Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Privacy-Preservation Framework based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET

Abdullah Alharthi[1], Qiang Ni[1], (Senior Member, IEEE), and Richard Jiang[1]

[1]School of Computing and Commutations, Lancaster University, Lancaster LA1 4YW, U.K.

Corresponding author: Abdullah Alharthi, (e-mail: a.m.alharthi@lancaster.ac.uk).

This work was supported in part by the EC H2020 Grant SANCUS, the EPSRC Grant EP/P009727/1 and the Leverhulme Trust Grant RF-2019-492.

ABSTRACT In the near future, intelligent vehicles will be part of the Internet of Things (IoT) and will offer valuable services and opportunities that could revolutionise human life in smart cities. The Vehicular Ad-hoc Network (VANET) is the core structure of intelligent vehicles. It ensures the accuracy and security of communication in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) modes to enhance road safety and decrease traffic congestion. However, VANET is subject to security vulnerabilities such as denial-of-service (DoS), replay attacks and Sybil attacks that may undermine the security and privacy of the network. Such issues may lead to the transmission of incorrect information from a malicious node to other nodes in the network. In this paper, we present a biometrics blockchain (BBC) framework to secure data sharing among vehicles in VANET and to retain statuary data in a conventional and trusted system. In the proposed framework, we take advantage of biometric information to keep a record of the genuine identity of the message sender, thus preserving privacy. Therefore, the proposed BBC scheme establishes security and trust between vehicles in VANET alongside the capacity to trace identities whenever required. Simulations in OMNeT++, veins and SUMO were carried out to demonstrate the viability of the proposed framework using the urban mobility model. The performance of the framework is evaluated in terms of packet delivery rate, packet loss rate and computational cost. The results show that our novel model is superior to existing approaches.

INDEX TERMS Vehicle driving, intelligent vehicles, vehicular and wireless technologies, VANET, biometric blockchain, privacy preservation

I. INTRODUCTION

With the rapid advancement in smart cities, the number of intelligent vehicles in mobile ad-hoc networks has raised significantly. In the next 10 years, the number of intelligent vehicles is expected to reach 2 billion across the globe [1]. Therefore, vehicular ad-hoc network (VANET) has been created which is equipped with wireless communication devices named as on-board unit (OBU). These devices have hardware security chip to store sensitive information of the vehicle. Communications in VANET, can be categorized into vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Sharing valuable information about the traffic between the vehicles will be via the dedicated short-range communication radio (DSRC) [2]. Each vehicle represents a node in the network and it has the capability of sending and processing information. Improving road safety, reducing the traffic accidents, and enhancing traffic flow are several aims of forming VANET [2]. However, due to the high mobility and volatility of vehicles in VANET, various attacks could be performed during the exchange of messages between vehicles among the network leading to severe impacts. Due to the decentralized nature of VANET the process of identifying misbehaving vehicle or users has become difficult task [3].

The privacy and authentication of the data were the biggest concerns of researchers in VANET in order to improve the security. With this intention, blockchain technology has attracted many academicians and researchers for its enormous advantages to be gained in terms of providing and playing major role for managing, controlling, and securing VANET [4]. The main characteristics of blockchain are the decentralized architecture which means that data will be stored

in a peer-to-peer network which is applicable for intelligent vehicles.

Moreover, security of blockchain as a distributed secure ledger that provides an essential solution to the issues in security and privacy in VANET due its cryptographic protocols [5]. Furthermore, blockchain will provide anonymity for vehicles and therefore it will be difficult to trace and discover the original identity of the vehicle due to the cryptography nature of blockchain. On the one hand, communication in VANET shall provide privacy preservation by employing anonymity of vehicles. The authorities shall be able to track the anonymity to identify the malicious vehicle, thus it should be made conditional [6]. The objective of this work are as follows:

1) *Single registration:* For ease of use, a VANET authentication system should support a single registration process whereby vehicles are only required to register once before being able to send messages to other road users.
2) *Message authentication:* To ensure that received messages are credible, the roadside units (RSUs) or vehicles should have the capacity to authenticate messages by verifying the identity of the sender and checking the message's timeliness and integrity
3) *Preserving privacy:* A vehicle's genuine identity must not be visible to other vehicles or RSUs and it should not be possible for a malicious actor to acquire identities through the analysis of any identity intercept.
4) *Traceability:* An efficient system should be in place allowing the trusted authority (TA) to trace the true identity of the vehicle if malicious behaviour takes place, e.g., false messages are transmitted to confuse other vehicles.

The contributions of this work are as follows:

1) A biometrics blockchain (BBC) framework is proposed to make communication in VANET more secure.
2) The biometrics features are combined with blockchain technology to provide reliable transmission of data, tracking the data exchanged and identification of the vehicle responsible in the case of falsely messages.
3) The performance of the framework is evaluated in terms of packet delivery rate, packet loss rate and computational cost.

Due to the requirements of the legacy system, diligence and statute, the vehicle registration data is kept by the Motor Vehicle Department. The data relating to vehicle communications in VANET is stored in blockchain to make it secure.

The structure of this paper is as follows: Section II presents the state-of-art in the area of VANET while section III presents the basics of VANET and blockchain. In section IV, we present the system architecture. Section V presents the simulation results and discussion. Finally, a conclusion is presented in section VI.

II. Related Work

VANETs creates an open access environment that poses significant challenges in terms of security and privacy, rendering it unsuitable for real-world implementation [7]. Under the Identity-based Batch Verification (IBV) scheme for V2V and V2I communication in VANETs proposed by Zhang et al. [8], a secure device is used to protect privacy. What is more, pseudo identities are generated locally as the system's master key is stored by every device. On the other hand, the unpredictable risk of system exposure to powerful attackers ensues from this type of storage of the system's master key. What is more, the resultant communication over-head and scalability issues were not considered in this scheme. Many researchers have focused on the raising issues in VANETs security such as privacy, anonymity and traceability.

Authors in [9] proposed a hybrid approach which fortifies the scheme by make use of pseudonymization with self-attestation. It is not required to govern these unless system stability compromise is not an issue. An authentication protocol without certificates was proposed by Tan et al. [10], which involves vehicle identity authentication among vehicles and Road Side Unit units. In order to enhance users' VANETs key security, [11] created a mechanism for secure authentication. However, a trusted third party is responsible for the execution of these two systems in the centralized system. Distributed security is not provided to identify malevolent users, Wu et al. [12] employed group signatures and one-time authentication. Unfortunately, bilinear pairing operations are costly at the tracing stage, which renders acing suspicious messages inefficient.

