neighbouring nodes have better signal strength than a service provider, they may want to become a helper (H). The server (S) will check whether the helpers have better channel conditions than S, and it checks the helper signal for noise interference and the noise ratio (SINR) to select the optimal helper. In this way, only if the cooperation is necessary or if cooperation can provide optimized transmission will the VANET go for cooperation; otherwise, direct transmission will continue. Moreover, upon receiving any request from a neighbouring node, the IoVs first check the authenticity of that requesting IoV before establishing any kind of communication.

4.3.5. Vehicular social networking

IoVs can use their built-in wireless communication facility to form temporary social networking called VSN. VSN could be utilised not only for entertainment or general communication purposes but also for sharing important information or emergency messages. In the traditional IEEE802.11p MAC protocol, all of the messages get similar importance and are thus treated equally. Thus, to provide priority to EMs as well to ensure the reliability of the communication, some changes are introduced in the packet structures. To improve the communication efficiency of other general purpose messages or services, some modifications are also made in our proposed protocol. Additionally, as there is no security and privacy preserving authentication method available, a blockchain based authentication protocol is introduced so that the IoVs can get a secure environment while communicating with unknown IoVs.

4.3.5.1. Emergency message transmission (EMT)

Lane change information, collision warning, congested road information, accident prevention warnings, traffic signal violation, barriers, obstacles, safe distance warning, etc. are considered as EMs. All of the nearby IoVs must know about this information to avoid fatal situations. However, because of their high speed, it is sometimes difficult to receive the EMs. A helper node may come forward to solve this issue by retransmitting the message. In IEEE 802.11p, all the transmitted messages are treated as equal and there is no special treatment for EMT. Thus, in this proposed method, NACK is introduced so that, if any IoV does not receive an EM, it can broadcast NACK to all the nearby IoVs. If no NACK is received, the transmission is considered as successful; otherwise, the sender will resend the EM to the NACK sender with the help of a helper node. The complete process is illustrated in Figure 4.3 by using a sample scenario.

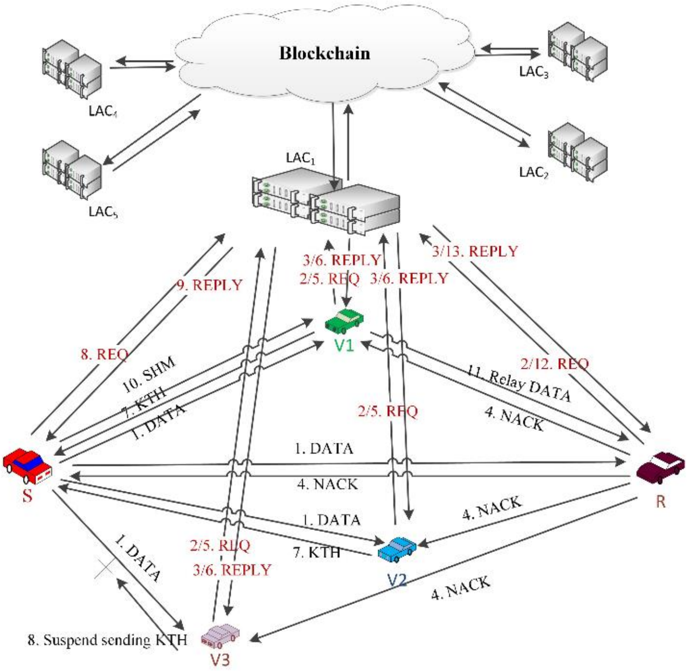


Figure 4.3. A sample scenario presenting EMT.

The complete process can be described as follows:

1. When an emergency situation comes, IoV (S) uses CCH to broadcast an EM. All of the receivers who receive that message will send the sender's public key (SPK) with the type of the IoV to the blockchain to get the authenticity of the S. A nearby local server will handle the request and search in the database and send authorization if it is found or un-authorized.

2. All the neighbouring nodes can sense that a message is broadcasted [79], but it may happen that, because of packet collision or weak network connections, a receiver (R) may not receive the EM. R will wait to receive it until Short Inter Frame Space (SIFS) and then broadcast NACK to its neighbours by informing that an EM transmission is unsuccessful.
3. A NACK packet includes a unique NACK-ID, public keys of the sender (SPK) and the receiver (RPK) and the SINR between them (see Figure 4.2).
4. S will wait for NACK until Ts (max time for successful transmission), and, if it does not receive any NACK within that time, it will consider the transmission to be successful.
5. The IoVs who receive NACK and want to help the receiver firstly check the authenticity of the NACK sender by sending a request to the blockchain. Upon getting confirmation of the R's authentication, it sends a Keen to Help (KTH) message to the sender by including NACK-ID, SPK and RPK. Helpers address (HPK) SINR between the helper and receiver and the packet id. KTH must be received by the sender within SIFS; otherwise, the transmission will be considered as successful, and no cooperation will be required.
6. Even after Ts sender can receive KTH, which also provides information about a failed transmission. From the KTH, the sender checks the authenticity of only the optimal helper i.e., the one that has the lowest SINR from the blockchain server. Then, S sends SHM to the helper by including NACK-ID, sender, receiver and selected optimal helpers' public keys. The sender stops receiving KTH from any other IoVs after sending the SHM.
7. For every fail transmission, there will be different NACKs and, based on SINR between the helpers, it may be different for the same receiver. The cooperation is initiated by the receiver, which ensures that cooperation is performed only when necessary and to ensure the reliability of the communication. A blockchain based authentication service ensures that no unauthorized or fake IoVs can interface with the communication. In Figure 4.4, a flow chart is given to show the steps. Blockchain based lightweight authentication protocol requires low computational time and storage. Thus,

before receiving any information from any vehicle or infrastructure, the authenticity of the sender needs to be checked to avoid spamming, Sybil, unknown source, DDoS and other security attacks. However, although the authentication process is adding extra time in the transmission, it is ignorable enough and ensures that the EMs will reach all the nearby IoVs within 100 ms.

