IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON MOBILE SERVICE COMPUTING WITH INTERNET OF THINGS

Received March 31, 2019, accepted April 17, 2019, date of publication April 29, 2019, date of current version May 10, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2913682

Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs

LIXIA XIE[1], YING DING[1], HONGYU YANG[1], AND XINMU WANG[2]
[1]School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China
[2]Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Corresponding author: Hongyu Yang (yhyxlx@hotmail.com)

This work was supported by the Civil Aviation Joint Research Fund Project of the National Natural Science Foundation of China under Grant U1833107 (Civil aviation information systems multi-dimensional security situation assessment and business affecting impact analysis).

ABSTRACT The modern intelligent transportation system brings not only new opportunities for vehicular Internet of Things (IoT) services but also new challenges for vehicular ad-hoc networks (VANETs). Apart from enhanced network performance, a practical and reliable security scheme is needed to handle the trust management while preserving user privacy at the same time. The emerging 5G mobile communication system is viewed as a prominent technology for ultra-reliable, low-latency wireless communication services. Furthermore, incorporating software-defined network (SDN) architecture into the 5G-VANET enables global information gathering and network control. Hence, real-time IoT services on transportation monitoring and reporting can be well supported. Both pave the way for an innovative vehicular security scheme. This paper investigates the security and privacy issue in the transportation system and the vehicular IoT environment in SDN-enabled 5G-VANET. Due to the decentralized and immutable characteristics of blockchain, a blockchain-based security framework is designed to support the vehicular IoT services, i.e., real-time cloud-based video report and trust management on vehicular messages. This paper explicitly illustrates the SDN-enabled 5G-VANET model and the scheduling procedures of the blockchain-based framework. The numerical simulation results also show that malicious vehicular nodes or messages can be well detected while the overhead and impact on the network performance are acceptable for large-scale scenarios. Through case studies and theoretical analysis, we demonstrate our design substantially guarantees a secure and trustworthy vehicular IoT environment with user privacy preserved.

INDEX TERMS Blockchain, 5G-VANET, IoT, security and privacy, SDN, trust.

I. INTRODUCTION

A. BACKGROUND OF THE VEHICULAR IOT IN SDN-ENABLED 5G-VANET

The development of modern intelligent transportation system requires enhanced network performance and introduces new challenges for Internet of things (IoT) in vehicular ad-hoc networks (VANET). Due to the disadvantages of IEEE 802.11p networks [1], e.g., poor scalability, low capacity and intermittent connectivity, the adoption of the long term evolution (LTE) mobile communication system to support vehicular applications [2] is a promising solution. 5G network is viewed as a key technology provide ubiquitous connectivity, ultra-reliable and low-latency communication [3] in VANET. 5G network is a user-centric networking principle which use a unified platform to address the service requirements [4]. The newly assigned spectrum enables new air interfaces with higher spectral and energy efficiency brought by the development of millimeter-wave [5] and massive multiple-input multiple-output (MIMO) arrays [6]. 5G also enables a strategy which leverages existing infrastructure as well as the envisioned access techniques. Hence, a wider range of services are available for users.

Software defined network (SDN) is expected to be incorporated into the 5G-VANET [7]. SDN is able to handle the time-varying nature of vehicular networks with much lower cost through simplified hardware, software and management [8]. The incorporation of SDN into VANET have been investigated by some initial researches. E.g., SDN provides an adaptive edge computing solution to monitor and react to quality of service (QoS) changes in vehicular networks with regressive admission control and fuzzy weighted

The associate editor coordinating the review of this manuscript and approving it for publication was Tie Qiu.

queueing [9]. A cooperative data scheduling scheme integrated at road side units (RSUs) has also been developed to promote the data dissemination by exploiting the synergy between vehicle-to-network (V2N) and vehicle-to-vehicle (V2V) communications [10]. Therefore, SDN can significantly enhance the IoT services in vehicular environment.

B. SECURITY AND TRUST CONCERNS IN THE VEHICULAR IOT ENVIRONMENT

Vehicular IoT security has become a critical issue and drawn increasing attention. Vehicles have more autonomy with their increasing on-board abilities of sensing, computation, and communication. Thus, vehicular networks are able to share large-volume of messages (e.g., high-definition videos) among vehicles and report them to the information operation or management center. New types of IoT services are enabled with emergency data/message transmission [11]. Such messages are great help of the safety guarantee in the transportation system and can promote the management efficiency with the awareness of traffic situations. But in a VANET, vehicles are usually unwilling to fully cooperate with and trust each other since they are strangers to each other in most cases. VANET is featured with high mobility and variability and malicious vehicles or misbehaviors are unavoidable in large-scale scenarios. The spread of incredible messages by malicious vehicular nodes greatly endanger the transportation system, e.g., claiming a clear road which is actually congested or with traffic accident. VANET needs to guarantee a secure IoT environment where service related messages are sourced from legitimate or trustworthy vehicles and infrastructures. These messages should be immutable, credible and authentic. Since there is no user can endure the leakage of his or her personal information, preserving user privacy in the message acquirement and delivery is another critical issue. Besides, the future trend in vehicular IoT services also demand the center-less trust, collaborative intelligence and spatiotemporal sensitivity [12].

This paper seeks for a solution with a blockchain based framework. We implement vehicular IoT services in this framework including real-time cloud-assisted video report and trust management on vehicular messages. Vehicles entering the 5G-VANET need to be authenticated. Authentication authorities guarantee the legitimacy of vehicles by issuing valid public-key certificates and private keys. Only after the vehicle has passed the validation can it continue to drive on the road and transmit real-time videos and road condition related messages. To preserve user privacy, the scheme stores the vehicle authentication information separately from user identity information, which means user identity is always opaque to operators and other vehicles. A vehicle reports the recorded videos per minute and spreads messages about the traffic conditions it witnessed. If a traffic accident occurs, all related video records and traffic messages will be checked.

Main contributions can be summarized as follows:

(1) We design a trust management system which is combined with blockchain. When a vehicle uploads a video, it is necessary to upload the traffic condition tag at the same time, and use the tag as road information for broadcasting and sharing with other vehicles. To prevent the attacked vehicle from interfering with traffic by issuing malicious or inaccurate information, the realness of the traffic information broadcast by a vehicle will be scored by the vehicles near it. RSU calculates the trust value of the tag according to the distance between the scoring vehicle and the tag sending vehicle, and packs the trust value into blocks.

