2019 IEEE 19th International Conference on Communication Technology

A Blockchain-Based Traffic Conditions and Driving Behaviors Warning Scheme in the Internet of Vehicles

He Bai† *, Cangshuai Wu† ‡, Yuexiang Yang, Geming Xia, Yue Jiang
College of Computer Science and Technology
National University of Defense Technology
Changsha, 410005, China
e-mail: *baihe0303@gmail.com, ‡wucangshuai17@nudt.edu.cn
† These authors contributed equally to this work.

***Abstract*—With the economic development, the number of cars is increasing, and the traffic accidents and congestion problems that follow will not be underestimated. The concept of the Internet of Vehicles is becoming popular, and demand for intelligent traffic is growing. In this paper, the warning scheme we proposed aims to solve the traffic problems. Using intelligent terminals, it is faster and more convenient to obtain driving behaviors and road condition information. The application of blockchain technology can spread information to other vehicles for sharing without third-party certification. Group signature-based authentication protocol guarantees privacy and security while ensuring identity traceability. In experiments and simulations, the recognition accuracy of driving behavior can reach up to 94.90%. The use of blockchain provides secure, distributed, and autonomous features for the solution. Compared with the traditional signature method, the group signature-based authentication time varies less with the increase of the number of vehicles, and the communication time is more stable.**

***Keywords*-warning scheme, Internet of Things, blockchain, group signature**

I. INTRODUCTION

With the rapid development of the information industry, in recent years, the application of the Internet of Things (IoT) has been emerging [1]. The IoT sets up a bridge not only between objects and goods but also between objects and people. As the application of the Internet of Things in the field of transportation, the core idea of the Internet of Vehicles is to integrate advanced sensing, data acquisition, network computing and intelligent planning technologies. Comprehensive awareness of vehicles and roads, and awareness control of each vehicle and every road, is an innovative application aimed at improving urban traffic efficiency and safety [2].

In China, the number of casualties caused by traffic accidents exceeds 120,000. This figure is 4-8 times that of developed countries [3]. The accident is mostly caused by the driving irregularity and the surrounding environment. According to research by scholar Miyaji M. [4], the human factor of traffic accidents reached 85%. Many insurance companies in the United States have found that [5], by installing surveillance cameras in cars, drivers are safer to drive in a supervised state. Therefore, effective supervision of the driver and early warning of the road becomes very necessary.

IoT solutions need to meet a variety of conditions, such as information channels, operating systems, information protocols, etc. The emergence of blockchain brings opportunities [6]. Bitcoin [7] was first proposed by Nakamoto in 2009, and many other forms of electronic cash have since been created with similar structures. At the same time, blockchain technology is also widely used in other fields such as the Internet of Things. Applying the blockchain technology to the early warning scheme can solve the problem of the security and distribution problems of the Internet of Vehicles.

At the same time, it is necessary to achieve a balance between privacy and traceability in this process. User related data may be lost or stolen due to poor access control and improper storage. Blockchain provides anonymity, but at the same time, we also need to be able to trace back to malicious nodes. The improved digital signature is a convenient and reliable solution for identity authentication. In the popularity of smartphones, it is possible for us to use the various sensors built in to detect and supervise driving behavior.

In this paper, we proposed a blockchain-based traffic conditions and driving behaviors warning scheme, aiming to achieve the following features:

(i) We obtain driving behavior information and road condition information through smart terminals.
(ii) We apply blockchain technology to provide security, protect information from tampering, and broadcast correct road conditions to other vehicle locations. Third party certification is not required unless in special circumstances.
(iii) A group signature strategy is proposed to optimize the blockchain asymmetric encryption and ensure traceability under privacy security.

The remainder of this paper is organized as follows. Section 2 discusses related works. The warning scheme design is described in Section 3. Section 4 shows the experimental simulation analysis. Section 5 gives the conclusion and the future work.

