Introduce Reward–Based Intelligent Vehicles Communication Using Blockchain

Madhusudan Singh
Yonsei Institute of Convergence Technology,
Yonsei University,
Seoul, South Korea

Shiho Kim
Yonsei Institute of Convergence Technology,
Yonsei University,
Songdo South Korea

***Abstract*—The Intelligent vehicle (IV) is experiencing revolutionary growth in research and industry, but it still suffers from many security vulnerabilities. Traditional security methods are incapable to provide secure IV communication. The major issues in IV communication are trust, data accuracy and reliability of communication data in the communication channel. Blockchain technology works for the crypto currency, Bit-coin, which is recently used to build trust and reliability in peer-to-peer networks having similar topologies as IV Communication. In this paper, we introduce an Intelligent Vehicle-Trust Point (IV-TP) mechanism for IV communication among IVs using Blockchain technology. The IVs communicated data provides security and reliability using our proposed IV-TP. This IV-TP mechanism introduced in the paper provides trustworthiness for vehicles behavior, and vehicles legal and illegal action. The introduced reward-based system is an exchange of some IV-TP among IVs, during successful communication.**

Keywords-Blockchain, intelligent vehicles, security, component, vehicular cloud, ITS

I. Introduction

Current ITS system uses ad-hoc networks for Vehicle communication such as DSRC, WAVE, Cellular Network and Cloud Networks [1], which does not guarantee secure data transmission [2]. Currently, vehicle communication application security protocols are based on cellular and IT standard security mechanism which are not up-to-date and suitable for ITS applications. Still many researchers are working to provide standard security mechanism for ITS [3]. Our proposal is based on a very simple concept of using Blockchain based trust environment for data sharing among Intelligent Vehicles using the IV-TP (Intelligent Vehicle-Trust Point). We are exploiting the features of Blockchain i.e. distributed and open ledger, which is encrypted with Merkel tree and Hash function (SHA-256) and are based on Consensus Mechanism (Proof of Work Algorithm). We have not mentioned the details of the Blockchain mechanism for our application Intelligent Vehicle data sharing due to the limitation of space.

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00560, Development of a Blockchain based Secure Decentralized Trust network for intelligent vehicles)

A. Blockchain Technology

Blockchain technology is distributed, open ledger, saved by each node in the network, which is self-maintained by each node. It provides peer-to-peer network without the interference of the third party. The blockchain integrity is based on strong cryptography that validates and chain blocks together on transactions, making it nearly impossible to tamper with any individual transaction without being detected [4].

We propose the secure environment peer-to-peer communication between intelligent vehicles without interfering/disturbing other intelligent vehicles. We also evaluate our proposed mechanism with intersection road scenario based use case.

II. Introduction of Proposed Intelligent Vehicle-Trust Point: Reward-Based Intelligent Vehicles Communication using Blockchain

We propose a reward based intelligent vehicles communication using blockchain technology. Our proposed mechanism uses three basics technologies including communication network enabled connected device, Vehicular Cloud Computing (VCC) and blockchain technology (BT).

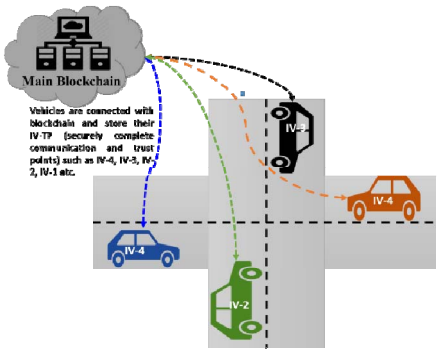

Fig. 1. Proposed blockchain Intelligent Vehicle Communication

A. Network enabled Connected device

It is an internet-enabled device, which can organize, communicate in VANET such as

Smartphone, PDA, Intelligent Vehicles, etc. [5].

B. Vehicular Cloud Computing

VCC is a hybrid technology that has a remarkable impact on traffic management and road safety by instantly using vehicle resources, such as computing, data storage, and internet decision-making [6].

C. Blockchain supported intelligent vehicles

Blockchain consists of a technically unlimited number of blocks which are chained together cryptographically in chronological order. In this, each block consists of transactions, which are the actual data to be stored in the chain.