To achieve pseudonyms control, [13] designed secure RSUs management. Regrettably, it is not possible to work efficiently in fields with RSUs which are presumed to be constrained and have low computation power in conventional VANETs. Decentralized, secure, blockchain-based, independent, and intelligent transportation systems were proposed by Yuan and Wang [14].

Rowan et al. [15] put forward an inter-vehicle session key establishment protocol and blockchain-based solution to secure communications. A privacy approach called (PPAS) was presented by Chuang et al. [16] for the purpose of achieving communication between infrastructure and vehicle in VANETs, which fulfilled authentication between the vehicle and the RSU as well as the majority of security conditions. However, this scheme is used to communicate with vehicles and does not provide a distributed system. An anonymous on-board network authentication protocol was proposed by Peng [17]. While this protocol ensures efficient user authentication and anonymity, the fake vehicles will not be identified. Authors in [18] suggested vehicular networks were suitable for blockchain-based anonymous authentication, and Lu et al. [19] designed an anonymous VANET reputation system based on the blockchain.

Although [18] and [19] preserve user privacy in the authentication process, they are not compatible with Bitcoins and their schemes do not involve a vehicle announcement

method. A different option to bypass the restrictions of saving many anonymous certificates in advance was proposed by Lu et al. [20], which preserves conditional privacy at the same time.

In the all the previous works authors have proposed pseudo numbers to protect real identities of the users which is vulnerable to guess using prior-knowledge. In our approach we have used biometric data of the user to generate a unique pseudo identity. The proposed methods utilize modified discrete cosine transformation and hash function to achieve the privacy.

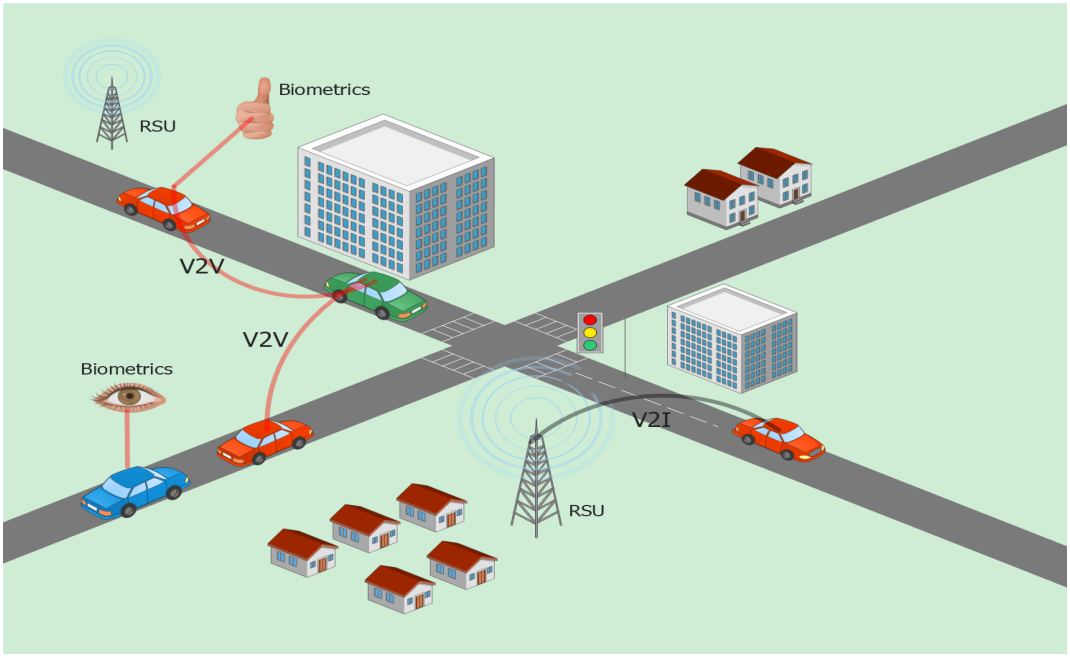

FIGURE 1. Proposed Vehicular Ad hoc Network

III. Preliminary VANET and Blockchain

VANET has started to play a major part in saving drivers' lives and possessions by broadcasting crucial event information with the progression of vehicular technology. Two main types of communication are associated with VANET: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Today, a third type of communication which is quite popular as well: Vehicle-to-Everything (V2X), when a vehicle communicate with everything acts cyclists, pedestrians, and any other entities [21]. In V2I, RSU will be located at both sides of the road as shown in figure 1 and vehicles driving through will communicate with RSU.

The protocol Wireless Access in Vehicular Environments (WAVE) provides the foundational standard for Dedicated Short-Range Communication (DSRC); this operates within the 5.9 GHz. The WAVE works on the IEEE 802.11p standard [22]. Communication with nearby vehicles is achieved using On-Board Units (OBUs), together forming ad hoc networks allowing for the distribution of communication [23]. One of the main goals of the VANET is to use safety messages to communicate with additional vehicles when reporting events, such as warnings, accident information, weather reports, information on traffic jams, and reports of ice cover among others. One needs to distribute certain event information rapidly, accurately, and with as little delay as possible because failure to do so can cause injuries to drivers and damage to vehicles. Among the key aspects used to guarantee communication security in VANET are node and event message trust therefore it becomes important to evaluate their reliability periodically [24].

A. Blockchain Technology

The blockchain technology is based on public distributed event ledger which incorporates each event that has transpired and been shared between participating nodes. It comprises a verifiable, definite record of every single incident that has ever taken place [25]. The majority of network nodes converges to validate each event in the blockchain database. There are two main blockchain types: public and private. The public blockchain is open access, meaning any entity can join and interact with it without needing an approval from a third party. The private blockchain is typified by controlled access [26]. Administrators can control who can view, join, and write in the blockchain. They can create consensus groups, due to which the private blockchain can become centralized. While public blockchain does not have this weakness, being completely decentralized and capable of withstanding malicious attacks [27]. Once a full node of a public blockchain is connected to other nodes in the network, the process of constructing a full blockchain will begin. The blockchain has some of the following basic features:

Distributed and trustless environment - It is possible to add any node to the blockchain to validate and synchronize the blockchain content in a distributed way without the requirement for a central control. This adds security and avoids any single point of failure. This helps to create trust in an otherwise trustless system

Immutability - Once recorded in the blockchain then no piece of information can be modified or deleted from the network. What is more, adding information arbitrarily is not possible

Privacy and anonymity - The blockchain help users to benefit from privacy and allow users to join anonymously that means that users cannot access each other's information. This helps to ensure that the system is secure, anonymous and private [28].

