sensors

MDPI

Article

A Blockchain-Based Authentication Protocol for Cooperative Vehicular Ad Hoc Network

A. F. M. Suaib Akhter [1], Mohiuddin Ahmed [2], A. F. M. Shahen Shah [3], Adnan Anwar [4], A. S. M. Kayes [5,*] and Ahmet Zengin [1]

[1] Department of Computer Engineering, Sakarya University, Serdivan 54050, Sakarya, Turkey; suaib.akhter@ogr.sakarya.edu.tr (A.F.M.S.A.); azengin@sakarya.edu.tr (A.Z.)
[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, Avcilar 34315, Istanbul, Turkey; afmsshah@gelisim.edu.tr
[4] Centre for Cyber Security Research and Innovation (CSRI), School of IT, Deakin University, Waurn Ponds, VIC 3216, Australia; adnan.anwar@deakin.edu.au
[5] Department of Computer Science and Information Technology, School of Engineering and Mathematical Sciences (SEMS), La Trobe University, Bundoora, VIC 3086, Australia
* Correspondence: a.kayes@latrobe.edu.au

Abstract: 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.

Keywords: Internet of Vehicles; Vehicular Ad hoc Network; blockchain; distributes storage; intelligent vehicles; Vehicular Social Networking; emergency vehicles; COVID-19

Citation: Akhter, A.F.M.S.; Ahmed, M.; Shah, A.F.M.S.; Adnan, A.; Kayes, A.S.M.; Zengin, A. A Blockchain-Based Authentication Protocol for Cooperative Vehicular Ad Hoc Network. *Sensors* **2021**, *21*, 1273. https://doi.org/10.3390/s21041273

Academic Editor: Rongxing Lu

Received: 19 January 2021
Accepted: 8 February 2021
Published: 11 February 2021

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 [1–4]. 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 [5]. 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 [6].

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 1.

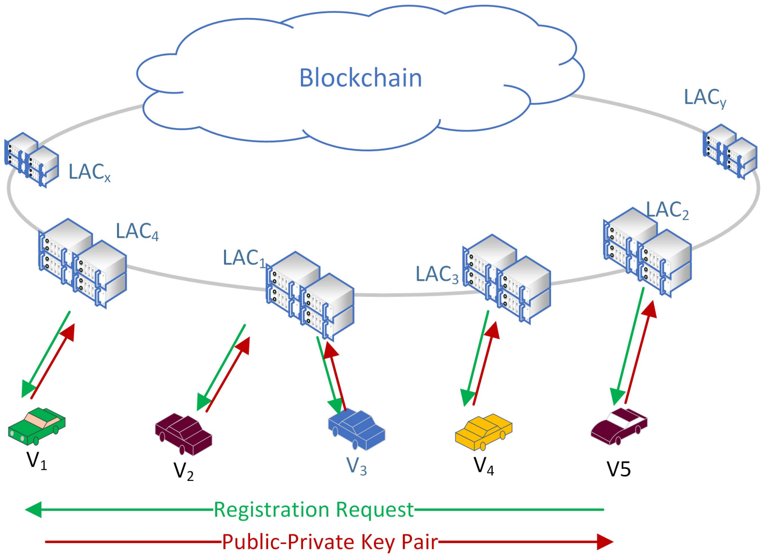


Figure 1. System structure and the registration process.

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 2. In Section 3, the structure of the blockchain based authentication schema is presented with the cooperative model of VANET. Section 4 provides the implementation details and, in Section 5, performance and security analysis of the proposed protocols are explained. Section 6 discusses the pros and cons of the proposed protocols and, finally, in Section 7, the paper is concluded by mentioning some of the possible future works.

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 [7,8], Internet of Things (IoT) [9], Smart grid [4], transportation services like smart airports [10], smart medical [11], 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 [12], trust and reputation management [13], event and message exchange management [14], intelligent payment [15], traffic investigation [16], 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 [17]. In [18], 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 [19,20], 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 [15]. 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 [21], Javaid et al. use CA for authentication and blockchain to store the authentication information, but did not mention the sign and verification overhead. In [22], 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 [23]. To increase the security services, the method generates high computational overhead. Similarly, several other protocols like [13,24–28] 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 [29,30]. All of the above mentioned protocols depending on the RSU demands expensive infrastructural supports [5]. 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 [12].