III. VEHICLES -TRUST POINT GENERATION

We propose an Intelligent Vehicles-Trust Point (IV-TP) crypto unique ID that is issued by vehicle seller/authorized dealers. This IV-TP is developed by blockchain crypto mechanism and is similar to bitcoin. This IV-TP is issued to every intelligent vehicle. During communication, vehicles provide IV-TP to build trust in the communication network. The Vehicular networks having blockchain enabled service/user data providers, manages the IV-TP.

IV-TP is an encrypted unique number, which is uniquely issued to every IV and called as IV-TP ID. Every IV has its own IV-TP ID, generated by the authorized authority. The IV-TP is earned by calculating some computation in the group communication. Greater the IV-TP attained by an IV, higher will be its respect and honor. With the help of IV-TP, one can get the complete history of vehicles (accident history, condition of IV, crime history, etc.). The IV-TP access method is show in figure 2.

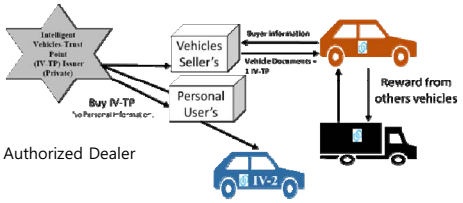

Fig. 2. IV-TP access methods

Blockchain technology based intelligent vehicles communicate with each other following the steps shown below: We have explained the process of IV-TP sharing and verification in figure 3.

A. Key generation

Firstly, each IV will generate its private and public key. The blockchain will maintain the public key of all IVs in network and when an IV want to communicate another IV then it will access the public key of another IV from the blockchain.

B. Digital Signature:

Secondly, each vehicle shall digitally sign the message to check integrity and non-repudiation of the message. With digitally signed message, receiver can easily find, that the message is not tampered, and the sender of the message is a valid IV in the network.

C. *Verification*

Lastly, the receiver after receiving message identifies the sender by verifying the digitally signed encrypted message. After verification, receiver decrypts the message with the public key of sender.

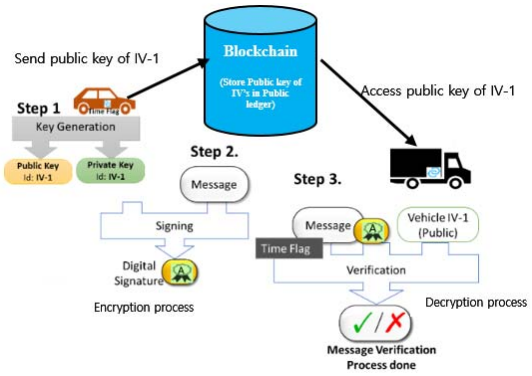

Fig. 3. Message process between two IV

Consensus Protocols

Broadcasted message will be validated only after verification by more than 50% of the network vehicles. This validation process is based on Proof of Driving (PoD) algorithm. PoD provides evidence that the vehicles are legal and are running in the same network shared by the approved vehicles at the communication time. All vehicles communication data will be managed on the vehicular cloud with the IV-TP ID. If in future, IV owners want to sell or change their IVs, then they can access their complete data history via the vehicular cloud.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00560, Development of a Blockchain based Secure Decentralized Trust network for intelligent vehicles)

REFERENCES

1. G. Yan and S. Olariu, "A probabilistic analysis of link duration in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1227–1236, Dec. 2011.
2. Singh, Irish, et al. "A novel privacy and security framework for the cloud network services," *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, IEEE, 2015, pp.301-305.
3. S. Olariu, M. Eltoweissy, and M. Younis, "Toward autonomous vehicular clouds," *ICST Trans. Mobile Commun. Comput.*, vol. 11, no. 7–9, pp. 1–11, Jul.–Sep. 2011.
4. Satoshi Nakomoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG 3 (2009).
5. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. IEEE INFOCOM*, San Diego, CA, 2010, pp. 1–9.
6. M. Singh, D. Singh, and A. Jara, "Secure cloud networks for connected & automated vehicles," *2015 International Conference on Connected Vehicles and Expo (ICCVE)*, Shenzhen, 2015, pp. 330-335. doi: 10.1109/ICCVE.2015.94