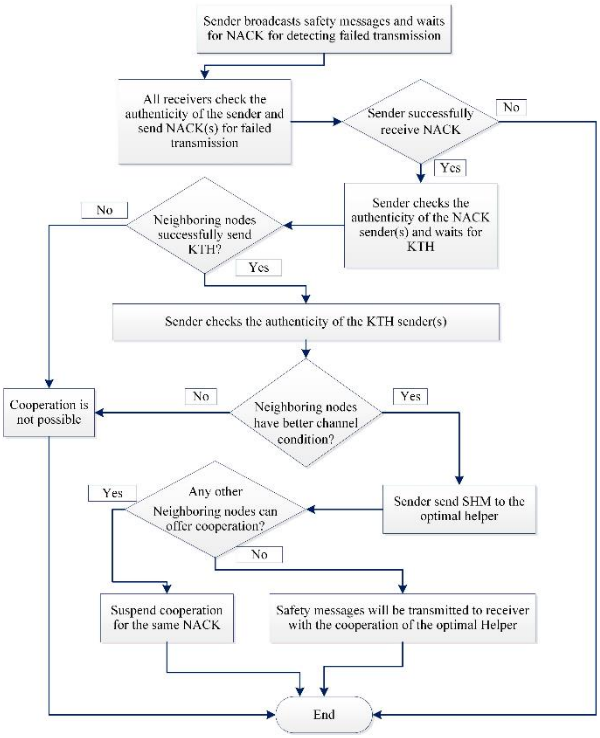

Sender broadcasts safety messages and waits for NACK for detecting failed transmission
All receivers check the authenticity of the sender and send NACK(s) for failed transmission
Sender successfully receive NACK
No
Yes
Sender checks the authenticity of the NACK sender(s) and waits for KTH
Neighboring nodes successfully send KTH?
No
Yes
Sender checks the authenticity of the KTH sender(s)
Neighboring nodes have better channel condition?
No
Yes
Cooperation is not possible
Sender send SHM to the optimal helper
Any other Neighboring nodes can offer cooperation?
Yes
No
Suspend cooperation for the same NACK
Safety messages will be transmitted to receiver with the cooperation of the optimal Helper
End

Figure 4.4. Flow chart of the proposed EMT protocol.

4.3.5.2. General message/service transmission (GMT)

Different types of web services, gaming services, information of nearby gas stations, parking, restaurants, hotels, advertisements, etc. are considered as GMT. It can be an IoV or RSU who offer services or want to send some information. It broadcasts the message or Wireless Access in Vehicular Environments (WAVE) service advertisement (WSA) by using the control channel. Interested IoVs may send Willing to Involve (WTI) to get the service. While an IoV is listening and planning to receive a service but facing weak network connections to communicate with the sender or server, a helper node (IoV or RSU) may come forward with better communication strength with the sender and the receiver. By this method, a cooperation process may start while transmitting GMT. The control messages will be transmitted by using CCH while the service will be transmitted by using the service channel (SCH). The complete process is illustrated in Figure 4.5 by using a sample scenario.

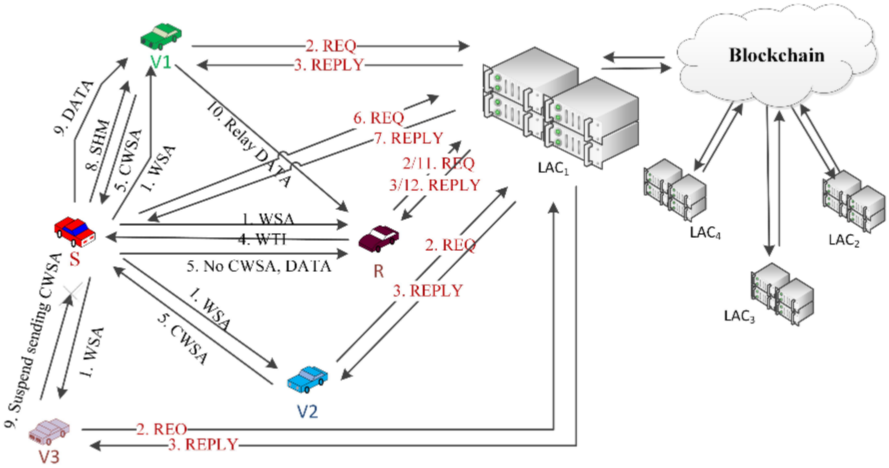


Figure 4.5. A sample scenario presenting GMT.

The complete process can be described as follows:

1. Whenever a sender or server want to offer a message or service, it broadcasts WSA by using the CCH. The WSA packet consists of WSA-ID, the public keys of the sender and the receiver, ID of the Basic Service Set (BSS-ID), Service ID (SER), SINR, the Enhanced Distributed Channel Access (EDCA), SCH of the sender, etc.
2. The interested IoVs can check the authenticity of the sender by initiating a search request to the blockchain server. After getting the positive confirmation from the authentication center, the receiver will send a WTI packet by including the WSA-ID, ID of the WTI (WTI-ID), SPK, RPK, SINR, etc.
3. If a potential receiver is not able to send Cooperative WAVE Service Advertisement (CWSA), the server will wait for a helper who has a better connection with the receiver.

4. A helper who wants to cooperate and have a strong connection between the sender and the receiver checks the authenticity of the receiver by using the blockchain. Then, it sends CWSA to the sender by including WTI-ID with SPK, RPK, helper's ID (HPK), SINRm channel information, etc.
5. A server will check the SINR of the helpers and discover the node with minimum SINR. Then, it will check the authenticity of the potential helper and send back SHM packet with the DATA. The server then transfers the data or general message or service to the helper, and the helper starts sending data to the receiver. The receiver checks the authenticity of the helper and then starts receiving by using a cooperative service.
6. After sending SHM to a helper, the server stops receiving any other CWSA with the same WSA-ID. In Figure 4.6, a flow chart is given to show the steps.

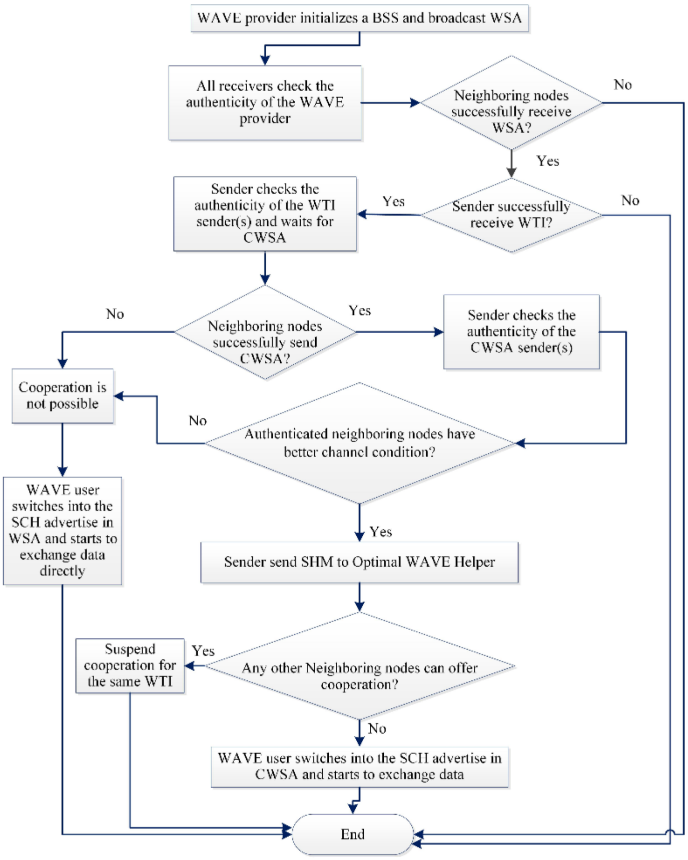

WAVE provider initializes a BSS and broadcast WSA
All receivers check the authenticity of the WAVE provider
Neighboring nodes successfully receive WSA?
No
Yes
Sender checks the authenticity of the WTI sender(s) and waits for CWSA
Yes
Sender successfully receive WTI?
No
No
Neighboring nodes successfully send CWSA?
Yes
Sender checks the authenticity of the CWSA sender(s)
Cooperation is not possible
No
Authenticated neighboring nodes have better channel condition?
WAVE user switches into the SCH advertise in WSA and starts to exchange data directly
Yes
Sender send SHM to Optimal WAVE Helper
Suspend cooperation for the same WTI
Yes
Any other Neighboring nodes can offer cooperation?
No
WAVE user switches into the SCH advertise in CWSA and starts to exchange data
End

Figure 4.6. Flow chart of the proposed GMT protocol.

