sustainability

MDPI

Article

A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET

A. F. M. Suaib Akhter [1], Mohiuddin Ahmed [2], A. F. M. Shahen Shah [3], Adnan Anwar [4,*] and Ahmet Zengin [1]

[1] Department of Computer Engineering, Sakarya University, Serdivan 54050, Sakarya, Turkey; suaib.akhter@ogr.sakarya.edu.tr
[2] School of Science, Edith Cowan University, Perth, WA 6027, Australia; mohiuddin.ahmed@ecu.edu.au
[3] Department of Electrical and Electronics Engineering, Istanbul Gelisim University, Istanbul 34315, Turkey; afmsshah@gelisim.edu.tr
[4] Centre for Cyber Security Research and Innovation (CSRI), School of IT, Deakin University, Waurn Ponds, Victoria 3216, Australia
* Correspondence: adnan.anwar@deakin.edu.au

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

Keywords: data security; Vehicular Ad hoc Networks; digital signatures; distributed storage; intelligent vehicles; wireless communication; emergency vehicle management

check for updates

Citation: Akhter, A.F.M.S.; Ahmed, M.; Shah, A.F.M.S.; Anwar, A.; Zengin, A. A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET. *Sustainability* **2021**, *13*, 400. https://doi.org/10.3390/su13010400

Received: 10 December 2020
Accepted: 30 December 2020
Published: 4 January 2021

1. Introduction

Vehicular Ad hoc Network (VANET) is a temporary wireless network that can be formed in order 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 [1] provides standards for VANET communication and the 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) between 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 1, examples of safety and non-safety messages are cited. In order 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 100 ms is required for maintaining SMT to ensure real time availability. On the other hand, there are some information that do not have any impact on the safety or security, but are beneficial, called NSMs. The NSM transmission (NSMT) does not require maintaining SDR, like SMT protocol.

Table 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	Advertisement
Barriers, obstacles, road block notification	GPS update
Signal or rule violation	Downloading entertaining contents

Several protocols are proposed to ensure better management and performance efficiency of VANET systems. 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. However, 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 Medium Access Control (MAC) protocol and packet structures to remove hidden node problem and increase the efficiency by minimizing delay and Packet Dropping Rate (PDR). Moreover, the proposed method handles SMs and NSMs separately and ensures an SDR of 100 ms for SMs. Thus, it can be considered to be 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 for increasing the performance of the VANETs. Because 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 have to face authentication, identification, confidentiality, integrity, and availability related threads and attacks [3,4]. Vehicle authentication is the most important security feature that a VANET system must ensure. In spite of high mobility and low configured computation support real time, authentication is required to maintain VANETs.

Typically a secure authentication system is based on Public Key Infrastructure (PKI), where a vehicle can prove its identity by sending an encrypted identification to the Local Authentication Center (LAC). LAC will decrypt the information and match it with the authorized vehicles list i.e., database and take a decision (accepts or rejects). Although the PKI based systems provide effective security, it is time consuming and mostly stored in the centralized server that has single point-of-failure problem. The time consumption of encryption and decryption increases with the level of security. Moreover, because of high mobility, each time that the vehicles move from one cluster to another one, the encryption overhead increases. Frequent encryption/decryption will increase the 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, then 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 that provides additional security, immutability, temper-resistance, traceability, transparency, robustness, etc. Although blockchain was invented to store public ledger related information, because of its varieties of security and other features, it has become popular to store different types of information in various applications [5–7]. Blockchain stores information as blocks that are chained together and it is not possible to update or delete any information from the blocks; thus, it is called temper-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 that 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 the 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 helps us 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 for registering vehicles inside an area (for example, state) and generating PKI keys for them. LACs maintain a local blockchain (LABC), where all of the locally registered vehicles' public keys are stored, and all of 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 of the LACs are the members of a Global Authentication Blockchain (GABC), where all of 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 of 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. In order 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 is authenticated in a cluster, the corresponding CH will immediately broadcast an SM by informing the existence of an EV, so that all of 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 in order to prove that the proposed authentication protocol can perform faster than some of the previously proposed methods. Numerical analysis is also 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 protocols.

The contributions of the paper can be summarized, as follows:

- 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.
- We propose a multi-level blockchain to increase the scalability, faster authentication service with decentralized and distributed storage support. In the top level, a global authentication center (GAC) is responsible for store all of the vehicle information in a blockchain, where all of the LACs are the members. However, to manage the vehicles internally, LACs also manage a blockchain called LABC, which enable the quick handover between internal clusters. All of the CHs are the members of the LABC.

- 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 proposed to increase the performance of the ACB-MAC system.
- In order 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 in order to obtain 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 the security, integrity, and confidentiality of the transmitted messages.

In Section 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. Section 4 describes the express services proposed for the EVs. Section 5 presents the implementation tools with the experiment details. Performance analysis of the authentication protocol and the VSN protocols are available in Section 6. Section 7 presents the security analysis of the proposed method. Finally, in Section 8, we conclude the paper with potential future works.

2. Related Works

2.1. Cluster Based VANET Systems

The advantages of cluster based systems in terms of performance and management is available in [8]. A cooperative Clustering-based Medium Access Control (CCB-MAC) protocol is proposed by Yang et al. to increase the reception rate and ensure the trustworthiness of the broadcasted message [9]. In another paper, Yang et al. proposed a multi-channel cluster based method that is targeted at ensuring the reliability of the transmitted message with additional QoS support [10]. Su et al. [11] 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 [12]. Their proposed method performs well in increasing network stability and channel utilization. All of 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 the decrement of throughput. TDMA protocols are not able to utilize all of the time slots of a frame due to a lack of neighbouring node. Thus, we can say that, the above mentioned [9–12] TDMA based protocols do not have efficient resource utilization capability. In [13], Hafeez et al. proposed a distributed multichannel and mobility-aware cluster-based protocol in short DMMAC, which utilizes the Fuzzy-logic Inference System for safety message transmission. Another safety message transmission method was proposed by Ucar et al. that was targeted to minimize the packet dropping rate and connection overheads, but only for safety messages transmissions [14]. In [15], 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, the 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. Accordingly, the above-mentioned methods are not free from these problems. However, for safety message transmission, it is required to maintain the SDR of 100 ms, which did not satisfy the above mentioned papers. However, some of them (for example, [9,12–14]) only provide solutions for emergency message transmission and others do not differentiate between messages, which reduces the importance of the emergency messages.

2.2. Blockchain Based Authentication

The authentication of vehicles are the primary requirement for VANET. Blockchain is utilized in order to store the registration information of the vehicles by Javaid et al. in their proposed method, called DrivMan [16]. Li et al. proposed a method, called SEBGMM, in order to ensure fast authentication and handover [17]. 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 [18], Malik et al. also used blockchain to store the authentication information and ensure the privacy of the vehicles. In order to minimize the cost of signature generation and verification, Ali et al. presented a certificate-less signature schema in [19]. It ensures the integrity and trust of vehicles, where a blockchain is used to store the identity of the authorized vehicles and another to store the unauthorized or revoked vehicles. In [20], 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. In [21,22], the researchers proposed a privacy-preserving trust model to provide 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 that are transferred between vehicles. A consortium blockchain was proposed by Zhang et al. in [23], where they store the authentication information with location, position, direction, and rule violation information of vehicles in order to ensure the security and temper-resistance of those information.

The previously proposed methods utilize blockchain for different purposes, including authentication. Most of them use a complex authentication method, which consumes much time. In [16], Javaid et al. used a certificate based method to allow or reject a vehicle's permission, but did not mention the computational overheads that were generated by the signature and the verification method. The proposed method proposed by Malik et al. used encryption, decryption, signature, and verification together, which generates high computational overhead [18]. The proposed method by Zhang et al. is also a signature based schema, where computational overhead is high [23]. Additionally, some previously proposed authentication protocols for VANET, like [24–29], also suffer from high computational overhead.

