A Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET

Mohiuddin Ahmed, *Senior Member, IEEE*, Nour Moustafa, *Senior Member, IEEE*, A. F. M. Suaib Akhter, Imran Razzak, *Senior Member, IEEE*, Ehsanuzzaman Surid, Adnan Anwar, *Member, IEEE*, A. F. M. Shahen Shah, *Senior Member, IEEE*, and Ahmet Zengin

***Abstract*— The Industrial Internet of Things (IIoT) is creating a massive impact in a wide range of applications. In addition, with the forthcoming 5G and 6G technologies, vehicular ad-hoc networks will have pioneer advancements. However, security concerns are not well addressed, as vehicular networks should be deployed at a large scale. To address the security concerns, especially to ensure secure emergency message transmission, a blockchain-based protocol is proposed in this paper, where one of the blockchains is to store the authentication information of the vehicle, and another one to store and distribute blockchain services. Experimental analysis revealed that the proposed blockchain-based protocols are superior than the existing ones in terms of several metrics.**

***Index Terms*— Authentication, blockchain, FDIA, IoV, PoC, VANET.**

I. Introduction

VEHICLES with communication capabilities through On-Board Unit (OBU), sensing the road and traffic conditions by using sensors and Global Positioning System (GPS) are called Intelligent vehicles (IVs). Typically, an IV can use these types of equipment to create a small area network temporarily called Vehicular Ad hoc Network (VANET) according to the IEEE 802.11p standard. A VANET is formed to exchange important information like collision warnings, signal violations, etc. as well as general information like parking, gas station information, etc. between the nearby vehicles. The most important part of VANETs is to share information between vehicles by creating a Vehicular Social Networking (VSN). In the typical transmission protocols all the messages are getting equal priorities, but to provide more importance to the emergency messages, these could be divided into two categories. Important information which has strict delay requirements (SDR) of 100ms for example lane change information, congested road information, safe distance warning, accident prevention warnings, collision warnings, signal violation, etc., are called Emergency Messages (EM) and need priority while broadcasting [1]. Services like web, gaming, and information of nearby gas stations, hotels, restaurants, parking advertisements, etc. are less important compared to the EMs and categorized as General Messages (GM). Therefore, a robust protocol is necessary to transmit the messages where the EMs will get highest priority. Unfortunately, while ensuring those facilities the researchers provide less attention to ensure the security, integrity, authenticity, durability of the communications which make the system vulnerable to several types of attacks [2]. Especially the security and integrity of the EMs are very important because attackers may change the content of the message or inject false information to misguide the IoVs. Therefore, it is a principal requirement to protect the EMs from different types of attacks [3].

Although blockchain was first inaugurated to provide a third-party free financial transaction system, several areas of computer science are utilizing blockchain for its extraordinary features like distribution, decentralization, tamper resistance, immutability, availability, transparency, etc. [4]–[10]. Several blockchain-based protocols are proposed for VANET for different types of applications and it is possible to utilize blockchain for authentication and efficient message transmission too. In this paper, a multiple blockchain-based EMT protocol is proposed where one of the blockchains is to store the authentication information of the vehicle, where another one to store and distribute the EMs. All the IoVs are required to register to the Local Registration Center (LRC) which is a member of the National Registration blockchain (NRBC). Because of NRBC, all the registered IoVs are available all over the country. Another blockchain LBC is maintained by the LRCs which is responsible to store and distribute the EMs transmitted by the local IoVs. Additionally, every LRCs maintain a local location database (LDB) to monitor and store location information of the local IoVs. The location server continuously checks the position information of the running IoVs and store for Proof-of-Presence (PoP). During EM generation the server checks the position of the IoVs and calculates the Emergency Message Receivable Area (EMRA) and picks the IoVs who are currently driving in that area. Then the LBC multi-casts the EM to the EMRA. All the

Manuscript received March 22, 2021; revised June 15, 2021, August 3, 2021, and August 28, 2021; accepted September 15, 2021. The Associate Editor for this article was B. B. Gupta. *(Corresponding author: Mohiuddin Ahmed.)*

Mohiuddin Ahmed is with the School of Science, Edith Cowan University, Joondalup, WA 6027, Australia (e-mail: m.ahmed.au@ieee.org).

Nour Moustafa is with the School of Engineering and Information Technology, University of New South Wales Canberra at ADFA, Canberra, ACT 2612, Australia.

A. F. M. Suaib Akhter and Ahmet Zengin are with the Department of Computer Engineering, Sakarya University, 54050 Sakarya, Turkey.

Imran Razzak and Adnan Anwar are with the School of IT, Deakin University, Geelong, VIC 3216, Australia.

Ehsanuzzaman Surid is with the Department of Electrical and Electronic Engineering, Islamic University of Technology, Gazipur 1704, Bangladesh.

A. F. M. Shahen Shah is with the Department of Electronics and Communication Engineering, Yildiz Technical University, 34349 Istanbul, Turkey.

Digital Object Identifier 10.1109/TITS.2021.3115245

members, as well as the blockchain, use the digital signature method to communicate with each other. By default, Ethereum uses Elliptic Curve Digital Signature Algorithm (ECDSA), but as the algorithm is time-consuming in this paper a comparatively lightweight signature algorithm RSA-1024 is used to ensure integrity, confidentiality, authenticity, attack prevention ability and non-repudiation of the vehicles. Moreover, all the IoVs are assigned a public-private key pair so that they can communicate by using their public key instead of their original identity. This preserves the privacy of the IoVs. Real identities are securely stored in their LRC as well as NRC.

Efficient broadcasting is another important issue, especially for EMTs. Generally, IoVs transmitted EMs by broadcasting so that all the nearby IoVs can receive them as soon as possible. Typical IEEE802.11p protocol does not provide acknowledgment facilities, thus there is no way to be confirmed that all the related IoVs received the transmitted EMs [11]. Some of the previously proposed methods implemented the acknowledgment protocols where multiple re-transmissions are required which also increase the number of packets results in more collision. Moreover, single-point-of-failure may harm the availability of transmissions. However, EMs are irrelevant for those IoVs who are driving in opposite direction or far in front of the sender. Thus, because of broadcasting without following any protocols most of the IoVs receive several inapplicable EMs. To address this problem, a blockchain is used that receives the location information of the IoVs periodically to transmit the EMs only to the relevant IoVs. This will remove the irrelevant transmission, extra load from the network to minimize the packet collision and the IoVs get rid of inappropriate EMs. The key contributions of the proposed method can be described as follows:

- Blockchain-based vehicle authentication and emergency message storage and distribution methods are proposed in this paper. One blockchain is used to store the public keys of all the registered IoVs in a country.
- Another blockchain is used by LRCs to store and distribute EMs transmitted by local IoVs. Multiple servers are available to ensure the distribution and decentralization of the blockchains.
- The LDB is proposed to receive the Proof of presence (PoP) of the IoVs. This will help to ensure that the requested and the receivable IoVs are currently driving and no fake or malicious entity is presented themselves as IoVs. This will help to protect the system from fake, unknown vehicles and Sybil attacks.
- All the communication between the IoVs and blockchain servers are encrypted by using the RSA-1024 light-weight digital signature algorithm which ensures authenticity, non-repudiation and integrity of the messages as well as protection from several attacks like fabrication, modification, etc.
- A cooperative General message transmission protocol is proposed to increase the throughput, transmission range, and to minimize PDR and delay of the system when direct communication is not available.