(2) In this system, proof-of-work and proof-of-stake are used to conduct regular elections. Malicious traffic broadcasting will be eliminated, and only traffic broadcasting that conforms to the real situation will be retained. Malicious vehicles (vehicles that disturb traffic order by broadcasting a lot of false road information) will be traced back to the system and temporarily banned. The privacy of legitimate vehicles will be protected and their anonymity will be maintained.

(3) Based on the centralized authentication and blockchain distributed trust management, a semi-centralized video and road condition trust management system is designed and simulated. Both theoretical analysis and numerical results show the superiority of the framework and the feasibility of large-scale deployment.

The rest of paper is organized as follows: Section II introduces the related work. Section III briefly introduces the system model proposed in this paper. Section IV describes blockchain based security framework in details. Section V presents the experimental results and gives the safety analysis. Section VI concludes the paper.

II. RELATED WORK

Video sharing and related services are necessary for vehicular systems [13]. The real-time transmission and storage of traffic video becomes possible [14] when 5G is applied to the VANET. Cloud-assisted IoT services are of great help not only for industrial mobile computing [15], but also for vehicular systems [16]. The photographic angle of the closed circuit television (CCTV) cameras installed in roadside has many blind spots [17], when there is a traffic accident, it is not easy to obtain the truth from a single angle of forensics and investigation. Therefore, it is of great significance for maintaining the information security of VANET to make the vehicles in VANET participate in road monitoring, and implement multi-angle real-time monitoring of road conditions and road condition broadcasting. In terms of trust management, this paper compares and analyses the centralized, decentralized schemes and gives a semi-decentralized scheme.

A. CENTRALIZED TRUST MANAGEMENT SYSTEM

In the VANET, if every vehicle joins the video system and becomes the supervisor and maintainer of road security, it will bring great convenience to the investigation of traffic accidents. At the same time, it also reduces the great potential safety hazards under the condition of supervision. In [18], a cloud-based video collection and analysis system named Kestrel is designed, which uses cheap visual features

to extract attributes. It solves the problem of path ambiguity by associating vehicle visual descriptors while realizes continuous monitoring in a heterogeneous camera network composed of fixed camera system and cameras on mobile devices. Reference [19] also presents a backpressure scheduling mechanism for data transmission in large-scale multi-hop IoT.

If a search system based on user identity is established, it will be beneficial to the management of road condition information but may threaten the privacy protection of video providers in the meantime. However, if there is no systematic management, it may be difficult to find volunteers to provide videos since the vehicle users as witnesses do not know that their videos can be used as evidence. Therefore, it is necessary to establish a privacy-preserving traffic information collection system, which enables vehicles to upload videos and road information anonymously while driving [13]. In [17], a specific method is proposed to facilitate the recording and sharing of videos for moving vehicles. It demonstrates the impact of some new network technologies on wireless broadcasting under 5G heterogeneous networks, and proposes a new 5G-VANET system model. It allows vehicles to report and upload road videos through vehicle authentication and video encryption schemes. At the same time, it provides protection for the identity of the participating vehicle and the privacy of video content.

B. DISTRIBUTED TRUST MANAGEMENT SYSTEM

Distributed system management can protect the invisibility of vehicle routing. Reference [13] proposed an automated public service system, View-map, which can share DashCam videos anonymously. DashCam is a vehicle-mounted camera that can record scenes around the vehicle. In [13], in order to protect user privacy, each video is represented as a view profile (VP). Anonymous VP takes the place of its owner to participate in the retrieval, validation and reward of the system. They are assigned trust scores by legitimate members of the system. The distributed trust management method allows users to get virtual cash while not being traceable to the source, maintaining the path anonymity of video vehicles.

Trust management system can not only collect videos for evidence obtaining in traffic accidents, but also be used to analyze real-time road conditions. In [20], a system based on blockchain technology is proposed to solve the problem of reliability evaluation of traffic conditions broadcast by vehicles. In this system, road information broadcast by vehicles can be scored by adjacent vehicles to generate trust ratings. RSUs collect the data and each one packages the information into a block and to try to add it to the blockchain. The system enhances the interaction between vehicles and uses mutual authentication between vehicles to confirm the broadcast information of traffic conditions. But in this system, whether the identity of the vehicle is true or not cannot be guaranteed. In addition, in terms of road reporting, if a single RSU is maliciously attacked, such as coming up with an attacker who modifies its collected content, it may cause the fact of the road information to be concealed or tampered with, resulting in inaccurate road conditions finally collected.

C. SEMI-DECENTRALIZED TRUST MANAGEMENT SYSTEM BASED ON BLOCKCHAIN

Centralized trust management is conducive to road condition collection and post-investigation, while protecting user privacy. But if malicious vehicles intentionally release wrong information, it will endanger road safety. Distributed trust management can judge the reliability of road conditions and other information according to the interaction between vehicles. But there is no unified authentication for a vehicle entering the VANET, and the legitimacy of the vehicle identity is not recognized.

This paper presents a semi-decentralized trust management scheme based on blockchain. It collects encrypted videos and upload them to the cloud while stores trusted traffic information into the blockchain. RSU is the node of blockchain election, and each RSU node can always reach a consensus. Even if an individual RSU node is attacked, it will not affect the accuracy of the information stored in the blockchain. The attacked RSU cannot store unreliable information into the blockchain by cheating. In this system, only legitimate vehicles can enter the VANET. After applying to the system for key pairs, their recorded road videos and traffic conditions can be shared. The message transmitted by a vehicle needs to be signed with the digital signature of it, which prevent the existence of counterfeit or forged traffic information. The road condition released by the vehicle will also be rated by other vehicles to ensure its reliability. Malicious vehicles will be notified and banned by the VANET. The system ensures the authenticity of information sources while protecting user privacy.

III. SYSTEM MODEL

A. OVERVIEW OF THE SDN-ENABLED 5G-VANET ARCHITECTURE

The system model of a SDN-enabled 5G-VANET is shown in FIGURE 1 and FIGURE 2, which is a HetNet architecture.

