DPKI Based Secure Communication Scheme For Self-driving Vehicle Networking*

Cao Yuan
Harbin Institute of Technology, Shenzhen
tsaoyuan@foxmail.com

Cao Li
Southern University of Science and Technology
12212752@mail.sustech.edu.cn

Hu Haojun
Harbin Institute of Technology, Shenzhen
hhj29132002@gmail.com

Hou Beijie
Shanghai Jiao Tong University
houbeijie@sjtu.edu.cn

Yang Jinqi
Xi'an Jiaotong University
jqyangxjtu@foxmail.com

ABSTRACT

This paper provides a design of the authentication and communication mechanism for futuristic self-driving vehicles, which based on DPKI and blockchain techniques.

To avoid long winded certificates and hierarchical certification bodies in traditional PKI framework[1], we implement a decentralized PKI (DPKI) in vehicular authentication and communication networks to enhance security and ensure reliable, rapid identity verification, aligning with the dynamic needs of future smart transportation systems[2].

In the DPKI framework we have designed, individual information is decentralized and recorded as Distributed Identifiers (DIDs) on a blockchain. Department of Motor Vehicles(DMV) is the only institution with the right to write information about vehicles into the corresponding block of the blockchain so as to facilitate the subsequent query of identity authentication.

In order to resolve communication challenges in vehicular networks which similar to the "two generals problem" and fully utilize the road infrastructure in future smart cities, we endow Road Side Units (RSUs) with multiple functions, including identity authentication, convoy assignment, and providing robust communication security in dynamic vehicular environments. After RSU distributes group session key to the convoy, vehicles in the convoy can use this key and team members' public keys for encrypted communication.

Keywords

Self-driving vehicles, Authentication, DKPI, Blockchain

*Paper from project of DOTA course, NUS SOC Summer Workshop 2024

1. INTRODUCTION

In recent years, with the rapid development of intelligent driving technology, self-driving vehicles have gradually entered the public eye.

Nowadays the successful deployment of the "Robot" self-driving vehicles called "Apollo Go" in Wuhan, China has become a significant milestone in the application of vehicular networks technology. Vehicular networks (V2X) facilitate the interconnection and communication between vehicles (V2V), vehicles and infrastructure (V2I), vehicles and networks (V2N), and vehicles and pedestrians (V2P), providing strong support for autonomous driving and intelligent transportation systems.

In actual traffic environments, the importance of information synchronization is particularly prominent. Take the phenomenon of phantom traffic jams, for instance. Phantom traffic jams refer to sudden traffic congestion that occurs without any apparent obstacle, caused mainly by abrupt deceleration or braking of vehicles, leading to a chain reaction of congestion. The occurrence of such phenomena is largely due to the lack of real-time information sharing and synchronization between vehicles. If each vehicle could promptly obtain the driving information of the vehicle in front, the probability of phantom traffic jams would be significantly reduced.

Another typical example is the green light start issue. When a traffic light turns green, usually the first vehicle starts, followed by the subsequent vehicles, resulting in lower overall traffic efficiency. If information synchronization among vehicles could be achieved through vehicular networks, all waiting vehicles could receive the green light signal simultaneously and start at the same time, thus greatly improving intersection traffic efficiency.

Therefore, the significance of vehicular networks technology lies not only in enhancing the intelligence of individual vehicles but also in optimizing the entire traffic system through information synchronization. This technology can not only reduce traffic congestion and improve road traffic efficiency but also effectively lower the accident rate, enhance driving safety, and provide a solid foundation for building intelligent

urban transportation systems.

2. BACKGROUND

In this section, we are going to introduce the key technologies used in our design, including blockchain, DPKI, and vehicle-to-vehicle symmetric session key establishment.

2.1 Blockchain Technology

Blockchain technology originated from Bitcoin as the underlying technology for which trust between multiple participants is established in a decentralized manner. The essence of blockchain is a decentralized distributed ledger database maintained by a peer-to-peer network (P2P). With the help of distributed storage technology, P2P network, consensus algorithm, chained data structure, digital signature, encryption algorithm and other cryptographic techniques to achieve the purpose of decentralization, non-tampering, anonymity, traceability and so on. As an innovative technology, blockchain has been rapidly developed and applied in various industries, with results such as Ether in the public chain, central bank digital currencies, Linux Foundation-supported Hyperledger, and so on.