To increase the reliability of communication and enhance the VSN area, the efficiency of cooperation is already proven [31]. Several types of cooperation protocols are presented by the researchers to improve the performance of VANETs. In [32], 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 [33]. The proposed method by Taghizadeh et al. is also for EM only but unable to fulfil the SDR of 100 ms [16]. Similarly, the concurrent transmission based MAC protocol by Zhang et al. also does not fulfil the SDR and is suitable only for GMTs [34].

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 [36], a cooperative downloading protocol was presented and, in [37], 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 [38]. 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 [38] is presented in [39], where the time slots are utilized more efficiently. Similarly, Zhang et al. presented cooperation where TDMA is used with central supervision [40] and, in [41], 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 [31].

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.

Problem Statements and Motivations

- 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.
- 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 [12].
- 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.
- 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.
- 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.
- 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.
- 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.

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.

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 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.

3.2. Authentication Process

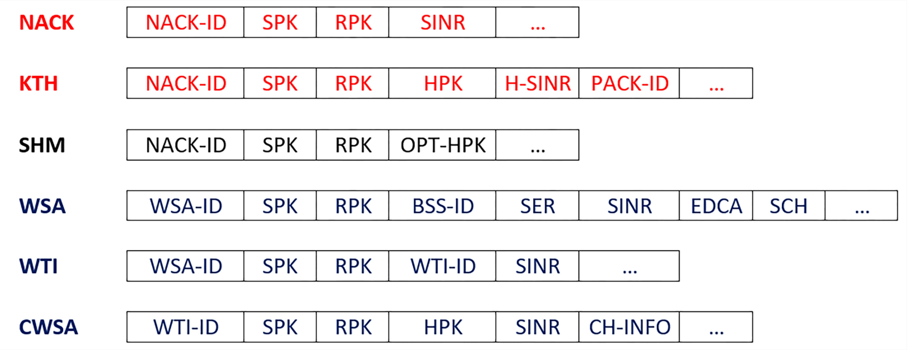
In the proposed method, there are two ways (direct and cooperative) to participate in a VSN. While driving, an IoV may receive a message or service advertisement from another source (vehicle, infrastructure, etc.). Before establishing a communication with the sender to check the authenticity of the sender, 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 [42]. 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 [43].

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 [44]. However, cooperation naturally creates extra overhead, duplication, etc., thus it requires proper management to get the best from the cooperation [31]. 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 2 and will discuss details of it in Section 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 2. Proposed packet structure for cooperative communication.

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.

3.4. *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.

3.4.1. 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 3 by using a sample scenario.