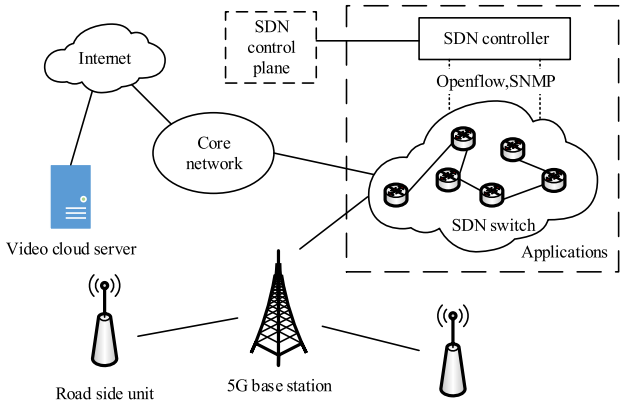


FIGURE 1. Integrating SDN into 5G-VANET system.

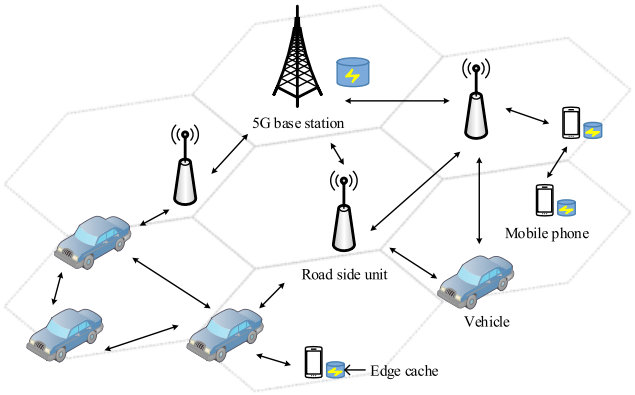


FIGURE 2. Radio Access Network in 5G-VANET system.

This architecture contains heterogeneous nodes including 5G base stations (gNBs), RSUs and vehicles with on-board units (OBUs). RSUs are supposed to serve as 802.11p wireless access points (APs) to communicate with the OBUs in the coverage range. The core network which includes trusted authority(TA) and department of motor vehicles(DMV) is connected to the Internet and video reports are stored at the video cloud server. Due to the drawback of 802.11p network (mainly the constrained bandwidth, poor scalability and intermittent connectivity), gNBs are deployed in the VANET to provide broadband wireless access to the Internet. V2V communication is also considered in this architecture to enable data sharing among vehicles. Vehicles outside or at the edge of RSU or gNB service range can thus use nearby vehicles for relay transmission.

To achieve a consistent policy and global management for the 5G-VANET, RUSs and gNBs are all controlled by a centralized SDN controller with OpenFlow protocol through high-capacity fiber optic backhaul links. The SDN data plane is made up of all the vehicles, RSUs and gNBs. The control plane is decoupled from the data plane. The SDN controller moves the control logic from the underlying infrastructure to the control layer. Vehicular applications can be implemented at the SDN controller to provide functions such as vehicle clustering and traffic management. The SDN controller is in charge of the global policies, including authentication, and mobility/traffic management, while the controller-defined policies are implemented at the data plane. The separation of the data plane and control plane provides a global view over the whole service area where programmable applications can be used to realize global functions. This brings an advantage of the coordination and information sharing in the HetNet architecture. The updates of the overall network policies can be either proactively after a predefined period of time or reactively requested by the infrastructure.

B. BLOCKCHAINS IN VEHICULAR NETWORKS

Traditional centralized network architecture is always threatened by attacks and falls in the lack of privacy. On the other hand, due to the decentralized features, blockchain has been viewed as a revolutionary technique on information security and privacy. Known as a disruptive innovation in financial industry (i.e., bitcoin presented by Satoshi Nakamoto [14]), a blockchain (shown in Fig. 3) is a distributed database maintaining a growing list of blocks chained to each other which maintains a consistent ledger without a centralized bank but through distributed node trading. It is managed by a distributed P2P network where each node is identified using a public key (PK). Communications between nodes, i.e., transactions, are encrypted by PKs and broadcast to the entire network. Each node can verify a transaction by validating the signature of the transaction generator against their PK, which ensures the trustless consensus of blockchain.

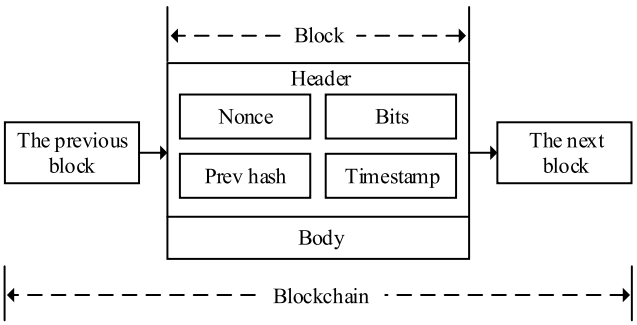


FIGURE 3. The Structure of a blockchain.

We implement a blockchain-based framework for security and privacy preserve in the SDN-enabled 5G-VANETs. All active nodes, including vehicles, RSUs, gNBs (5G base stations), form an overlay P2P network to maintain a blockchain. A real-time video-report service of the traffic situations and message interaction among nearby vehicles are enabled in the vehicular system. We believe the immutability and accountability of the source messages can be well guaranteed by exploiting the features of blockchain. Thus the security and efficiency of the vehicular system are greatly enhanced.

IV. BLOCKCHAIN BASED SECURITY FRAMEWORK

A. REAL-TIME VIDEO REPORT AND MESSAGE SHARING SERVICE

1) VEHICLE REGISTRATION

Each vehicle has a 5G subscriber identification module(SIM) number in the 5G-VANET. Here we use *ID* to denote the SIM number. Each *ID* is fixed for one particular vehicle necessarily. It is stored in the operator's database along with the same vehicle's device number. Here we use *Dnum* to denote the device number. Take vehicle V_m as an example to introduce the registration process. When V_m enters the system, it can go online only after the operator has verified that V_m's *Dnum* and its *ID* are matched and either of them has not been changed. Then V_m randomly generates a unique symmetric key *SKE* for the process of registration.