A. Paper Organization

Some previously proposed blockchain-based message transmission methods and some of the cooperation protocols are discussed with their pros and cons in section II. The proposed system structure is described with the registration and message transmission methods in section III. The implementation method is described with the tools and setup details in section IV. The performance analysis of both of the message transmission protocols is presented in section V. Finally, in section VI (conclusion), enhancements of the proposed methods are presented with future research direction.

II. Previous Works

The section is divided into three parts to explain the utilization of blockchain in VANET first, followed by previously proposed cooperative message transmission protocols. Finally, the problem statement with the motivation of this work is explained in the last section.

A. Utilization of Blockchain in VANET

Several areas of VANET are utilizing blockchain for its extraordinary features like distribution, decentralization, tamper resistance, immutability, availability, transparency, etc. Message and event information storing and distributing are one of the areas where blockchain is implemented. For example, a consortium blockchain is utilized by Zhang *et al.* in [12] to store important information like position, direction, location as well as authentication information of the vehicles. Blockchain is used by Javaid *et al.* to store registration information as well as the status of the vehicles [13]. To ensure fast authentication and handover Li *et al.* proposed a method called SEBGMM [14]. 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 [15], [16] authors also use blockchain to store the authentication information and ensure the privacy of the vehicles. Ali *et al.* presented a method to ensure integrity and trust of vehicles where a blockchain is used to stores the identity of the authorized vehicles and another to store the unauthorized or revoked vehicles [17]. In [18], [19] researchers proposed a privacy-preserving trust model to provides security features including transparency, conditional anonymity, efficiency and robustness. They used two blockchains to store the identity of the certified vehicles, revoked vehicles. Another blockchain is also used to store the messages which are transferred between vehicles. In the proposed method of Zhang *et al.* important event information like traffic violations, accidents are stored by a blockchain for future investigation [20]. To handle a load of computational support they used Mobile Edge Computing (MEC).

It is clear that blockchain is used to utilize its security features but In the above-mentioned papers all the events or messages are considered similar and thus all of those are stored. But it requires a huge amount of storage and creates too much computational overhead. Some of them use multiple blockchains to store different types of information but suffers from scalability problem [14], [17]–[19], [21]. In [22], it requires removing old data to allocate new data.

Zhang *et al.* use RSUs for storage support for blockchain but RSU requires extra infrastructural expanses [12]. In [20] only critical information is stored but sometimes related emergency messages are required to get a clear idea about the incident. However, to increase the scalability in [21]–[23] multiple levels of blockchain are proposed where local blockchains synchronized with the global one to minimize the storage overhead.

B. Cooperative Message Transmission Protocols

For the communication reliability and the enhancement of the VSN area, the cooperation efficiency is proven [11]. Researchers have worked with several cooperation protocols to make better VANETs. In [24], an Emergency Message Transmission (EMT) system has presented a cluster-based VANET which can only be formed when the channel is free. Woo *et al.* [25] proposed an EMT cooperative protocol but they did not consider the effect of mobility. In [26] Taghizadeh *et al.* considered EMT but the criteria do not fulfillment of SDR of 100ms. Zhang *et al.* showed a transmission MAC protocol in their work but it was for GMTs only and is not able to fulfill the SDR. The proposed method of Zhou *et al.* suffers from an increased possibility of collision as they utilized RTS/CTS handshaking which creates additional overhead [27]. The RTS/CTS handshaking is not applicable for EMTs. In [28], [29], a cooperative downloading protocol is presented where relay broadcasting is demonstrated but neither work discussed the transmission delay and PDR. In [30], Bharati *et al.* proposed a cooperation method for Time Division Multiples Access (TDMA). But the work supported point-to-point (P2P) only and due to the unavailability of slots broadcasting of EMs is not possible. Although more efficient use of the time slots is proposed in [31], the problem remains the same. Omar *et al.* showed a TDMA based method VeMAC in [32] and Zhang *et al.* explained how TDMA with central supervision can be used in [33]. The dynamic infrastructure of VANETs and high mobility causes minimization of throughput and adds additional delay as it is not possible to utilize the radio resources properly in TDMA.

C. Motivations

Although blockchain could be utilized to get efficient features it is difficult to implement that for lightweight devices. As the devices are not able to perform complex encryption-decryption operations. Moreover, ensuring distribution storage requires higher storage because of data duplication. Therefore it requires well planned, controlled implementation of blockchain. On the other hand, cooperation can be proved efficient only when it is designed and maintained properly. Typical cooperation-based systems face several obstacles to implement a proper cooperative message transmission system. Therefore improving the cooperative protocol is still an open area of research. This research is targeted to find a secured and efficient cooperative transmission method.

III. System Structure

This section is divided into two parts to describe the proposed system structure. The registration process of the IoVs is discussed followed by the details of VSN which includes the description of the blockchain-based emergency message transmission (EMT) protocol and cooperative general message transmission (GMT) protocol.

A. Vehicles' Registration

Two blockchains are used in this structure. One is to store the registration information of the IoVs called national registration blockchain (NRBC) and another to store and manage the distribution of the local EMT called local blockchain (LBC). All the IoVs are required to register to the LRC to get the pair of the public-private key. LRC generates a key pair for the IoVs and stores all their information in a secured storage system to preserve their privacy. For any type of communication, the IoVs will be known by their public keys to hide their original identity. A blockchain called NRBC is there to store the public keys of the IoVs and share them with the blockchain which handles the EMT i.e., LBC. Additionally, every LRCs maintain a local location database (LDB) to monitor and store location information of the local IoVs. Local tracking is a real-time process and the databases that store the location information need to be updated very frequently. Thus there will be a lot of update operations running always and the server is always busy. On the other hand, blockchain is a secured database and needs to perform multiple tasks before storing any information and frequent updating as well as broadcasting is difficult to manage. However, too much replication will also require additional time and energy. Thus, in the proposed system we did not involve blockchain to store and manage location information rather location database provides the location information only when the blockchain server requests for it. The location server continuously checks the position information of the running IoVs and store for Proof-of-Presence (PoP). During EM generation the server checks the position of the IoVs and calculates the EMRA and picks the IoVs who are currently driving in that area. Then the LBC multi-casts the EM to the EMRA.