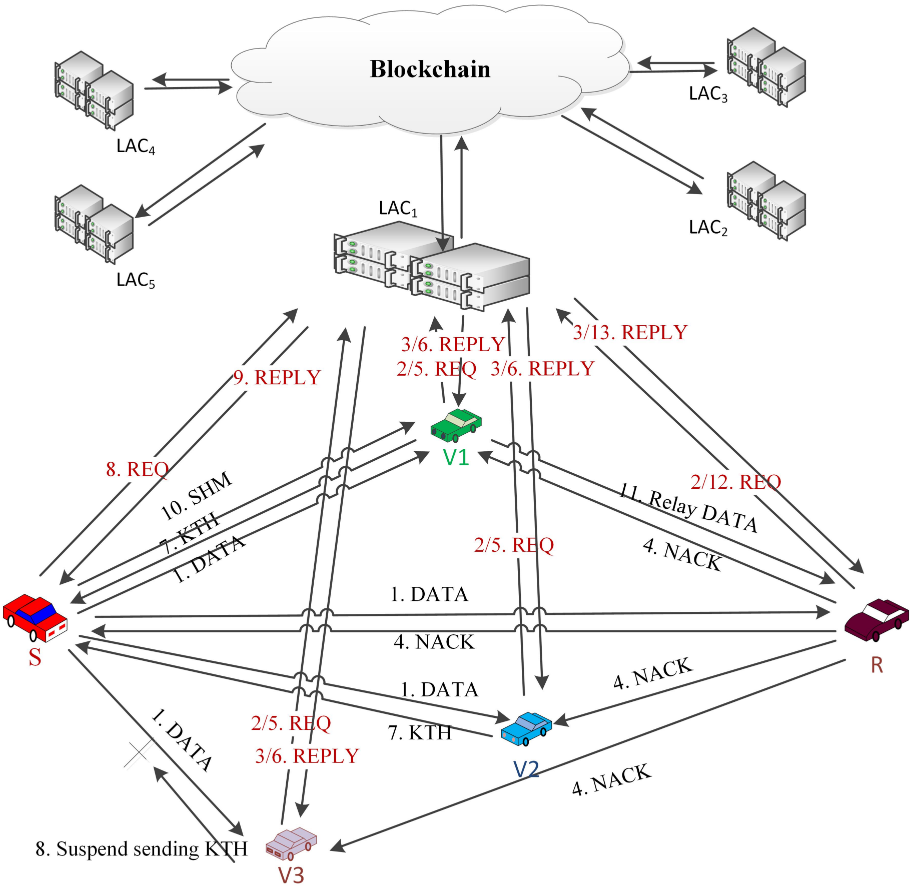


Figure 3. A sample scenario presenting EMT.

The complete process can be described as follows:

- 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.
- All the neighbouring nodes can sense that a message is broadcasted [38], 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.
- 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 2).
- S will wait for NACK until T_s (max time for successful transmission), and, if it does not receive any NACK within that time, it will consider the transmission to be successful.
- 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.
- Even after T_s 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.
- 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, 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.