In this paper, it is assumed that only DMV saves all the license plate numbers and SIM numbers. Here we use *Num* to denote the license plate number of a vehicle. DMV sends a request message to TA for the registration of V_m. It is worth

noting that the mapping between a vehicle's *Num* and its *ID* is only stored in DMV, thus providing a layer of privacy protection for its true identity. Therefore, although TA knows V_m's *ID*, it does not know the true identity of V_m. TA checks whether the public key and private key of V_m are already existed in its repository(where the key pairs are saved) and whether V_m's public-key certificate is still in the valid period. If there are no V_m's key pairs stored in the repository or the public-key certificate of V_m's has expired, TA will issue V_m's public-key certificate and private key which are encrypted by *SKE* in case that other vehicles can get them. The procedure of the vehicle registration can be described as algorithm 1.

Algorithm 1 Vehicle Registration

Input:
Initial vehicle V_m
TA's public key PUB_{TA}
A random symmetric key *SKE*
Time k // *validity period of the registration*

Output:
V_m's public-key certificate $Pcert_m$
V_m's public key PUB_m
V_m's private key PRI_m

V_m enters the VANET
Operator select *Dnum* from DATABASE
  Where *ID* = *ID* of V_m
if *Dnum* != *Dnum* of V_m **then**
  Fails
else
  V_m is available to the Internet
end if
V_m do
  Use PUB_{TA} to encrypt *SKE* as En(*SKE*)
  Send (*Num* of V_m, *ID* of V_m, En(*SKE*)) to DMV
DMV do
  Insert into IDENTITY_PAIRS(*Num*, *ID*)
  Select *Num* of V_m, *ID* of V_m
  Where not exists(select * from IDENTITY_PAIRS Where *Num* = *Num* of V_m and *ID* = *ID* of V_m)
  Use PUB_{TA} to encrypt *SKE* and *ID* of V_m as En(*SKE*, *ID* of V_m)
  Send En(*SKE*, *ID* of V_m) to TA
TA do
  Decrypt En(*SKE*, *ID* of V_m)
  Select * from KEY_PAIRS
if not exists(PUB_m, PRI_m) **then**
  Issue (PUB_m, PRI_m) validity of k
  Encrypt (PUB_m, PRI_m) with *SKE*
else
  Fails
end if
DMV forwards encrypted (PUB_m, PRI_m) to V_m
V_m decrypts encrypted (PUB_m, PRI_m) with *SKE*
V_m obtains PUB_m and PRI_m
Successful registration

2) ROAD CONDITION REPORT

After the registration, V_m records video files of the road condition through its onboard camera during the way and calculates the message digest of them [21]. The procedure is taken every 1 minute as a term. The road condition is marked as $tag_{m,j}$ and the location is marked as $place_m$ in the meanwhile of each term, where j acts as a timestamp. V_m uses *SKE* to encrypt the hash value of the video and signs the information generated during that minute. Then V_m sends the message to the nearby nodes X (X includes RSU and other vehicles) as broadcasting. If a node nearby V_m receives the message, the public-key certificate of V_m will be checked by it to make sure that V_m has a legal identity within a valid period. After the verification, the message will be forwarded to other nodes and will be finally uploaded to the gNBs by RSU. The encrypted data will be uploaded to the cloud server through step-by-step forwarding. If the RSU near the V_m has no available storage space, the message sent by V_m will be forwarded by $n(n \geq 1)$ hops through other vehicles and the validity of the message will be authenticated at each hop. The procedure of the road condition report can be described as algorithm 2.

The data transmission is encrypted, which means only the source vehicle and the cloud server know the video content. In case that the video data may be tampered by the inter-medium nodes over the transmission hops, or the cloud server itself may be attacked, a message-digest scheme is thus given. A malicious node may report fake video content and the authentication should check the digital signature of the video's message-digest. A vehicle is required to not only report video records related to itself, but also spread necessary messages e.g., its own driving operations and the road situations to vehicles nearby or located in a certain area. These messages are of great help for other vehicles' driving decisions but fake messages will severely degrade the efficiency of this mechanism with a safety threaten. Therefore, we handled the message sharing among vehicles as transactions in a blockchain, which means all messages can be found in the blockchain and traced out the source vehicle while all the records are immutable. This guarantees the accountability of the message source nodes in this service and malicious vehicles will be punished by the mechanism. The number of transactions in the blockchain is determined by the message rate of each vehicle since one message is mapping to one transaction.

Fake messages or malicious nodes are unavoidable, and thus a temporary center node, i.e., the miner, is needed to be elected to broadcast its message and reach a consensus. Periodic elections are conducted in all RSUs to produce a miner who adds new blocks to the blockchain. In this system, an election method combining proof-of-work and proof-of-stake is designed and applied to elect miners.As shown in Figure3, the block header data of each block generated by RSU should include four parts: nonce, bits, prev hash and

Algorithm 2 Road Condition Report

Input:
V_m's public-key certificate $Pcert_m$
V_m's public key PUB_m
V_m's private key PRI_m

Output:
Road video Vid
Road condition tag

while minute++ **do**
  V_m do
    Record a video file $Vid_{m,j}$
    Record $place_m$ and sign $place_m$ with PRI_m
    Record $tag_{m,j}$ and sign $tag_{m,j}$ with PRI_m
    Hash($Vid_{m,j}$)
    Encrypt $Vid_{m,j}$, Hash($Vid_{m,j}$) with SKE as En($Vid_{m,j}$, Hash($Vid_{m,j}$))
    Sign En($Vid_{m,j}$, Hash($Vid_{m,j}$)) with PRI_m
    Broadcast signed $place_m$, $tag_{m,j}$, En($Vid_{m,j}$, Hash($Vid_{m,j}$)) together with $Pcert_m$
end while
for time = 0;; time++ **do**
  Node X receives the broadcast message
end for
if $X \leftarrow$ Other Vehicles **then**
  Check the validity of signature
  if pass **then**
    Forward it
  else
    Fails
  end if
end if
if $X \leftarrow$ RSUs **then**
  Check the validity of signature
  if pass **then**
    Upload it to the gNBs
  else
    Fails
  end if
end if
gNBs uploads the updated data

timestamp. The proof-of-work election method achieves the goal by using RSU as a node to calculate the hash value of the data stored in the header of the block and constantly changing the nonce value until the first x-bit of the hash result is exactly 0. Bits is the hash threshold of proof-of-work. The achievement of proof-of-work is that the hash value of the data stored in the header of the block calculated by a miner must be less than its hash threshold. The proposed miner election scheme is:

$$Hash(nonce, prehash, bits, timestamp) \leq B_r \quad (1)$$

where B_r is the hash threshold of RSU_r, r denotes the number of RSU. Several hash functions can be utilized in the proposed system, and the SHA-256 algorithm is commonly used. The calculation of the hash threshold using algorithm SHA-256 is:

$$B_r = 2^{256-x} - 1 \quad (2)$$

where B_r meets the requirement that the first x-bit is exactly 0. Each RSU node continuously change the value of its nonce, and calculates the hash value of the block header including the nonce. If the hash value calculated by an RSU is lower than its hash threshold, that RSU can be selected as a miner and can publish its block.