978-1-7281-0535-2/19/$31.00 ©2019 IEEE

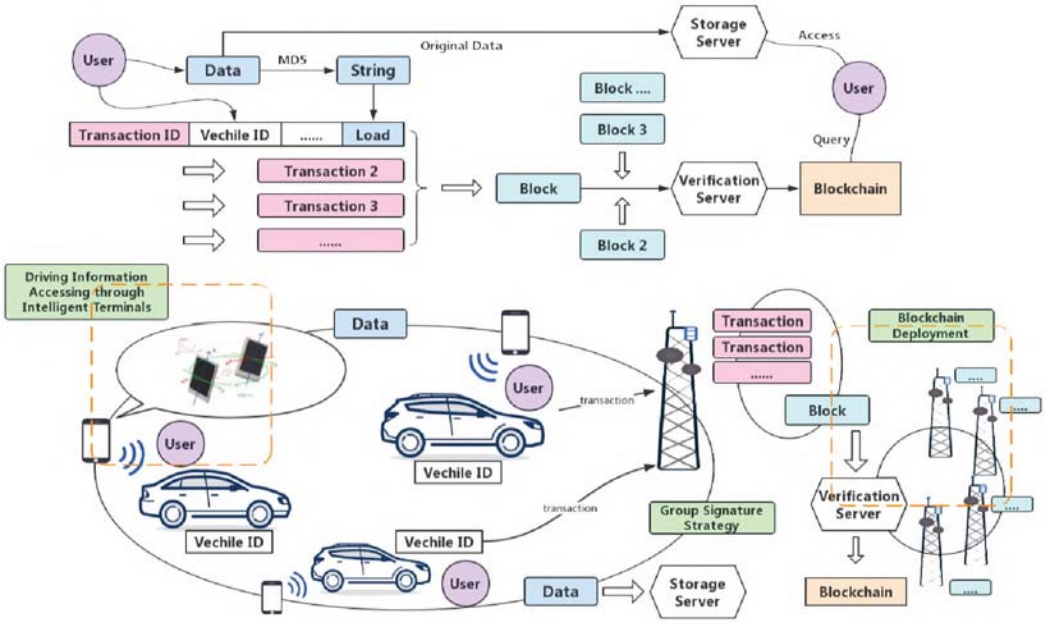

Fig. 1. The overall design of the warning scheme

II. Related Works

A. Vehicle Sensor Research and Warning Scheme Design

Driving information and behavior information are obtained mainly through on-board sensors, cameras, radars, and so on. Naturalistic Driving Study (NDS) proposed by The second Strategic Highway Research Program (SHRP 2) is one of the most famous projects to record and collect driving data [8], [9]. Meanwhile, Oliver et al. transform sensor and camera data into streams and use hidden Markov models to predict [10]. The research of [11] introduces an Advanced Driver Training System for security warnings for smart vehicles. These methods have high requirements for the vehicles used, so the usage rate and penetration rate are not satisfactory.

The built-in sensors are limited to promotion, and [12] proposes solutions for external sensors. Data acquisition is performed through the built-in gyroscope, accelerometer, magnetic sensor and GPS of the smartphone. Pimwadee et al. [13] enhances the accuracy and relevance of recognition.

B. Blockchain Applying in the IoT and Signature Encryption

Blockchain technology has been widely used in various fields by scholars at home and abroad, including the field of Internet of Things and cloud computing. The authors in [14] introduce four areas in the IoT that can be solved by applying blockchain technology. [15] describes the need for data exchange in combination with the IoT and blockchain and [16] describes the resolution of privacy issues. [17]–[19] propose the application of the reputation mechanism and the block management in the untrusted environment. And [20] lists the problems and prospects of the integration of blockchain and edge computing. The use of blockchain technology has achieved good results in many production environments.