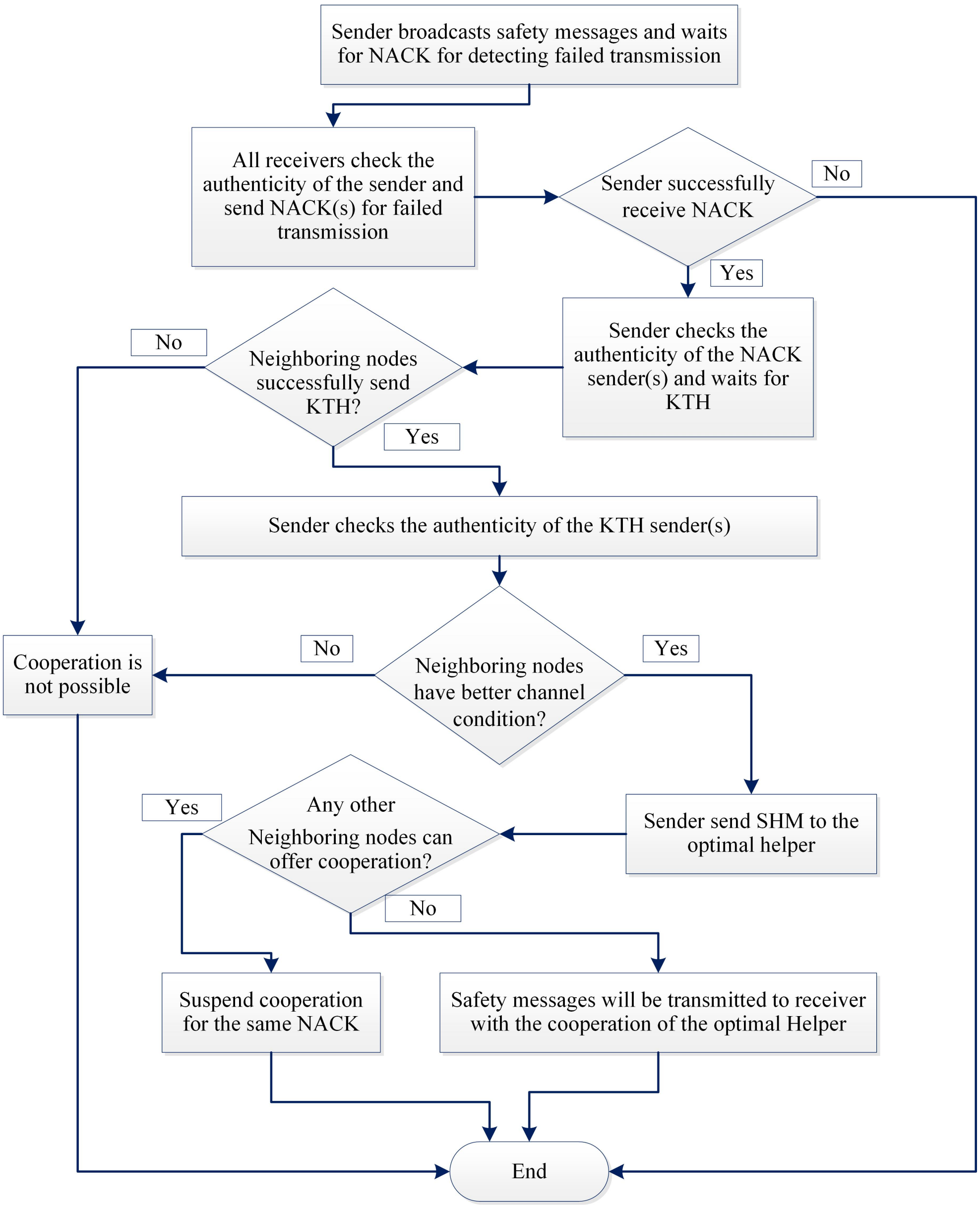

Sender broadcasts safety messages and waits for NACK for detecting failed transmission
All receivers check the authenticity of the sender and send NACK(s) for failed transmission
Sender successfully receive NACK
No
Yes
Sender checks the authenticity of the NACK sender(s) and waits for KTH
Neighboring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

Figure 4. Flow chart of the proposed EMT protocol.

3.4.2. 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 5 by using a sample scenario.

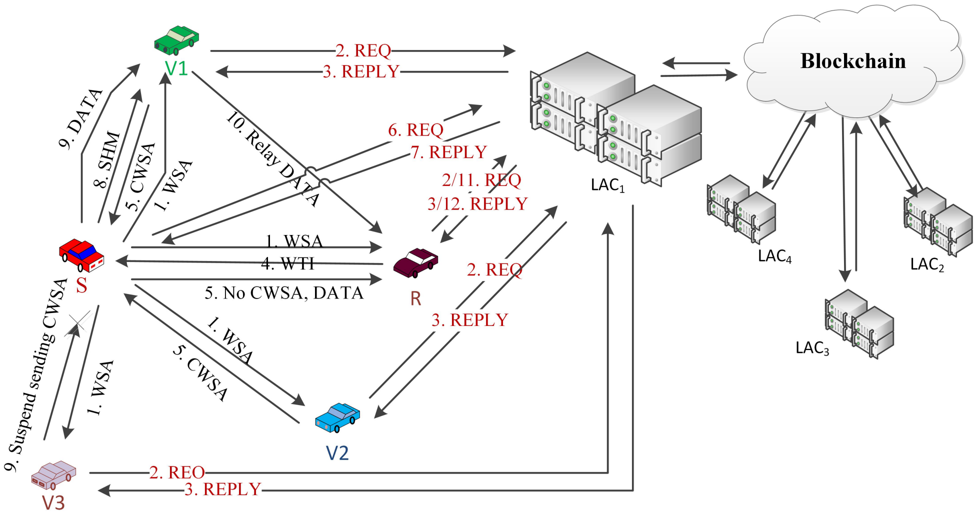


Figure 5. A sample scenario presenting GMT.

The complete process can be described as follows:

- 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.
- 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.
- 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.
- 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.
- 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.
- After sending SHM to a helper, the server stops receiving any other CWSA with the same WSA-ID. In Figure 6, a flow chart is given to show the steps.