4.4. Implementation

As proof of concept, the proposed blockchain based authentication protocol is implemented by using multiple virtual machines (VMs). To implement the above-mentioned scenario in Figure 4.3 and Figure 4.5, five VMs are configured to represent sender, receiver and three potential helper IoVs. A VM is also configured to represent a nearby LAC and a blockchain server. Configurations of the VMs are presented in Table 4.1.

Table 4.1. Implementation parameters for blockchain based authentication.

Machine	No of CPU	Memory	Storage	OS
LAC-VM	2	3 GB	30 GB	Ubuntu-18.04.4-desktop-amd64
IoV-VMS	1	2 GB	20 GB	Ubuntu-18.04.4-desktop-amd64
IoV-VMR	1	2 GB	20 GB	Ubuntu-18.04.4-desktop-amd64
IoV-VMH1	1	2 GB	20 GB	Ubuntu-18.04.4-desktop-amd64
IoV-VMH2	1	2 GB	20 GB	Windows 7 Ultimate (64 Bit)
IoV-VMH3	1	2 GB	20 GB	Windows 7 Ultimate (64 Bit)

For the blockchain server machine, truffle framework [28] is used which provides a client side development environment to write, run, and test scripts for the blockchain. Additionally, it also provides network management supports. To emulate an Ethereum blockchain, a well-known emulator Ganache [29] is used. Ganache provides all facilities of blockchain with customization, logging, and debugging supports. A Node Packet Manager (NPM) [31] is used to support JavaScript, and a node server [32] is used to implement the client side.

All the machines that represent IoVs use a Metamask [30] ethereum wallet to securely communicate with the blockchain. As Metamask is platform independent and also comes as an extension to almost all types of internet explorers, IoVs using any type of machine or operating system can thus connect with the blockchain without any complexity. In the experiment, multiple platforms are used to test the system compatibility.

A server side script is written in the form of a smart contract by using the solidity programming language. The script consists of two functions: one for IoV registration and another one for searching operation. The first one is used by the LAC when a new IoV comes for registration and another one can be used by any IoVs to query for the authenticity of another IoV. For request, the requesting IoV will add the SPK with its type and send to the server. The server will reply with the requested SPK and 1, i.e., authentic if the SPK is found in the database, or 0 i.e., unknown if not found. IoVs keep a list of the requests and responses in their local storage to avoid sending requests for the same IoV's authentication information.

4.5. Performance Analysis

Performance analysis of the proposed method is divided into two parts. In the first part, the efficiency of the cooperative transmission protocol is explained followed by the efficiency of the proposed authentication protocol.

4.5.1. Cooperative transmission protocol

The effectiveness of cooperative transmission to improve the reliability of communication in VANET is proved. However, it creates additional overhead and thus, without proper management protocol, it becomes inefficient. In the proposed method, some methods are applied to improve the efficiency of cooperative communication. Firstly, cooperation is used only when it is required; otherwise, the system performs direct communication and, secondly, classification of messages to ensure the priority of the EMs.

To test the VANET with randomly distributed N number of vehicles running on a multi-lane road, the normalized throughput of the proposed cooperative protocol (S) can be given as:

$$S = E_p/T_e \tag{4.1}$$

where Ep denotes the length of the transmitted payload and Te denotes the slot time. From this equation, the throughput of the cooperative communication can be calculated as:

$$S = P_s P_{busy} L \,/\, (P_h[(1-P_{busy})T_{slot} + P_{busy}P_sT_s + P_{busy}(1-P_s)T_c]) \tag{4.2}$$

Here, P_s = probability of successful transmissions, P_{busy} = probability to find that the channel is busy, L = length of the packets, P_h = probability of not getting a helper, T_{slot} = slot time, T_s = probability of successful transmission with cooperation and T_c = probability of collision.

If CA denotes the number of cooperation attempts, PDR can be given as:

$$PDR = (1-P_s)^{C}{}_{A} \tag{4.3}$$

Average packet delay can be given as:

$$E[D_{CT}] = T_e-CT\ [\ N - (P_{fdrop} * (W_0+1) / (1 - P_{fdrop}) * 2)\ ]. \tag{4.4}$$

where W_0 and P_{fdrop} denote contention window size and final packet drop probability, respectively. T_e is the Markov state time spent for a vehicle, which can be given as:

$$T_e = (1-P_{busy})T_{slot} + P_{busy}P_sT_s + P_{busy}(1-P_s)T_c \tag{4.5}$$

All the equations are proved and discussed in detail in [72]. Numerical analysis is presented in the next sections by comparing with the traditional MAC protocols. Data used for the analysis are presented in Table 4.2. For the numerical analysis, IoVs' speed is considered as 80 km/h, and they are moving in an ideal environment. The effect of velocity is not considered in this analysis, although variations of velocity may change the performance of the system. Moreover, the effect of velocity for vehicles' could be found in [72,85].

Table 4.2. Sample data.

Parameter	Symbol	Value
Slot time	Tslot	20 (μs)
Propagation delay	Tdelay	1 (μs)
DCF & Short Inter-frame space	DIFS, SIFS	50, 10 (μs)
Size of the packet	Lh, L	50, 512 (bytes)
Control packets	NACK. KTH, SHM	20, 26, 24 (bytes)
Control packets	WTI, WSA, CWSA	24, 25, 27 (bytes)
Transmission range, arrival rate	Rd, Rc, l	11, 1, 0.5 (Mbps)
Contention window size	CW	64
Transmission range	r	500
Lane width	W	5 (m)
IoVs density	DT	0 - 0.5 (veh/m)
IoVs velocity	v	80 km/h
Average inter-vehicle distance	b	10 (m)

4.5.1.1. Throughput

In the recommended procedure for both EM and transmission in VANETs, there is a major increase in throughput. Up to a certain extent, throughput rises, then throughput declines, as can be seen in Figure 4.7. For the analysis, Ph is considered as 0.5 in the normal case, Ph ≤ 0.4 as optimal and Ph ≥ 0.7 as the worst case. Since fewer IoVs do not cause crashes, with growing IoVs, throughput continues to increase, so, after the number of IoVs grows more, further IoVs may cause further accidents and decreases in throughput. It is also evident that the higher likelihood of having support would improve throughput, as the S-R connection would be more reliable to transmit the packet, and the transmission by cooperation will be quicker with good channel condition. Due to the availability of helpers, the throughput for the suggested protocol in optimum situations is higher than average. Nevertheless, owing to the unavailability of support, the opposite situation is viewed in the worst case. Through more aides, more collaboration benefits will be made.