Moreover, all of the methods are dependent on Road Side Unites (RSUs), where the infrastructure costs are high [30]. On the other hand, some other methods, like [31,32], suffer from high storage overhead. Additionally, all of the vehicles, including emergency vehicles, considered to be similar, which means that the emergency service provider vehicles will not obtain any extra facilities from the proposed methods. Thus, in this paper, we proposed a lightweight and faster authentication protocol by utilizing a cluster based system that 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.

2.3. Motivations

Firstly, it requires expensive infrastructures to implement RSU based VANETs and 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. In order 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 100 ms 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 of the vehicles are considered to be equal, which means that there are no particular facility for the emergency vehicles. In order 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. We introduce RTS/CTS handshaking in the proposed method to remove these shortcomings.

Fifth, privacy-preserving authentication is a principal requirement for VANETs in order to ensure security, confidentiality, trustability, etc. However, to ensure high performance, i.e., increased throughput, lower PDR, and delay, sometimes the security is compromised in the previously proposed VANET systems. The lack of proper authentication protocols may allow for malicious entities to enter and cause severe accidents inside a VANET. Moreover, a 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. In order 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.

Sixth, to ensure flexible, immutable, transparent, and robust authentication in a decentralized environment, q blockchain-based light-weight authentication system for vehicles is introduced. Typical certificate oriented authentication protocols are not capable of providinng all of these facilities, as well as signature generation and verification have higher computational overhead, which is described in the previous sub-section (see Section 2.2). Additionally, the proposed method is also targeted to minimize the transmission delay as well as computational and storage overhead for authentication.

3. System Structure

In this paper, we proposed a tree structure, where a GAC is considered to be the root of the tree (see Figure 1). All of the LACs are in the second level, where all of them are connected to a blockchain, called GABC. GABC stores all of the information regarding the vehicles of a large area. LAC consists of several numbers of clusters that come 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 members of another blockchain, called LABC, which stores all of the local vehicles' public keys. Whenever a vehicle comes to join in a cluster, the corresponding CH check its the entry in the LABC to authenticate. In the fourth level, there are vehicles that are connected to their corresponding clusters. All of the communications between vehicles are handled by the CH under the cluster.

3.1. Cluster Formation

All of the vehicles moving through same direction will form a cluster. All of the vehicles are equipped with On Board Unit (OBU), Global Positioning System (GPS), etc., with high speed 5G internet connection and communication capability. Figure 2a illustrates the 0 finite state machine (FSM), which is the cluster formation for (English edited, Please confirm) GV. A GV is selected as CH and others become CMs. EVs will not participate in the process of becoming a CH, but rather wait to join in a cluster as CM. CH is responsible for managing all of the communication between the vehicles, i.e., the CH acts as the center of VSN. CH is also responsible for communicating with the LABC and the neighbour CHs. In order to support cluster based system and increase the efficiency of the message transmission, especially 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). Figure 2b presents the changes.

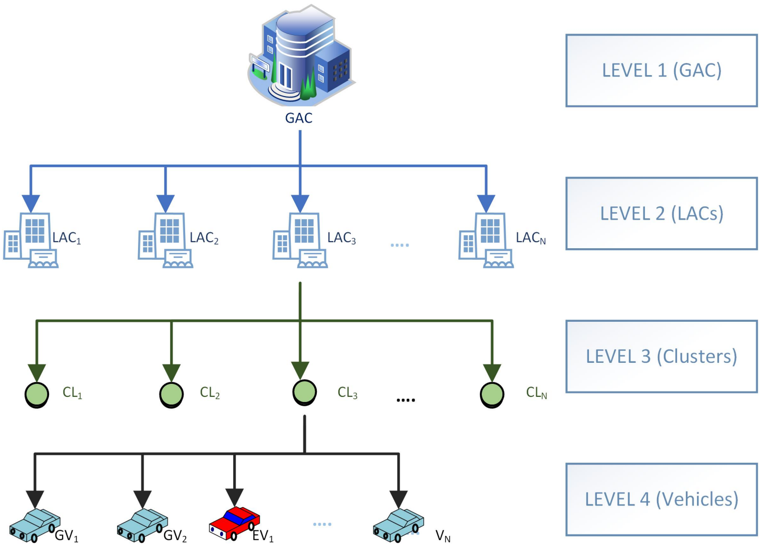
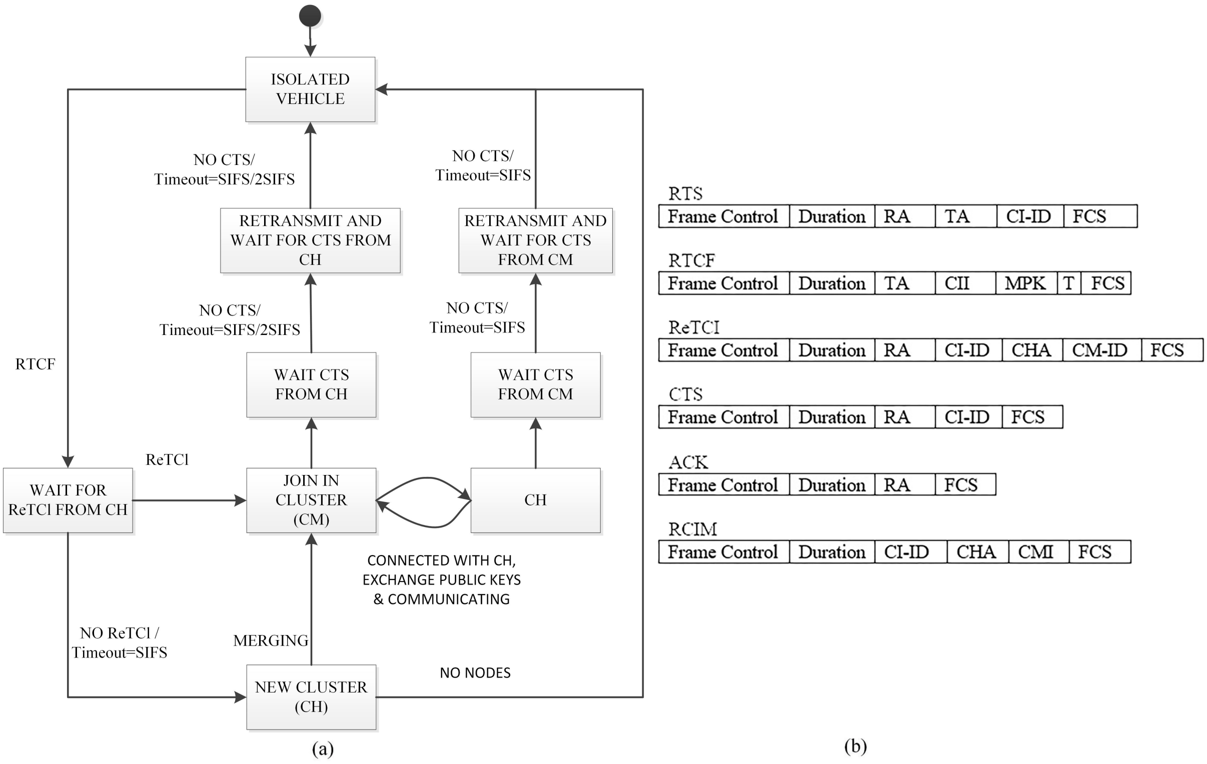


Figure 1. Tree structure of the proposed method.



RTS

Frame Control	Duration	RA	TA	CI-ID	FCS

RTCF

Frame Control	Duration	TA	CII	MPK	T	FCS

ReTCl

Frame Control	Duration	RA	CI-ID	CHA	CM-ID	FCS

CTS

Frame Control	Duration	RA	CI-ID	FCS

ACK

Frame Control	Duration	RA	FCS

RClM

Frame Control	Duration	CI-ID	CHA	CMI	FCS

Figure 2. (**a**) Finite state machine (FSM) and (**b**) updated packet structure of the proposed method.