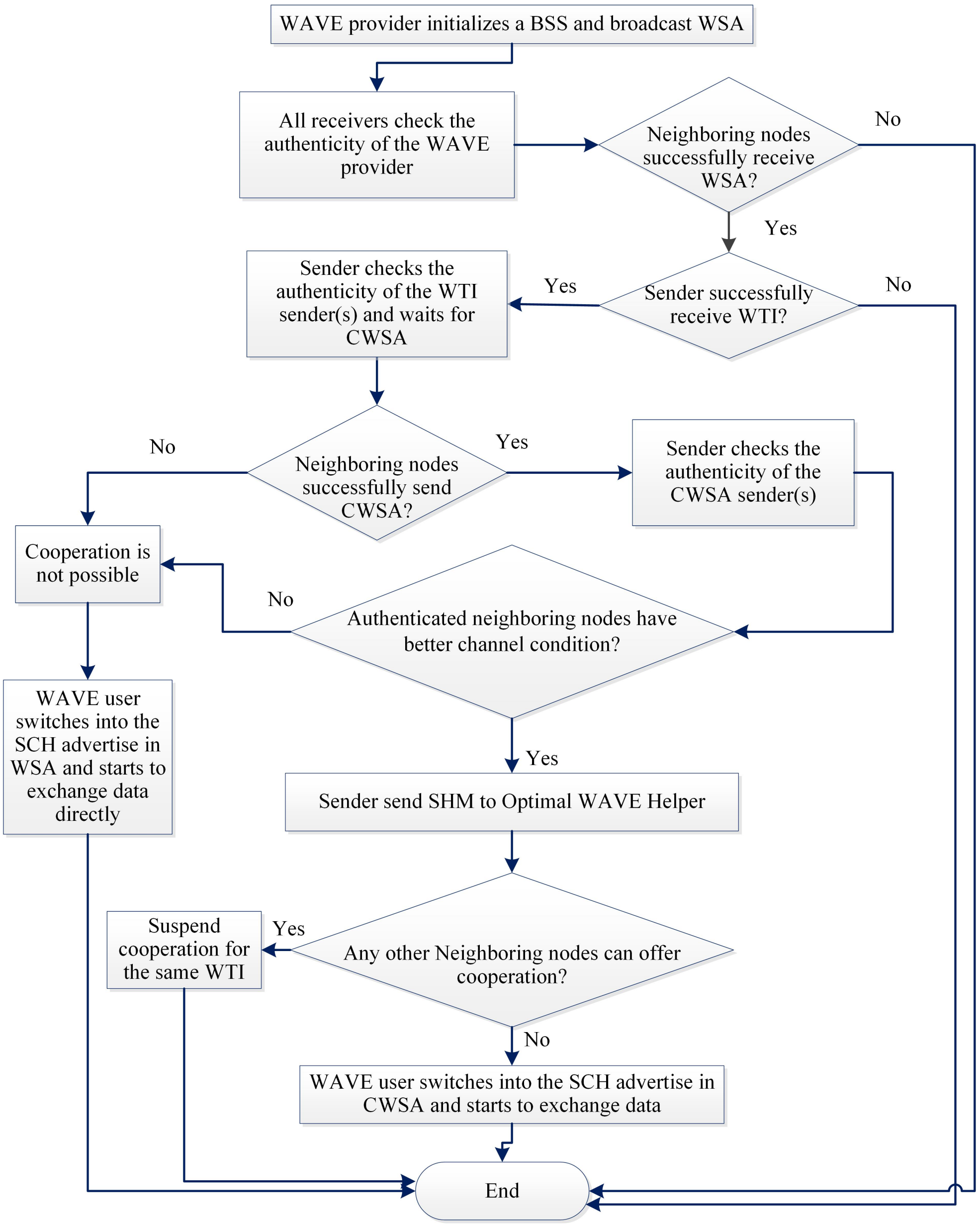

WAVE provider initializes a BSS and broadcast WSA
All receivers check the authenticity of the WAVE provider
Neighboring nodes successfully receive WSA?
No
Yes
Sender successfully receive WTI?
Yes
No
Sender checks the authenticity of the WTI sender(s) and waits for CWSA
Neighboring nodes successfully send CWSA?
No
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 6. Flow chart of the proposed GMT protocol.

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 Figures 3 and 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 1.

For the blockchain server machine, truffle framework [45] 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 [46] is used. Ganache provides all facilities of blockchain with customization, logging, and debugging supports. A Node Packet Manager (NPM) [47] is used to support JavaScript, and a node server [48] is used to implement the client side.