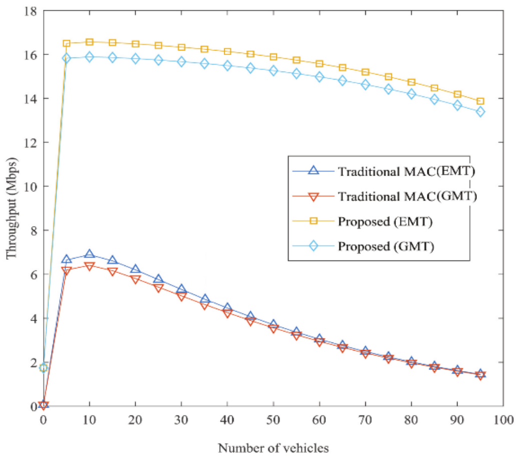


Figure 4.7. Throughput against no. of IoVs.

4.5.1.2. Delay

The average packet latency against the number of vehicles is seen in Figure 4.8. With the number of IoVs, the total packet delay grows when there are more packets to be transferred. These additional packets will compete for transmission in the same time slot for the channel, resulting in an increased channel busy likelihood as well as a probability of collision. Therefore, there is an increased average packet latency. Since this final packet drop possibility is minimized by the proposed protocol and the probability of effective transmission rises, the average packet delay is decreased.

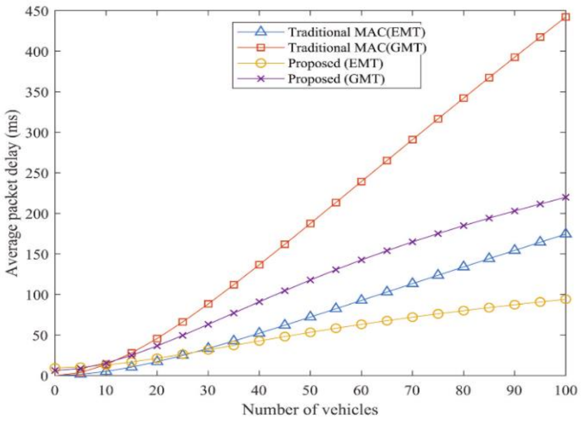


Figure 4.8. Delay versus no. of IoVs.

4.5.1.3. Packet dropping rate (PDR)

Figure 4.9 demonstrates PDR versus the number of vehicles. If the risk of crashes increases, PDR increases with the growing number of cars. The probability of packet arrival increases as there are more vehicular nodes, which would result in more accidents. The proposed protocol's PDR benefit is important. By decreasing PDR, the proposed protocol guarantees efficient transmission. In addition, a distinction is given between the various sizes of the contention window (W0). When W0 is greater, the increased back-off period decreases the collision and reduces the failure of the packet, thus decreasing the PDR.

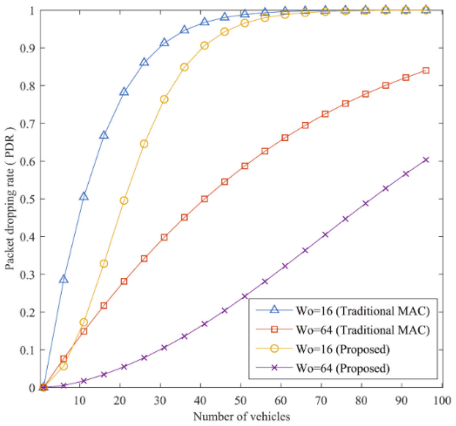


Figure 4.9. Comparison of the proposed method's PDR with traditional MAC.

4.5.2. Authentication Protocol

For VANETs, safe and secure communication is a basic requirement. Generally, vehicles can create a VSN with nearby vehicles by using built-in tools according to the IEEE802.11 standards. However, the protocol is unable to provide authentication or identity preservation facility. However, typical signature based authentication protocols require comparatively high configured computers to perform. Moreover, RSU based authentication protocols require an additional infrastructural cost. Thus, an authentication protocol is proposed by utilizing blockchain technology, and, by using an internet connection, IoVs can check the authenticity of the neighbour vehicles before starting communication with them.

4.5.2.1. Computational overhead

By default, Ethereum uses ECDSA for signature and verification while communicating with the member nodes. However, in the proposed method, the RSA-1024 algorithm is used instead of ECDSA to minimize the execution time. It requires 1.55 ms time for signing and verifying a message (1.48 ms for signing and 0.07 ms for verifying) by a 1.5 GHz processor [38]. Therefore, the total time required to send an authentication request and get the response is 3.10 ms. Moreover, for RSA-1024, key generation requires 97 ms [37]; thus, every second, 10 keys can be generated.

Traditional ECDSA is utilized by Lin et al. in their proposed BCPPA protocol, where it requires 3.6 ms to sign and 7.2 ms to verify, i.e., 10.8 ms to complete their authentication process [60], which is approximately three times more than the proposed protocol. Several certificate-based and other types of authentication methods have been proposed previously, which also require comparatively higher time than our proposed method. For example, proposed authentication protocol by Wang et al. (B-TSCA), Azees et al. (EAPP), Zhang et al. (DSSCB), Zhang et al. (IBV), Shao et al. (IBCPPA), and Xrongxing et al. (SPRING) required 10 ms, 12 ms, 13.5 ms, 14.7 ms, 15.9 ms, and 20.1 ms, respectively [62,15,86,87,88,89]. Comparison between these protocols are illustrated in Figure 4.10.

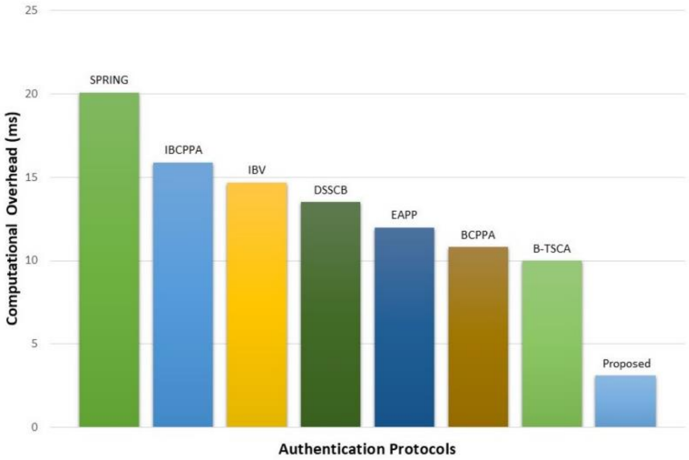


Figure 4.10. Comparison between time requirements of different authentication protocols.