B. TRUST MANAGEMENT ON VEHICULAR MESSAGES

1) TRAFFIC INFORMATION COLLECTION

Vehicles judge the reliability of road condition tags and score them in the process of message forwarding. Scores can only be rated as +1 or -1. For example, suppose vehicle V_n receives a message broadcast by V_m. V_n authenticates the legal identity of V_m and get the traffic tag $tag_{m,j}$ and the location of $place_m$ contained in the message. V_n cannot know the specific content of $Vid_{m,j}$. It only judges the reliability of $tag_{m,j}$. The trustworthiness of $tag_{m,j}$ is scored by V_n. When V_n agrees with the road condition indicated by $tag_{m,j}$, the tag is scored +1. When V_n considers that the road condition indicated by $tag_{m,j}$ is not true, the tag is scored -1. Then V_n signs its location and the score made for $tag_{m,j}$, and uploads them to the nearby RSU along with its public key certificate $Pcert_{n,k}$. The message can be expressed as $\{Pcert_{n,k}$, Si(ID_m, ID_n, $mark_{m,j,p}$, $place_n$)$\}$.

RSU receives the message and confirms the source of it, and then classifies the received information of road condition at time j into $\{E_{j,1}, E_{j,2}, E_{j,3}, \ldots E_{j,p}\}$ according to the location of the road section, where p denotes the road section number, $E_{j,p}$ represents the road condition of section p at time j. $E_{j,p}$ includes $\{e^1_{j,p}, e^2_{j,p}, e^3_{j,p}, \ldots e^m_{j,p}\}$, where $e^m_{j,p}$ represents the traffic condition of road section p at time j broadcast by vehicle V_m. The division of messages at other times is the same as that at time j.

2) TRUST VALUE COMPUTATION

RSU classifies the scores made by forwarding vehicles it has received into $\{S_{j,1}, S_{j,2}, S_{j,3}, S_{j,p}\}$, where p represents the road section number, $S_{j,p}$ represents the scores for the road condition of section p at time j, including $\{s^{j,p}_{1,m}, s^{j,p}_{2,m}, s^{j,p}_{3,m}, \ldots s^{j,p}_{n,m},\}$, where $s^{j,p}_{n,m}$ represents the score V_n made for the road condition of road section p broadcast by V_m at time j. Since not all scores in set $S_{j,p}$ have the same credibility, vehicles closer to the place where the tag generated often score more credibly than vehicles farther from it. Therefore, the trust value of the score made by a forwarding vehicle is defined as:

$$o^{j,p}_{n,m} = e^{-\frac{|p_n - p_m|}{\alpha}} \quad (3)$$

where $o^{j,p}_{n,m}$ represents the trust value score for $s^{j,p}_{n,m}$, p_m denotes the road section of vehicle V_m and p_n denotes the road section of the video forwarding vehicle V_n, $|p_n - p_m|$ denotes

the distance between the two vehicles, α is a parameter for adjusting the rate, which will also be used in Formula (6).

Assuming that the attacker cannot control most of the vehicles, weighted aggregation can improve the reliability of the trust value. The definition of the trust value of the road condition at section p broadcast by V_m at time j is:

$$o_m^{j,p} = \frac{\sum_{i=1}^{n} s_{i,m}^{j,p} * o_{i,m}^{j,p}}{n}, \quad (s_{i,m}^{j,p} \neq 0, o_{i,m}^{j,p} \neq 0) \tag{4}$$

where $o_m^{j,p}$ represents the trust value of the road condition at section p broadcast by V_m at time j, V_m represents the video recording vehicle, $s_{n,m}^{j,p}$ and $o_{i,m}^{j,p}$ can only be calculated if $s_{i,m}^{j,p}$ and $o_{i,m}^{j,p}$ are both equal to zero in the Formula (4).

If the scoring vehicle is further from the broadcast address of the tag, the reliability of the scoring will be reduced. Therefore, when the trust value $o_{n,m}^{j,p}$ is greater than 0.5, $s_{n,m}^{j,p}$ is scored credible. The score with a trust value of no more than 0.5 will be discarded. Therefore, the trust value of score $S_{j,p}$ for the road condition of section p at time j is calculated as:

$$o^{j,p} = \frac{\sum_{i=1}^{n} \sum_{l=1}^{m} s_{i,l}^{j,p} * o_{i,l}^{j,p}}{n}, \quad (s_{i,l}^{j,p} \neq 0, o_{i,l}^{j,p} > 0.5) \tag{5}$$

where $o^{j,p}$ represents the trust value RSU calculated for $S_{j,p}$. There may be more than one vehicle broadcasting the road condition of section p at time j, therefore we use l to represent the number of the vehicles broadcasting the road condition at the same road section of p and the same time of j. RSU stores the calculated trust values into the trust values set O_r and tries to add them together with the corresponded road conditions to the blockchain, where r represents the RSU number who collects road conditions and calculates trust values. Tags with negative scores are tagged as untrustworthy tags. RSU counts the *ID* of vehicles who issue untrustworthy tags and uploads the *ID* of vehicles with high frequency of false positives to TA regularly over a period of time.