Table 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-VM$_S$	1	2 GB	20 GB	Ubuntu-18.04.4-desktop-amd64
IoV-VM$_R$	1	2 GB	20 GB	Ubuntu-18.04.4-desktop-amd64
IoV-VM$_{H1}$	1	2 GB	20 GB	Ubuntu-18.04.4-desktop-amd64
IoV-VM$_{H2}$	1	2 GB	20 GB	Windows 7 Ultimate (64 Bit)
IoV-VM$_{H3}$	1	2 GB	20 GB	Windows 7 Ultimate (64 Bit)

All the machines that represent IoVs use a Metamask [49] 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.

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.

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:

$$S = \frac{E_p}{T_e} \tag{1}$$

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

$$S = \frac{P_s P_{busy} L}{P_h[(1 - P_{busy})T_{slot} + P_{busy}P_s T_s + P_{busy}(1 - P_s)T_c]} \tag{2}$$

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,
T_c = probability of collision.

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

$$PDR = (1 - P_s)^{C_A} \tag{3}$$

Average packet delay can be given as:

$$E[D_{CT}] = T_{e-CT}(N - \frac{P_{fdrop}}{1 - P_{fdrop}} \frac{W_0 + 1}{2}). \tag{4}$$

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:

$$T_e = (1 - P_{busy})T_{slot} + P_{busy}P_s T_s + P_{busy}(1 - P_s)T_c \tag{5}$$

All the equations are proved and discussed in detail in [31]. Numerical analysis is presented in the next sections by comparing with the traditional MAC protocols. Data used for the analysis are presented in Table 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 [31,50].

Table 2. Sample data.

Parameter	Symbol	Value
Slot time	T_{slot}	20 (s)
Propagation delay	T_{delay}	1 (s)
DCF & Short Inter-frame space	DIFS, SIFS	50, 10 (s)
Size of the packet	L_h, 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	R_d, R_c, l	11, 1, 0.5 (Mbps)
Contention window size	CW	64 (bytes)
Transmission range	r	500 (m)
Lane width	w	5 (m)
IoVs density	D_T	0–0.5 (veh/m)
IoVs velocity	v	80 (km/h)
Average inter-vehicle distance	b	10 (m)

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 7. For the analysis, P_h is considered as 0.5 in the normal case, $P_h \leq 0.4$ as optimal and $P_h \geq 0.7$ 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.

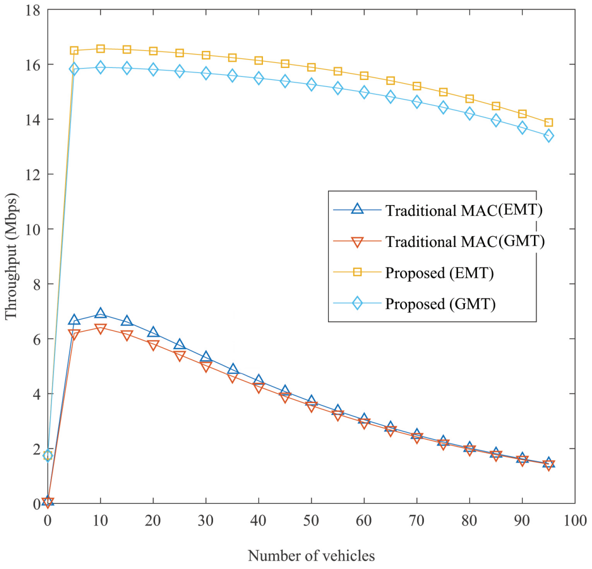


Figure 7. Throughput against no. of IoVs.

5.1.2. Delay

The average packet latency against the number of vehicles is seen in Figure 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.