IoVs can move anywhere in the country and can send a request to nearby LACs to get the authentication information of required IoVs. A member of the blockchain close to LACs stores all the IoVs information. Thus, they can provide immediate response only by searching its local storage. Searching requires ignorable time; however, proposed classification increases the efficiency of searching. If 20% of IoVs are EVs, the searching will be 80% faster for EVs and 20% faster for GVs.

4.5.2.2. Storage overhead

The information of every registered IoVs is stored as a blockchain transaction. Each Ethereum transaction requires 508 bytes [40]. It requires approximately 192 bytes (128-byte key + other information) to store IoV information; and the total storage requirements are 700 bytes. Thus, it requires 700 MB of space to store a million IoVs' information. A previously proposed method by Salem et al. and Li et al. requires 1073.8 MB and 1172.3 MB to store a million vehicles' identity information [60,61]. Therefore, the proposed method requires a lower amount of storage, and storing one billion pieces of IoV information requires only 68 GB of space.

4.5.3. Security Analysis

The primary objective of the proposed method is to ensure the security of the IoVs while communicating with each other. The security services provided by the proposed method are discussed as below.

1. The proposed method ensures the authenticity of the message or service provider vehicles. Whenever an IoV broadcast any EM, before accepting that message, IoVs first check the authenticity of that vehicle. Similarly, with the proposed schema, IoVs are able to ensure the authenticity of the help seeker and the helper too.
2. RSA-1024 provides security that provides security strength of 80-bits. Thus, it requires 280 operations to break the key that is strong enough for low power vehicles [36].

3. IoVs are registered with their real identity, but afterwards identified by their public keys. During any type of communication, IoVs use their public keys instead of real IDs, which preserve their privacy. The original identities are stored safely in a blockchain based secured system, and an attacker will not be able to get the real identity of the vehicles even if they got the key pairs.
4. The communication with the blockchain is encrypted by a digital signature algorithm that ensures security, confidentiality, integrity, and non-repudiation of the transaction. Encryption also prevents the message from being modified or fabricated by attackers and also from the man in the middle (MITM) attack.
5. LACs perform physical verification of the IoVs during registration so that no fake software can perform any kind of malicious operations in the proposed system. It makes the system safe from different types of unknown source attacks, Sybil attacks and prevents any action performed by unauthorized entities. Moreover, as all the IoVs are required to be authenticated to perform any operation in the VANET, the system is safe from deadly DDoS attacks [90] as well.
6. As multiple servers (LACs) are available to provide services in every province, the system is fully distributed and decentralized in the aspect of storage and execution.
7. Blockchain with smart contracts added some extraordinary features like immutable storage facility, transparent storing and transactions, flexibility in accessing and managing, tamper-resistance storage, the fairness of transactions, and robustness of the stored data.

4.6. Discussion

Initiating an authentication protocol for VANET ensures a secured environment for communication. Internet supported authentication does not require additional infrastructural cost expenses. However, as it creates extra overhead, the lightweight digital signature algorithm RSA-1024 is used to ensure dependable security measures. Although, by default, Ethereum blockchain uses ECDSA for encryption, the proposed method minimizes the signature and verification time by using RSA-1024.

To ensure availability and other facilities mentioned in the previous section, a blockchain based distributed and decentralized server is proposed (hosted by LACs). All the connected LACs are the members of the blockchain to share their registered IoVs information and help to create VSN between them. The storage requirement for the server is also very low. Although the vehicles of a country are considered in this paper, it is easy to cooperate with the LACs from neighbour countries to increase the availability of the system.

The security analysis part discloses the security services as well as the attack prevention capabilities of the proposed method. However, the additional facilities provided by blockchain are also discussed there.

To give importance to the emergency information, classification for VSN is proposed that can successfully deliver data to the vehicles within SDR of 100 ms. The VANET who use traditional MAC does not have these facilities.

IoVs are generally equipped with lower computational power and storage. Moreover, they are running by using different operating systems. By considering these issues, in the proposed system, a lightweight encryption method is used so that it can be processed by the computers with minimum configuration. Additionally, as a passive member of the system, the IoVs does not require large storage facilities, and the developed system is platform independent. Thus, the IoVs do not need additional computational power or storage for the proposed system and required less time than some of the previously proposed protocols.

Classification of IoVs increase the authentication speed as well as ensure priorities to the EVs while driving. The authentication speed of both types of IoVs increases with the percentage of EVs. In the current pandemic situation and, in the future, this classification will create a great impact in the field of ITS and IoV.

Cooperation, while required, is a proved protocol to increase the reliability of communication and additionally increase the range of communication. The efficiency and performance of this protocol with the proposed optimization are proven by using numerical analysis.

4.7. Conclusions

Ensuring the identity of IoVs is an essential requirement before establishing communication in VANET. Hence, authenticity of the server is of paramount importance due to the ever growing amount of cyber attacks [91,92] on IoVs. To protect the IoVs from cyber criminals and to ensure confidentiality, security and privacy, in this paper, a blockchain based authentication protocol is proposed for cooperative VANET where IoVs will check the authenticity of other IoVs before establishing a connection. All the vehicles require internet communication capability to register to the LACs as IoV. All the LACs are members of the authentication blockchain and are able to add new IoV information as well as check the authenticity of the requested IoVs. With the help of the blockchain, LACs are connected together to form a decentralized, distributed, secured, and robust authentication service. While developing the authentication schema, IoVs' computational, storage capabilities are considered and thus a lightweight digital signature algorithm RSA-1024 is used instead of the typical ECDSA. The performance analysis shows that it requires a minimum amount of time (only 3.1 ms) where many of the previously proposed protocols require at least 10 ms for authentication. Moreover, the storage requirements are also minimum for the LACs while the IoVs do not require additional storage capacity to use the proposed method as all the information is stored in the blockchain.

Although the authentication speed is fast, the classification of IoVs is proposed to increase the authentication speed by eight times for EVs and two times for GVs. Additionally, introducing EVs types allows them to drive more efficiently as, whenever GVs come to know about the existence of EVs, they will clear a lane for

EVs. All the vehicles related to COVID-19 related help service, hospital, ambulance, medical services, fire service, emergency help, etc. will be considered as EVs and get special facility while driving.

However, because of the high mobility and dynamic nature of VANETs, it is difficult to maintain a strong or stable communication link between two vehicles. To increase the range of communication as well to ensure the reliability of the transmission link, the efficiency of cooperation is already famous. Thus, in this paper, a cooperation protocol is also proposed to increase the transmission efficiency to form VSN.

However, while too many IoVs' information are stored in the blockchain, performance of the system will be decreased. Thus, as a potential future work, it is possible to enhance the scalability of the system for example, a multi-level blockchain where the central server will store all the vehicles' authentication information and the LAC only stores the information of the vehicles registered under the LAC. LACs could collect information from the national server or a central system while required. Moreover, to ensure the security and reliability of the EMs, behaviour analysis of the IoVs could be added in the future and used for reputation management of IoVs.