The system model of blockchain technology can be roughly divided into six layers from top to bottom: application layer, contract layer, incentive layer, consensus layer, network layer, and data layer, as shown in Figure 1:

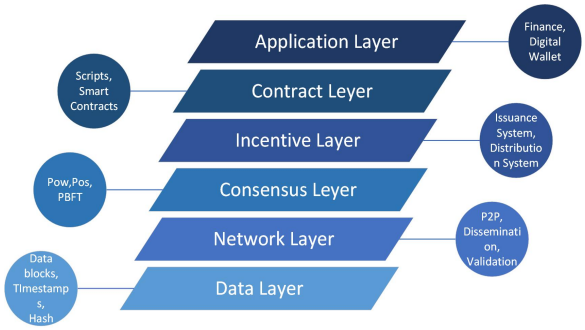

Figure 1: Blockchain Architecture

1. Application Layer: The application layer of the blockchain encapsulates various application scenarios and cases to provide users with various services and applications such as Finance and Digital Wallet.

2. Contract Leyer: The contract layer is responsible for encapsulating various programmable scripts, algorithms, and smart contracts to enable deterministic and automated execution of instructions. For example, a smart contract is a piece of code that is stored, verified, and executed on the blockchain so that it can be automatically executed without a third party if a defined constraint is met. By replacing humans with programmed algorithms to arbitrate and enforce contracts, this will save us huge costs of trust.

3. Incentive Layer: The incentive layer consists of a system for issuing and distributing economic incentives, which aims to provide certain incentives for network nodes to participate in the security verification of the blockchain, such as mining in Bitcoin.

4. Consensus Leyer: The use of consensus algorithms and consensus mechanisms to allow highly decentralized network nodes to reach a consensus in the blockchain network and decide which node can add a new block to the main chain is one of the core technologies of the blockchain.

5. Network Layer: The network layer mainly realizes the mechanism of distributed network through P2P technology, the network layer includes P2P networking mechanism, data dissemination mechanism and data verification mechanism. Due to P2P characteristics, when data is transmitted between nodes, even if some nodes or networks are destroyed, it will not affect the transmission of other parts.

6. Data Layer: The data layer mainly describes the physical form of the blockchain, which is the chain structure on the blockchain starting from the genesis block, and contains the block data, chain structure of the blockchain, as well as the random numbers, timestamps, public keys, private key data on the block, etc. It is the lowest data structure in the whole blockchain technology.

2.2 Decentralized PKI (DPKI)

DPKI represents an advancement and refinement of the traditional PKI framework. Current centralized PKIs suffer from an over-reliance on trusted central authorities (CAs), which undermines the autonomy of users in managing their identities. This centralized model introduces critical vulnerabilities, notably the susceptibility to single points of failure through erroneous certificate issuance by third parties, and susceptibility to Man-in-the-Middle (MITM) attacks, where deceptive CAs can falsely gain trust. Furthermore, the emergence of quantum computing has compromised the security of widely used cryptographic algorithms such as RSA and ECC, making them increasingly unreliable.

Given these concerns, the implementation of a decentralized PKI (DPKI) is crucial in vehicular communication networks to enhance security and ensure reliable, rapid identity verification, aligning with the dynamic needs of future smart transportation systems.

In the DPKI framework we have designed, individual information is decentralized and recorded as Distributed Identifiers (DIDs) on a blockchain. This setup allows users to independently manage and modify the content displayed within their own DIDs.

Third-party entities, such as roadway infrastructure or vehicle management organizations, can authenticate specific segments of a user's DID and log this information into their respective blocks. Under this system, the disclosure of all information is controlled by the individual, thus ensuring the privacy and security of vehicular data. Additionally, since third-party entities are responsible only for authenticating segments of data, the risk of a single point of failure is mitigated.