3.2. Cluster Membership

All of the inactive, i.e., parked vehicles, are the members of the inactive cluster. Whenever a vehicle becomes active, it broadcasts 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 obtaining positive feedback from the database, send(s) ReTCl back 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, the 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 find any cluster to join after short inter-frame space (SIFS) timeout, it will create a new cluster and become CH of the cluster. However, the EVs will not form a cluster or become a CH, but rather continue moving until receiving any ReTCl.

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 of 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 of the vehicles have to register to the LAC before obtaining a road permit. LAC is responsible for physically verifying and generating a public-private key pair for each of the vehicles. Subsequently, it creates a transaction in the GABC by entering the required information. By this way, all of the LACs obtain the information regarding 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, in order to increase the scalability, all of the LACs maintain a blockchain, called LABC, by storing the 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 of the CHs under same state are the members of the LABC (as the third level of the tree) and, thus, obtained the list of all the locally registered vehicles. Hence, 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 of 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. The application scenario is demonstrated in Figure 3.

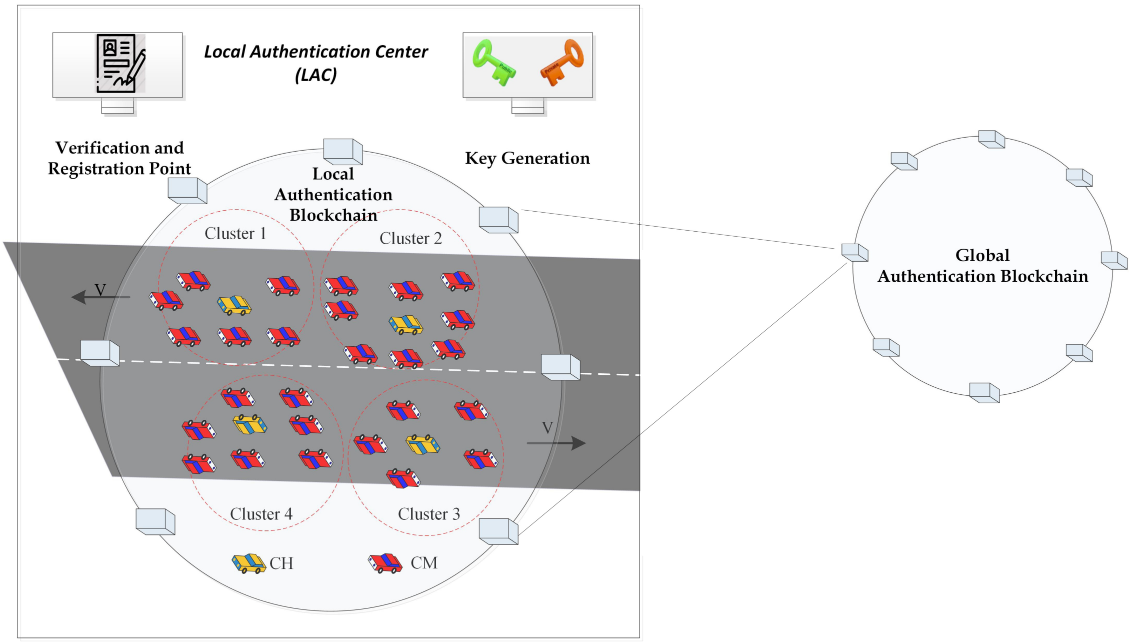


Figure 3. Application scenario with local and global authentication center.

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 in order to send the public key and the type of the requested vehicle within the control packet. The type field is used, which only requires 1 bit, where 0 and 1 represent GV and EV, respectively. Rather than searching for all of the vehicles from the blockchain, the system will search according to the category, which increases the efficiency of searching. If 10% of the vehicles are EV, then it is possible to get 10 times faster authentication than a system, where all of the vehicles are considered as the same. After receiving the RTCF, CH will generate a transaction in the LABC in order to search for the received MPK. Reply will come in form of 0 and 1 to represent valid and invalid, respectively. The computational time required for the whole process is discussed in the performance analysis section.

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 the 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. The flow chart presented in Figure 4a shows the inter cluster authentication method.

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, then 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. Because all of the CHs store the LABC, disabling temporary public keys will reduce the storage requirements and also reduce the download time for the new CH while copying the LABC's transactions. The flow chart (see Figure 4b) describes the authentication details.

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 due to 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 that 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.

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

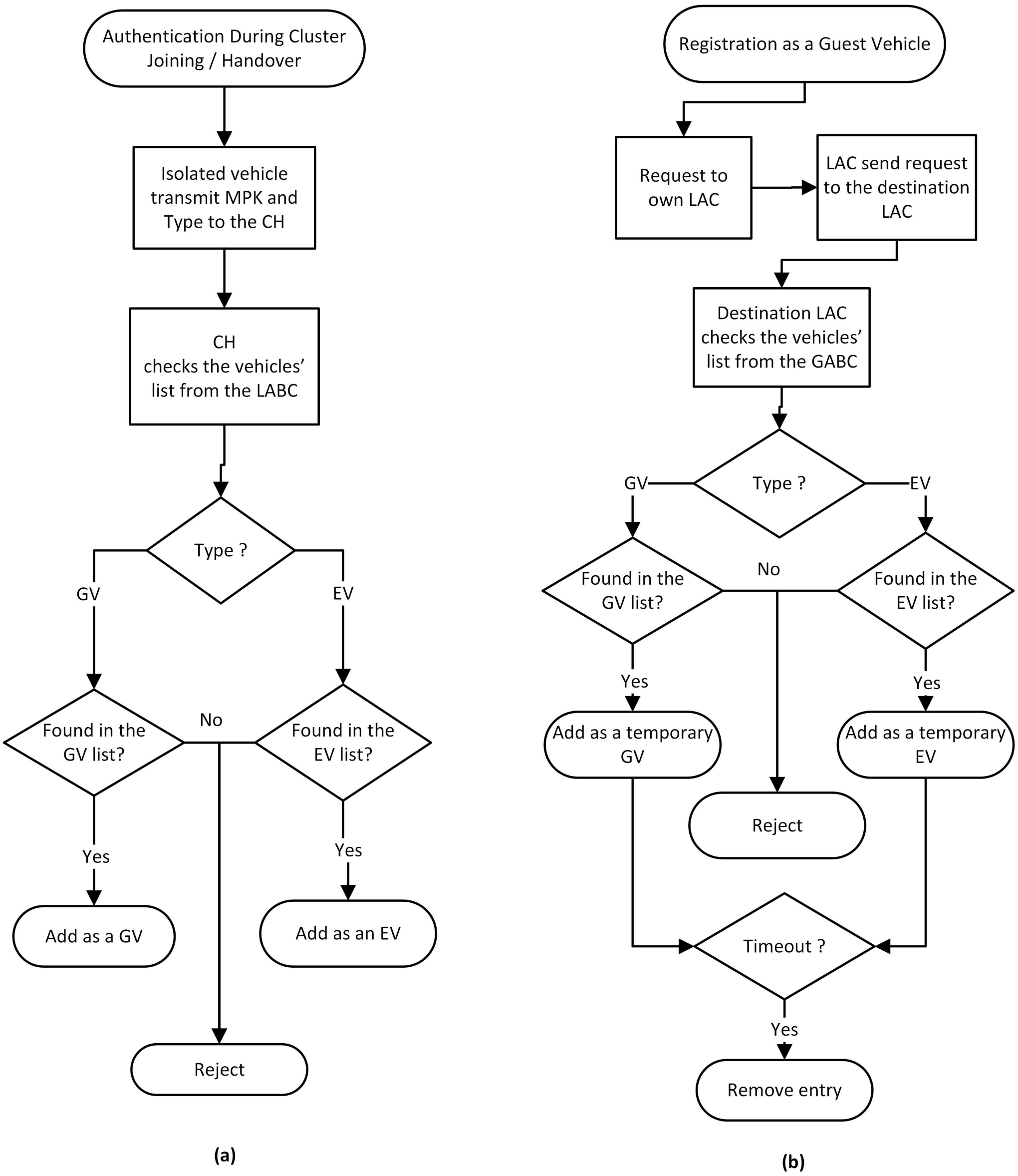

Authentication During Cluster Joining / Handover
Isolated vehicle transmit MPK and Type to the CH
CH checks the vehicles' list from the LABC
Type ?
GV
EV
Found in the GV list?
No
Found in the EV list?
Yes
Yes
Add as a GV
Add as an EV
Reject
(a)
Registration as a Guest Vehicle
Request to own LAC
LAC send 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 4. Flow chart demonstrates vehicle authentication during (**a**) cluster joining and (**b**) guest vehicles' registration.