The Internet of Vehicles improves the user's driving experience, but it also causes safety challenges for vehicle users. [21] proposed a privacy protection access control scheme for privacy issues in the Internet of Vehicles. Based on the storage space and computing power of current restricted devices, the authors in [22] reviewed the principle and implementation mechanism of lightweight passwords. The scheme of Zhao et al. [23] uses blind authentication technology to protect vehicle location privacy information. Digital signature is a convenient and reliable solution for identity authentication, but its signature length and computational complexity are often the main bottlenecks restricting its large-scale application in the Internet of Vehicles.

III. The Design of Warning Scheme

A. Overall Design

The overall design of the scheme is shown in Fig.1. It is divided into the following parts. The smart terminal collects data and performs identification and analysis. It then uploads traffic and driving information to the edge node. An edge node is a type of server node with a certain computing power that is widely deployed near the road. The data collected by each smart terminal is very helpful to each user and is packaged into a transaction in a unified format. The edge node processes each transaction. Based on the group signature-based identity authentication protocol, the edge node issues certificates and keys to communicates with users in the group and transmit traffic information. The edge node, while communicating with the user, packages the transactions into blocks and submits them to the verification server. After verification, the server adds the blocks submitted by many edge nodes to the blockchain. Edge nodes or users can query the blockchain to get the information

they need. Managers can also analyze and process urban traffic information through the chain.

B. Terminal data collection and analysis

The traditional method of vehicle data acquisition is to obtain the status information of the vehicle through the OBD (On-Board Diagnostics) system of the vehicle itself, and obtain the vehicle position data through the GPS sensor. The disadvantage is that the support of the relevant sensors is required, and large-scale promotion cannot be achieved. In this scheme, data collection is integrated into the smart terminal (such as a smartphone). The scheme uses the built-in acceleration sensor and gyro sensor of the smartphone to collect driving data. During the acquisition process, since the intelligent terminal and the vehicle remain relatively stationary, the motion state of the vehicle can be reflected by the motion state of the smartphone.

We selected a normal turn of the vehicle for 5 seconds and a sharp turn for 3 seconds. The acceleration and angular velocity changes obtained by the smartphone are shown in Fig.2. The x-axis and y-axis represent angular velocity and acceleration variations (y-axis) for different actions in duration (x-axis). It can be seen that the difference in values is sufficient to judge the characteristic of the driving actions. Similarly, we also intercepted a series of sample data such as deflection, vibration, and rapid acceleration.

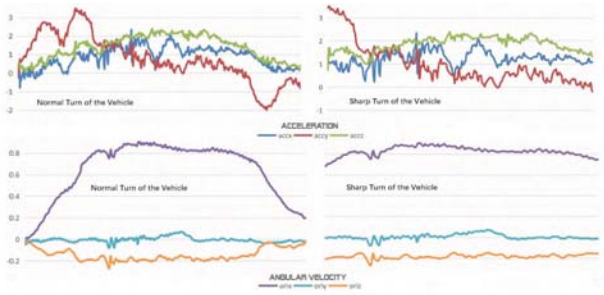

Fig. 2. The acceleration and angular velocity changes of the vehicle turns

It is worth noting that random, irregular noise may occur during actual driving, and these difficult-to-determine noises are likely to interfere with our identification work. Even though the vehicle is stationary, sensor data can still jitter. To this end, we chose a weighted moving average filter [24] to eliminate noise. After manually marking some of the data, the learning is performed by the support vector machine. Each time the data is collected, it is sent to the feature recognition module for endpoint detection and characteristic calculation to identify driving behaviors. We use different kernel functions and penalty factors to tune the parameters.

Increasing driving accidents are more likely to result from driver's irregular driving. However, when the driver's driving behavior is under supervision, their driving will be more cautious. The identification of driving events can help to supervise the entire driving process and provide early warning of dangerous driving behaviors.

C. Authentication Protocol Based on Group Signature

According to the characteristics of the Internet of Vehicles communication, a lightweight protocol was proposed for fast and efficient authentication. Group managers are usually served by an edge node within the group (the tower in the Fig.1). In the first phase, the manager creates a public-private key pair, broadcasting the public key and parameters to the vehicles in the range. In the second phase, the networked vehicle submits its authentication information to the manager through the blind signature. After certification, the manager issues a group certificate to the vehicle. In the third phase, the vehicle signs the status information through the certificate and the group public key, and communicates with the surrounding vehicles through the edge node. Anonymous information can only be interpreted by legal vehicles.