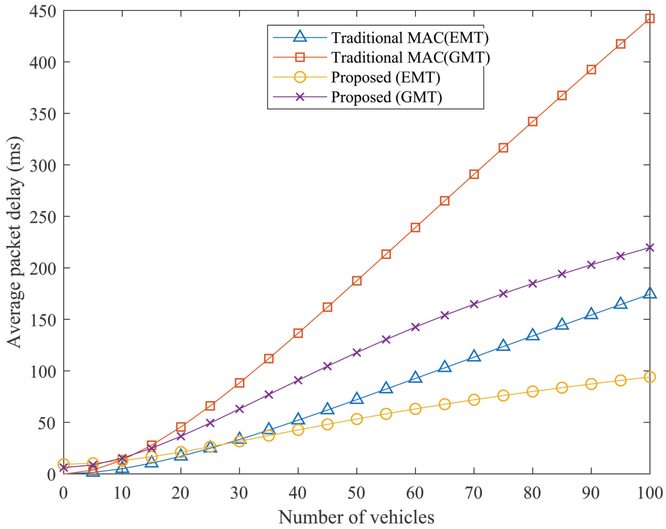


Figure 8. Delay versus no. of IoVs.

5.1.3. Packet Dropping Rate (PDR)

Figure 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 (W_0). When W_0 is greater, the increased backoff period decreases the collision and reduces the failure of the packet, thus decreasing the PDR.

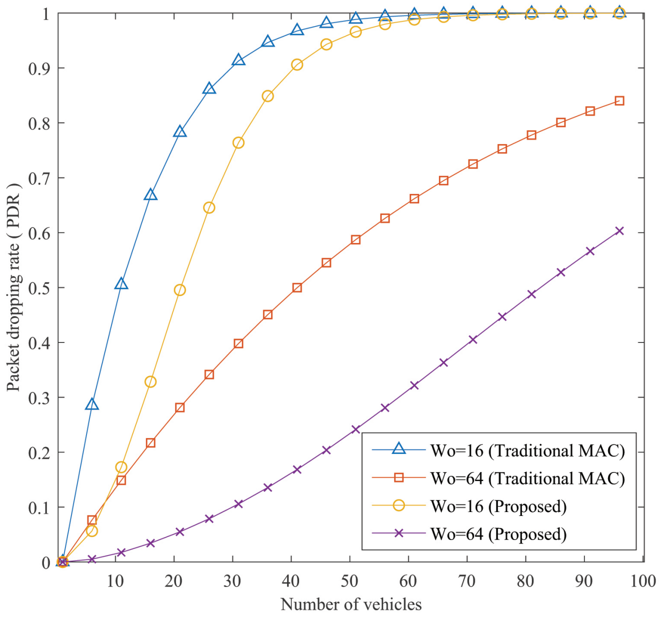


Figure 9. Comparison of the proposed method's PDR with traditional MAC.

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.

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 [51]. 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 [43]; 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 [24], 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 [13,22,25–28]. Comparison between these protocols are illustrated in Figure 10.

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.

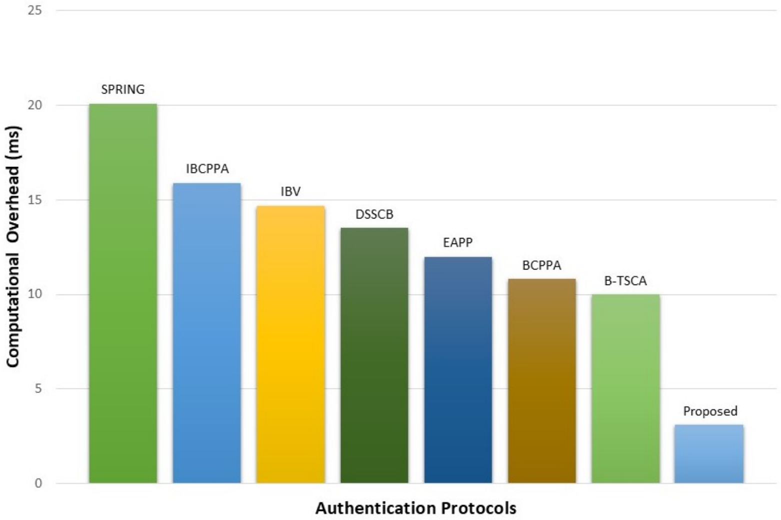


Figure 10. Comparison between time requirements of different authentication protocols.