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 types of vehicles, i.e., CH and CMs, can leave the cluster if they need to. Figure 5 presents the detailed process. The figure has four parts: (i) Figure 5a 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 the 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.

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 the 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. Figure 5b summarizes the whole process.

In the last two parts of Figure 4c,d, we have adopted the notion S and D, which denote 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 to another CM, then the timeout happens for 2SIFS interval. Within the waiting time, if no CTS is received by the CM, then the RTS message is retransmitted. Figure 5c shows the case when CM retransmits the RTS, while Figure 5d shows the case when CH retransmits the RTS.

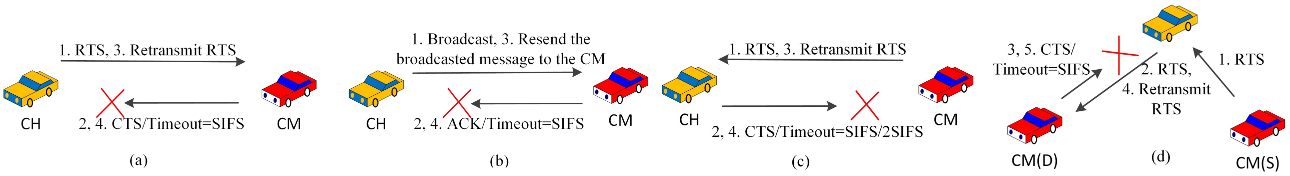

1. RTS, 3. Retransmit RTS
CH
2, 4. CTS/Timeout=SIFS
CM
(a)
1. Broadcast, 3. Resend the broadcasted message to the CM
CH
2, 4. ACK/Timeout=SIFS
CM
(b)
1. RTS, 3. Retransmit RTS
CH
2, 4. CTS/Timeout=SIFS/2SIFS
CM
(c)
3, 5. CTS/ Timeout=SIFS
2. RTS, 4. Retransmit RTS
1. RTS
CM(D)
(d)
CM(S)

Figure 5. Cluster leaving process 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 (**d**) no CTS is received from a destination CM

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 need to be satisfy strict time requirements. These safety messages are reliably transmitted from CMs to CH using the RTS or CTS mechanism. The usage of RTS and CTS help 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 to be 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. Figure 6a illustrates the complete process of the proposed safety message transfer protocol and the handshaking between the vehicles during SMT are shown in Figure 6b,c.

3.8. Non-Safety Message Transmission (NSMT)

Similar to the safety message transmission that was discussed in the previous section, our proposed VANET model also proposes non-safety message transmission protocol in order 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*). CH and CM both act 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 while using the RTS or CTS mechanism. Once the receiver CM receives the messages, then 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 to be 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]. Figure 7a summarizes the whole concept of non-safety message transmission and Figure 7b–d illustrate the handshake between the vehicles during NSMT.

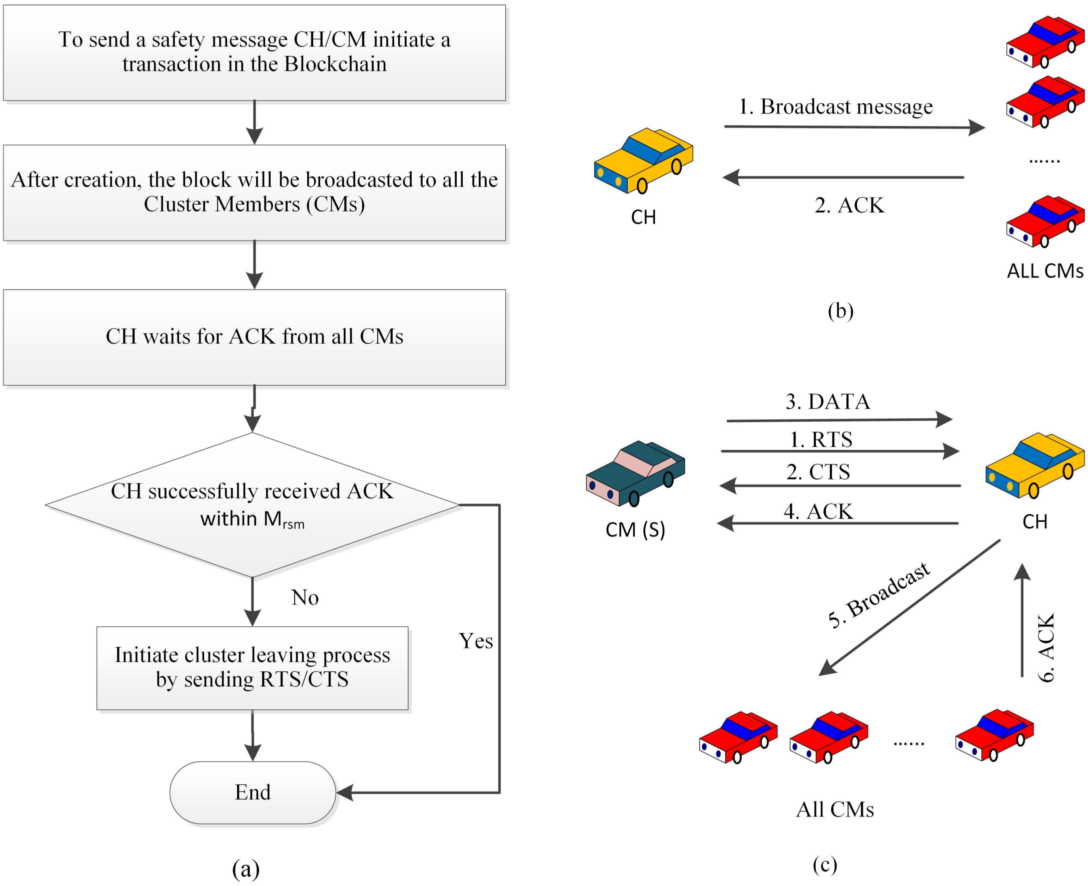

To send a safety message CH/CM initiate a transaction in the Blockchain
After creation, the block will be broadcasted to all the Cluster Members (CMs)
CH waits for ACK from all CMs
CH successfully received ACK within M_{rsm}
No
Yes
Initiate cluster leaving process by sending RTS/CTS
End
(a)
1. Broadcast 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 6. (**a**) Flow chart demonstrates safety message transmission and (**b**,**c**) handshake between vehicles during safety message transmission (SMT).