A national registration center (NRC) maintains another blockchain named NRBC and all the LRCs are connected with the NRBC as a member node to share the IoVs registration information. In this way, all the IoVs' information is accessible to all the LRCs. While any IoV visits any other LRC area, it can send a request to the LRC to get temporary EMT services. The LRC will check the registration information of the visiting IoV by performing a search operation in the NRBC. Upon getting confirmation from the NRBC, the LRS informs the LBC (who is handling the EMT) to consider that IoV as a member and a potential EM sender and receiver. To ensure the presence of the vehicles a PoP method is proposed. All the IoVs' positions inside a local area are monitored by the LRC. IoVs periodically transmit their location information as PoP. This will be used by the blockchain server to distributes the EMs to the appropriate IoVs.

B. Emergency Message Transmissions (EMT)

The EMs must come from a verified source and in an understandable format by maintaining their integrity. Moreover, it should be distributed among required vehicles and may

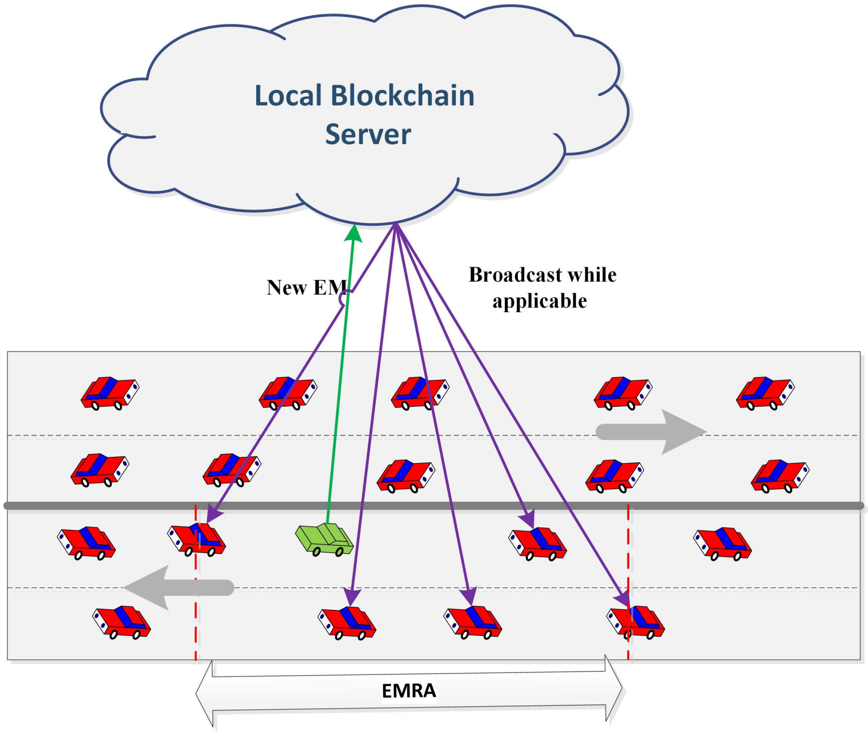

Fig. 1. EM distribution by blockchain server.

require to be stored for future traffic Investigations. By considering all these facts a blockchain is utilized in the proposed method. Blockchain stores the EMs in a decentralized and distributed environment and distributes the EMs to the required IoVs by analyzing their positions. All the communication between the IoVs and the blockchain is secured by RSA-1024 encryption which ensures the authenticity of the sender, confidentiality and integrity of the EMs. Moreover, as the IoVs use their public keys to communicate their privacy is preserved. Details of the method is illustrated in Figure 1.

During registration, each IoV receives their public keys, becomes a member of the LBC. While driving, whenever any IoV wants to share an EM, it will initiate a transaction in the blockchain. The server will check the identity of the requested IoV and perform the mining to generates an EM. A component of the server periodically monitors the position of the registered IoVs which is transmitted by all the registered IoVs as PoP. After generating the EM, the server will check the current position of the sender and then checks for the members under EMRA. Generally, 50m in front of the sender and 100m behind are considered as EMRA and it can be changed according to the traffic condition. For example, on the highway, the threshold can be more than the congested area. By collecting the public keys of the IoVs driving under EMRA, the server transmits the EM to those IoVs. In this way, the system ensures that an IoV only receives relevant EMs and does not overload with the unwanted or irrelevant EMs. All the EM transactions are stored with a period and the server will automatically delete the EMs after the validity of the EMs is finished. Before deleting the EM, the server sends the data to the local storage system to preserve the information for future investigations. As it requires a good amount of storage to store all the EMs and most of them are irrelevant for particular IoVs, the IoVs do not store all the data rather it stores only the EMs received from the LBC server. In Figure 2 the method is showcased.

Ethereum blockchain use ECDSA as their default signature method but in the proposed method to minimize the signature and verification time we introduce RSA-1024, a lightweight signature method but secure enough. Typical ECDSA require 10.8ms for signature and verification where RSA-1024 requires only 3.10ms but provides a security strength of 80-bit [34]. As a signature-based system, the proposed method provides security, confidentiality, integrity, source authentication and non-repudiation with privacy preservation. The blockchain-based storage system provides flexibility, fairness, temper-resistance, robustness and transparency of data service. Experiment results show that the proposed EMT maintains the SDR of 100ms while distributing the EMs.

C. General Message Transmission (GMT)

IEEE 802.11 provides a set of wireless local area network (WLAN) standards together with PHY and MAC layer protocol which can be used by smart vehicles, IoT, etc. to create ad hoc networks (VANET) between them and can perform social networking. IEEE 802.11 supports various frequency bands which can be divided into control and data channel [35]. Most of the previously proposed VANET protocols use a control channel for handshaking and a data channel for data transmission. All the systems suffer from packet collision problems because of frequent message transmissions, but as in our proposed method EMs are transmitted by using internet GMT can utilize both the control and data channel for communication which increase the throughput of GMT. Generally,