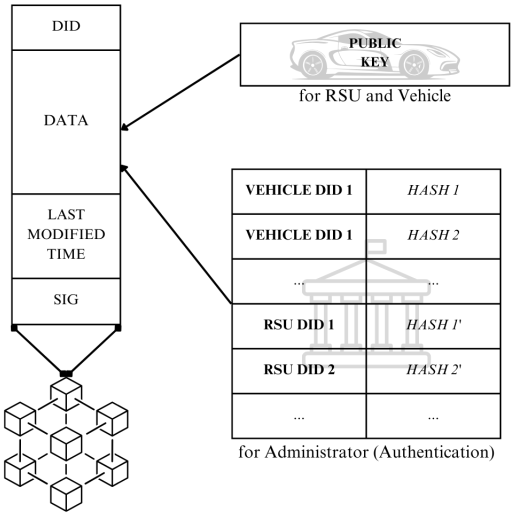

Figure 2: DID Format

Furthermore, the decentralized storage of all user blockchain data in roadside infrastructure devices makes Man-in-the-Middle (MITM) attacks impractical. Figure 2 shows the system architecture diagram of the format used for storing data on the blockchain.

2.3 Authentication and Key Establishment

In the context of vehicle-to-vehicle(V2V) communication, authentication and key establishment are two critical aspects for safeguarding the communication process against malicious adversaries. Authentication involves verifying whether the identities of the communicating parties are legitimate, serving as a prerequisite for secure communication and laying the groundwork for the establishment of session keys. Key establishment occurs after mutual authentication, where entities generate a symmetric encryption key through certain methods. By using the established key, the communication content is encrypted for transmission. Compared to asymmetric key communication, using symmetric session keys for communication is undoubtedly more efficient.

3. DESIGN

Our proposed design for solving phantom traffic jams incorporates several key components that collectively enhance communication, authentication, and synchronization within vehicular networks. This design addresses the "Two Generals' Problem" in vehicular communication by utilizing RSUs to ensure reliable message transmission, thus preventing infinite confirmation loops and enhancing overall system integrity and efficiency. The detailed design covers identity authentication, group assignment, secure communication, and the protocols for adding and exiting group members, providing a robust framework for dynamic vehicular environments,as shown in Figure 3.

3.1 Architecture Components

In our proposed design for solving the phantom traffic jam and enhancing the traffic flow, there are several important elements that form the framework of the whole program. The following is a detailed description of these elements:

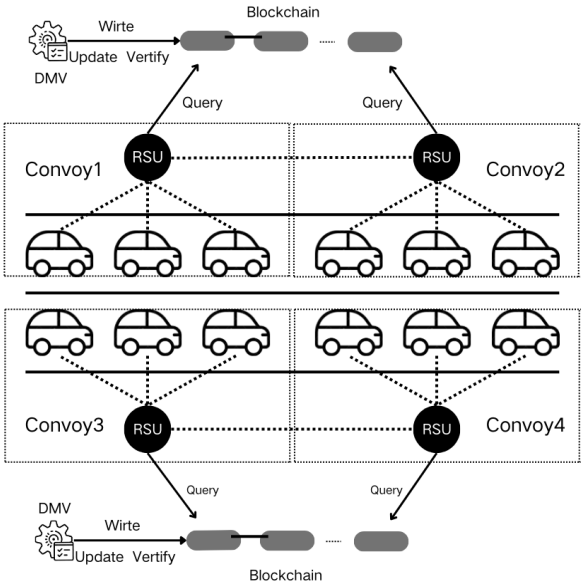

Figure 3: Scene Design

1. Vehicle: The vehicle is the basic unit of communication, authentication and information synchronization for the entire traffic and is the most important entity in our design solution. Vehicles are equipped with OBU (On board Unit) which is used to communicate with RSU (Road Side Unit) and other vehicles. The database inside the vehicle stores a large amount of information, such as the DID of the vehicle itself, relevant information about the vehicle, a table of information about the vehicles of the same group of teammates, and its own public and private keys. In addition, the vehicle has its own decision-making system for processing and acting on the information it receives. Since the decision-making and scheduling issues are out of the scope of our design discussion, we assume that the vehicle's decision-making system is absolutely secure and will not be damaged or receive attacks.