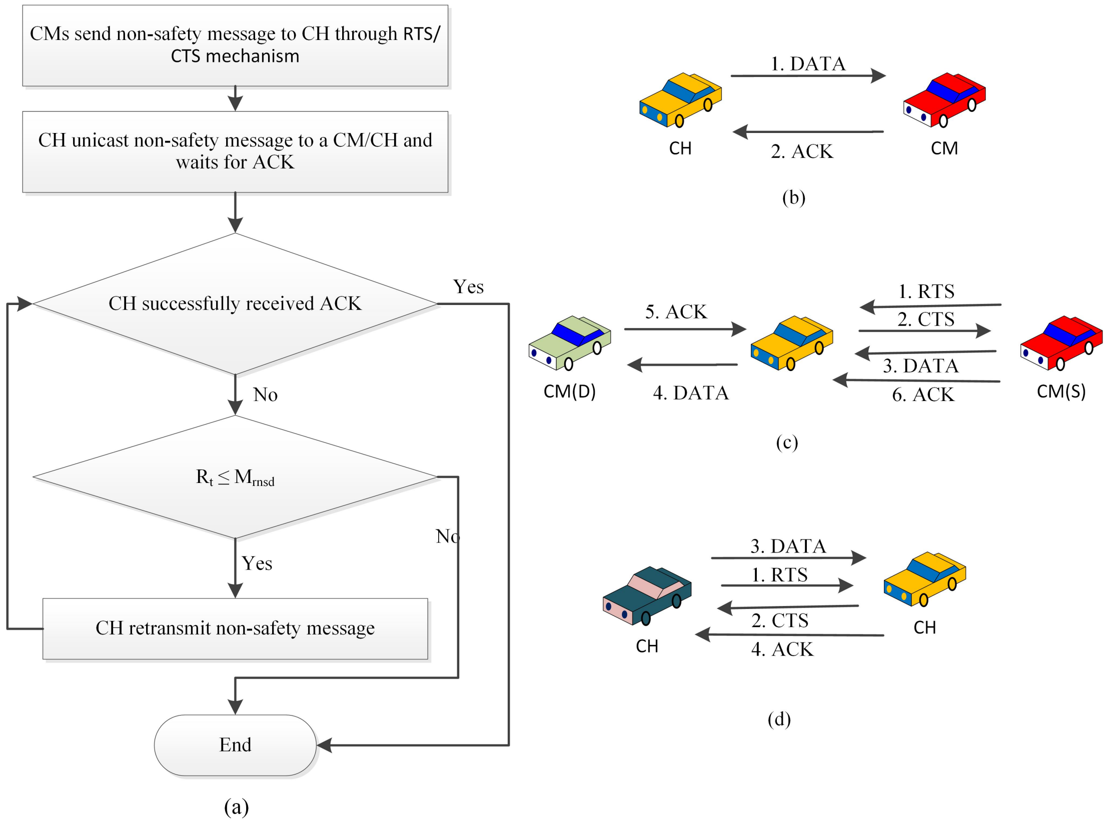

CMs send non-safety message to CH through RTS/ CTS mechanism
CH unicast non-safety message to a CM/CH and waits for ACK
CH successfully received ACK
Yes
No
$R_t \le M_{rnsd}$
Yes
No
CH retransmit non-safety message
End
(a)
1. DATA
2. ACK
CH
CM
(b)
5. ACK
4. DATA
1. RTS
2. CTS
3. DATA
6. ACK
CM(D)
CM(S)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

Figure 7. (**a**) Flow chart demonstrates Non-safety message transmission and (**b**–**d**) handshake between vehicles during NSM transmission (NSMT).

4. Emergency Vehicle Management

The proposed method ensures particular support for EVs. Firstly, the vehicles are divided into two parts in order to keep the EVs separate from the general vehicles. This will increase the searching speed during authentication. If all of 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 of the vehicles are together.

On the other hand, during inter-cluster handover after completing the authentication process, the CH immediacy broadcasts an SM to all of its members to inform regarding the presence of an EV. After receiving the SM, all of the vehicles will clear the left lane, so that the EV will obtain 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.

5. Implementation

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

5.1. Tools

5.1.1. 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 that are written in smart contract by using this framework. Additionally, it provides network management, scripting, and client-side development services [33].

5.1.2. Ganache Emulator

Ganache is a virtual ethereum blockchain emulator [34]. It can be used as real blockchain, as it provides all of 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 platformed independently and two variants (UI and CLI) are available. UI version is used for this implementation.

5.1.3. Metamask Ethereum Wallet

In this implementation, metamask wallet [35] is presented for currency management in the ethereum blockchain. All of the members will use metamask to connect and perform transactions in the blockchain. 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.

5.1.4. Node Packet Manager (NPM)

Both of the blockchains are hosted on the web for easy access. NPM [36] 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 [37] is used in order to develop the client-side in HTML.

5.2. 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 in order to provide web based services. All of the LABC are members of this blockchain. All of the machines are using Ubuntu-18.04.4-desktop-amd64 operating system and are connected to each other by using internet connections. The parameters are available in Table 2.

Another VM is configured with the same programs and is considered to be 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 that is installed in the Firefox web browser. By using RPC, a metamask is connected to the virtual private blockchain hosted in the VM. During a 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.

Table 2. Configuration of the experimental setup.

Machine	No of CPU	Memory	Storage	OS
GABC-VM	2	3 GB	40 GB	Ubuntu-18.04.4-desktop-amd64
LABC-VM	2	3GB	30 GB	Ubuntu-18.04.4-desktop-amd64
CH-VM$_1$	1	2 GB	20 GB	Ubuntu-18.04.4-desktop-amd64
CH-VM$_2$	1	2 GB	20 GB	Windows 7 Ultimate (64 Bit)

All of the local CHs are the members of the LABC. Two more VMs with two different OSs are configured in order to represent the CHs, as a member CH will download all of the contents of the LABC. During vehicle registration in the cluster, these CH-VMs use a metamask wallet to perform search operations in the LABC. Whenever a vehicle becomes CH, it becomes a member of the LABC and it will download all of the transactions, i.e., local vehicles' public keys and types.

All of the necessary programmings for vehicle authentication during cluster joining and temporary access permission are written using solidity, which is a popular language for writing smart contracts. The program for the GABC consists of two functions, the first one to add a new vehicle in the blockchain and the second to view or search the existing public keys from the database. All of 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 in order to check the authentication of the vehicles during cluster joining process. There is another function that 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 for disabling the entry of the visitor vehicle. This one is used to reduce the storage requirement and all the members (LAC and all of the CHs) updated their storage accordingly.

During cluster joining, after receiving the public key and the 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, then the CH will store the key in the CM list and start communicating as a member.

For temporary access permission, a 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 register 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 be generated, which disables the entity from the LABC.

6. Performance Analysis

6.1. Performance Analysis of the Authentication Protocol

The CH will check the validity of the requested vehicle's public key from the LABC in order to ensure secured authentication whenever a vehicle wants to join in a cluster. The communication between the CH and blockchain server is secured by the RSA-1024 PKI algorithm. Before sending the public key of the requested vehicle, the CH digitally signs that by using its private key and sending a search request to the blockchain server. The server decrypts the message, performs a search in the blockchain, and sends the results by signing it with its own private key. The result will only be 1 bit in order to confirm the authentication where 0 and 1 represent not found and found, respectively.

For faster authentication, the RSA-1024 digital signature algorithm is used, as it lightweight and provides comparatively strong security. RSA-1024 has a security strength of 80-bits, which signifies that it requires at least 2^{80} operations in order to guess the private key [38]. 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 methods use Road Side Unites (RSUs) to handle the authentication, but those infrastructures are too costly.

6.1.1. Computational Overhead

For the ACB-MAC system, its requires 1.48 ms to sign and 0.07 ms (total 1.55 ms) in order to verify a signature that is generated by RSA-1024 digital signature algorithm for a 1.5 GHz processor [39]. Although the reply is only 1 bit, for request and reply, it required maximum 3.10 ms.

In [24], Lin et al. used the Elliptic Curve Digital Signature Algorithm (ECDSA), where their proposed method has an average computational latency of 3.6 ms for sign and 7.2 ms for verification (total 10.8 ms). However, in [25], Wang et al. proposed two different methods that are authenticated during joining and handover. It took an average of 10 ms and 20 ms for initial and handover authentication, respectively. The proposed method performs better in terms of computational cost than other authentication protocols, like SPRING [27], IBCPPA [28], IBV [26], DSSCB [23], EAPP [29], BCPPA [24], and B-TSCA [25]. Figure 8a shows the comparison between different previously proposed methods.

During registration, the LAC is responsible for generating keys for the vehicles. A computer with a 3.1 GHz processor and 4 GB memory will only require 97 ms to generate keys for a vehicle [38], which means that it is possible to generate at least 10 keys in every second. Searching for a vehicle during authentication for a dedicated blockchain server and then encrypting one bit of data before sending the response 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 10% EV exists in a database, then the search for the EV will become 10 times faster than a database, where all of the vehicles are not classified. This way, the proposed method ensures faster authentication for both vehicle types.