Structure of Blockchain

The block has a header, metadata and a collection of transactions as shown in figure 2. The block header size is 80 bytes, while the transaction size is variable and varies based on the nature of application.

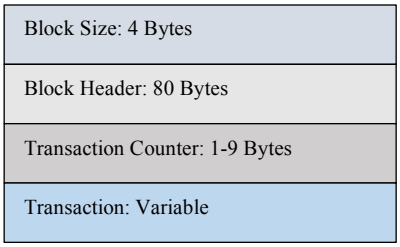

FIGURE 2. Structure of the Block [29]

These nodes are then divided into two categories: non-mining nodes and mining nodes.

Non-mining Nodes - Since the intent of non-mining nodes is to only receive and broadcast requests for data sharing transactions, they do not need the same number of resources as a mining node. It is worth noting that all nodes maintain a complete and authenticated copy of the blockchain and the sensors in relation to the smart contracts. It is believed that all nodes have a legitimate access to the blockchain network, and in each round of transactions, the vehicle sensors upload data to the blockchain network.

Mining Nodes - These nodes are responsible for validating data-sharing transfers and compiling them into data blocks. These nodes are required to use computer computing capabilities on a regular basis in order to solve cryptographic problems and submit blocks to the blockchain network. Since each vehicle has a legitimate link to the blockchain, the vehicle will encrypt the data gathered with a private key before forwarding it to the blockchain with a signature as a request for storage.

Transaction and Consensus Mechanism - A blockchain transactions are created by acquiring a data packet from the vehicles. The gateway carries out a series of transactions that generates vast numbers of data, including data, control and results transactions. Consequently, the data are located on the blockchain by a reference pointer. The contract name, type of transaction, data relation, the sender/receiver address, block number, signature, public and private keys are typically used in the transaction format. For a quick and stable consensus algorithm, selecting safe or effective blockchain nodes is a critical factor. The safe nodes that act as a miner are chosen on the basis of several factors, including computer power, storage capacity, prestige, mining costs, production and bandwidth. We have chosen the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) to classify the credibility of the blockchain mining node [30].

Nowadays, proof-of-work (PoW) has established itself as an important consensus framework for validating transactions through mathematical challenges. The mining node gathers all transactions before a block is created in the Merkle tree and iteratively hashes the data it collects.

The process of hashing terminates when the hash of transactions becomes equal to or less than a pre-determined target value (T_h) called as a threshold as expressed in equation (1) [31, 32]. The $\mathcal{H}$ represents SHA-512 hash function and b_c presents the current block.

$$\mathcal{H}(n \,||\, \mathcal{H}(b_c)) \leq T_h \tag{1}$$

The probability to discover nonce of proof H can be expressed as the equation (2) [31, 32].

$$P(\mathcal{H} \leq T_h) = \frac{T_h}{2^{512}} \tag{2}$$

After successfully computing the target hash, the miner sends the proof to each node in the blockchain network, along with data transactions and other data, in order for other miners to re-compute $\mathcal{H}$ and thereby connect the new block to the network.

B. Blockchain and VANET

In order to design a trusted, secure, and decentralized autonomous framework was proposed for intelligent transportation system (ITS) [33]. To design an efficient VANET the blockchain is integrated in a self-managed manner [34]. Blockchain technology can combine with multiple applications at a system level that can enables the smart contract system within VANET.

The blockchain can be easily integrated with many useful applications such as vehicle insurance, traffic regulation, vehicle tax and weather forecasts with privacy and trust. This blockchain based secure multiple channels of communication between vehicles improves the data sharing security. A blockchain-based mechanism that would protect the user's private data in the course of providing and updating vehicle technology such as remote wireless software was proposed [35].

In another work authors proposed a trust management system for intelligent vehicle which is based on blockchain technology. The vehicles can verify the messages from other vehicles using Bayesian inference models. In this method vehicles generate rating for other vehicles. The offset value of the specific vehicle's trust is determined by the RSU. The data is aggregated into blocks to enhance the traffic efficiency and the safety is characterized by reliability factor [36].

In another work of electric vehicle (EV), a decentralized blockchain smart grid system was proposed to reduce the overall charging cost of EV users and the grid network's power fluctuation level. A specific blockchain-based EV energy storage program for EV battery charge rate, capacity, grid dynamics, and EV user behaviour were all put forward for consideration. [37].

In another work authors have proposed a technique in vehicle-to-grid (V2G) networks to enable data sharing without compromising user data safety using blockchain. This mechanism supports anonymity and audits that includes data registration and maintenance procedures based on blockchain technology [38].

In another related work authors have examined the management safety in connection with charging piles and EVs. Authors have proposed a safety model based on smart contracts and lightning networks to enhance the transaction security of charging piles and EVs [39]. The blockchain's role in enhancing IoT security was evaluated and found that blockchain fragmentation was likely to result in low sensitivity of ill-meant participants [40].

The blockchain authentication protocol was proposed that enables cognitive radio network spectrum sharing that serves as a means to access wireless bandwidth in a competing CR to be able to use as media access control (MAC) protocol [41]. Specoins, the virtual currency they proposed, will be used as payment for the access to spectrum [41].

IV. Proposed Biometrics Blockchain Framework

We have proposed a blockchain based framework that uses biometrics in VANETs to protect privacy, with vehicles employing a public-private key pair provided by the TA to communicate with other parties. By employing blockchain techniques, such a decentralized framework will be trustworthy, secure, and allow messages to be disseminated securely. Standard blockchain is associated with cryptocurrency; but this blockchain handles safety event messages with no employment of cryptocurrency. From this point safety event messages will be employed as event messages.

This novel BBC design is suitable for protecting the security of safety messages within VANET in real-world scenarios. The blockchain will retain and manage event message history alongside each vehicle's trust level reliably, immutable, and with good distribution.

Every country will have one unique blockchain with independent management and maintenance to record vehicle information.