2. RSU(Road Side Unit): The road test units are distributed around the road and are set up at regular intervals.The RSUs will communicate with the vehicle wirelessly for authentication and grouping of the vehicle. At the same time, RSUs will also communicate with each other through wired communication for message delivery and synchronization between different groups. Since RSUs are set up by the government, it is assumed that RSUs are unattackable and communication with RSUs is absolutely trustworthy.

3. DMV(Department of Motor Vehicles): Each vehicle has to register the unique DID and related information of the vehicle in the corresponding DMV before leaving the factory, and the DMV will write the DID and the hashed related information into the corresponding block of the blockchain so as to facilitate the subsequent query of identity authentication. At the same time, each vehicle has to undergo annual inspection within the prescribed annual inspection cycle, and after passing the annual inspection, provide proof to the DMV, which will verify the vehicle information on the blockchain. If a vehicle fails the annual inspection or is not inspected in a timely manner, the DMV will periodically delete the information of the corresponding vehicle. In our design, we assume that the DMV is absolutely trustworthy and the information it writes is absolutely true and will not be tampered with.

3.2 Two Generals' Problem: the reason for RSU

Imagine a scenario where two armies are stationed at the north and south foot of a mountain, planning to attack an enemy force positioned on the mountain. Since neither army can breach the enemy's defenses independently, they decide to synchronize their attack. To coordinate, General A sends a messenger to convey the agreed-upon time of attack to General B. However, due to the presence of enemy ambushes along the route, it remains uncertain whether B has received the message. If General B does receive the message, he must then confirm receipt back to General A. Yet, this introduces a new uncertainty—General B does not know if his confirmation has reached General A, necessitating a return confirmation from A. This recursive process of confirming receipt could theoretically extend indefinitely, as the last general to send a message cannot be sure it was received.

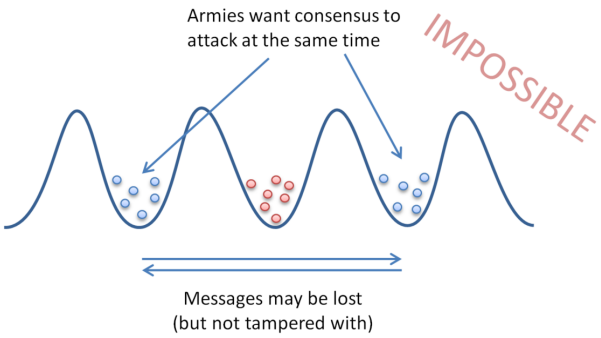

Figure 4: Two Generals's Problem

Similarly, communication within a fleet of vehicles encounters analogous challenges. Assuming that the communication channels between vehicles are unreliable, the scenario of perpetual confirmations arises during the synchronization process. To address this, we introduce the use of Road Side Units (RSUs). RSUs, capable of transmitting signals at higher power or making targeted optimizations for signal reception and transmission, effectively render communication between the RSU and vehicles as highly reliable. This transformation allows us to convert an unreliable communication channel into two reliable ones, thereby providing an engineering solution to the classic "two generals problem."

The deployment of Road Side Units (RSUs) effectively resolves the communication challenges in vehicular networks, similar to the "two generals problem." As reliable intermediaries, RSUs enhance the integrity and efficiency of vehicle-to-vehicle and vehicle-to-infrastructure communications by preventing infinite confirmation loops. Consequently, a critical function of RSUs is to provide robust communication security in dynamic vehicular environments.

3.3 Detailed Design

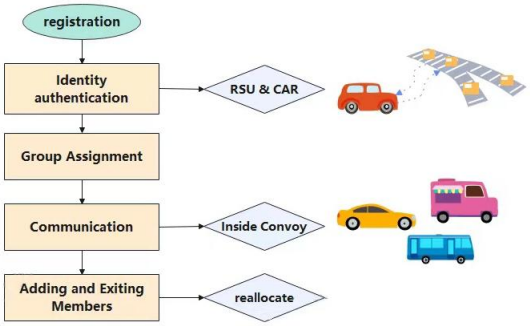

Figure 5: Design

3.3.1 Identity Authentication

This stage contains mutual authentication between vehicles and RSUs. Suppose vehicles have finished registration. In the authentication stage, vehicles first verify RSUs' identity by checking its signature in broadcast messages. Once verified, vehicle send a group assignment request and using vehicle's private key to generate a signature.