3) MINER ELECTION

The hash threshold of different RSUs may be different depending on the value of x. In this system, proof-of-stake is used to determine the difficulty of an RSU being elected as a miner and adding a new block. The value of x is related to the sum of RSU's trust value $o^{j,p}$ for vehicles and is calculated as:

$$x = int(e^{-(\frac{F_t * G_r}{\alpha} - e)}) \tag{6}$$

where α is a variable parameter greater than 0. α also appeared in Formula (3) to control the generation time of a new block. In this paper, we set the value of α to 100. G_r represents the sum of the trust values calculated by RSU_r. The larger the value of G_r is, the smaller the value of x will be. The increasing of the hash threshold comes with the decreasing of x, which means that the lager the hash threshold is, the greater the probability of an RSU of being elected as the miner and add a new block to the blockchain will be. G_r is calculated as:

$$G_r = \sum_{o^{j,p} \in O_r} o^{j,p} \tag{7}$$

where $o^{j,p}$ represents the trust value RSU_r calculated for $S_{j,p}$. Set O_r are constituted of trust values of different times and different locations. The more reliable the road traffic information collected by RSU_r is, the more likely RSU_r is to succeed in running for the miners. Once RSU_r is elected as a miner and its block is added to the blockchain, the elements of set O_r stored in RSU_r will be emptied.

At the same time, in order to prevent the right to be elected as a miner being occupied by a few RSUs with older blocks for a long time, a value correction function F_t is proposed in Formula (6) to solve the problem that the RSUs with older blocks may monopolize the voting rights. Function F_t is defined as follow,

$$F_t = \begin{cases} 1 & (t < t_1) \\ 1 - \beta t & (t_1 < t < 2t_1) \\ 0 & (if\ F_t > 0\ and\ t = 2t_1) \end{cases} \tag{8}$$

where t is the time that RSU_r has spent since it last cleaned up elements in set O_r, t_1 represents the average time-consuming for a success miner election during a given period of time. F_t always equals to 1 when t is less than t_1. When t is greater than t_1 and less than $2t_1$, the value of F_t decreases gradually. β is a coefficient greater than 0, which is used to control the reduction rate of F_t. When the value of F_t is reduced to zero, it will not continue to decrease. The range of F_t is controlled between [0,1]. At the same time, the elements of the collection O_r will be cleared, while t is reset to 0 to restart the timing. If the value of F_t is still greater than 0 when the value of t has increased to $2t_1$, the elements of set O_r will also be cleared and t will be reset to 0 to restart the timing. Other RSUs verify the validity of the nonce value when they receive a block sent by an elected miner. Then they add the block to their own blockchains. If an RSU receives multiple valid blocks at the same time, it branches on the blockchain. Because of the distributed consensus mechanism of blockchains, only the longest fork accepted by most RSUs will be retained over time.

4) VEHICLE CREDIBILITY ASSESSMENT

Once an accident takes place, the associated video can be downloaded from the cloud server and its content may be used to check the explicit situations. The traceability can only be achieved through the SIM numbers in 5G networks. The license plate numbers are only known by DMV and will not be revealed, which means that it need the support of a trusted third party besides a decentralized blockchain framework. As long as the report phase is in time, the road information uploaded with videos can also be used for traffic balancing, i.e., the transportation control center can know the traffic load of the entire region and evacuates the congested vehicles to the free roads.

Inspired by [20], an RSU can make trust rating on the message provided by nearby vehicles and try to upload it to the blockchain as a transaction. The trust rating for a vehicle can be calculated according to all the associated records in the blocks and corresponding reward or punishment is given to the vehicle based on the trust policies. Traditional methods rely on individual effort to check and evaluate the messages with the information provided by a few related or nearby vehicles. But the blockchain provides a consensus mechanism with the immutable information in the blocks used for validation. The message detections can be conducted with all the ratings for the related vehicles and their records stored in the blocks. Message detection accuracy (MDA) is used as the performance metric, which is defined as:

$$MDA = (TP + TN)/(TP + FN + FP + TN). \quad (9)$$

TP (true positive) denotes the number of true messages regarded as true ones; TN (true negative) denotes the number of fake messages regarded as fake ones; FP (false positive) denotes the number of fake messages regarded as true ones; FN (false negative) denotes the number of true messages regarded as fake ones. It is apparent that a higher MDA means higher detection accuracy on message credibility.

V. EXPERIMENTAL RESULTS AND ANALYSIS

A. EXPERIMENT CONFIGURATIONS

We carry out the simulation through OMNeT++ 4.5 [22], [23], and crypto++ library 5.6.2 [24]. All numerical experiments are carried out on the laptop with Intel Core i7 and 16 GB RAM and display card GeForce 920 M. The size of considered transportation area is set as 1000m × 1000m. The RSUs act as 802.11p Aps and we set the bandwidth as 10Mbps, and for the gNBs we set bandwidth as 1Gbps. We set the numbers of RSUs and gNBs as 30 and 25 separately and they are assumed to be uniformly distributed in the area. We assume the number of vehicles ranges from 200 to 500 and try to evaluate the network performance under different network densities. Vehicles are also uniformly distributed and have the speed of 110km/h in random directions. V2N communication range is set as 100m, and for V2V communication, the range is set as 50m.

SHA-256 is used as the hash algorithm in the blockchain, i.e., hashed result = dhash(input) = SHA256(SHA256(input)). In this experiment we test the time overhead of three video encryption algorithms AES/CBC (256-bit key), Twofish/CTR (256-bit key), and Serpent/CTR (256-bit key) to find out whether the network can handle the video report service. We try to compare the detection accuracy on malicious nodes between the blockchain-based framework and the individually detection. Furthermore, we also evaluate the transmission delay of the blockchain transactions with different message rates and different number of vehicles to demonstrate the scalability and the feasibility for deployment the blockchain based framework in the 5G-VANET.

B. NUMERICAL RESULTS AND DISCUSSIONS

FIGURE. 4. gives the processing time of blocks in the blockchain. The miners in the blockchain periodically generate blocks and we implement a light-weight scheme which introduces a little time overhead.

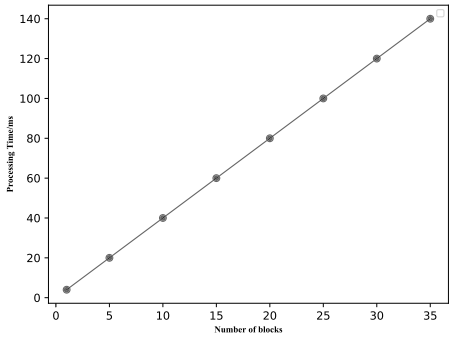


FIGURE 4. Processing time versus number of blocks.