A. Entities of Framework

1) TRUSTED AUTHORITY

The trusted authority (TA) is responsible for initializing the system, deploying smart contracts, registering vehicles and revoking registrations. The assumption is made that the TA has significant capacities for computation and communication and will not be working with any other party.

2) MOTOR VEHICLE DEPARTMENT (MVD)

The Motor Vehicle Department (MVD) has several responsibilities which include vehicles registration, maintaining vehicles records, the MVD authorizes the TA to issue the certificates and public keys to the vehicles after the verification process is completed from MVD.

3) VEHICLE

The vehicle undertakes services for the driver and will carry an OBU that cannot be tampered. The assumption is made that the preloaded information carried by the OBU is protected against malicious attack. Additionally, the vehicle will employ the OBU to communicate wirelessly with other entities.

4) ROAD SIDE UNIT (RSU)

The roadside unite is roadside infrastructure which has the capability of communicating wirelessly with all vehicles inside a defined range. It is capable of receiving instant messages from vehicles, verifying them and passing them on either to nearby vehicles or the traffic management centre.

5) BLOCKCHAIN

The blockchain represents the decentralized foundational architecture of BBC. It is responsible for secure handling of the transactions (safety messages) exchanged by vehicles across the network.

6) MESSAGES

Messages in VANET can be classified into two forms or groups which are beacon and safety event messages. The former are disseminated at set intervals to give information to all vehicles in an area of the position such as driving information to allow all the vehicular nodes in an area to be cooperatively aware in order to manage traffic. Safety event messages are disseminated when critical events are present, e.g., hazards, traffic accidents, etc.

B. Biometrics based Authentication

During the registration phase when vehicle information along with driver's detail will be sent to TA. This information will contain the finger print of the driver to ensure the identity. The on-board unit (OBU) will have finger print scanner.

The authentication of the driver's identity will be done using modified discrete transformation (MDCT). During the registration, the driver will put this fingerprint which is further processed by MDCT to generate a cancellable fingerprint template. The cancellable biometric system will transform the biometric identity of the driver and store the cancellable reference template in the cancellable template database (Cf_T) in the TA and OBU. The Cf_T is used in registration of vehicle to grant access to the vehicular ad hoc network. The authentication of the driver is achieved via two processes: enrolment and authentication. During enrolment, the vehicle driver's biometrics data Ca_T is registered in the database. At the time of authentication, the driver's biometrics is captured as $Cf_T{}^*$ which is compared against other reference template in the database at TA.

The Euclidean distance (ED) has been deployed to match the captured and reference data based on the similarity. If both the data matches, the driver will be registered on the VANET.

The proposed method uses MDCT, the feature vector F_V has dimension of $M \times N$ such that $N \leq M$. The feature extraction is based on the DCT matrix such as $f: R \rightarrow \hat{R}$ that maps $R \in \{x_0, \ldots . x_{K-1}\}$ into $\hat{R} = \{X_0, \ldots . X_{K-1}\}$ according to the below equation (3):

$$X_i = \frac{1}{2}(x_0 + (-1)^i x_{K-1}) + \sum_{n=1}^{K-2} x_n \cos\left[\frac{\pi}{K-1} ni\right] \quad (3)$$

Where $i = 0, \ldots K-1$

DCT is highly invertible. So here MDCT is proposed to make it non-invertible. Assume a column vector as shown in equation (4):

$$V_l = \begin{bmatrix} v_1 \\ v_2 \\ . \\ . \\ . \\ v_p \end{bmatrix} \quad (4)$$

The values in the vector V_l belongs to unique positive integers. The column V_l is produced using random distribution. The V_l represents that l number of transformation values can be produced. The V_l is employed to create sub-matrix R, donated as $\bar{R}$, i.e. i^{th} column of the $\bar{R}$ is the $v_i{}^{\text{th}}$ column of R for $(i = 1,2, \ldots . p)$. Therefore, size of $\bar{R}$ is $p \times M$. The $\bar{R}$ is created from a random factor v_i, while partial DCT-based has been obtained on F_V using a non-invertible Cf_T by the following equation (5):

$$Cf_{T_{(p \times N)}} = \bar{R}_{(p \times M)} F_{V_{(M \times N)}} \quad (5)$$

The $\bar{R}$ is created from the DCT matrix R , therefore, cancellable transformation in equation (5) tends to be a non-invertible because of $\bar{R}$ a column-reduced sub matrix of R. Finally, the matching process is done by using the following equation (6):

$$M_p = \begin{cases} 1 & \text{ED}(Cf_T, Cf_T{}^*) < th \\ 0 & \text{OW} \end{cases} \quad (6)$$

The $\text{ED}(Cf_T, Cf_T{}^*)$ is computed as follows:

$$\text{ED}(Cf_T, Cf_T{}^*) = \frac{g^Y g}{Cf_T{}^Y Cf_T + Cf_T{}^{*Y} Cf_T{}^*} \quad (7)$$

Where $g = Cf_T - Cf_T{}^*$ and Y transpose of a real vector/matrix.

The symbols used in the proposed model is presented in table 1 as follows:

TABLE I :NOTATIONS

Notation	Description
V_i	Identity of vehicle *i*
KU_i	Public-key of vehicle *i*
V_p	Vehicle pseudo id
KR_i	Private-key of vehicle *i*
v_{reg}, v_{mod}, v_{chas}, v_{rank}	Vehicle registration number, model chassis number, ranking
O_i	On-board unit of vehicle *i*
D_i	Driver's information
d_{name}, d_{bio}, d_{lic}, d_{rank}	Driver name, biometrics data, license, ranking
M_i	Message sent by vehicle *i*
$\mathcal{H}$	Cryptographic hash function
C_i	Certificate of Vehicle i
M_Type	Message type: beacon, alert
$\mathcal{E}$	Encryption function
$\mathcal{D}$	Decryption function
E_{id}	Event identification number
E_{loc}	Event location
E_{type}	Event type
T	Event timestamp
t	Current time
R_i	Reputation of the sending vehicle *i*
th_f, th_R	Freshness and Reputation threshold

C. System Modelling

1) BIOMETRICS AUTHENTICATION

As detailed previously, it is crucial for VANET that vehicles should be registered. Verification of a vehicle's physical attributes must be undertaken before they can participate in the network. All vehicles must undergo such protocols to be awarded a valid certificate and so be allowed to join the network. It should be noted that as with every other transaction that forms part of a vehicle's blockchain, the genesis block uses a public and private key supplied by the TA. At the time of verification of vehicle's information and the vehicle's authorized user's biometric data is used by the TA. In this instance, biometric data will serve as continuous identity information.