For each vehicle's request, RSU first search the blockchain trying to find a block recording this vehicle's identity. Once found, compute the Hash value of vehicle's public key and compare with value in the block. If consistent, authentication passed.

RSU performs batch verification on a set of request messages with signatures to complete the identity authentication of a group of vehicles.

3.3.2 Group Assignment

In this stage, RSU computes and sends group session key to vehicles assigned in the same group. RSU first uses all the DIDs of one group and a random number seed to generate a group session key for this group[3]:

$$K_{Group} = F\{DIDs, seed\}$$

Then in the key-distribution stage, RSU encrypts the session key with vehicles' public keys and sends to corresponding cars respectively. When vehicles receive message, they decrypt it with private key to obtain group session key. Meanwhile, RSU tells every vehicle some information about their teammates.

Vehicles with the same group session key belong to a common group. This process can be analogized to WeChat's face-to-face Group building, where the session key is the same number chosen.

3.3.3 *Communication*

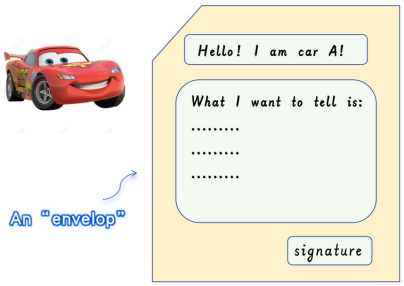

Figure 6: An Analog Of Message Envelop

If car A wants to communicate with car B in the same convoy, let's say, message is m. A should give a digital signature to this message. The specific way is to compute the digest of m using Hash function, then encrypt the digest with A's private key. A then encapsulates who it is, message m, and A's signature in an "envelop" and encrypts the "envelop" using group session key. After that, A send this whole "envelop" to car B. An analog of message envelop is like Figure 6. The specific encryption process is shown in Figure 7.

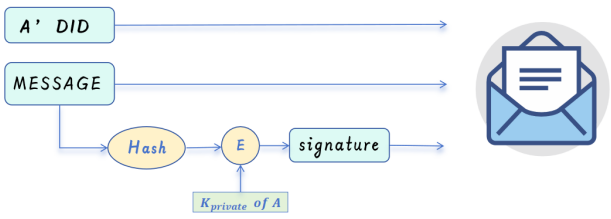

Figure 7: Composition Of The Envelope

When car B receive this envelop, B first decrypts it with session key, then B will get A's "name", message, followed by A's signature. B can verify message source by decrypt signature with A's public key and compare the results with the hash value of message.

3.3.4 *Adding and Exiting Members*

Before a car gets on the road, it needs to search the nearby RSU. In detail, the new car broadcast a request to check whether there are RSU nearby.After verification the new car's identity, every RSU that receives the message responds to it. The reply message contains its group number and other necessary information. If the car receive more than one responses,it will choose the first one as it is either the closest or the fastest. The car then send a new request to the chosen RSU, telling that it want to get a group identity.

The RSU reply with group identity for the new car,using which the new car can communicate with other cars in the same group, along with a list of other cars information in this group.The RSU also send a notification message to all the cars in this group except the new car, which contains information of the new car. After receiving this message, other car add the new car's information to its member list. As shown in the Figure 8, after the 4-way handshake, the new car will formally join a group.And the RSU will begin to server for this car.