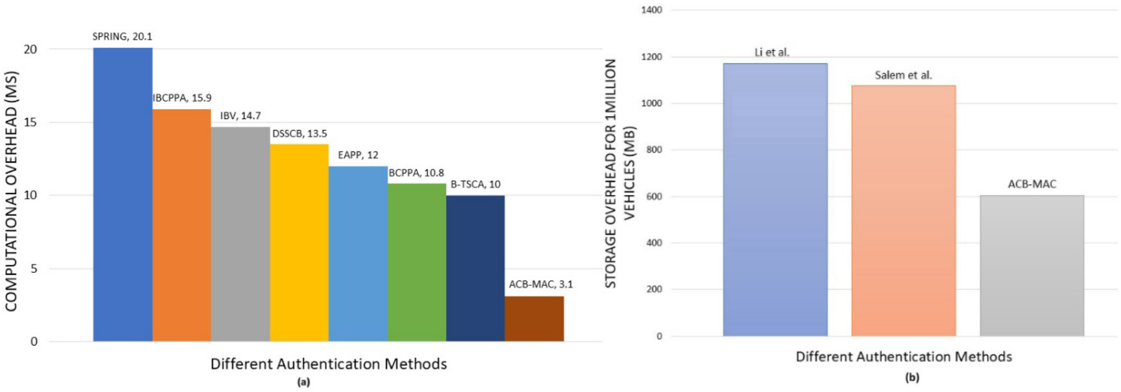


Figure 8. (**a**) Computational and (**b**) storage overhead comparison with the proposed cluster-based Medium Access Control (ACB-MAC) protocol.

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, in order to store one public key (generated by RSA-1024) of a vehicle, it requires approximately 636 bytes (508 byte header + 128 byte public key). Thus, a LAC with one-illion vehicles only requires 606 MB of storage. Similarly, CHs have to store the same information, thus they also require similar storage. In [31], it requires 1172.3 MB to store one-million identity information of the vehicles and 810.3 MB for a data total 1982.6 MB. While, in the proposed method of Salem et al., it requires 1126 bytes for vehicle authentication, i.e., 1.05 GB of storage required, which is double our proposed method [32]. Figure 8b shows the comparison between different previously proposed methods. Thus, a vehicle may require at least 606 MB of storage to become a member of LACB, which is a very small amount to ensure security, authenticity, privacy, etc. of vehicles, and it is a minimum of the mentioned methods.

6.1.3. Propagation Delay

The enhancement of internet speed in the 5G technology enables faster communication between vehicles and infrastructures. In order 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. In order to download data for one million vehicles, i.e., 606 MB of data, it will require less than 5 s with a download speed of only 1 Gbit/second.

6.2. Performance Analysis of VSN

In order 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 of the required equations are previously derived in [2].

6.2.1. Throughput Analysis

In order to calculate the throughput of the safety and non-safety messages, we have considered *S* as the normalized throughput and it is presented by the following equation (as derived in [2]).

$$S_k = \frac{P_s P_{busy} L}{T_e} = \frac{P_s P_{busy} L}{P_i T_{slot} + P_{busy} P_s T_s + P_{busy}(1 - P_s) T_c} \tag{1}$$

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 a collision. From this equation, normalized throughput for SMT for *kth* cluster can be presented as:

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

Additionally, for NSMT, it can be presented as:

$$S_{knsm} = \frac{(x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)}L}{(1-P_{(t-cl)})^{(x-1)}T_{slot}+(x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)}T_{s-nsm}+[(1-(1-P_{(t-cl)})^{(x-1)})-((x-1)P_{(t-cl)}(1-P_{(t-cl)})^{(x-2)})]T_c} \tag{3}$$

From these equation, we can calculate the normalized system throughput of the system, being presented as:

$$S = \sum_{k=1}^{j} S_k \tag{4}$$

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 the PDR of SMT will be:

$$PDR_{sm} = (1 - P_s)^{M_{rsm}} \tag{5}$$

Additionally, if M$_{rnsm}$ is the maximum retransmission limit, then the PDR of NSMT will be:

$$PDR_{nsm} = (1 - P_s)^{M_{rnsm}} \tag{6}$$

6.2.3. Delay Analysis

The time that is required to transmit a message successfully is considered as the 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:

$$E[D] = E[T_{interval}] - \frac{P_{fdrop}}{1 - P_{fdrop}} \times E[T_{drop}] \tag{7}$$

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:

$$E[D_{sm}] = T_e(n - \frac{P_{drop}}{1 - P_{drop}} \times \frac{2}{1 + CW + M_{rsm}CW/2}) \tag{8}$$

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

$$E[D_{nsm}] = T_e(n - \frac{P_{drop}}{1 - P_{drop}} \times \frac{2}{1 + CW + M_{rnsm}CW/2}) \tag{9}$$

6.2.4. Numerical Analysis and Discussions

A numerical analysis is performed by using MATLAB to present the performance of the ACB-MAC protocol. Numerical research is performed. Where each road width is 5 m, a VANET of randomly distributed cars driving through a two-lane road is considered. In a cluster, we assume that all of the vehicles 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 in order to compare it with the proposed method. Besides, a quantitative comparison is described with previous methods that are based on clusters. Table 3 provides the value of variables used in numerical analysis.

Table 3. Data used for numerical analysis.

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

Figure 9a,b display the changes in the system throughput with the increment of the number of vehicles and also with the different cluster sizes, respectively. The cluster size shown in Figure 9a 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, which causes more collisions and deteriorates throughput. In addition, Figure 9b indicates that the throughput depends on the cluster size also. For the clusters with a large amount of vehicles, the probability of packet collision is high, which will minimize the throughput. On the other hand, a cluster with small amount of vehicles is not able to utilize the available bandwidth. Because 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, awaiting for CTS is not necessary. However, NSM is targeted for a CM, not for all CMs. Therefore, NSM would not be broadcast. After RTS and CTS delivery, NSM will be transmitted to the intended CM in order to prevent hidden node issues and confirm that the CM is still in the cluster.

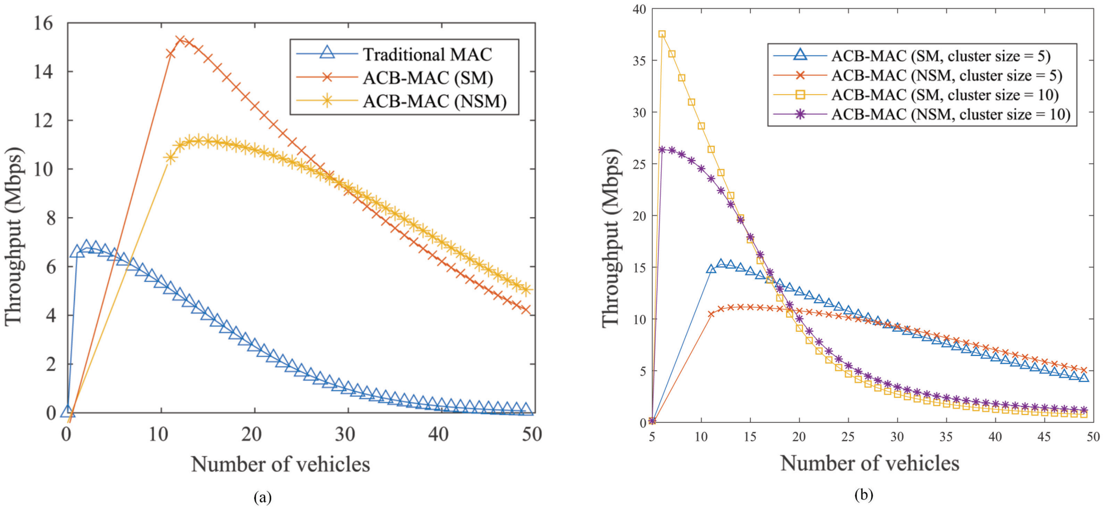


Figure 9. (**a**) Comparison of throughput against number of vehicles and (**b**) throughput of the proposed method under different cluster sizes.