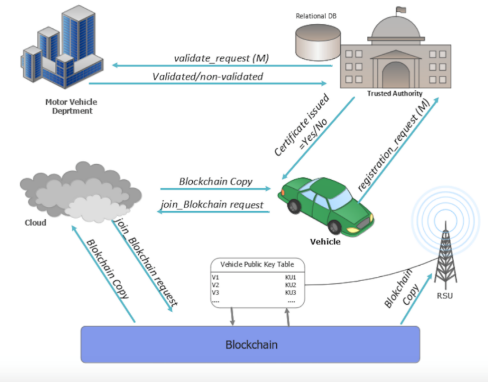

FIGURE 3. Registration Process

2) VEHICLE REGISTRATION ON BBC

When a vehicle joins the system for the first time, it needs to register with a TA. The biometric data of the vehicle's authorized user and the vehicle data is sent to the TA in order to get a pair of keys in return. The registration process begins with obtaining a real identity of the vehicle from the MVD, and sending the biometric data of the vehicle's authorized user and vehicle ID to the TA. Thereafter, the TA verifies the existence of the real vehicle identity from MVD, if verified, the TA will verify the biometric information of authorized vehicle's user, if this too is verified, the TA then generates the certificate that includes a pair of keys according to the vehicle ID and user's biometric data as shown in figure 3. The TA saves the biometrics information in highly secure database, that will be further used to track the real-identity of vehicle in the case of malicious activity. The complete process of registration is shown as follows:

Vehicle Registration Process

Input: V_i, D_i,
Output: Success/Failure
Begin
fetch: V_i: $v_{reg} \leftarrow O_i, v_{mod} \leftarrow O_i, v_{chas} \leftarrow O_i, v_{chas} \leftarrow O_i\}$
Compute $d_{bio} \leftarrow Cf_{T_{(p\times N)}}$
Compute $\mathrm{ED}(Cf_T, Cf_T^*)$ *from equation (5)*
if $(\mathrm{ED}(Cf_T, Cf_T^*) < th)$ **then**
fetch: D_i: $\{d_{name} \leftarrow O_i, d_{lic} \leftarrow O_i, d_{rank} \leftarrow O_i\}$
Join the network
generate KU_i, KR_i
$M_i = Sign_{KR_i}(KU_i, V_i, D_i \| \mathcal{H}(KU_i \| V_i \| D_i \| d_{bio}))$
Certificate=registration_request (M_i)
if *Certificate=TRUE*
Join blockchain (***C****i*)
else
error: unauthorize driver
endif
endif
End

3) JOIN BLOCKCHAIN

Once the vehicle is successfully registered, it can join the blockchain. The vehicle can join the chain by getting update copy of the blockchain. Thus, the vehicles in VANET can download and append to the blockchain. In the proposed framework, the blockchain performs the function of a distributed ledger that saves the important historical data of vehicles along with safety messages. Any vehicle that experiences a critical event, such as an accident, will broadcast the safety message to neighbouring vehicles in the network.

Vehicle Joining Process

Input: Ci, M_i
Output: Success/Failure
Begin
status=validate_ certificate (Ci)
if *status=valid*
$V_p = \mathcal{H}(d_{bio})$
Update vehicle pseudo id
GetBlockchainCopy ()
while *(Event)*
Broadcast (M_i)
endwhile
else
error: invalid certificate
end if
end

4) MESSAGE RECEPTION

Every vehicle in VANET will continuously receive message from the network. Based on the message type and priority level, appropriate action will be taken by the vehicle. The process of message retrieval is shown as follows:

Get Message Process
Begin
M=GetMessage ()
if *M_Type=safety*
status=Validate_Message ()
if *(status=validated)*
Broadcast(M)
If *node=miner*
AppendToBlockchain(message)
endif
else
discard(M)
endif
endif
End

5) MESSAGE BROADCAST

All the vehicles in VANET broadcast the information about their positions, status and other details through a message called beacon messages. Whenever a vehicle wants to transmit these messages to any proximate RSUs and vehicles, then message will be encrypted and signed the sending vehicle's private key. The message may consist of details such as the event ID, event type, event timestamp, and event location. The process for broadcast and verification is shown as follows:

Broadcast Message Process
Begin
$M = Sign_{KR_i}(\mathcal{E}(E_{id} \| E_{loc} \| E_{type} \| T))$
SendToAll(M)
End

Verify Message
Begin
if $(t - T) > th_f$
if $R_i > th_R$
Broadcast $(\mathcal{D}_{KU_i}(M))$
endif
endif
End

After receiving the message by the vehicles, the messages are first checked the freshness of the received message using the verification process.
The receiving vehicle compares the timestamp, reputation rate of the sender, verifies the message, and decrypts it using the sender's public key. If the verification process is successful and the message is valid, then the receiving vehicle can rebroadcast the event message to other vehicles.

6) UPDATE BLOCKCHAIN

The message generated from the vehicle can be added to the blockchain in the form of a transaction. However, adding every message to the blockchain will lead to the communication and computational overhead. Therefore, we have proposed adding only safety messages that are validated. The complete process for adding a new message in the blockchain is shown as follows:

Blockchain Append Process
Input: Message
Output: Success/Failure
Begin
Block: structure {H_1, KU_i,V_i, Di, T}
Block=$UnSign_{KU_i}(H(M))$
H_2= $\mathcal{H}$ *(Block)*
If $H_1 = H_2$ *then*
Validate Transaction
Append Transaction to Block
Distribute Update of blockchain
Finish ()
else
error: malicious message
discard (M)
endif
End

7) DE-RESGISTRATION PROCESS

The de-registration process may be invoked by the registering authority or it may be requested by the vehicle depending on the situation. The complete process for de-registering vehicle is shown below.
Vehicle De-registration Process
Input: Certificate, request
Output: Success/Failure
Begin
If *(certificate=valid and request=TRUE) then*
De-register vehicle
Update Vehicle Data from TA/CA
endif
End

V. Results and Discussion

To demonstrate the correctness and effectiveness of the proposed model the network performance was analysed with respect to presence and absence of denial of services. We present a comparative analysis with the existing algorithm such as ASC [42], LAKAP [43], BC-VANET [3] and found to be superior in terms of packet delivery, packet loss and computational cost. In the simulation model the assumption is that vehicle communicate with each other either using V2V or V2I model. Also, every vehicle has OBU, sensors and GPS device. The model assumes multiple RSU and some of them were in malicious role as well.
The simulation has been performed using OMNeT++, Veins and SUMO to demonstrate the correctness of the proposed model using IEEE 802.11p/1609.4 protocols. The trace control interface (TraCI) which is a middle interface between OMNeT++ and SUMO++ that provides a TCP based communication between these two simulators. To evaluate the model, we have chosen the parameters as shown in table 3 and 4 which consist of 100 vehicles with a maximum speed of 50 m/s. The length and width of the vehicle is 4m and 2.5m respectively. The number of RSU in the experiment are 15 while the coverage of a single RSU is 2 km.