CHAPTER 5. CONCLUSION

In this thesis, the extraordinary services of blockchain are implemented to provide a decentralized and distributed storage service that provides security, integrity, authenticity, attack and privacy preservation capacity, etc. for VANET. Detailed investigation was done to find out the area where and how blockchain can be implemented in this area as well as the application and efficiency have also been analysed. Then, firstly a secure message transmission method is implemented for cluster-based VANET and then to remove the authentication-related problem another method was implemented by using blockchain. However, to improve the performance of the blockchain a multi-level structure is presented and to minimize the encryption-decryption cost rather than the typical ECDSA, the RSA-1024 encryption algorithm is used to improve the throughput. Finally, to increase the area of the thesis another authentication system was developed for cooperative VANETs. To implement the system several novel steps were being taken for example updating the MAC packet structure, multi-level blockchain structure, etc. Performance analysis is presented convincingly which presents that the proposed method performs more economically in terms of storage and computational time consumption. Additionally, the supportive systems also performed better than traditional MAC protocol and also than some of the previously proposed protocols. Security analysis shows that the proposed methods ensure integrity, non-repudiation, immutability, privacy preservation and attack prevention capabilities, etc. Outcomes of the thesis are recognized by several top-ranked journals by publishing three of the works. In future, we are going to develop a reputation management system for intelligent vehicles for trust evaluation and management.

REFERENCES

[1] A. Kishida, M. Iwabuchi, T. Shintaku, T. Sakata, T. Hiraguri, and K. Nishimori, "IEEE standard for local and metropolitan area networks part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications ieee standard for local and metropolitan area networks part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, 2012," IEICE Transactions on Communications, vol. 96, no. 2, pp. 419–429, 2013.

[2] A. S. Shah, H. Ilhan and U. Tureli, "CB-MAC: a novel cluster-based MAC protocol for VANETs," IET Intelligent Transport Systems, vol. 13, no. 4, pp. 587–595, 2018.

[3] I. Ali, M. Gervais, E. Ahene and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," Journal of Systems Architecture, vol. 99, pp. 101636, 2019.

[4] M. Ahmed, "False image injection prevention using iChain" Applied Sciences, vol. 9, no. 20, pp. 4328, 2019.

[5] M. Ahmed and A.-S. K. Pathan, "Blockchain: can it be trusted?" Computer, vol. 53, no. 4, pp. 31–35, 2020.

[6] Rinkeby Testnet, "Rinkeby test network," 2020. [Online]. Available: https://www.rinkeby.io/.

[7] H. Wang, R. P. Liu, W. Ni, W. Chen and I. B. Collings, "VANET modelling and clustering design under practical traffic, channel and mobility conditions," IEEE Transactions on Communications, vol. 63, no. 3, pp. 870–881, 2015.

[8] F. Yang and Y. Tang, "Cooperative clustering-based medium access control for broadcasting in vehicular ad-hoc networks," IET Communications, vol. 8, no. 17, pp. 3136–3144, 2014.

[9] F. Yang, Y. Tang and L. Huang, “A multi-channel cooperative clustering-based MAC protocol for VANETs,” in 2014 Wireless Telecommunications Symposium. IEEE, Washington, DC, USA, pp. 1–5, 2014.

[10] H. Su and X. Zhang, “Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3309–3323, 2007.

[11] N. Gao, L. Tang, S. Li and Q. Chen, “A hybrid clustering-based MAC protocol for vehicular ad hoc networks,” in 2014 International Workshop on High Mobility Wireless Communications. IEEE, Beijing, China, pp. 183–187, 2014.

[12] K. A. Hafeez, L. Zhao, J. W. Mark, X. Shen and Z. Niu, “Distributed multichannel and mobility-aware cluster-based MAC protocol for vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 62, no. 8, pp. 3886–3902, 2013.

[13] S. Ucar, S. C. Ergen and O. Ozkasap, “Multihop-cluster-based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination,” IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp. 2621–2636, 2015.

[14] M. Zhang, C. Li, T. Guo and Y. Fu, “Cluster-based content download and forwarding scheme for highway VANETs,” China Communications, vol. 15, no. 4, pp. 110–120, 2018.

[15] X. Zhang and X. Chen, “Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network,” IEEE Access, vol. 7, pp. 58 241–58 254, 2019.

[16] U. Javaid, M. N. Aman and B. Sikdar, “DrivMan: driving trust management and data sharing in VANETS with blockchain and smart contracts,” in 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). IEEE, Kuala Lumpur, Malaysia, pp. 1–5, 2019.

[17] L. Xie, Y. Ding, H. Yang and X. Wang, “Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs,” IEEE Access, vol. 7, pp. 56 656–56 666, 2019.

[18] M. Wagner and B. McMillin, “Cyber-physical transactions: a method for securing VANETs with blockchains,” in 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC). IEEE, Taipei, Taiwan, pp. 64–73, 2018.

[19] X. Zhang, R. Li and B. 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, Shenzhen, China, pp. 258–259, 2018.

[20] R. Shrestha, R. Bajracharya and S. Y. Nam, “Blockchain-based message dissemination in VANET,” in 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS). IEEE, Kathmandu, Nepal, pp. 161– 166, 2018.

[21] R. Shrestha, R. Bajracharya, A. P. Shrestha and S. Y. Nam, “A new type of blockchain for secure message exchange in VANET,” Digital Communications and Networks, vol. 6, no. 2, pp. 177-186, 2019.

[22] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng and C.-C. Liu, “Blockchain-based traffic event validation and trust verification for VANETs,” IEEE Access, vol. 7, pp. 30 868–30 877, 2019.

[23] M. Singh and S. Kim, “Branch based blockchain technology in intelligent vehicle,” Computer Networks, vol. 145, pp. 219–231, 2018.

[24] C. Lai and Y. Ding, “A secure blockchain-based group mobility management scheme in VANETs,” in 2019 IEEE/CIC International Conference on Communications in China (ICCC). IEEE, Changchun, China, pp. 340–345, 2019.

[25] Z. Lu, Q.Wang, G. Qu and Z. Liu, “Bars: a blockchain-based anonymous reputation system for trust management in vanets,” in 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE, New York, NY, USA, pp. 98– 103, 2018.

[26] Z. Lu, W. Liu, Q. Wang, G. Qu and Z. Liu, “A privacy-preserving trust model based on blockchain for VANETs,” IEEE Access, vol. 6, pp. 45 655– 45 664, 2018.

[27] B. Leiding, P. Memarmoshrefi and D. Hogrefe, “Self-managed and blockchain-based vehicular ad-hoc networks,” in Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, Heidelberg, Germany, pp. 137–140, 2016.

[28] Truffle Blockchain Group, “Truffle suite,” 2020. [Online]. Available: https://www.trufflesuite.com/.