5.2.2. Storage Overhead

The information of every registered IoVs is stored as a blockchain transaction. Each Ethereum transaction requires 508 bytes [52]. 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 [29,30]. Therefore, the proposed method requires a lower amount of storage, and storing one billion pieces of IoV information requires only 68 GB of space.

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.

- 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.
- RSA-1024 provides security that provides security strength of 80-bits. Thus, it requires 2^{80} operations to break the key that is strong enough for low power vehicles [53].
- 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.
- 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.
- 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 [54] as well.

- 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.
- 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.

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.

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 [55,56] 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.

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. and A.S.M.K.; 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.S.M.K. and A.A.; visualization, A.F.M.S.S.; supervision, A.S.M.K., 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.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Ahmed, M. (Ed.) *Blockchain in Data Analytics*; Cambridge Scholars Publishing: Newcastle upon Tyne, UK, 2020.
2. Ahmed, M. False image injection prevention using iChain. *Appl. Sci.* **2019**, *9*, 4328.
3. Ahmed, M.; Pathan, A.S.K. Blockchain: Can It Be Trusted? *Computer* **2020**, *53*, 31–35.
4. 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.
5. 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.
6. 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.

7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186.
15. 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; IEEE: New York, NY, USA, 2019; pp. 85–90.
16. 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.
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; IEEE: New York, NY, USA, 2019; pp. 340–345.
18. 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.
19. 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; IEEE: New York, NY, USA, 2018; pp. 98–103.
20. 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.
21. 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; IEEE: New York, NY, USA, 2019; pp. 1–5.
22. 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.
23. 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; IEEE: New York, NY, USA, 2018; pp. 674–679.
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. 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.
26. 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.
27. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A threshold anonymous authentication protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720.
28. 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.
29. 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.

30. Salem, A.H.; Abdel-Hamid, A.; El-Nasr, M.A. The case for dynamic key distribution for PKI-based VANETS. *arXiv preprint* **2016**, arXiv:1605.04696.
31. 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.
32. Yang, F.; Tang, Y. Cooperative clustering-based medium access control for broadcasting in vehicular ad-hoc networks. *IET Commun.* **2014**, *8*, 3136–3144.
33. 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.
34. 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.
35. 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.
36. Zhang, J.; Zhang, Q.; Jia, W. VC-MAC: A cooperative MAC protocol in vehicular networks. *IEEE Trans. Veh. Technol.* **2008**, *58*, 1561–1571.
37. Bharati, S.; Zhuang, W. CRB: Cooperative relay broadcasting for safety applications in vehicular networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 9542–9553.
38. Bharati, S.; Zhuang, W. CAH-MAC: Cooperative ADHOC MAC for vehicular networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 470–479.
39. 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.
40. 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.
41. 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.
42. Ethereum Glossary. Available online: https://ethereum.org/en/glossary/ (accessed on 8 December 2020).
43. 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; IEEE: New York, NY, USA, 2016; pp. 302–306.
44. 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.
45. Truffle Suite. Available online: https://www.trufflesuite.com/ (accessed on 8 April 2020).
46. Ganache. Available online: https://www.trufflesuite.com/ganache (accessed on 8 April 2020).
47. NPM (Software). Available online: https://en.wikipedia.org/wiki/Npm_software (accessed on 8 April 2020).
48. GitHub Lightweight Node Server. Available online: https://github.com/johnpapa/lite-servers (accessed on 8 April 2020).
49. Metamask. Available online: https://metamask.io/ (accessed on 8 April 2020).
50. 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.
51. 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; IEEE: New York, NY, USA, 2018; pp. 70–74.
52. Wood, G.; others. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
53. Barker, E.; Dang, Q. Nist special publication 800-57 part 1, revision 4. Available online: https://csrc.nist.rip/library/alt-SP800-57part1rev4.pdf (accessed on 8 April 2020).
54. Ahmed, M. Thwarting DoS Attacks: A Framework for Detection based on Collective Anomalies and Clustering. *Computer* **2017**, *50*, 76–82. doi:10.1109/MC.2017.3571051.
55. Ahmed, M.; Mahmood, A.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2015**, *60*, 19–31.
56. 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.