A. Simulation Parameters

TABLE III
OMNET SIMULATION PARAMETERS

Parameters	Values
Simulation time	3000 s
Queue length of the MAC	10
Bit rate of MAC	15 Mbps
Maximum Transmission Attempts	20
Transmission Power	100 mW
Contention Window of MAC	10
PHY. Sensitivity	-80 dBm
Interval to update	0.01s

TABLE IV
SUMO SIMULATION PARAMETERS

Parameters	Values
Number of vehicles	100
Max. speed of Vehicle	50 m/s
Maximum Acc.	3 m/ s^2
Maximum Dec.	5 m/s^2
The length of the vehicle	4 m
The width of the vehicle	2.5 m
RSUs No	15
Coverage of RSU	2 km.
Sigma	0.5

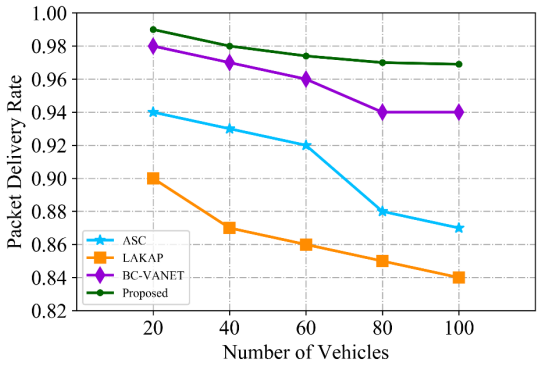

Figure 4. PDR without denial-of-service attack

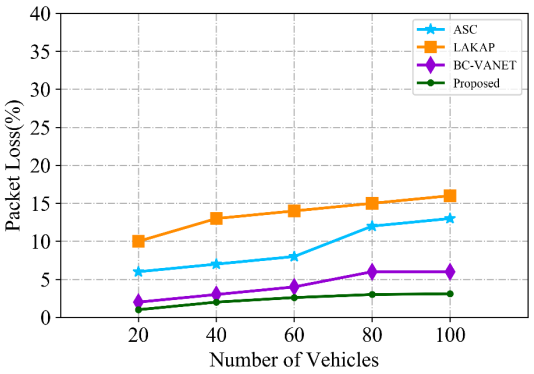

Figure 5. Packet loss without DoS attack

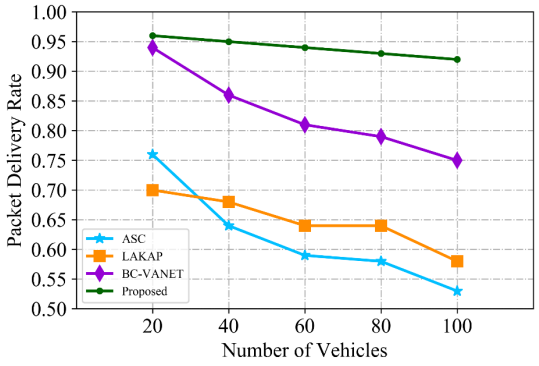

Figure 6. PDR with DoS attack

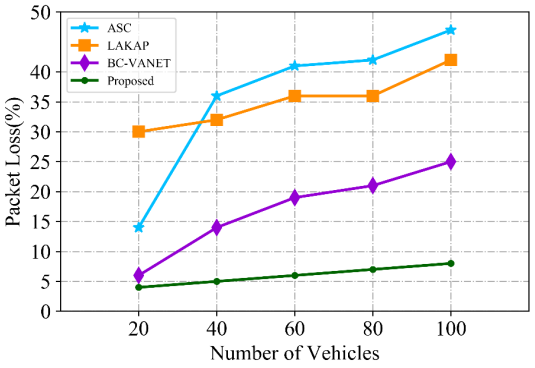

Figure 7. Packet loss with DoS attack

B. Packet Delivery Rate

The packet delivery rate refers to the proportion between the total packet sent and received in the network as show in equation (8).

$$PDR = \frac{S_p}{R_p} \tag{8}$$

Figure 4 shows the impacts of PDR in the absence of an attacker in the network. The proposed model has high PDR of 0.99, however, BC-VANET [3], ASC [42] and LAKAP [43] have PDRs of 0.98, 0.94, and 90 respectively. The average PDR of the proposed model is 0.97 with 20 vehicles in the network. We can observe that the highest delivery rate is 0.98 which has dropped slightly when the number of vehicles is increasing in the network. Similarly, as can be seen in figure (5) packet loss is lower when there are fewer vehicles in the network and increases slightly when the number of vehicles increases. The proposed model has the lowest packet loss rate.

Figure (6) shows the effect on PDR when there is an attacker in the network. The proposed model has high PDR of 0.96, however, BC-VANET [3], ASC [42] and LAKAP [43] have PDRs of 0.94, 0.75, and 0.70 respectively. We can observe that the highest PDR is 0.96 with an attacker present in the network; however, this drops to 0.92 as the number of vehicles in the network increases. The proposed model has the lowest packet loss rare. Similarly, the packet loss while it has an attacker as can be seen in figure (7) when the number of vehicles were less than the packet loss was low and slightly increased when the number of vehicles increases. However, the proposed model has the lowest packet loss as compared to BC-VANET [3], ASC [42] and LAKAP [43].

C. Computational Cost

Figure (8) shows that the proposed model has less computational cost as compared with BC-VANET [3], ASC [42] and LAKAP [43]. In the beginning with 20 vehicles the proposed model has a time cost of 0.1ms while with BC-VANET [3], ASC [42] and LAKAP [43] the cost is 0.13, 2.8 and 4.0 respectively. As the number of vehicles in the network increases from 20 to 100, the computational cost also increases from 0.1ms to 0.3ms, however, this is still very low compared with existing approaches.