In the event of an accident or a malicious vehicle spreading false information, the manager can traverse and identify the vehicle through the private key reserved by the vehicle in the group signature. The characteristics of this scheme are as follows: The group members can be freely added without changing the group public key. Moreover, the signature length and the calculation amount of the verification opening algorithm are also irrelevant to the number of group members, so that the space-time overhead of the member in identity authentication can be greatly reduced.

D. Blockchain in the Warning Scheme

As shown in Figure 1, every traffic condition and driving data sent by vehicles in the network can be regarded as a transaction. Data is aggregated to the edge node to form a block, broadcasting within the group. Traffic information and driving behaviors are complex, but the format of transactions is relatively uniform, not all situations can be expressed through the transactions. Irregular raw data will be stored in the extra storage server and converted into an md5 code to be added to the transaction as a payload.

The core idea of blockchain design is to form a large distributed network through edge nodes. Each edge node is responsible for collecting and scheduling vehicle nodes in the area (including issuing keys, recording information, etc.). For the vehicles (users), they can obtain the required information by querying the blockchain. At the same time, they can also receive broadcast information provided by the current edge node as long as having a group signature. For regulators, it is convenient to trace vehicle data and road condition information due to the public and transparent nature of the blockchain. It is more conducive to them to analyze the data flow and make reasonable scheduling. For malicious nodes, false information is also easy to trace. Both edge nodes and regulators can find malicious nodes by traversing.

The consensus algorithm is one of the key points of the blockchain. For economic currency, PoW is a successful consensus algorithm but the huge resource consumption makes it unsuitable for application on the Internet of Vehicles environment. Both PoS and DAG are suitable for this scheme model. Besides, in our other article, we also specifically discuss the

analysis of consensus algorithms suitable for the combination of edge computing and blockchain, and propose a hybrid consensus to deal with this situation. Therefore, in this article, we will not discuss the advantages and disadvantages brought about by various consensuses.

The Internet of Vehicles is a network in which the road condition information is changing all the time. The information sent by the vehicle nodes at a certain time only indicates states at this moment. Therefore, the messages are time-sensitive and obsolete information persists in the edge nodes is a heavy burden. The transactions in the block have extra time attributes. As time passes, the value of the time attribute in the transaction will continue to decrease until it dies, unless similar information reappears. When most of the transactions in a block die out (to reach the threshold), the block dies. The traffic information represented in this block will no longer be time-sensitive. These dead data will be saved by storage servers instead of edge nodes.

Due to the time sensitivity of the network, delay is also a problem that cannot be ignored. TSN (Time Sensitive Network) may become a better solution at present. With the popularity of 5G technology, 5G applications will be more than 100 times faster than traditional 4G networks, and will lead the new mode of data transmission, providing a better solution for the delay of the Internet of Vehicles.

IV. Simulation and Experiment

A. Driving Behaviors Evaluation

In the experiment, the smart terminal used to collect data is the iPhone 7. The configuration of the data processing terminal is Ubuntu 16.04, i5 processor and 8 GB of memory. Data collection was performed on taxis and family cars. We recorded vehicle driving videos and manually labeled the driving events. The sample record selected a 15-minute video containing 97 driving events. The test data set selected a 30-minute driving video with a total of 157 driving events. By selecting different kernel functions and penalty factors, the accuracy of the identification is shown in Table 1.

