A security architecture of VANET based on blockchain and mobile edge computing

XiaoDong Zhang
College of Computer Science
Inner Mongolia University
Hohhot, China
cszxd@imu.edu.cn

Ru Li*
College of Computer Science
Inner Mongolia University
Hohhot, China
csliru@imu.edu.cn

Bo Cui
College of Computer Science
Inner Mongolia University
Hohhot, China
cscb@imu.edu.cn

***Abstract*—The development of Vehicular Ad-hoc NETwork (VANET) has brought many conveniences to human beings, but also brings a very prominent security problem. The traditional solution to the security problem is based on centralized approach which requires a trusted central entity which exists a single point of failure problem. Moreover, there is no approach of technical level to ensure security of data. Therefore, this paper proposes a security architecture of VANET based on blockchain and mobile edge computing. The architecture includes three layers, namely perception layer, edge computing layer and service layer. The perception layer ensures the security of VANET data in the transmission process through the blockchain technology. The edge computing layer provides computing resources and edge cloud services to the perception layer. The service layer uses the combination of traditional cloud storage and blockchain to ensure the security of data.**

Keywords—blockchain, mobile edge computing, VANET, security

I. INTRODUCTION

The development of the VANET has brought many conveniences to human beings in safety and entertainment. However, security is the main concern, which includes the data security protection problem in transmission process, the security problem of VANET data stored in the data center, the access control and the privacy protection of the VANET data.

The traditional solution to the security problem is based on centralized approach which requires a trusted central entity. However, through a trusted central entity, there exists the single point of failure problem. Moreover, there is no approach of technical level to ensure security of data which is stored in trusted central entity, currently only through the legal means.

Blockchain is a distributed technology. It uses cryptography and hash functions to store data in a chain to ensure that data are tamper-resistant and traceable. And the technology uses a consensus protocol to ensure data consistency. Therefore, blockchain technology can be applied to the VANET environment to solve the security problem and remove the dependence on trusted central entities. However, the process of consensus has to solve the large computational problem which cannot be done on computing resources constrained vehicles.

As a new type of technology, Mobile Edge Computing (MEC) can be used not only to offload computationally intensive tasks from mobile devices to edge networks, but also to optimize processing before sending data to the core network, and to provide edge cloud services for mobile users at the edge.

Therefore, this paper proposes a security architecture of VANET which combines blockchain and MEC. It uses blockchain to ensure that data are tamper-resistant and traceable, and uses edge computing to solve the large computational problem of blockchain consensus process.

The rest of the paper is organized as follows. Section II introduces the current research on the combination of VANET, blockchain and edge computing, and analyzes the existing problems. Section III proposes the structure of this paper. Section IV discusses how the architecture guarantees the security of VANET. Section V summarizes the full paper.

II. RELATE WORK

Many studies have introduced blockchain technology to solve security problems in VANET. There are two main types of researches. One is combining the VANET with blockchain only, and the other is introducing concept of edge computing based on the combination of the VANET and blockchain.

In the researches of combining VANET with blockchain, most of them introduce the concept of blockchain, and do not make full use of the advantages of blockchain technology to ensure that data are tamper-resistant and traceable. In[1], the author proposed an authentication and secure data transfer algorithm based on blockchain. However, the vehicle needs to be registered in the centralized Registration Authority. In[1], there still exists a single point of failure problem. In[2], Madhusudan Singh proposed IV-TP to place the public key on the IV-TP which implemented by the blockchain. This paper only ensured the security of the public key without really guaranteeing the security of the VANET data. In[3], the author combined public key infrastructure (PKI) with vehicle and roadside unit (RSU) to form a blockchain network, which also ensured the security of public key.

In the researches of introducing MEC, Zehui Xiong introduced edge computing into architecture of the combination of VANET and blockchain [4], which used to solve the large computational problem in blockchain consensus process. However, they focused on the management of edge computing resources without considering the blockchain network instability problem caused by vehicle mobility.

This paper is supported by the Inner Mongolia Autonomous Region science and technology planning project (Cloud computing and Internet of Things based application technology development. No.201702019).

978-1-5386-4870-4/18/$31.00 ©2018 IEEE

III. Proposed Architecture

This paper proposes a security architecture of VANET based on blockchain and MEC. As shown in Figure 1, the architecture consists of three layers, namely perception layer, edge computing layer, and service layer. The perception layer comprises vehicle and RSU, together forming blockchain network. The edge computing layer provides computing resources and edge cloud services for the perception layer. The service layer includes cloud services and blockchain.