Figure 10a displays the PDR against the number of vehicles. 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, which is more than NSM, since the retransmission threshold for NSM is lower, and, without RTS/CTS delivery, SM is instantly transmitted. While the PDR of SM are larger than NSM, until all of the ACKs are obtained, SM can be retransmitted. Figure 10b shows the average delay of the packet versus the number of vehicles. As the number of vehicles increases, the average packet delay increases significantly. The risk of collision, as well as PDR and delay, increase with the increment in the number of vehicles. When the traffic is less, the delay of NSMT is a little higher because of RTS/CTS, but the delay becomes less than traditional MAC as traffic rises. However, the latency for transmission of SM is lower than traditional MAC and the ACB-MAC protocol reaches the 100 ms latency requirement for SM.

In the same network model, the overall throughput that is attained against the number of vehicles in developed cluster-based schemes is approximately 1.1 Mbps, 1.3 Mbps, and 11 Mbps, respectively, for [8,12,15]. In the CB-MAC protocol, on the other hand, the maximum throughput is about 15 Mbps. In [11], the latency for SM is 151 ms, which is more than the requirement of latency of SM. The average delay is larger than the SDR [14]. It is clear that the proposed method continuously maintains high throughput as well as the SDR of 100 ms for SMT.

6.3. Discussions

The proposed method successfully utilizes a light weight digital signature method in order 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 3.10 ms, which outperforms some of the previously proposed methods ([23–29]). Moreover, the storage requirements for the proposed method is smaller than [31,32]. In order 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 two times for GV than the method, where all of 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 of the vehicles are using 5G high-speed internet connection; thus, the propagation delay during authentication is ignorable.

In order to remove the huge expanses of the RSU based VANETs, in this paper we proposed a 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 quick broadcasting algorithm of the SMT ensures the SDR of 100 ms. Additionally, RTS/CTS supported NSMT protocol removes the shortcomings of the hidden node problems in order to increase the throughput and 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 a maximum throughput of 15 Mbps, which is better than some of the previously proposed methods, for example, [8,12,15].

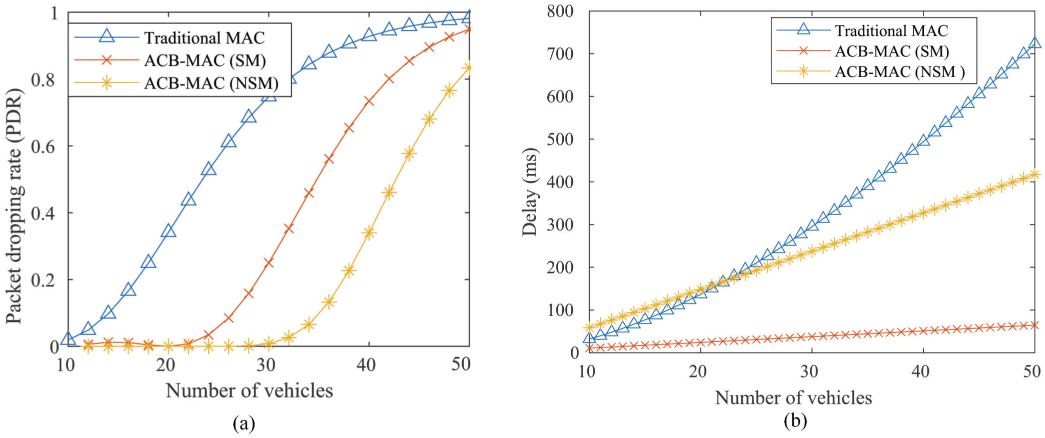


Figure 10. (**a**) Packet Dropping Rate (PDR) and (**b**) Delay of the proposed method against number of vehicles.

7. Security Analysis

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

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, the blockchain based storage system verify the authenticated vehicles. During any transaction in any of the blockchain, the vehicles and the LAC confirm its authenticity and non-repudiation by signing the messages while using their private keys.

7.2. Preserving the Privacy of the Vehicles

All of 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 is strongly preserved. Additionally, it is not possible to obtain the real identity, even if attackers got the public-private key pairs of a particular vehicle.

7.3. Security, Confidentiality and Integrity of the Transactions

All the transaction in the proposed ACB-MAC protocol is signed by the senders to ensure 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 2^{80} number of operations are required to break the keys [41]. All of the transactions are checked by the hash value in order to ensure the integrity of the transactions.

7.4. Attack Prevention

- RSA-1024 digital signature algorithm is considered to be secured until the primary key is broken by the attacker [42]. Accordingly, the communication between the vehicles and LAC are theoretically secured in the proposed ACB-MAC protocol.
- 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.
- The proposed digital signature algorithm uses hash value in order 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.
- ACB-MAC is free from DDoS attack, as no unauthorized vehicles can perform any transaction. Physical and public key verification are both required to become a member of a cluster.

7.5. Decentralization, Flexibility, Temper-Resistance, Immutability, Fairness, Transparency, and Robustness

- 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.
- Ethereum is a platform that is independent and accessible by using metamask wallet [35] from Windows, MAC, Linux, etc., as well as from cellphone operating systems, like iOS and Android.
- All of the vehicles information details are stored in a blockchain, thus the information is free from single-point-of-failure and, together, ensure their robustness.
- Blockchain is also famous for its hash based chronological storage technique, which ensures tamper resistance and immutability of the authentication information of the vehicles.
- All of the members are treated equally by the blockchain to ensure fairness between the members. In order to provide additional and faster facilities to the EVs, we have used other techniques outside the blockchain.
- Smart contract is utilized in order to allow guest vehicles temporarily. It also allows for removing the guest vehicles from the LABC automatically after the requested time period.

8. Conclusions

A cluster based method is presented in this paper in order to manage VSN, where one of the vehicle become CH to manage the communication as well to check the authenticity of the vehicles during the cluster joining process. For VSN, the transmitted messages are divided into two categories; important information is considered as SM that must be delivered within SDR of 100 ms, 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 blockchains is used in order to store the detailed information regarding 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 of the LACs are the members of the GABC and all of 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 in order to ensure faster member authentication. In the proposed method, in order 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 two times for GV than the method, where all of 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 in order to inform all of the members to clear the left lane and give free passage to the EV. This way, the 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 in order to ensure the safety, security, integrity, confidentiality, etc. of the communication between vehicles and blockchains. Additionally, blockchain provides robust, decentralized, and distributed database services, including security, flexibility, temper-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. The results show that it requires 3.10 ms time for the authentication process, which is better than [23–29]. However, to store one-million vehicles' authentication information, it requires 606 MB, which is minimum and less than the proposed method, like [31,32]. Because of high speed 5G internet, the proposed method requires ignorable propagation time. Moreover, internet based communication removes the high infrastructures expense. Mathematical and numerical analysis of the proposed message transmission protocols were also presented, which shows that the proposed method provides better throughput, lower delay, and lower PDR from the traditional MAC protocols and other previously proposed method, like [8,12,15]. In the future, we are planning to implement a consensus protocol with the blockchain in order to collect abnormal behaviours of the vehicles from their neighbour vehicles for behavioural analysis or reputation management. It will add some more security features, for example, removing the possibility of compromised attacks and also helping to take actions against malicious or abnormal behaviours.