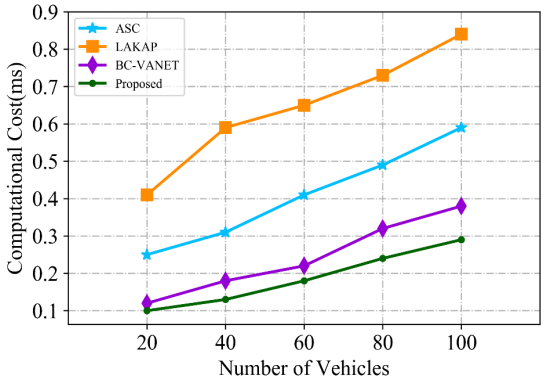

Figure 8. Computational cost of the proposed model

D. Security Analysis

We analyse the security of our proposed model which meets the security criteria.

1) SECURE REGISTRATION

The registration of the vehicle ensures security using public and private keys. The keys are stored in the OBU which is a tamper proof memory. The vehicle is registered only when the registration data is verified with MVD. The data is sent to network by signing with private key of the vehicle.

$$M_i = Sign_{KR_i}(KU_i, V_i, D_i \| \mathcal{H}(KU_i \| V_i \| D_i)) \quad (8)$$

The length of the RSA signature key is 1024 bit long. The signature is a bit of string of $\lceil log_2 N \rceil$-1 bits that provides strong security.

2) DATA INTEGRITY

We can denote the cost of authentication as T_a which has H as hash function, signature and match functions. Additionally, E_c represents the encryption cost. The T_{hash} can be evaluated using the hash function. The vehicle authentication process takes $2T_{hash}$ and further time t_δ to compare hash functions H_1 and H_2.

The cost involved in vehicle authentication for hashing will be $2H$ while the encryption cost can be derived by adding the hash cost as $1H + E$. The TA cost may be derived by combining the decryption and verification cost. The total cost is expressed in equation (9):

$$2H + E + D \quad (9)$$

3) PRIVACY PRESERVATION AND TRACEABILITY

Vehicle identity should not be revealed to anyone. Without detection by the RSU or other drivers, the messages should be completely invisible. We achieved this by creating a unique id using biometrics and taking the hash (SHA-512) as follows:

$$V_p = \mathcal{H}\ (d_{bio} \leftarrow Cf_{T_{(p \times N)}}) \quad (10)$$

Now, every vehicle has a unique 512-bit pseudo identity. The MVD and TA can only find the real identity of a vehicle by looking at the database stored in the blockchain. The traceability will be needed whenever there is a malicious activity of any fake message is generated by a vehicle.

VI. Conclusion

In this paper, we present a novel biometrics blockchain framework (BBC) to secure data sharing among vehicles in a VANET environment. Our novel BBC framework can protect the security of messages within VANET in real-world scenarios. The proposed framework not only provide security and trustworthiness of the communication between vehicles, but also keep anonymity without exposing the original identity of authorized users. Additionally, biometric is combined with blockchain technology to provide reliable transmission of data, keep track of data being exchanged and identify the responsible vehicle in the case of false messages. The simulation under the OMNET++, veins and SUMO is carried out to demonstrate the viability of the proposed framework. The performance of the framework is evaluated in terms of packet delivery rate, packet loss rate and computational cost. Therefore, the obtained results reveal that the proposed model is superior in comparison with existing approaches. As a part of future work, we will extend the model for computing ranking and reputation of vehicles and drivers using machine learning techniques.

REFERENCES

[1] X. Zhang and X. Chen, "Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network," in IEEE Access, vol. 7, pp. 58241-58254, 2019,
[2] R. Brendha and V. S. J. Prakash, "A survey on routing protocols for vehicular Ad Hoc networks," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2017, pp. 1-7,
[3] Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. Sensors 2019, 19, 4954
[4] Khan, M. and Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, pp.395-411.
[5] S. Roy, M. Ashaduzzaman, M. Hassan and A. R. Chowdhury, "BlockChain for IoT Security and Management: Current Prospects, Challenges and Future Directions," 2018 5th International Conference on Networking, Systems and Security (NSysS), Dhaka, Bangladesh, 2018, pp.
[6] Z. Lu, W. Liu, Q. Wang, G. Qu and Z. Liu, "A Privacy-Preserving Trust Model Based on Blockchain for VANETs," in IEEE Access, vol. 6, pp. 45655-45664, 2018,
[7] L. Zhu, C. Chen, X. Wang, and A. O. Lim, ''SMSS: Symmetric-masquerade security scheme for VANETs,'' in Proc. 10th Int. Symp. Auton. Decentralized Syst., Mar. 2011, pp. 617–622.
[8] 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. IEEE INFOCOM-27th Conf. Comput. Commun., Apr. 2008, pp. 246–250.
[9] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, ''Efficient and robust pseudonymous authentication in VANET,'' in Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw., 2007, pp. 19–28.
[10] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, ''Secure certifi-cateless authentication and road message dissemination protocol in VANETs,'' Wireless Commun. Mobile Comput., vol. 2018, May 2018, Art. no. 7978027.
[11] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, ''Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks,'' IEEETrans. Intell. Transp. Syst., vol. 17, no. 4, pp. 1015–1028, Apr. 2016.
[12] Q.Wu, J. Domingo-Ferrer, and Ú. Gonzalez-Nicolas, ''Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications,'' IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.
[13] B. Qin, Q. Wu, J. Domingo-Ferrer, and W. Susilo, ''Robust distributed privacy-preserving secure aggregation in vehicular communication,'' Control Cybern., vol. 42, no. 2, pp. 277–296, 2012.
[14] Y. Yuan and F.-Y. Wang, ''Towards blockchain-based intelligent transportation systems,'' in Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC), Nov. 2016, pp. 2663–2668.
[15] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, ''Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels,'' 2017, arXiv:1704.02553. [Online]. Available: https://arxiv.org/abs/1704.02553
[16] M.-C. Chuang and J.-F. Lee, ''PPAS: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks,'' in Proc. Int. Conf. Consum. Electron., Commun. Netw. (CECNet), Apr. 2011, pp. 1509–1512.
[17] X. Peng, ''A novel authentication protocol for vehicle network,'' in Proc. 3rd Int. Conf. Syst. Inform. (ICSAI), Nov. 2016, pp. 664–668.
[18] 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./12th IEEE Int. Conf. Big Data Sci. Eng. (Trust- Com/BigDataSE), Aug. 2018, pp. 674–679.