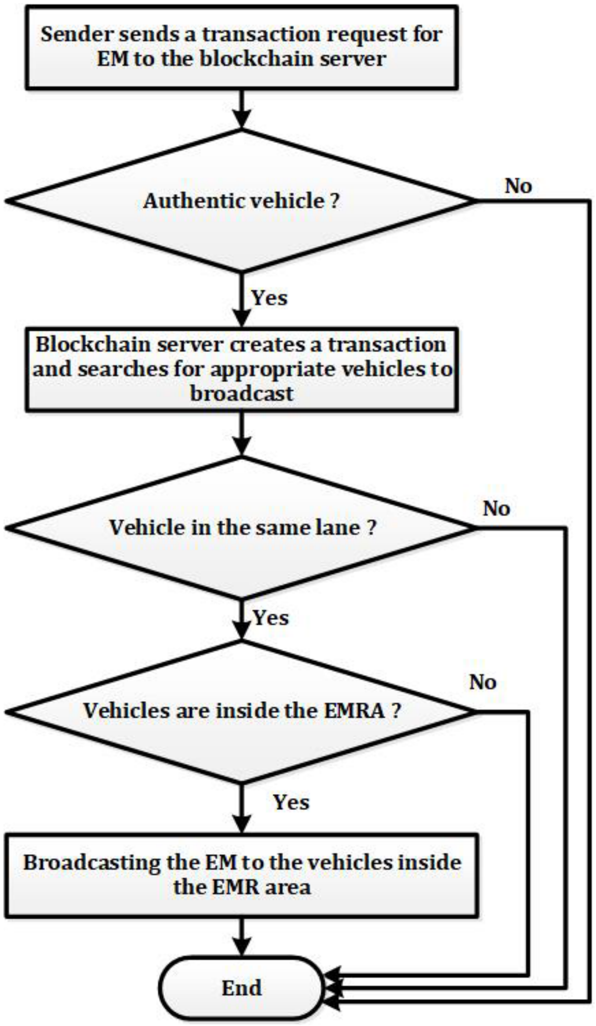
Sender sends a transaction request for EM to the blockchain server
Authentic vehicle ?
No
Yes
Blockchain server creates a transaction and searches for appropriate vehicles to broadcast
Vehicle in the same lane ?
No
Yes
Vehicles are inside the EMRA ?
No
Yes
Broadcasting the EM to the vehicles inside the EMR area
End

Fig. 2. Flow chart to describe the EMT protocol.

if any IoV or infrastructure wants to share any information or service it will broadcast that information by using the control channel. Before sending the service advertisement (WSA) by using CSMA/CA the sender senses the availability of a free channel.

Interested IoVs can send a Willing to Involve (WTI) packet and get services directly from the sender. But if there is a weak connection between the IoVs, the server waits for a helper node from neighbor IoVs who have a better connection with both the sender and receiver. IoVs can send a Cooperative WAVE Service Advertisement (CWSA) packet by adding the WTI number, sender and receiver's public key and the Signal to Noise Interference and the Noise Ratio (SINR) between the helper and the receiver. The sender may receive multiple CWSA for the same WTI, in that case, the sender will select the one with lower SINR as helper node by sending Selected Helper Message (SHM) and data. Then the helper starts relaying the data and the sender stop receiving any more CWSA from other nodes. A flow chart is presented in 3 to show the GMT step-by-step.

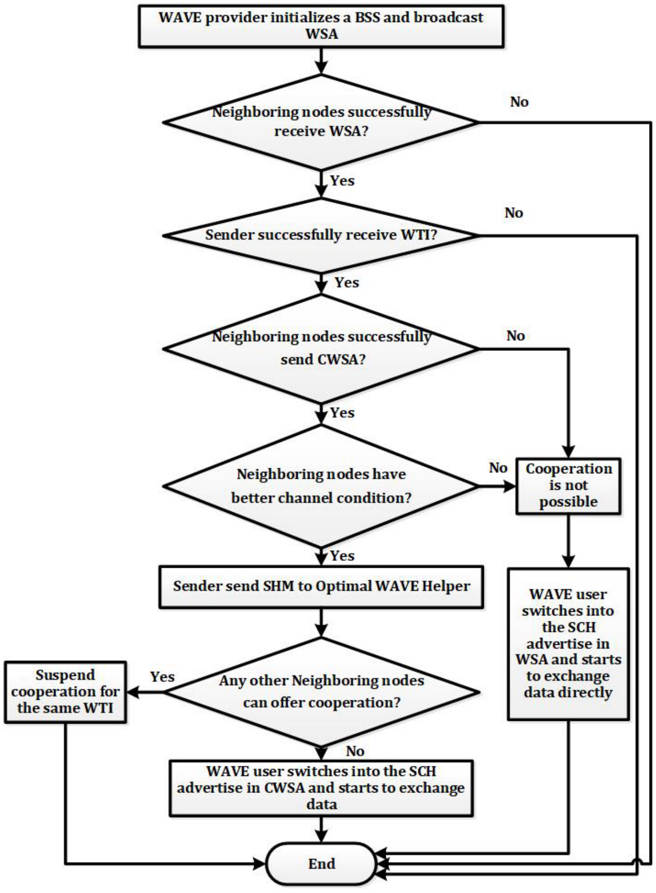
WAVE provider initializes a BSS and broadcast WSA
Neighboring nodes successfully receive WSA?
No
Yes
Sender successfully receive WTI?
No
Yes
Neighboring nodes successfully send CWSA?
No
Yes
Neighboring nodes have better channel condition?
No
Cooperation is not possible
Yes
Sender send SHM to Optimal WAVE Helper
WAVE user switches into the SCH advertise in WSA and starts to exchange data directly
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

Fig. 3. Flow chart of proposed GMT protocol.

IV. Implementation

A Proof of Concept (PoC) is presented for the proposed EMT protocol by using the Ethereum blockchain. Generally, miners are there to perform blockchain transactions but as the proposed method deals with lightweight devices, a server is introduced to perform the mining tasks for the IoVs. Usually, the LRCs can set up multiple servers for mining and ensure distributed storage facility, however, it is also possible to utilize EDGE systems for that. A Virtual Machine (VM) is configured with Ubuntu-18.04.4-desktop-amd64 to perform the mining. The tools used and the implementation details are discussed below.

A. Tools

Truffle framework [36] is used to implement the EMT module. This is a well-known testing framework for the Ethereum blockchain. Furthermore, truffle gives the advantage for auto testing of codes, manage smart contracts and deploy. Services like scripting, client-side development and network management are also possible with truffle. A private Ethereum blockchain Ganache [37] offered by the truffle suite is used as LBC. Decentralized Application (DApp) development is possible to emulate by Ganache. It also offers features that help to debug information and examine the blocks and transactions. Moreover, it is available to the leading operating platforms such as Windows, Linux and Mac. Ganache also provides the UI and CLI version but for the proposed project the UI version has been used. Metamask [38] is a wallet that allows performing transactions in Ethereum blockchains. Metamask is compatible with both phone and computer users. Facilities like access, pay and control of the application are provided by it.

TABLE I
CONFIGURATION OF THE VIRTUAL MACHINES USED FOR THE EXPERIMENT

Machine	CPU	Memory	Storage	OS
NRC	2	3GB	30GB	Ubuntu-18.04.4
LRC_1	1	2GB	20GB	Ubuntu-18.04.4
LRC_2	1	2GB	20GB	Windows 7 Ultimate
IoV_1	1	2GB	20GB	Ubuntu-18.04.4
IoV_2	1	2GB	20GB	Windows 7 Ultimate

For Android and iOS, there are apps whereas in browsers it comes in form of browser extension in Brave, Firefox and chrome. Besides, it supports Remote Procedure Call (RPC) which allows connecting with virtual private blockchain like Ganache. In the proposed method, NPM [39] is used to execute JavaScript. For interaction with the smart contract, the client-side in HTML was developed by using Lightweight Node Server [40].

