ARN- for Privacy-Preserving Authentication Scheme for VANETs using Blockchain

Mr. K.Manivannan
Head of Department(IT) ,
Department of Information Technology,
V.S.B Engineering College,
Karur, Tamilnadu, India

Ms. T.Gowerthini,
Department of Information Technology,
V.S.B Engineering College,
Karur, Tamilnadu, India

Ms. K.Vaishnavi,
Department of Information Technology,
V.S.B Engineering College,
Karur, Tamilnadu, India

Ms. R.Suvalakshmi,
Department of Information Technology,
V.S.B Engineering College,
Karur, Tamilnadu, India

***Abstract*— Vehicle ad-hoc network (VANETs) in smart vehicle communication and intelligent transportation system one of the most promising applications. However, user authentication and encryption still has two major problems VANETs. The key is to prevent the vehicle from inside the fake news broadcast, while maintaining the privacy of vehicle tracking attacks. In addition, in the traditional model, the transaction does not provide a distributed data storage and dispersion of law and order, so that a third party may initiate dishonesty. Dispersed between the vehicle system architecture of intelligent vehicle safety Internet communications access authentication scheme between block chain based technology, we propose a traceable, and through the use of vehicles and roadside units (RSUs). In one aspect, the program allows the vehicle to the vehicle using false cars (V2V) and vehicle-to-infrastructure (V2I) communication in a non-anonymous fully trusted environment. On the other hand, transparency of the vehicle authentication and published by the preform efficiently block chain technology. In addition, the transaction information is tamper-resistant, it provides a different cloud servers distributed and decentralized nature. Finally, the theoretical analysis and simulation, we plan to build secure and decentralized VANETs system framework, accountability and privacy protection. VANET their discussion on technical and security challenges. We discussed possible attacks against these attacks can achieve some key programs. We use different parameters to compare solutions. Finally, we have discussed the mechanism used in the solution.**

Keywords—Blockchain, VANETs, Authentication.

I. INTRODUCTION

A Now the absolute number of day, road traffic will affect the safety and efficiency of traffic environment. About 120 people have been killed in road accidents every year. With the rapid development of urbanization, the wisdom of the city has caused widespread concern academia and industry. It is estimated that the number of cars around the world will reach 20 billion in the next 10-20 years. Road traffic Security has been a challenging traffic management issues. One possible way is to provide Vehicle traffic information so that they can use to analyze traffic environment. It can be achieved through the exchange of information between vehicle traffic environments. All vehicles moving in nature, requiring a mobile network, it can self-organize and not be able to support the work of the infrastructure. With the progress in microelectronics, it is possible to integrate the device into a single network node and the wireless unit and the interconnect, i.e. ad hoc network. In addition, the network is becoming a mobile ad hoc network.

The VANETs system comprises four main components, i.e., the Trusted Authorities (TAs), the Application Servers (ASs), the Roadside Units (RSUs), and the vehicles, which is equipped with Onboard Units (OBUs). The responsibility of TAs is to maintain the whole system. The work of ASs is to provide a further data analysis. The RSUs are along the roadside deployment, which serve as transfer stations or carry out the authentication works to lighten the burden of the TAs. The OBUs are embedded in the vehicles to collect and process the traffic-related information and communicate with other entities. Appears on-board self-organizing network (VANETs) has brought great convenience, and for people comfortable driving experience. Two types of communication, that –Vehicle-to-infrastructure (V2I) and vehicle-to-vehicle communication (V2V) communication is established VANETs promote cooperation and sharing between automotive short-range communications via Dedicated Short Range Communications (DSRC) radio.

Fig. 1. Intelligent Vehicles Information Environment

In V2I communication, the vehicles communicate directly with the RSUs fixed on the roadside. The vehicles

communicate directly with each other to exchange information in V2V communication. The vehicles (OBUs) communicate with the RUSs and other vehicles via a public wireless channel. Through the wired channel, the RSUs also connect with TAs and ASs. In VANETs, utilizing Dedicated Short Range Communications (DSRC) standard, each vehicle periodically broadcasts the vehicle-related condition messages (e.g., speed, turning intention, direction, and position) and traffic-related safety messages (e.g., congestion state, traffic events, and weather) every 100–300 milliseconds (ms). On one side, all the messages are forwarded to the traffic control center (AS) by the RSUs through a wired connection. Based on the received messages, the management strategy and optimized control can be generated by the traffic control center to improve efficiency and traffic safety through analyzing the current traffic load at each intersection. On the other side, an early response can be made by vehicles under specific situations such as emergent braking, traffic jams, accidents, etc. The appearing of VANETs stems from enhancing the safe driving conditions and road safety. As the traffic-related messages are transmitted in the wireless channel, the malicious attackers can easily eavesdrop, modify, replay, and delete the messages.