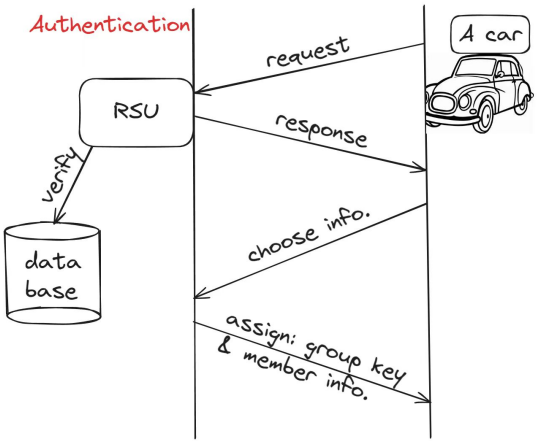

Figure 8: Adding Members Handshake

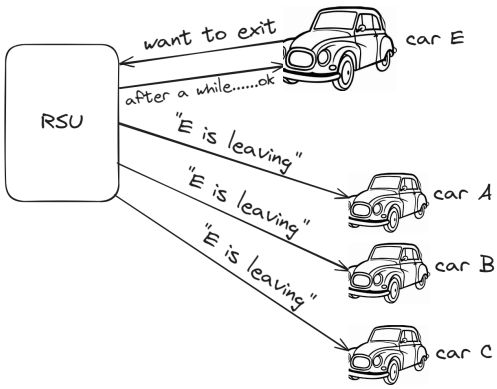

Figure 9: RSU Response When Vehicle Exits

Leaving the convoy is a bit more complicated.

In general, since the RSU has fixed position, the position shift of the vehicle may trigger the exit and re-entry. Since the vehicle needs to maintain communication with the RSU while driving all the time, leaving the convoy triggers a handover process.

Each RSU has a area called marginal region. Just like its name, marginal region is the area relatively far away from RSU center, but also under the control of RSU. Two RSU can have overlapping marginal region. When car enters the marginal region, it is probably going to leave the convoy. Firstly, the car sends a message to RSU expressing it wants to leave and its original RSU finds the next RSU that may provide service based on the direction it is traveling. The

original RSU sends a message to new RSU, info it that a new car will enter it's area.

At the meanwhile, RSU sends the leaving car information to new RSU. The leaving car starts a 2-way handshake,same as the last two steps of 4-way handshake above. When the new RSU accepts the vehicle, it notifies the original RSU.

The original RSU then delete the info of that vehicle,and send member-exit message to all its existing members. Existing members simply delete its relative info and will be unable to communicate to that car directly.

Eventually, the car officially dropped out of the group that it was previously in.

4. CONCLUSIONS

In this paper we propose a secure communication scheme for self-driving vehicle Networking. The integration of Decentralized Public Key Infrastructure (DPKI) and blockchain technology presents a groundbreaking approach to addressing the authentication and communication challenges inherent in the realm of self-driving vehicles. This shift towards decentralization not only streamlines the authentication process but also significantly enhances the security and reliability of vehicular communication networks, thereby meeting the dynamic demands of future smart transportation ecosystems.

Within our proposed DPKI framework, the utilization of Distributed Identifiers (DIDs) recorded on a blockchain ensures a decentralized storage of individual vehicle information. This innovative approach empowers entities such as the Department of Motor Vehicles (DMV) with the capability to record pertinent vehicle details directly onto the blockchain, facilitating efficient identity verification processes.

Furthermore, our design addresses the communication challenges akin to the "two generals problem" in vehicular networks by equipping Roadside Units (RSUs) with advanced functionalities. This strategic enhancement not only optimizes the utilization of road infrastructure in smart cities but also paves the way for seamless and secure vehicular communication, marking a significant advancement towards the realization of efficient and safe autonomous transportation systems.

5. REFERENCES

[1] Qingsen Zhu, Research on Security Authentication in UAV Ad Hoc Networks, pages 2-3, April 2023.

[2] Christopher Allen, Arthur Brock,Vitalik Buterin,Jon Callas,Duke Dorje,Christian Lundkvist,Pavel Kravchenko,Jude Nelson,Drummond Reed, Markus Sabadello,Greg Slepak, Noah Thorp,and Harlan T Wood, Decentralized Public Key Infrastructure, A White Paper from Rebooting the Web of Trust, pages 7-9, 2015.

[3] Zhiwang He,Blockchain-based Internet of Vehicles Authentication Scheme, pages 24-34, April 2023.