B. Experiments

In reality, for EMT, a dedicated EDGE server is possible to be rented which is simulated here. For implementing the EMT module several VMs are prepared with two different operating systems. Configuration of the VMs is presented in Table I. Two VMs are configured as LRC_1 and LRC_2, one as NRC and two as sender and receiver IoV. For the experiment, multiple data sending and receiving is tested along with some IoV migration between LRC_1 and LRC_2. To do that, at first, Ganache was installed and considered as an LBC. Then all the prerequisites and dependencies like NPM are installed to run the truffle framework.

EMT blockchain has two kinds of operations. The first operation is storing an EM and then deleting them after a specific time limit. A smart contract is written, consisting of three functions first of which is to view the blocks, the second function is to add an EM as blockchain transaction and the third function marks to delete an EM. The smart contract is written in solidity and deployed by using truffle.

Next, the metamask wallet extension was installed in the firefox browser in the VMs which represents the IoVs. In the metamask, the custom RPC is used to connect with the Ganache blockchain server which is running in the server VM. For registering with the blockchain, the IoVs used their public keys. Considering the IoVs are registered to the LRS, thus have permission to request for transaction in the blockchain. For paying the fees, Ganache provides 100 ethers to IoVs, i.e., the gas during a transaction. For testing, two of the IoVs addresses (public keys) are provided as receivable IoVs. A function is implemented to receive those addresses from the monitoring server. After the test trail in the local VM, the results reflect that all functions work soundly and are transmitted to the IoVs who are under the EMRA.

Moreover, the smart contract is also tested in the Rinkeby [41] test network which is another online testing platform for ethereum blockchain. The smart contract in the proposed method has been tested in the Remix IDE (integrated Development Environment), a platform-independent environment [42]. It is possible to get the block and transaction details from the etherscan website [43]. The program is running fine on that platform too.

V. PERFORMANCE ANALYSIS

In this paper, two different protocols are proposed for EMT and GMT, thus the performance of these protocols is presented separately in this section. Blockchain-based EMT is evaluated according to the computational and storage overhead while the GMT are evaluated by their throughput, average delay and PDR.

A. Blockchain Based EMT

Proposed blockchain-based EMT protocol the usage of RSA-1024 algorithm ensures the security, confidentiality and integrity of the EMs. As soon as an IoV wants to start a transaction in the blockchain, it signs the EM with its private key which ensures non-repudiation and also authenticity. Additionally, blockchain-based distribution ensures that only the authenticated or verified vehicles can receive the EMs.

In this paper, instead of ECDSA, RSA-1024 is proposed to make it usable for lightweight vehicles. The difficulty of breaking the key i.e., security strength for RSA-1024 is measured as 80 bits, which means if attackers trying to break the key will need to perform at least 2^{80} operations [44]. Various reports suggest that 80-bit security is below the trademark but a system operating with low computational power, like IoT and IoV, is considered to be secure.

The main time-consuming protocol is the signature and the verification time, thus in this paper, only those are considered and propagation delays between the IoVs and the server are considered ignorable as a high-speed internet connection is used to communicate with the blockchain.

1) Computational Overhead: For ECDSA a total of 10.8ms is required where 3.6ms is needed to sign and 7.2 ms is needed to verify in the BCPPA protocol [45]. On the other hand, the proposed method uses RSA-1024 to minimize the time of execution. A total of 1.55ms is necessary for signing and verifying a message (for signing 1.48ms is needed and 0.07ms is needed for verifying) by a processor that has a clock speed of 1.5GHz [46]. This is approximately 3 times more than the protocol used ECDSA. Some of the other methods, for example, B-TSCA, EAPP, DSSCB, IBV, IBCPPA and SPRING ([12], [47]–[51]) are presented in Figure 4 who use different types of encryption required higher time to sign and verify than the proposed protocol. Therefore, by using the RSA-1024, 64 messages can be signed and verified within the SDR i.e., 100ms. The EMT protocols proposed by Su *et al.* faces avg delay is 151ms [52] while the method by Ucar *et al.* also required more than 100ms to transmit a single message [53].

2) Storage Overhead: The size of the Ethereum block header is around 508 bytes [54]. Consider if an EM has generated in every 10 seconds or 6 per minute and the car is active for 10 hours, the storage overhead would only 508 × 6 × 60 × 10 = 1.74 MB/day. This is a small amount of storage and hence would allow it to be stored for a longer period. Therefore if there are 100,000 IoVs are driving every day, it required to store 170GB of data every day. According to the density of the vehicles and the storage capacity, the server will decide when to delete the old data from the blockchain. However, to store the public keys of the IoVs requires 128 byte

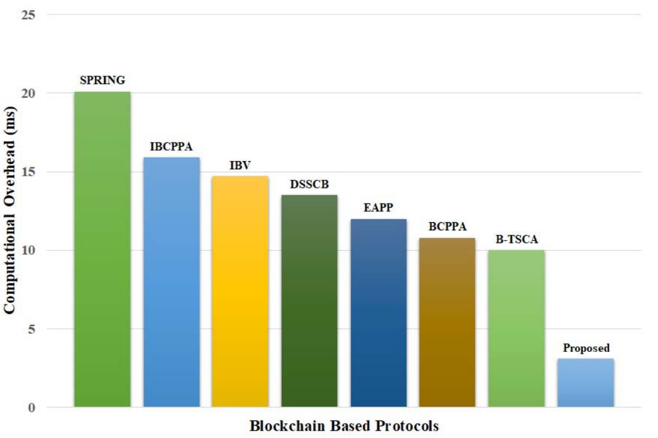

Fig. 4. Signature and verification time requirements of different blockchain-based protocols.

additional space which makes the header size 636 bytes. Thus if there are ten million registered IoVs in the country, it requires only 5.92GB of storage to store them as blockchain transactions.

B. Cooperative GMT

Speed and density of the vehicles are one of the major concerns of this experiment. IoVs running at 20 - 140 km/h speed with a density of 0 - 0.5 vehicles/meter are considered for the numerical analysis. However, the effect of velocity, density and others on the performance could be found in [11], [55]. If randomly scattered N number of IoVs are driving on a multi-lane road the transmission throughput S can be expressed as:

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

Here, P$_s$ = successful transmission probability, P$_{busy}$ = probability of channel being busy, L = length of the packets, P$_h$ = not getting a helper (probability), T$_{slot}$ = slot time, T$_s$ = probability of successful cooperative transmission, T$_c$ = Chances of collision.