TABLE I
The Accuracy Comparison of Different Penalty and Kernel

Penalty\Kernel	0	1	2	3
0.1	77.70%	39.39%	8.92%	0.63%
0.25	81.53%	43.95%	13.38%	5.73%
0.4	85.35%	58.60%	18.47%	8.92%
0.55	94.90%	70.70%	21.65%	12.10%
0.7	89.18%	68.15%	21.02%	11.46%

From this we can conclude that when it is a linear kernel function with the penalty factor (parameter c) between 0.55 and 0.7, it has the best recognition results. In the actual driving process, the judgment of driving behavior and road condition information will be more complicated. The experiments and simulations presented in this paper are only used for testing feasibility.

B. Authentication Protocol Performance

The authentication experiment was simulated by two PC of the same configuration with Ubuntu 16.04 and 8GB of memory. By simulating the scenario of cooperative communication between vehicles, one host is used to simulate the edge node and the other is to simulate a plurality of vehicle nodes. As shown in Fig. 3, under the group signature-based authentication protocol, although the consumption of authentication time increases as the number of vehicles increases, the overall change is small. The time for cooperative communication after authentication also tends to be stable. Because this scheme can freely increase group members without changing the group public key. Moreover, the length of the signature and the amount of computation of the verification open algorithm are also not related to the number of group members. Therefore, the space-time overhead of members in identity authentication can be greatly reduced. While meeting the time-sensitive communication of the Internet of Vehicles, it also protects the privacy of users.

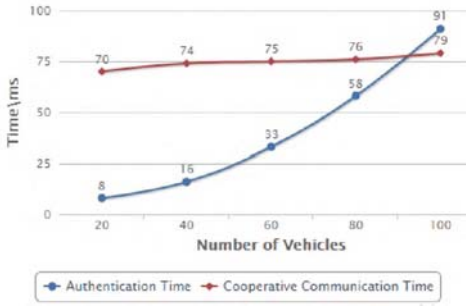

Fig. 3. The relationship between authentication time and number of vehicles

C. Blockchain Simulation Performance

The simulation of the blockchain is based on IBM-Watson-IoT. The client simulates a central server and a plurality of vehicle nodes, and the peer nodes are used to simulate edge nodes. Experiments show that applying the blockchain to the network can reach a consensus on a real road condition information, generate a transaction and package it into a block. Users can quickly obtain this information by means of broadcast or active query to achieve early warning.

The advantages of the blockchain are obvious. In this era of data explosion, the amount of data generated is constantly rising, and the amount of calculation is also increasing. Distributed systems can offer higher performance, faster computing speeds, and better price/performance comparing with the existing methods. The use of blockchain facilitates decentralized control of distributed systems and does not require trusted third parties to make rules. Data transparency and auditability allow a complete copy of each transaction executed in the system to be stored on each peer-to-peer node of the blockchain. The use of blockchain also guarantees the security and integrity of the Internet of Vehicles. The blockchain has the characteristics of non-tamperable data,

which can verify the transaction and solve the problem of vehicle data integrity. When the blockchain is maliciously manipulated, all block structures need to be changed. This change allows other nodes to know that the node has been tampered with by others and can be immediately detected.

V. Conclusions and Future Directions

The advantages of the scheme presented in this paper are lightweight, privacy protection and distributed. It is more convenient and free to obtain driving behavior information and road condition information through intelligent terminals than to modify vehicle modules. At the same time, the performance of intelligent terminals is increasingly strong, which is more suitable for future development. Privacy security protection is a part that cannot be ignored. The group signature-based authentication protocol protects privacy while being suitable for large-scale car networking applications and ensures traceability. The application of blockchain provides a better distributed choice. Public and transparent ledger is more conducive to the operation of the entire system.

In the future work, We will pay more attention to the safety considerations of the warning scheme. We plan to take advantage of Incentive mechanism to make the entire solution more self-organizing.

Acknowledgment

The work is supported in part by the National Natural Science Foundation of China (NSFC) under grants 61572026.

References

[1] Stergiou C, Psannis K E, Kim B G, et al. Secure integration of IoT and cloud computing[J]. Future Generation Computer Systems, 2018, 78: 964-975.