II. MOTIVATION

Blockchain is a database used for storage in a decentralized network. However, Blockchain is not only used in financial applications. Moreover, we can design a transaction to match our application.

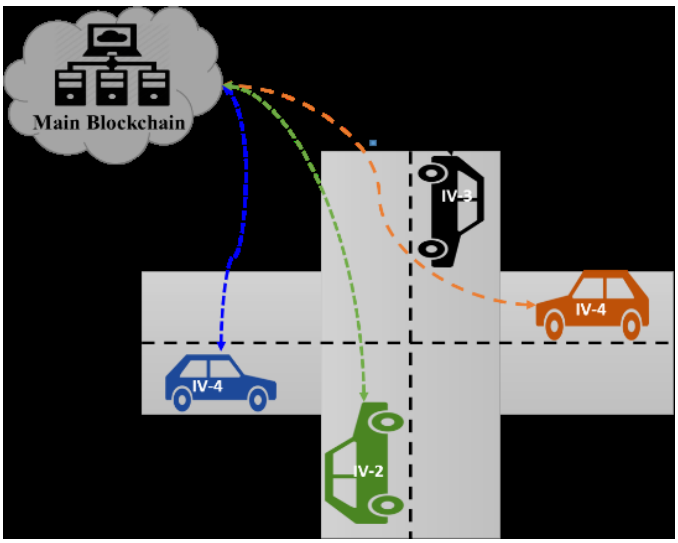

Fig. 2. Proposed blockchain Intelligent Vehicle Communication

A. Technical Terms

First, it is important to clarify the meaning of several technical terms relating to Blockchain. Table I provides a list of these terms and their meaning.

Term Description	Term Description
Decentralized	The system that stores data across the network.
Transparent	Everyone in the node and can see the ledger that share amount decentralized network.
Miner	Transaction verifier
Consensus	A v method used to verify the transaction.
Forks	The problem that arises when the node is used for different version of Blockchain.
Hash	One-way hash function to check the integrity of a transaction or message.
Node	The ledger in the Blockchain system.
Timestamp	A date and time in the computer system used as an electronic time stamp for the transaction.

TABLE 1. Technical Terms

B. Characteristics of VANET

- **High Mobility:** The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy.
- **Network topology:** Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.
- **Unbounded network size**: VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.
- **Frequent exchange of information:** The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.
- **Wireless Communication:** VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication. Time Critical: The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

III. PREVIOUS WORK: BLOCKCHAIN TECHNOLOGY FOR INTELLIGENT TRANSPORTATION SYSTEM

In which all the challenges, security VANET has been less attention so far. VANET package contains key information about the life, it is necessary to ensure that these packets are not inserted or an attacker to modify; the same, they are correct and promptly notify the transportation environment within the driver's responsibility should be established. These security issues are not similar, general communication network. Web, mobile, geographical dimension relationship, etc. so as to achieve other network security problems and different from. Some drawbacks of existing system as follows

A. Security Challenges in VANET

Security challenges must VANET architecture, security protocols, and encryption algorithms such as the design process to consider the following list of some security challenges.

- **Real time Constraint**: VANET is time-critical information about the safety of the place should be Transmission delay of 100 milliseconds delivery. Therefore, to achieve a real sense of time constraints

should be fast encryption algorithm. Messages and entity authentication must be done in time.

- **Data Consistency Liability**: Even in VANET authentication node can execute malicious accident or activities may interfere with the network. Therefore, a mechanism should be designed to avoid such inconsistency. Between data received from different nodes to particular information on the correlation avoid this type of inconsistency.
- **Low tolerance for error**: Some protocols are designed base on probability. VANET using the operation key information for life in a very short period of time.

B. *Attackers on Vehicular Network*

In order to ensure VANET, we need to find out who is the attacker, their properties and the ability to damage the system. On the basis of the ability of these attackers may be of three types.

- **Insider and Outsider**: The industry is a network, and the authentication component. Outsider intrusion and attack capabilities, thus limiting.
- **Malicious and Rational**: Malicious attacker would have no personal interests in order to attack. They just hurt the function of the network. Rational self-interest of the attacker, so they can be foreseen.
- **Active and Passive**: Active attackers generate signals or packet whereas passive attackers only sense the network.