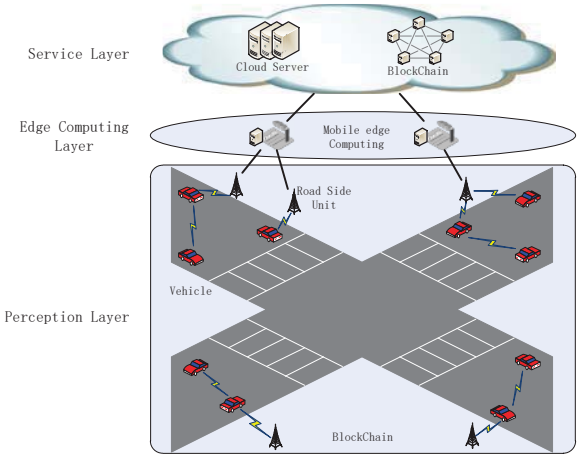

Fig. 1 Security architecture of VANET based on blockchain and MEC

A. Perceptual layer

Because of the constraint of computing resource and the mobility, the vehicle cannot perform all blockchain functions, including wallet (save address and private key), miner (mining), complete blockchain (save all blockchain data) , network routing (validate and propagate transaction block information, discover and maintain connections to peer nodes). In this paper, vehicle performs the functions of wallet and network routing.

The RSU connects each other by wired communication, forming stable blockchain network which can ensure a unique ledger in VANET. Therefore, all blockchain functions are performed on the RSU. Even while one vehicle is moving, it can communicate with RSU directly or through other vehicles.

B. Edge computing layer

There are lots of transactions occurred in VANET environment. If all the consensus work of the blockchain transaction is completed in RSU, it will inevitably affect the network performance and bring high delay. Therefore, This paper offloads the computational intensive work to MEC, and the result is returned to the RSU after completion. MEC is also responsible for handling other computational intensive work, such as video or image processing, etc.

C. Service layer

The VANET generates a lot of data. If putting all data on blockchain, it is not suitable. Because the blockchain is distributed storage, each blockchain node stores all the data, which consumes lots of resources. So, for data stored in the service layer, part of the data which are tamper-resistant and traceable, such as traffic accident data, traffic violation data, etc. , are stored using blockchain. The other part of data are stored on the cloud service.

IV. Discussion

This section focuses on how the architecture guarantees the security of VANET.

In this security architecture, vehicles and RSUs in the perception layer together form blockchain network to improve the security of VANET. However, in the VANET, the data generated by the VANET generally are stored in the cloud or a centralized platform so as to provide data support for other applications. Considering a large amount of data in the VANET, the perception layer does not have enough space to store. Therefore, in this security architecture, the VANET data are still stored in the cloud of the service layer, which does not violate the architecture of the VANET itself. In order to ensure the security of data in cloud, the data which are tamper-resistant and traceable are stored using blockchain. While, other data adopt the original storage method of the cloud, guaranteeing security by cloud computing architecture.

At the perception layer, the main challenge is security of data during transmission. So, blockchain in the perception layer is used to solve the security problem in the transmission process. And the data solving the security problem in transmission process need to be stored in perception layer blockchain. By combining MEC, the perception layer can ensure the security of VANET data in transmission process.

V. Conclusion

This paper proposes a security architecture of VANET based on blockchain and MEC. The architecture includes three layers, namely perception layer, edge computing layer and service layer. The perception layer ensures the security of VANET data in the transmission process through the blockchain. The edge computing layer provides computing resources and edge cloud services for the perception layer. The service layer uses the combination of traditional cloud storage and blockchain to ensure the security of data.

Acknowledgment

This paper is supported by the Inner Mongolia Autonomous Region science and technology planning project (Cloud computing and Internet of Things based application technology development. No.201702019).

References

[1] Arora A, Yadav S K. Block Chain Based Security Mechanism for Internet of Vehicles (IoV)[J]. 2018.

[2] Singh M, Kim S. Intelligent Vehicle-Trust Point: Reward based Intelligent Vehicle Communication using Blockchain[J]. arXiv preprint arXiv:1707.07442, 2017.

[3] Lasla N, Younis M, Znaidi W, et al. Efficient Distributed Admission and Revocation using Blockchain for Cooperative ITS[C]//New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on. IEEE, 2018: 1-5.

[4] Xiong Z, Zhang Y, Niyato D, et al. When mobile blockchain meets edge computing: challenges and applications[J]. arXiv preprint arXiv:1711.05938, 2017.