The packet dropping rate (PDR) can be represented as below:

$$PDR = (1-P_s)^{C_A} \tag{2}$$

where C$_A$ is the number of cooperation tries. Then system delay is represented by

$$E[D_{CT}] = T_{e-CT}(N - \frac{P_{fdrop}}{1-P_{fdrop}} \frac{W_0+1}{2}). \tag{3}$$

where W$_0$ and P$_{fdrop}$ is the contention window size and final packet drop probability, respectively. The Markov state time spent on a vehicle (T$_e$) can be represented as

$$T_e = (1-P_{busy})T_{slot} + P_{busy}P_sT_s + P_{busy}(1-P_s)T_c \tag{4}$$

The equations are derived by Shah *et al.* in [11]. A test scenario is used to represent the performance analysis of the cooperative GMT by using MATLAB. The enhancement in throughput by minimizing PDR and delay are explained in the next sections. Table II, represents the data used for the numerical analysis.

TABLE II
SAMPLE DATA 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 packets	WTI, WSA	24, 25 (bytes)
Control packets	CWSA, SHM	27, 24 (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	20 - 140 (km/h)
Average inter-vehicle distance	b	10 (m)

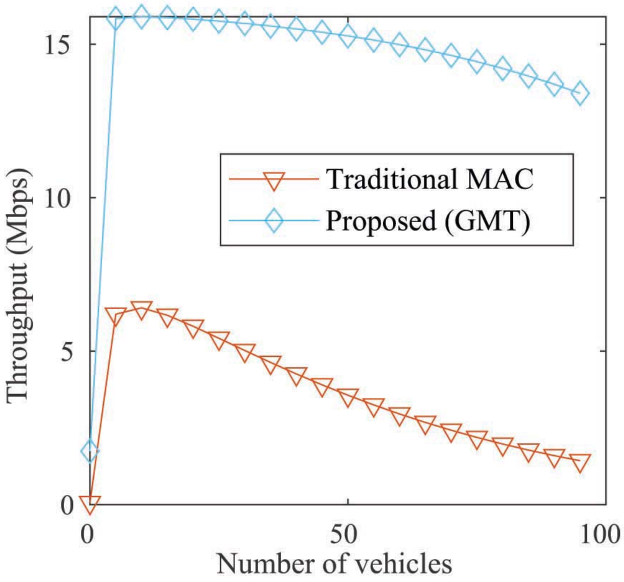

Fig. 5. Throughput against number of IoVs.

1) Throughput: Figure 5 describes the relationship between the throughput and the IoVs. In the case of GMT, the proposed procedure shows a huge increase in throughput than traditional MAC. The figure depicts the rise of throughput up to a certain portion and then there is a decline in the throughput. Initially, the number of IoVs is less and there are no accidents but as the number of IoVs start increasing there is a chance for accidents to occur and hence throughput decreases. The throughput may improve with a higher value of support because of a reliable S-R connection that will send the packet. This cooperation of transmission is faster with a better channel condition. Better than average throughput is obtained for the proposed protocol when optimized helpers are available. The worst throughput comes while there is a lack of helpers. When the aids are greater, there is going to be more collaboration benefits.

2) PDR: Figure 6 gives the PDR against the number of IoVs. With the increment of the IoVs, PDR increases as the risk of crashes are higher. More number of vehicular nodes indicates a higher probability of packet arrival increasing accidents. One important aspect of the proposed protocol is the minimized PDR compared to traditional MAC.

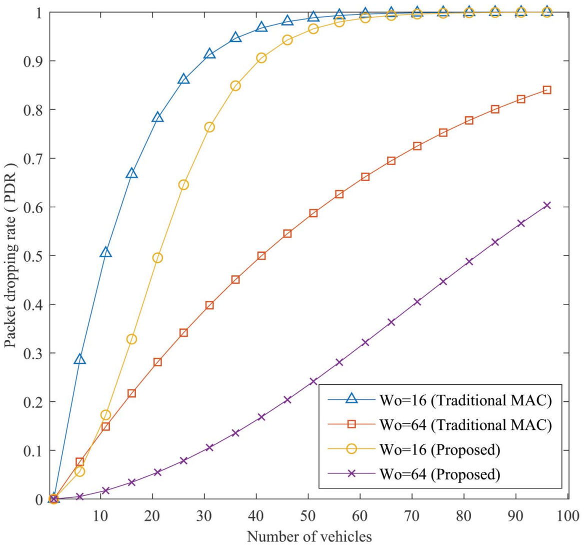

Fig. 6. PDR analysis for different contention windows.

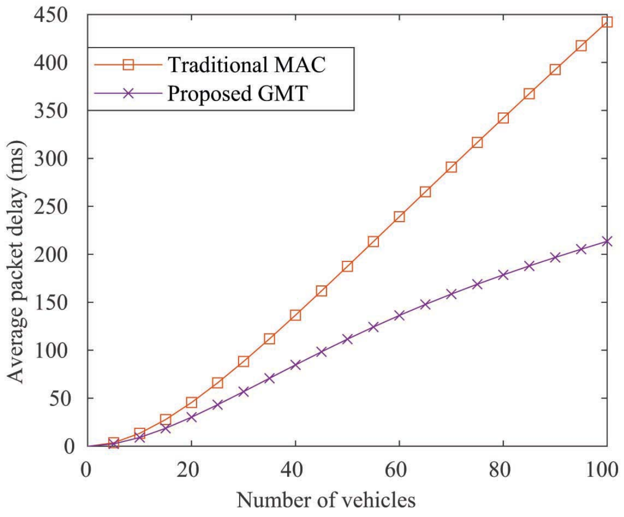

Fig. 7. Average packet delay vs number of IoVs.

Efficient transmission is a key aspect of the proposed protocol which is achieved by decreasing the PDR. Different contention windows (W_0) can be distinguished in the protocol. A higher W_0 would decrease the PDR significantly as packet failure is less and the number of collisions decreases with the increment of the back-off period. Additionally, as the EMs are transmitted through the internet thus the control channels remain free which has a good impact on decreasing the PDR.

3) Delay: The relation between the average packet latency and IoV numbers is shown in Figure 7. As the IoV number grows, the total packet delay increases as there is a higher number of packets to be transferred. When numbers of packets compete to be transmitted during the same time slot, the probability of collision increases because there is a higher chance of the channel being busy. These cause increment of the average packet latency. By using CSMA/CA collision avoidance technique and selecting the helping node by checking the SINR, the proposed protocol increases the probability of effective transmission by reducing packet drop probability and the average packet delay.