[29] Truffle Blockchain Group, “Ganache,” 2020. [Online]. Available: https://www.trufflesuite.com/ganache.

[30] ConsenSys Formation, “Metamask,” 2020. [Online]. Available: https://metamask.io/.

[31] Isaac Z. Schlueter, “NPM,” 2020. [Online]. Available: http://www.npmjs.com/.

[32] J. Papa, “lite-server,” 2020. [Online]. Available: https://github.com/johnpapa/lite-server.

[33] Ethereum Foundation, “Ethereum,” 2020. [Online]. Available: https://Ethereum.org/.

[34] Ethereum Foundation, “Remix ide,” 2020. [Online]. Available: https://remix.Ethereum.org/.

[35] Etherscan “The Ethereum Blockchain Explorer,” 2020. [Online]. Available:https://etherscan.io/.

[36] E. Barker and Q. Dang, “NIST special publication 800-57 part 1, revision 4,” NIST, Tech. Rep, 2016. [Online]. Available:https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/archive/2016-01-28.

[37] S. R. Singh, A. K. Khan, and S. R. Singh, “Performance evaluation of RSA and elliptic curve cryptography,” in 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I). IEEE, Noida, India, pp. 302– 306, 2016.

[38] R. K. Nirala and M. D. Ansari, “Performance evaluation of loss packet percentage for asymmetric key cryptography in VANET,” in 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). IEEE, Solan Himachal Pradesh, India, pp. 70–74, 2018.

[39] S. Ucar, S. C. Ergen and O. Ozkasap, “Multihop-cluster-based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination,” IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp. 2621– 2636, 2015.

[40] G.Wood, “Ethereum: a secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, no. 2014, pp. 1–32, 2014.

[41] M. A. Karabulut, A. Shah and H. ˙Ilhan, “Performance modeling and analysis of the IEEE 802.11 MAC protocol for VANETs,” Journal of the Faculty of Engineering and Architecture of Gazi University, vol. 35, no. 3, pp. 1575-1587, 2020.

[42] A. S. Shah, H. Ilhan and U. Tureli, “Performance and complexity analysis of MAC protocol for VANETs,” in 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, Vancouver, BC, Canada, pp. 1081–1086, 2019.

[43] M. A. Karabulut, A. S. Shah and H. Ilhan, “Performance modeling and analysis of the IEEE 802.11 DCF for VANETs,” in 2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, Munich, Germany, pp. 346–351, 2017.

[44] M. A. Karabulu t, A. S. Shah and H. Ilhan, “The performance of the IEEE 802.11 DCF for different contention window in VANETs,” in 2018 41st International Conference on Telecommunications and Signal Processing (TSP). IEEE, Athens, Greece, pp. 1–4, 2018.

[45] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” IEEE Journal on Selected Areas in Communications, vol. 18, no. 3, pp. 535–547, 2000.

[46] D. Malone, K. Duffy and D. Leith, “Modeling the 802.11 distributed coordination function in nonsaturated heterogeneous conditions,” IEEE/ACM Transactions on Networking, vol. 15, no. 1, pp. 159–172, 2007.

[47] X. Ma, X. Chen and H. H. Refai, “Unsaturated performance of IEEE 802.11 broadcast service in vehicle-to-vehicle networks,” in 2007 IEEE 66th Vehicular Technology Conference. IEEE, Baltimore, MD, USA, pp. 1957–1961, 2007.

[48] M. I. Hassan, H. L. Vu and T. Sakurai, “Performance analysis of the IEEE 802.11 MAC protocol for DSRC safety applications,” IEEE Transactions on Vehicular Technology, vol. 60, no. 8, pp. 3882–3896, 2011.

[49] Q. Wu and J. Zheng, “Performance modeling of IEEE 802.11 DCF based fair channel access for vehicular-to-roadside communication in a non-saturated state,” in 2014 IEEE International Conference on Communications (ICC). IEEE, Sydney, NSW, Australia, pp. 2575–2580, 2014.

[50] M. Al-Bassam, “SCPKI: a smart contract-based PKI and identity system,” in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, United Arab Emirates, pp. 35–40, 2017.

[51] W. Stallings, Network security essentials: applications and standards (international edition), 4/e, Pearson Education India, 2011. [Online]. Available: http://thuvienso.bvu.edu.vn/handle/TVDHBRVT/15994.

[52] Association, I.S., others. IEEE Std 802.11-2016, IEEE Standard for Local and Metropolitan Area Networks—Part 11: Wireless LANMediumAccess Control (MAC) and Physical Layer (PHY) Specifications, 2016.

[53] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," Vehicular Communications, vol. 1, no. 2, pp. 53 – 66, 2014.

[54] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," IET Communications, vol. 4, no. 7, pp.894–903, 2010.

[55] A. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. P. Mahmud,M. K. Nasir, and R. M. Noor, "Distb-condo: Distributed blockchain-basediot-sdn model for smart condominium," IEEE Access, vol. 8, pp. 209 594–209 609, 2020.

[56] H. Wang, R. P. Liu, W. Ni, W. Chen, and I. B. Collings, "Vanet modeling and clustering design under practical traffic, channel and mobility conditions,"IEEE Transactions on Communications, vol. 63, no. 3, pp. 870–881, 2015.

[57] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE). IEEE, 2018, pp. 674–679.

[58] A. Kulathunge and H. Dayarathna, "Communication framework for vehicular ad-hoc networks using blockchain: Case study of metro manila electric shuttle automation project," in 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE). IEEE, 2019, pp. 85–90.

[59] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," Information Sciences, vol. 462, pp. 262–277, 2018.

[60] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, “Bcppa: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks,” IEEE Transactions on Intelligent Transportation Systems, 2020.

[61] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, “Fadb: A fine-grained access control scheme for vanet data based on blockchain,” IEEE Access, vol. 8, pp. 85 190–85 203, 2020.

[62] C. Wang, J. Shen, J.-F. Lai, and J. Liu, “B-tsca: Blockchain assisted trustworthiness scalable computation for v2i authentication in vanets,” IEEE Transactions on Emerging Topics in Computing, 2020.

[63] A. H. Salem, A. Abdel-Hamid, and M. A. El-Nasr, “The case for dynamic key distribution for pki-based vanets,” arXiv preprint arXiv:1605.04696, 2016.

[64] Ferrer, B.R., Mohammed, W.M., Lastra, J.L.M., Villalonga, A., Beruvides, G., Castaño, F., Haber, R.E. “Towards the adoption of cyber-physical systems of systems paradigm in smart manufacturing environments”. In Proceedings of the 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), Porto, Portugal, 18–20 July 2018, IEEE: New York, NY, USA, 2018, pp. 792–799.

[65] Fernandez-Carames, T.M., Fraga-Lamas, P. “A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories”. IEEE Access 2019, 7, 45201–45218.