[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] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ''ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,'' in Proc. IEEE INFOCOM-27th Conf. Comput. Commun., Apr. 2008, pp. 1229–1237
[21] O. Kaiwartya et al., "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," in IEEE Access, vol. 4, pp. 5356-5373, 2016, doi: 10.1109/ACCESS.2016.2603219.
[22] Y.L. Morgan, Notes on DSRC and WAVE standards suite: its architecture, design, and characteristics, IEEE Commun. Surv. Tutorials 12 (4) (2010), 504518.
[23] M. Raya, P. Papadimitratos, V.D. Gligor, J. Hubaux, On data-centric trust establishment in ephemeral ad hoc networks, in: IEEE INFOCOM 2008 - the 27th Conference on Computer Communications, Phoenix, AZ, 2008, pp. 1238–1246.
[24] K. N. Qureshi, S. Din, G. Jeon and F. Piccialli, "Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges With Future Aspects," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.2994972.
[25] Reyna, A. et al. (2018) 'On blockchain and its integration with IoT. Challenges and opportunities', Future Generation Computer Systems, 88(2018), pp. 173–190. doi: 10.1016/j.future.2018.05.046.
[26] S. Roy, M. Ashaduzzaman, M. Hassan and A. R. Chowdhury, "BlockChain for IoT Security and Management: Current Prospects, Challenges and Future Directions," 2018 5th International Conference on Networking, Systems and Security (NSysS), Dhaka, Bangladesh, 2018, pp. 1-9, doi: 10.1109/NSysS.2018.8631365.
[27] T. Jiang, H. Fang and H. Wang, "Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4640-4649, June 2019, doi: 10.1109/JIOT.2018.2874398.
[28] Shrestha, R. et al. (2020) 'A new type of blockchain for secure message exchange in VANET', Digital Communications and Networks. Elsevier Ltd, 6(2), pp. 177–186. doi: 10.1016/j.dcan.2019.04.003.
[29] Khan M.A., Algarni F., Quasim M.T. (2020) Decentralised Internet of Things. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-030-38677-1_1
[30] V. Balioti, C. Tzimopoulos and C. Evangelides, "Multi-criteria decision making using TOPSIS method under fuzzy environment. application in spillway selection", Proceedings, vol. 2, no. 11, pp. 2-8, 2018.
[31] Rivest, R.L., Shamir, A., Wagner, D.A.: Time-lock puzzles and timed-release crypto. Technical Report MITLCSTR-684, MIT (February 1996)
[32] Mahmoody M., Moran T., Vadhan S. (2011) Time-Lock Puzzles in the Random Oracle Model. In: Rogaway P. (eds) Advances in Cryptology – CRYPTO 2011. CRYPTO 2011. Lecture Notes in Computer Science, vol 6841. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22792-9_3
[33] Yong Yuan and Fei-Yue Wang, "Towards Blockchainbased Intelligent Transportation Systems", 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Windsor Oceanico Hotel, Rio de Janerio, Brazil, Nov.1-4, 2016.
[34] Benjamin Leiding, Parisa Memarmoshrefi, and Dieter Hogrefe. "Self-managed and blockchain-based vehicular ad-hoc networks", In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp '16), ACM, New York, NY, USA, 2016, p.137-140.
[35] Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak, "Blockchain: A distributed solution to automotive security and privacy", eprint arXiv:1704.00073, March 2017.
[36] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain- based decentralized trust management in vehicular networks," IEEE Internet Things J., to be published
[37] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," IEEE Access, vol. 6, pp. 25657–25665, 2018.
[38] F. Gao et al., "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," IEEE Netw., vol. 32, no. 6, pp. 184–192, 2018
[39] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," IEEE Access, vol. 6, pp. 13565–13574, 2018
[40] N. Kshetri, "Can blockchain strengthen the Internet of Things?" IT Prof., vol. 19, no. 4, pp. 68–72, Aug. 2017.
[41] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," IEEE Veh. Technol. Mag., vol. 13, no. 1, pp. 32–39, Mar. 2018.
[42] ACC: Ying, B.; Nayak, A. Anonymous and lightweight authentication for secure vehicular networks. IEEE Trans. Veh. Technol. 2017, 66, 10626–10636.
[43] LAKAP: Wazid, M.; Das, A.K.; Kumar, N.; Odelu, V.; Reddy, A.G.; Park, K.; Park, Y. Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. IEEE Access 2017, 5, 14966–14980.

Abdullah Alharthi, received master's degree in Networks and Security from the University of Kent, Canterbury, Kent, United Kingdom in 2018. He is currently working towards the Ph.D. degree with the School of Computing and Communication, Lancaster University, Lancaster, United Kingdom. His research interest includes Network Security, IoT Security, Vehicular Ad-hoc Networks (VANETs) security and privacy, and Blockchain.

QIANG NI (M'04–SM'08) is a Professor and the Head of the Communication Systems Group, School of Computing and Communications, Lancaster University, Lancaster, U.K. His research interests include the area of future generation communications and networking, including green communications and networking, millimetre-wave wireless communications, cognitive radio network systems, non-orthogonal multiple access (NOMA), heterogeneous networks, 5G and 6G, SDN, cloud networks, energy harvesting, wireless information and power transfer, IoTs, cyber physical systems, AI and machine learning, big data analytics, and vehicular networks. He has authored or co-authored 300+ papers in these areas. He was an IEEE 802.11 Wireless Standard Working Group Voting Member and a contributor to various IEEE wireless standards.

Richard Jiang is currently a Senior Lecturer (Associate Professor) in the School of Computing & Communications at Lancaster University, UK. He is a Fellow of HEA, and an Associate Member of EPSRC College. He currently holds a Leverhulme Research Fellowship.
Dr Jiang's research interest mainly resides in the fields of Artificial Intelligence, XAI, Neural Computation, Biomedical Image Analysis, Intelligent Systems, and Biometrics & Privacy. His recent research has been supported by grants from EPSRC , Leverhulme Trust, Qatar Science Foundation and other industry funders. He has supervised and co-supervised over 10 PhD students. He authored over 80 publications and was the lead editor of two Springer books.