C. Discussions

To increase the efficiency and minimize the scalability problem a multi-level blockchain is proposed for EMT in this paper. Performance analysis shows that it requires less computational time and storage to perform the EMT efficiently. Additionally, RSA-1024 is used to minimize the computational cost and time which provide pretty good security for lightweight devices like IoV, IoT, etc. Blockchain is used to ensure availability, security, confidentiality, integrity, non-repudiation, attack prevention capability, etc. Moreover, multi-level structure enhanced the scalability of the transmission as only the local IoVs are handled by the LRCs and thus workload is less. NRC is there to manage the migration process and monitors all the transactions. To increase the communication efficiency and reliability high-speed internet connection is used which is faster and available than the IEEE802.11 protocol. Most importantly, experimental results show that it is possible to transmit more than 64 messages within the SDR i.e., 100ms. ECDSA of the 255-bit key provides a security strength of 112 bit while RSA-1024 provides 80-bit security. Although, it is less than the standard security standard, for lightweight devices this one is considered as pretty good security [1].

The novel idea of EMRA is used to minimize unnecessary transmission of EMs and which increases the efficiency of the system too. To minimize the pressure to the LBC, a separate database (LDB) is used to monitor the location information of the IoVs. It minimizes overloading of too much location information as the blockchain only stores the location information during an EMT. Finally, IEEE 802.11 based cooperative message transmission protocol can remove the infrastructural cost of RSU as well increase the area of transmission by performing one or more transmission helpers. Additionally, numerical analysis shows that it outperforms traditional MAC protocols and can deliver GMs faster than previously proposed protocols. Consensus is one of the core parts of blockchain but it requires high computational power to calculate the complex hash function and also time-consuming. For a VANET system where the vehicles do not have the high computational capacity and as emergency messaging systems expect real-time services, implementing consensus is difficult for emergency message transmission. However, decentralization is possible without consensus because all the information of the vehicles are stored in all the local registration centers where all of them stored them in multiple servers and additionally global registration centers also stores the same information and thus all the local registration centers have a copy of all the other local registration centers information. In this way, the proposed system provides two levels of decentralization and distributed database to store the emergency messages. Consensus provides the trustability of the members, but all the vehicles are physically verified by the local registration centers and no unregistered vehicles can enter the social communication system. However, while performing the message transmission blockchain server check the public key information of the sender and the receiver. Thus, if any untrusted or unknown vehicles enter the system, during transmission it can be detected by the server. In this way, the proposed system ensures trustability without using heavyweight and expansive consensus protocol.

In this paper, although an area is considered for simulation purposes, it can be upgraded to a global vehicular communication model by following the same model or by increasing another layer as Global Registration Center (GRC) and a blockchain as GRCB. As it requires more testing and structural changes in the blockchain, we have considered this as our potential future work.

VI. Conclusion and Future Research

This paper presents a Proof of Concept (PoC) for EMT protocol by using Ethereum blockchain. Performance analysis is presented for both the EMT and GMT to show the efficiency of the proposed method. Performance of the EMT is evaluated according to the computational and storage consumption while for GMT throughput, PDR and delay analysis are presented to show the enhancements of the proposed method over traditional MAC protocols. In particular, the paper contributes the following: a robust blockchain-based vehicle authentication and emergency message storage and distribution protocols.The proposed protocol can handle false data injection, unknown vehicles and Sybil attacks using RSA-1024 that reduces computational and storage consumption. It requires some structural changes and more testing to implement the proposed system for a wider area. We are considering this as our potential future work. Additionally, storage optimization and data deletion related experiments are going on to find a better solution.

References

[1] M. Ahmed, N. Moustafa, and A. Zengin, “A secured message transmission protocol for vehicular ad hoc networks,” *Comput., Mater. Continua*, vol. 68, no. 1, pp. 229–246, 2021.

[2] M. Ahmed and A.-S.-K. Pathan, “False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure,” *Complex Adapt. Syst. Model.*, vol. 8, no. 1, pp. 1–14, Dec. 2020.

[3] Y. Cao, T. Jiang, O. Kaiwartya, H. Sun, H. Zhou, and R. Wang, “Toward pre-empted EV charging recommendation through V2V-based reservation system,” *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 5, pp. 3026–3039, May 2021.

[4] M. Ahmed and A.-S. K. Pathan, “Blockchain: Can it be trusted?” *Comput.*, vol. 53, no. 4, pp. 31–35, 2020.

[5] M. Ahmed, “False image injection prevention using iChain,” *Appl. Sci.*, vol. 9, no. 20, p. 4328, Oct. 2019.

[6] A. Rahman *et al.*, “DistB-Condo: Distributed blockchain-based IoT-SDN model for smart condominium,” *IEEE Access*, vol. 8, pp. 209594–209609, 2020.

[7] G. N. Nguyen, N. H. L. Viet, M. Elhoseny, K. Shankar, B. B. Gupta, and A. A. A. El-Latif, “Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with ResNet model,” *J. Parallel Distrib. Comput.*, vol. 153, pp. 150–160, Jul. 2021.

[8] V. Poonia, M. K. Goyal, B. B. Gupta, A. K. Gupta, S. Jha, and J. Das, “Drought occurrence in different river basins of India and blockchain technology based framework for disaster management,” *J. Cleaner Prod.*, vol. 312, Aug. 2021, Art. no. 127737.

[9] Mamta, B. B. Gupta, K.-C. Li, V. C. M. Leung, K. E. Psannis, and S. Yamaguchi, “Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system,” *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 12, pp. 1877–1890, Dec. 2021.

[10] C. Esposito, M. Ficco, and B. B. Gupta, “Blockchain-based authentication and authorization for smart city applications,” *Inf. Process. Manage.*, vol. 58, no. 2, Mar. 2021, Art. no. 102468.

[11] A. F. M. Shahen Shah, H. Ilhan, and U. Tureli, “RECV-MAC: A novel reliable and efficient cooperative MAC protocol for VANETs,” *IET Commun.*, vol. 13, no. 16, pp. 2541–2549, Oct. 2019.

[12] X. Zhang and X. Chen, “Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network,” *IEEE Access*, vol. 7, pp. 58241–58254, 2019.

[13] U. Javaid, M. N. Aman, and B. Sikdar, “DrivMan: Driving trust management and data sharing in VANETs with blockchain and smart contracts,” in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5.

[14] C. Lai and Y. Ding, “A secure blockchain-based group mobility management scheme in VANETs,” in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Aug. 2019, pp. 340–345.

[15] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, “Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks,” in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Aug. 2018, pp. 674–679.

[16] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, A. S. M. Kayes, and A. Zengin, “A blockchain-based authentication protocol for cooperative vehicular ad hoc network,” *Sensors*, vol. 21, no. 4, p. 1273, Feb. 2021.

[17] I. Ali, M. Gervais, E. Ahene, and F. Li, “A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs,” *J. Syst. Archit.*, vol. 99, Oct. 2019, Art. no. 101636.

[18] Z. Lu, Q. Wang, G. Qu, and Z. Liu, “BARS: A blockchain-based anonymous reputation system for trust management in VANETs,” in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Aug. 2018, pp. 98–103.