[66] Dorri, A., Kanhere, S.S., Jurdak, R. “Towards an optimized blockchain for IoT”. In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017, IEEE: New York, NY, USA, 2017, pp. 173–178.

[67] Loklindt, C., Moeller, M.P., Kinra, A. “How blockchain could be implemented for exchanging documentation in the shipping industry”. In International Conference on Dynamics in Logistics, Springer: Berlin/Heidelberg, Germany, 2018, pp. 194–198.

[68] Mettler, M. “Blockchain technology in healthcare: The revolution starts here”. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016, IEEE: New York, NY, USA, 2016, pp. 1–3.

[69] Akhter, A., Ahmed, M., Shah, A., Anwar, A., Zengin, A. “A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET”. Sustainability 2021, 13, 400.

[70] Wang, C., Shen, J., Lai, J.F., Liu, J. “B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs”. IEEE Trans. Emerg. Top. Comput. 2020.

[71] Taghizadeh, H., Solouk, V. “A novel MAC protocol based on cooperative master-slave for V2V communication”. In Proceedings of the 2015 38th International Conference on Telecommunications and Signal Processing (TSP), Prague, Czech Republic, 9–11 July 2015, IEEE: New York, NY, USA, 2015, pp. 1–5.

[72] Shah, A.S., Ilhan, H., Tureli, U. “RECV-MAC: A novel reliable and efficient cooperative MAC protocol for VANETs”. IET Commun. 2019, 13, 2541–2549.

[73] Yang, F., Tang, Y. “Cooperative clustering-based medium access control for broadcasting in vehicular ad-hoc networks”. IET Commun. 2014, 8, 3136–3144.

[74] Woo, R., Han, D.S. “A cooperative MAC for safety-related road information transmission in vehicular communication systems”. In Proceedings of the 1st IEEE Global Conference on Consumer Electronics 2012, Tokyo, Japan, 2–5 October 2012, IEEE: New York, NY, USA, 2012, pp. 672–673.

[75] Zhang, L., Jin, B., Cui, Y. “A concurrent transmission enabled cooperative MAC protocol for vehicular ad hoc networks”. In Proceedings of the 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS), Hong Kong, China, 26–27 May 2014, IEEE: New York, NY, USA, 2014, pp. 258–267.

[76] Zhou, T., Sharif, H., Hempel, M., Mahasukhon, P., Wang, W., Ma, T. “A novel adaptive distributed cooperative relaying MAC protocol for vehicular networks”. IEEE J. Sel. Areas Commun. 2010, 29, 72–82.

[77] Zhang, J., Zhang, Q., Jia, W. “VC-MAC: A cooperative MAC protocol in vehicular networks”. IEEE Trans. Veh. Technol. 2008, 58, 1561–1571.

[78] Bharati, S., Zhuang, W. “CRB: Cooperative relay broadcasting for safety applications in vehicular networks”. IEEE Trans. Veh. Technol. 2016, 65, 9542–9553.

[79] Bharati, S., Zhuang, W. “CAH-MAC: Cooperative ADHOC MAC for vehicular networks”. IEEE J. Sel. Areas Commun. 2013, 31, 470–479.

[80] Bharati, S., Thanayankizil, L.V., Bai, F., Zhuang, W. “Effects of time slot reservation in cooperative ADHOC MAC for vehicular networks”. In Proceedings of the 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 9–13 June 2013, IEEE: New York, NY, USA, 2013, pp. 6371–6375.

[81] Zhang, R., Cheng, X., Yang, L., Shen, X., Jiao, B. “A novel centralized TDMA-based scheduling protocol for vehicular networks”. IEEE Trans. Intell. Transp. Syst. 2014, 16, 411–416.

[82] Omar, H.A., Zhuang, W., Li, L. “VeMAC: A novel multichannel MAC protocol for vehicular ad hoc networks”. In Proceedings of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, China, 10–15 April 2011, IEEE: New York, NY, USA, 2011, pp. 413–418.

[83] Ethereum Glossary. Available online: https://ethereum.org/en/glossary/ (accessed on 8 December 2020).

[84] Shah, A., Islam, M., Alam, M. “Cooperative communication: An overview”. In Cooperative Communication In Wireless Networks, LAP LAMBERT Academic Publishing: Saarbrucken, Germany, 2013, pp. 7–23.

[85] Luan, T.H., Ling, X., Shen, X. “MAC in motion: Impact of mobility on the MAC of drive-thru Internet”. IEEE Trans. Mob. Comput. 2011, 11, 305–319.

[86] Zhang, C., Lu, R., Lin, X., Ho, P.H., Shen, X. “An efficient identity-based batch verification scheme for vehicular sensor networks”. In Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008, IEEE: New York, NY, USA, 2008, pp. 246–250.

[87] Rongxing, L., Xiaodong, L., Xuemin, S. “SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks”. In Proceedings of the IEEE INFOCOM, San Diego, CA, USA, 15–19 March 2010, pp. 1–9.

[88] Shao, J., Lin, X., Lu, R., Zuo, C. “A threshold anonymous authentication protocol for VANETs”. IEEE Trans. Veh. Technol. 2015, 65, 1711–1720.

[89] Azees, M., Vijayakumar, P., Deboarh, L.J. “EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks”. IEEE Trans. Intell. Transp. Syst. 2017, 18, 2467–2476.

[90] Ahmed, M. Thwarting “DoS Attacks: A Framework for Detection based on Collective Anomalies and Clustering”. Computer 2017, 50, 76–82.

[91] Ahmed, M., Mahmood, A., Hu, J. “A survey of network anomaly detection techniques”. J. Netw. Comput. Appl. 2015, 60, 19–31.

[92] Bostami, B., Ahmed, M., Choudhury, S. “False Data Injection Attacks in Internet of Things”. In Performability in Internet of Things, Fadi, T., Ed., Springer: Cham, Switzerland, 2019, pp. 47–58.

RESUME

Name Surname : A F M SUAIB AKHTER

EDUCATION

Degree	School	Graduation Year
PhD.	Sakarya University / Institute of Natural Sciences / Computer and Information Engineering	Continue
Master	University of Dhaka / Institute of Information Technology	2012
Degree	Islamic University of Technology / Computer Science and Information Technology	2008
High School	New Govt. Degree College	2004

JOB EXPERIENCE

Year	Place	Position
2011-2013	Manarat International University, Bangladesh	Lecturer
2009-2011	Dhaka International University, Bangladesh	Lecturer

FOREIGN LANGUAGE

English

PRODUCTS (article, paper, project, ets.)

1. “A blockchain-based authentication protocol for cooperative vehicular ad hoc network,” Sensors, vol. 21, no. 4, 2021.
2. “A secured message transmission protocol for vehicular ad hoc networks,” Computers, Materials & Continua, vol. 68, no. 1, pp. 229–246, 2021.

3. “A secured privacy-preserving multi-level blockchain framework for cluster-based vanet,” Sustainability, vol. 13, no. 1, p. 400, 2021.

HOBBIES

Photography