As shown in FIGURE. 5, when malicious node has low proportion, the trust of the messages transmitted among the vehicular system can be guaranteed and vice versa. When the portion of malicious is over 5%, we can see the advantage of the blockchain based detection over an individually detection with a disparity of 5% to 15%.

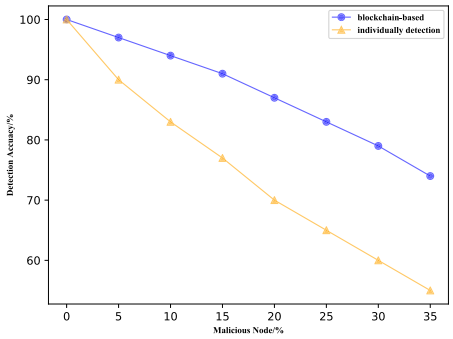


FIGURE 5. Detection accuracy vs proportion of malicious nodes.

As shown in FIGURE. 6, If the message rate of each node increases, the network will have more burden since it is needed not only to transmit the messages but also broadcast the increasing transactions. We believe the real-time effectiveness of the message can be guaranteed with the rate of at least 1 per minute. And, even the message rate is at 10 per minute, the transmission delay is also acceptable (no more than 50ms) mainly due to the high bandwidth of 5G-VANET.

As shown in FIGURE. 7, the time overhead for the video encryption is ranging from about 20ms to 160ms with different encryption algorithms and video size. Generally, when the video report phase is more frequent, the video size is smaller as well as less encryption time overhead. In the considered scenario, the video report takes place from 1 to 10 times per minute for each vehicular. For a several seconds video content, even with high definition, the corresponding video size will lead to an acceptable time overhead on encryption.

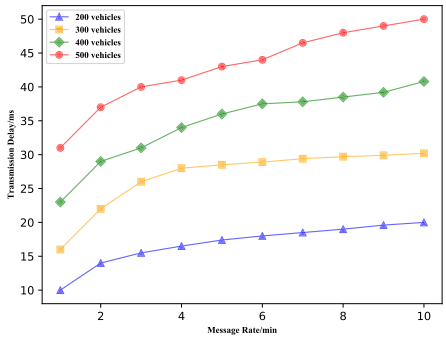


FIGURE 6. Transaction transmission delay vs message rate.

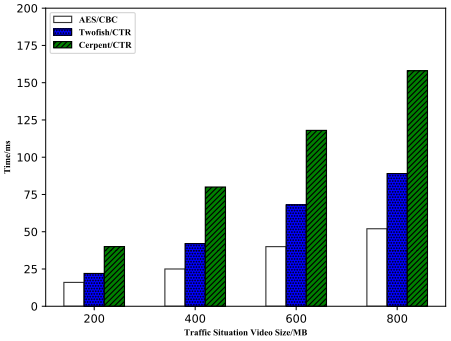


FIGURE 7. Video encryption time overhead.

Which means, the encrypted video can meet the requirement of real-time effectiveness.

C. SAFETY ANALYSIS

1) PROTECTION OF USER PRIVACY AND SECURITY

A vehicle's SIM number is fixed for the specific vehicle and cannot be changed. The operator verifies that there is no change of the SIM number of a same vehicle when a vehicle requests access to the Internet. The vehicle will not be able to access to the Internet if its SIM number and device number are not matched. Vehicles upload recorded videos to the operator's network server. The operator cannot view the content of the videos directly because the videos are encrypted. Only the license plate number can uniquely indicate the real identity of a vehicle. The information of private keys is only stored in TA anonymously. TA cannot know the real identity of a vehicle by its SIM number. At the same time, the mapping between license plate number of a vehicle and its SIM number is only stored in DMV, thus providing a layer of privacy protection for the real identity of the vehicle. Receivers can verify the sender's identity by its digital signature to ensure the authenticity of the uploaded videos. Therefore, it is possible to prevent an attacker from uploading a fake video by attacking a legitimate vehicle. Receiver can also check the integrity of videos by calculating hash functions of them so that you can guarantee that videos cannot be tampered with during uploading.

Encrypted videos can be downloaded from the network. Video contributors can decrypt the videos and view the content of the them using the symmetric key submitted by themselves when registering with the 5G-VANET. Others can't decrypt or get the content of the encrypted videos by downloading them directly. If there is a traffic accident and it is necessary to investigate and collect evidence, clients or police can find videos of the time and route on the Internet. With the help of operators, they can apply to TA for symmetric keys used in video encryption to decrypt the content of the obtained videos. This process does not expose the license plate number of the video recording vehicle, thus protecting the privacy of the video provider.

2) MALICIOUS VEHICLE ANALYSIS

In this system, the tags sent by vehicles will be scored by other vehicles according to the road conditions they broadcast. If there is a malicious vehicle or an attacked and compromised vehicle sending incorrect road condition tags, those tags will be rated more negatively than positively by other vehicles and be viewed as untrustworthy information. For example, if the information broadcast by vehicle V_m is continuously evaluated as untrustworthy over a period of time, RSU can send the SIM number of V_m to TA. If TA receives reports from multiple RSUs who identify the same vehicle as suspicious, the registration information of the vehicle will be reported to DMV. DMV finds the real identity of malicious vehicles in the database, and temporarily pulls them into the blacklist so that they cannot register in the vehicle network for a period of time. Serious cases will be reported to operators and relevant law enforcement agencies (police) for processing.

3) MALICIOUS SCORING

If a tag is scored maliciously, such as a credible tag being scored negatively or an untrustworthy tag being scored positively, it will not affect the broadcast credibility of specific road conditions in this system. During a period of time, there will be many cars broadcasting road conditions of the same section. And there will be many vehicles rating the reliability of the same road conditions. Therefore the scores given by a single vehicle has a slight effect on the reliability evaluation of the road conditions. If an attacker wants to disrupt the reliability of traffic broadcasting, he must get the majority of the ratings. Such a huge cost is obviously hard for attackers to achieve. Therefore, the credibility of tag scoring results can be guaranteed.