[19] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, “A privacy-preserving trust model based on blockchain for VANETs,” *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[20] X. Zhang, R. Li, and B. Cui, “A security architecture of VANET based on blockchain and mobile edge computing,” in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 258–259.

[21] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, “Blockchain-based traffic event validation and trust verification for VANETs,” *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[22] M. Singh and S. Kim, “Branch based blockchain technology in intelligent vehicle,” *Comput. Netw.*, vol. 145, pp. 219–231, Nov. 2018.

[23] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, “A new type of blockchain for secure message exchange in VANET,” *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 177–186, May 2020.

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

[25] R. Woo and D. S. Han, “A cooperative MAC for safety-related road information transmission in vehicular communication systems,” in *Proc. 1st IEEE Global Conf. Consum. Electron.*, Oct. 2012, pp. 672–673.

[26] H. Taghizadeh and V. Solouk, “A novel MAC protocol based on cooperative master-slave for V2V communication,” in *Proc. 38th Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2015, pp. 1–5.

[27] T. Zhou, H. Sharif, M. Hempel, P. Mahasukhon, W. Wang, and T. Ma, “A novel adaptive distributed cooperative relaying MAC protocol for vehicular networks,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 1, pp. 72–82, Jan. 2011.

[28] J. Zhang, Q. Zhang, and W. Jia, “VC-MAC: A cooperative MAC protocol in vehicular networks,” *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1561–1571, Mar. 2009.

[29] S. Bharati and W. Zhuang, “CRB: Cooperative relay broadcasting for safety applications in vehicular networks,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9542–9553, Dec. 2016.

[30] S. Bharati and W. Zhuang, “CAH-MAC: Cooperative ADHOC MAC for vehicular networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 470–479, Sep. 2013.

[31] S. Bharati, L. V. Thanayankizil, F. Bai, and W. Zhuang, “Effects of time slot reservation in cooperative ADHOC MAC for vehicular networks,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 6371–6375.

[32] H. A. Omar, W. Zhuang, and L. Li, “VeMAC: A novel multichannel MAC protocol for vehicular ad hoc networks,” in *Proc. IEEE Conf. Comput. Commun. Workshops*, Apr. 2011, pp. 413–418.

[33] R. Zhang, X. Cheng, L. Yang, X. Shen, and B. Jiao, “A novel centralized TDMA-based scheduling protocol for vehicular networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 1, pp. 411–416, Feb. 2015.

[34] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, and A. Zengin, “A secured privacy-preserving multi-level blockchain framework for cluster based VANET,” *Sustainability*, vol. 13, no. 1, p. 400, Jan. 2021.

[35] *IEEE Standard for Local and Metropolitan Area Networks—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Standard 802.11-2016, 2016.

[36] ConsenSys Software. *Truffle suite*. Accessed: Apr. 8, 2020. [Online]. Available: https://www.trufflesuite.com/

[37] ConsenSys Software. *Ganache*. Accessed: Apr. 8, 2020. [Online]. Available: https://www.trufflesuite.com/ganache

[38] ConsenSys Formation. *Metamask*. Accessed: Apr. 8, 2020. [Online]. Available: https://metamask.io/

[39] NPM. *NPM (Software)*. Accessed: Apr. 8, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Npm_$software$

[40] J. Papa. *Github Lightweight Node Server*. Accessed: Apr. 8, 2020. [Online]. Available: https://github.com/johnpapa/lite-servers

[41] Rinkeby Test Net. *Rinkeby Test Network*. Accessed: Apr. 8, 2020. [Online]. Available: https://www.rinkeby.io/

[42] Ethereum Foundation. *Remix Ide*. Accessed: Apr. 8, 2020. [Online]. Available: https://remix.ethereum.org/

[43] *Etherscan*. Accessed: Apr. 8, 2020. [Online]. Available: https://etherscan.io/

[44] E. Barker and Q. Dang, "Nist special publication 800-57 part 1, revision 4," NIST, Gaithersburg, MD, USA, Tech. Rep., 2016.

[45] C. Lin, D. He, X. Huang, N. Kumar, and K.-K.-R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 30, 2020, doi: 10.1109/TITS.2020.3002096.

[46] R. K. Nirala and M. D. Ansari, "Performance evaluation of loss packet percentage for asymmetric key cryptography in VANET," in *Proc. 5th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Dec. 2018, pp. 70–74.

[47] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1386–1396, Jul. 2021.

[48] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[49] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. 27th Conf. Comput. Commun.*, Apr. 2008, pp. 246–250.

[50] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.

[51] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. INFOCOM*, Mar. 2010, pp. 1–9.

[52] H. Su and X. Zhang, "Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3309–3323, Jun. 2007.

[53] S. Ucar, S. C. Ergen, and O. Ozkasap, "Multihop-cluster-based IEEE 802.11p and LTE hybrid architecture for VANET safety message dissemination," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2621–2636, Apr. 2016.

[54] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[55] T. H. Luan, X. Ling, and X. Shen, "MAC in motion: Impact of mobility on the MAC of drive-thru internet," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, pp. 305–319, Feb. 2012.

Mohiuddin Ahmed (Senior Member, IEEE) is currently a Lecturer with the School of Science, Edith Cowan University, Australia. His research interests include blockchain applications in the IoT, machine learning, digital health, and unmanned aerial vehicles.

Nour Moustafa (Senior Member, IEEE) is currently a Senior Lecturer with the School of Engineering and Information Technology, UNSW Canberra, Australia. His research interests include cyber security, in particular, network security, the IoT security, and machine learning techniques.

A. F. M. Suaib Akhter is currently working as a Researcher at Sakarya University, Sakarya, Turkey. His research interests include wireless communication, vehicular *ad-hoc* networks, intelligent vehicles, network security, distributed systems, and machine learning.

Imran Razzak (Senior Member, IEEE) is currently a Senior Lecturer with the School of Information Technology, Deakin University, Australia. His research interests include machine learning and data analytics in general, particularly in healthcare industry.

Ehsanuzzaman Surid is currently pursuing the bachelor's degree in electrical and electronics engineering with the Islamic University of Technology. He is an active IEEE member attending and organizing various campus-based initiatives.

Adnan Anwar (Member, IEEE) is currently a Lecturer in cyber security with the School of Information Technology, Deakin University. He is broadly interested in the security research for critical infrastructures and application of machine learning and optimization techniques to solve cyber security issues for industrial systems.

A. F. M. Shahen Shah (Senior Member, IEEE) has been working as an Assistant Professor with the Department of Electronics and Communication Engineering, Yildiz Technical University. His current research interests include cross-layer design, modeling, and performance analysis of wireless communications systems.

Ahmet Zengin is currently an Associate Professor at Sakarya University, Turkey. His main research interests include parallel and distributed simulation and the high level architecture.