[2] Chen M, Tian Y, Fortino G, et al. Cognitive internet of vehicles[J]. Computer Communications, 2018, 120: 58-70.

[3] Zhang Z, He Q, Gao J, et al. A deep learning approach for detecting traffic accidents from social media data[J]. Transportation research part C: emerging technologies, 2018, 86: 580-596.

[4] Miyaji M, Danno M, Oguri K. Analysis of driver behavior based on traffic incidents for driver monitor systems[C]//2008 IEEE Intelligent Vehicles Symposium. IEEE, 2008: 930-935.

[5] How snapshot works[EB/OL].http://www.progressive.com/auto/snapshot-how-it-works/.

[6] Khan M A, Salah K. IoT security: Review, blockchain solutions, and open challenges[J]. Future Generation Computer Systems, 2018, 82: 395-411.

[7] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.

[8] Dingus T A, Klauer S G, Neale V L, et al. The 100-car naturalistic driving study. Phase 2: results of the 100-car field experiment[R]. United States. Department of Transportation. National Highway Traffic Safety Administration, 2006.

[9] Klauer S G, Dingus T A, Neale V L, et al. The impact of driver inattention on near-crash/crash risk: An analysis using the 100-car naturalistic driving study data[J]. 2006.

[10] Oliver N, Pentland A P. Graphical models for driver behavior recognition in a smartcar[C]//Proceedings of the IEEE Intelligent Vehicles Symposium 2000 (Cat. No. 00TH8511). IEEE, 2000: 7-12.

[11] Naik N, Jenkins P, Davies P, et al. Native web communication protocols and their effects on the performance of web services and systems[C]//2016 IEEE International Conference on Computer and Information Technology (CIT). IEEE, 2016: 219-225.

[12] Johnson D A, Trivedi M M. Driving style recognition using a smartphone as a sensor platform[C]//2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC). IEEE, 2011: 1609-1615.

[13] Chaovalit P, Saiprasert C, Pholprasit T. A method for driving event detection using SAX on smartphone sensors[Z]. IEEE, 2013450-455

[14] Kuzmin A. Blockchain-based structures for a secure and operate IoT[C]//2017 Internet of Things Business Models, Users, and Networks. IEEE, 2017: 1-7.

[15] Huang Z, Su X, Zhang Y, et al. A decentralized solution for IoT data trusted exchange based-on blockchain[C]//2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017: 1180-1184.

[16] Cha S C, Chen J F, Su C, et al. A blockchain connected gateway for BLE-based devices in the internet of things[J]. IEEE Access, 2018, 6: 24639-24649.

[17] Zhang Y, Wu S, Jin B, et al. A blockchain-based process provenance for cloud forensics[C]//2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017: 2470-2473.

[18] Yang C, Chen X, Xiang Y. Blockchain-based publicly verifiable data deletion scheme for cloud storage[J]. Journal of Network and Computer Applications, 2018, 103: 185-193.

[19] Xia Q I, Sifah E B, Asamoah K O, et al. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE Access, 2017, 5: 14757-14767.

[20] Yang R, Yu F R, Si P, et al. Integrated blockchain and edge computing systems: A survey, some research issues and challenges[J]. IEEE Communications Surveys Tutorials, 2019, 21(2): 1508-1532.

[21] Mei Y. Research on the Privacy Preservation for VANET[J]. Huazhong University, 2014.

[22] Yang W, Wan W, Chen Y, et al. Review on lightweight cryptography suitable for constrained devices[J]. Journal of Computer Applications, 2014, 34(7): 1871-1877.

[23] Zhao Z, Chen J, Zhang Y, et al. An Efficient Revocable Group Signature Scheme in Vehicular Ad Hoc Networks[J]. KSII Transactions on Internet Information Systems, 2015, 9(10).

[24] Zhuang Y, Chen L, Wang X S, et al. A weighted moving average-based approach for cleaning sensor data[C]//27th International Conference on Distributed Computing Systems (ICDCS'07). IEEE, 2007: 38-38.