4) RSU BEING ATTACKED AND COMPROMISED

If an RSU is attacked, it will try to add inaccurate trust evaluation values to the blockchain during the miner election. But even if it wins the election by fraudulent means, other RSUs will deprive the fraudulent RSU of the right to add blocks on the blockchain after verifying the digital certificates. If an RSU maliciously broadcasts fake malicious vehicles to TA (that is, normal vehicles being broadcast as malicious vehicles), it will not be able to cause TA and DMV to penalize

the vehicles. Vehicles are considered untrustworthy only if they are reported by multiple RSUs in the meantime. Similarly, attackers cannot attack multiple RSUs at the same time because their resources are limited. Therefore legal vehicles will not be affected.

VI. CONCLUSION

In this paper, we propose a decentralized blockchain-based security framework for vehicular IoT environment in SDN-enabled 5G-VANETs. The blockchain is maintained by a P2P network formed by all active nodes in the vehicular system including OBUs, RSUs, and gNBs. The vehicles broadcast the real-time road situation messages to each other and the blockchain records the all the messages as well as the message sources. Exploiting the immutable feature of blockchain, the accountability of the source message is validated. We also implement a real-time video report service into this framework. The videos are encrypted and then uploaded to the cloud servers and can be used to check whether they match the related messages. With the support of the blockchain-based framework, we present the trust management for the vehicular system in case that malicious nodes may claim fake messages or messages may be tempered. Both theoretical analysis and experiment results illustrate the efficiency of our framework since the detection accuracy of the malicious nodes are significantly improved. The feasibility of large-scale deployment is well demonstrated by the evaluation on the overhead introduced by the video encryption and the transmission of both messages and videos.

REFERENCES

[1] R. A. Uzcategui, A. J. D. Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 126–133, May 2009.

[2] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: A survey," *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 148–157, May 2013.

[3] D. Soldani and A. Manzalini, "Horizon 2020 and beyond: On the 5G operating system for a true digital society," *IEEE Veh. Technol. Mag.*, vol. 10, no. 1, pp. 32–42, Mar. 2015.

[4] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 111–117, Jan. 2018.

[5] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.

[6] R. Zhang, Z. Zhong, J. Zhao, B. Li, and K. Wang, "Channel measurement and packet-level modeling for V2I spatial multiplexing uplinks using massive MIMO," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7831–7843, Mar. 2016.

[7] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani, "Overcoming the key challenges to establishing vehicular communication: Is SDN the answer?" *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 128–134, Jul. 2017.

[8] S. Sezer *et al.*, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, Jul. 2013.

[9] M. Jutila, "An adaptive edge router enabling Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1061–1069, Dec. 2016.

[10] K. Liu, J. K. Y. Ng, V. C. S. Lee, S. H. Son, and I. Stojmenovic, "Cooperative data scheduling in hybrid vehicular ad hoc networks: VANET as a software defined network," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1759–1773, Jun. 2016.

[11] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu, "TMED: A spider-Web-like transmission mechanism for emergency data in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8682–8694, Sep. 2018.

[12] C. Wu, Z. Liu, T. Yoshinaga, Y. Ji, and D. Zhang, "Spatial intelligence toward trustworthy vehicular IoT," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 22–27, Oct. 2018.

[13] M. Kim, J. Lim, H. Yu, K. Kim, Y. Kim, and S. Lee, "ViewMap: Sharing private in-vehicle dashcam videos," in *Proc. 14th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, 2017, pp. 163–176.

[14] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Oct. 2016.

[15] T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah, and B. Chen, "SIGMM: A novel machine learning algorithm for spammer identification in industrial mobile cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2349–2359, Apr. 2018.

[16] W. He, G. Yan, and L. D. Xu, "Developing vehicular data cloud services in the IoT environment," *IEEE Trans. Ind. Inform.*, vol. 10, no. 2, pp. 1587–1595, May 2014.

[17] T. Zhang, A. Chowdhery, P. Bahl, K. Jamieson, and S. Banerjee, "The design and implementation of a wireless video surveillance system," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, 2015, pp. 426–438.

[18] H. Qiu *et al.*, "Kestrel: Video analytics for augmented multi-camera vehicle tracking," in *Proc. IEEE/ACM 3rd Int. Conf. Internet-of-Things Design Implement. (IoTDI)*, Apr. 2018, pp. 48–59.

[19] T. Qiu, R. Qiao, and D. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, Jan. 2018.

[20] 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.

[21] R. Rivest, *The MD5 Message-Digest Algorithm*, document RFC 1321, 1992.

[22] A. Varga, "Using the OMNeT++ discrete event simulation system in education," *IEEE Trans. Educ.*, vol. 42, no. 4, p. 11, Nov. 1999.

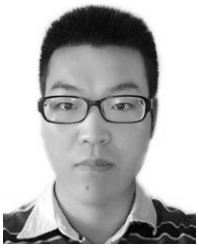
[23] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3–15, Jan. 2010.

[24] E. Tremel, "Real-world performance of cryptographic accumulators," M.S. thesis, Dept. Comput. Sci., Brown Univ., Providence, RI, USA, 2013.

LIXIA XIE received the M.S. degree in software engineering from Nankai University, Tianjin, China, in 2005. She is currently a Professor at the School of Computer Science and Technology, Civil Aviation University of China. Her main research interests include network and information security, and civil aviation information system analysis and design.

YING DING received the B.S. degree in software engineering from Northeast Normal University, Changchun, China, in 2017. She is currently pursuing the master's degree at the School of Computer Science and Technology, Civil Aviation University of China. Her main research interests include network and information security, and civil aviation information system analysis and design.

HONGYU YANG received the Ph.D. degree in computer science and technology from Tianjin University, Tianjin, China, in 2003. He is currently a Professor at the School of Computer Science and Technology, Civil Aviation University of China. His main research interests include network and information security, and civil aviation information system analysis and design.



XINMU WANG received the B.S. degree from Shandong University, Shandong, China, in 2015. He is currently pursuing the master's degree at the Department of Computer Science and Technology, Tsinghua University, Beijing, China. His main research interests include hybrid satellite terrestrial networks, mobile and wireless networks, and wireless multicast.