Author Contributions: Conceptualization, A.F.M.S.A. and M.A.; methodology, A.F.M.S.A. and A.F.M.S.S.; software, A.F.M.S.A.; validation, A.A., M.A. and A.Z.; formal analysis, A.F.M.S.A.; investigation, A.F.M.S.A. and A.A.; resources, A.F.M.S.S.; data curation, A.A.; writing—original draft preparation, A.F.M.S.A.; writing—review and editing, A.A.; visualization, A.F.M.S.S.; supervision, A.Z. and M.A.; project administration, M.A.; funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MAC	Medium Access Control
ACB-MAC	Authentication for Cluster Based MAC protocol
ITS	Intelligent Transport System
IPS	Intelligent Payment System
VANET	Vehicular Ad hoc Network
OBU	On Board Unit
RSU	Road Side Unit
VSN	Vehicular Social Networking
SDR	Strict Delay Requirement
PKI	Public Key Infrastructure
PDR	Packet Dropping Rate
GV	General Vehicle
EV	Emergency Vehicle
CH	Cluster Head
CM	Cluster Member
TDMA	Time Division Multiple Access
PoC	Proof of Concept

FSM	Finite State Machine
UML	Unified Modeling Language
GPS	Global Positioning System
RClM	Request to Cluster Merging
RTCF	Request to Cluster Formation
ReTCl	Registration to Cluster
RTS	Request to Send
CTS	Clear to Send
SIFS	Short Inter-Frame Space
MPK	Member's Public Key
ClI	Cluster Information
CM-ID	Cluster Member Identity
CHA	Cluster Head Address
CMI	Cluster Member Information
Rt	Number of Retransmission
M_{rsm}	Maximum Retransmission Limit for SM
ACK	Acknowledgement
M_{rnsm}	Maximum Retransmission Limit for NSM
SM	Safety Message
NSM	Non-Safety Message
SMT	Safety Message Transmission
NSMT	Non-safety Message Transmission
GAC	Global Authentication Center
LAC	Local Authentication Center
GABC	Global Authentication Blockchain
LABC	Local Authentication Blockchain
RPC	Remote Procedure Call
NPM	Node Packet Manager
DApp	Decentralized Application
VM	Virtual Machine
CCH	Control Channel

References

1. Association, I.S. *IEEE Std 802.11-2016, IEEE Standard for Local and Metropolitan Area Networks—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; IEEE: Piscataway, NJ, USA, 2016.
2. Shah, A.S.; Ilhan, H.; Tureli, U. CB-MAC: A novel cluster-based MAC protocol for VANETs. *IET Intell. Transp. Syst.* **2018**, *13*, 587–595.
3. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66.
4. Isaac, J.T.; Zeadally, S.; Camara, J.S. Security attacks and solutions for vehicular ad hoc networks. *IET Commun.* **2010**, *4*, 894–903.
5. Ahmed, M. False image injection prevention using iChain. *Appl. Sci.* **2019**, *9*, 4328.
6. Ahmed, M.; Pathan, A.S.K. Blockchain: Can It Be Trusted? *Computer* **2020**, *53*, 31–35.
7. Rahman, A.; Islam, M.J.; Rahman, Z.; Reza, M.M.; Anwar, A.; Mahmud, M.A.P.; Nasir, M.K.; Noor, R.M. DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium. *IEEE Access* **2020**, *8*, 209594–209609.
8. Wang, H.; Liu, R.P.; Ni, W.; Chen, W.; Collings, I.B. VANET modeling and clustering design under practical traffic, channel and mobility conditions. *IEEE Trans. Commun.* **2015**, *63*, 870–881.
9. Yang, F.; Tang, Y. Cooperative clustering-based medium access control for broadcasting in vehicular ad-hoc networks. *IET Commun.* **2014**, *8*, 3136–3144.
10. Yang, F.; Tang, Y.; Huang, L. A multi-channel cooperative clustering-based MAC protocol for VANETs. In Proceedings of the 2014 Wireless Telecommunications Symposium, Washington, DC, USA, 9–11 April 2014; pp. 1–5.
11. Su, H.; Zhang, X. Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3309–3323.
12. Gao, N.; Tang, L.; Li, S.; Chen, Q. A hybrid clustering-based MAC protocol for vehicular ad hoc networks. In Proceedings of the 2014 International Workshop on High Mobility Wireless Communications, Beijing, China, 1–3 November 2014; pp. 183–187.
13. Hafeez, K.A.; Zhao, L.; Mark, J.W.; Shen, X.; Niu, Z. Distributed multichannel and mobility-aware cluster-based MAC protocol for vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2013**, *62*, 3886–3902.
14. Ucar, S.; Ergen, S.C.; Ozkasap, O. Multihop-cluster-based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination. *IEEE Trans. Veh. Technol.* **2015**, *65*, 2621–2636.

15. Zhang, M.; Li, C.; Guo, T.; Fu, Y. Cluster-based content download and forwarding scheme for highway VANETs. *China Commun.* **2018**, *15*, 110–120.
16. Javaid, U.; Aman, M.N.; Sikdar, B. DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
17. Lai, C.; Ding, Y. A Secure Blockchain-Based Group Mobility Management Scheme in VANETs. In Proceedings of the 2019 IEEE/CIC International Conference on Communications in China (ICCC), Changchun, China, 11–13 August 2019; pp. 340–345.
18. Malik, N.; Nanda, P.; Arora, A.; He, X.; Puthal, D. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In Proceedings of the 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), New York, NY, USA, 1–3 August 2018; pp. 674–679.
19. Ali, I.; Gervais, M.; Ahene, E.; Li, F. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *J. Syst. Archit.* **2019**, *99*, 101636.
20. Kulathunge, A.; Dayarathna, H. Communication framework for vehicular ad-hoc networks using Blockchain: Case study of Metro Manila Electric Shuttle automation project. In Proceedings of the 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE), Colombo, Sri Lanka, 28 March 2019; pp. 85–90.
21. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. Bars: A blockchain-based anonymous reputation system for trust management in vanets. In Proceedings of the 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), New York, NY, USA, 1–3 August 2018; pp. 98–103.
22. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access* **2018**, *6*, 45655–45664.
23. Zhang, X.; Chen, X. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *IEEE Access* **2019**, *7*, 58241–58254.
24. Lin, C.; He, D.; Huang, X.; Kumar, N.; Choo, K.K.R. BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**. doi:10.1109/TITS.2020.3002096
25. 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**. doi:10.1109/TETC.2020.2978866.
26. 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; pp. 246–250.
27. Rongxing, L.; Xiaodong, L.; Xuemin, S. SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. In Proceedings of the 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
28. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A threshold anonymous authentication protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720.
29. 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.
30. Leiding, B.; Memarmoshrefi, P.; Hogrefe, D. 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, 12–16 September 2016; pp. 137–140.
31. Li, H.; Pei, L.; Liao, D.; Chen, S.; Zhang, M.; Xu, D. FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain. *IEEE Access* **2020**, *8*, 85190–85203.
32. Salem, A.H.; Abdel-Hamid, A.; El-Nasr, M.A. The case for dynamic key distribution for PKI-based VANETS. *arXiv* **2016**, arXiv:1605.04696.
33. Truffle Suite. Available online: https://www.trufflesuite.com/ (accessed on 8 April 2020).
34. Ganache. Available online: https://www.trufflesuite.com/ganache (accessed on 8 April 2020).
35. Metamask. Available online: https://metamask.io/ (accessed on 8 April 2020).
36. NPM (Software). Available online: https://en.wikipedia.org/wiki/Npm_software (accessed on 8 April 2020).
37. GitHub Lightweight Node Server. Available online: https://github.com/johnpapa/lite-servers (accessed on 8 April 2020).
38. Singh, S.R.; Khan, A.K.; Singh, S.R. Performance evaluation of RSA and elliptic curve cryptography. In Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 14–17 December 2016; pp. 302–306.
39. Nirala, R.K.; Ansari, M.D. Performance Evaluation of Loss Packet Percentage for Asymmetric Key Cryptography in VANET. In Proceedings of the 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 20–22 December 2018; pp. 70–74.
40. Wood, G.; others. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.

41. Barker, E. *Recommendation for Key Management: Part 1—General*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2006; doi:10.6028/NIST.SP.800-57pt1r5.
42. Al-Bassam, M. SCPKI: A smart contract-based PKI and identity system. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, UAE, 2–6 April 2017; pp. 35–40.