C. *Attacks in the VANET*

- **Impersonate:** In attackers to impersonate attack assumed authority node status and privileges, or use network resources may not be available to it under normal circumstances, or disrupt the normal operation of the network. This type of attack is carried out by active attackers. They may be insiders or outsiders. Such attacks are attacks multilayer attacker could exploit a vulnerability to any network layer, transport layer or application layer.
- **Session hijacking**: Most of the certification process is done at the start of the meeting. Therefore, it is very easy to hijack the session after establishing the connection. In this attack, the attacker to take control session between nodes.
- **Routing attack:** Re-routing attacks that exploit vulnerabilities to attack Network layer routing protocols. In this type of attack the attacker, or discard the packet routing process or interfere with the network.

IV. PROPOSED SYSTEM

There have been too many VANET related premiums. All of these previous works are to achieve their security objectives based on different technologies, in order to prevent attacks VANETs described. In this section, we will analyze the main VANETs existing proposals to provide security services. As a result, the reader will find the most relevant trends and requirements of each security tool most commonly used passwords. Although usability issues in the design of all mechanisms must be considered, some specific mechanisms have also been described. Each section will focus on different security needs.

A. *Advantages of VANET*

- **ARAN (Authenticated Routing for Ad hoc network):** This is based on AODV, but it includes spoofing attacks stop. ARAN the use of public key encryption, and requires its public key certificate is known to all nodes in the server. It uses the timestamp freshness route. The source node broadcasts a route discovery packet (RDP) found routes to all neighbors. Each node maintains a record it received from its neighbor to the message. All messages received after neighbors the same message is forwarded to them with their own logo and certificate neighbors. When receiving the message by the destination, the first node in response to receiving from the message. No intermediate node can reply the RDP other then destination even if that intermediate node knows the path of destination. Destination unicast responses from the reverse (REP) Destination to source. All REP signed by the sender by checking the next hop.
- **Identification mechanisms**: Car environment related identity management an interesting feature. With respect to a conventional computer network, in which no centralized registration exists, uniquely identifies the vehicle from the start. In fact, the process is carried out by two manufacturers and legal authority. Manufacturers' vehicle identification number assigned to each vehicle (VIN). On the other hand, the legal department has requested the vehicle license plate. Both logos are different in nature. Wherein VIN as to uniquely identify the intent of producing a vehicle license plate is assigned to each vehicle registration Management domain.
- **Authentication and privacy issues:** With respect to the electronic identification, Hubaux like. Presents a natural extension of so-called electronic license plate license plate (ELP). The certificate is issued by a legitimate organization, allowing the vehicle to determine not only get, but also to their authentication. However, since this credential include vehicle's true identity, which makes it possible to track vehicles.

B. *Methods to implement*

SEAD (Secure and Efficient Ad hoc Distance Vector): The new routing protocol security, to prevent attackers who create any other node incorrect routing and more incongruous. It is based Destination sequenced distance vector (DSDV) routing. SEAD support of its nodes with limited CPU's Processing power, and from DoS attacks, in which attackers

try to consume excess network bandwidth protection. It uses a one-way hash function, rather than the more expensive asymmetric encryption operation. One-way hash function is selected by a random initial node valley created.

SMT (Secure Message Transmission): Secure messaging protocol proposed, the agreement is light Weight and end to end manner. It requires a security association between the source destinations. It does not use encryption intermediate node. Source first found path found by existing routing protocol, and determines the initial set of valid path for communication (APS). After the completion of a set of the source APS. Each outgoing message source dispersed into a plurality of parts and across different routes coded and transmitted. Each dispersion sheet carrying a MAC (Message Authentication Code), which is used to check the integrity and authentication of its source. Rate path based on the received APS or APS failure in different packet, the source node. Target only verification Acknowledgment and sends an acknowledgment to the source.

NDM (Non-Disclosure Method): This method of location information in a mobile IP protection. They Problem solving traffic analysis and disclosure of the location. The NDM method assumes that multiple independent safety agency, each SA public and private key pair. So this method is based on asymmetric encryption. The sender transmits the message to the receiver process, without disclosing any location information. Communication between the sender and the receiver goes through a security association. SAi know the address of each of the ASI-1 and the ASI + 1. . The sender sends a message to SA1, SA2 and SA1 sends it to the other. Each message package and SA It's public key. However, an attacker may thus fill the variable length of the communication scheme via their message is also introduced during the trace.

C. Comparison table

Solution	Methodology		
	Attacks Covered	***Technology used***	***Security requirements***
ARAN	Replay Attack Impersonation False Warning	Cryptographic Certificate	Authentication Message Integrity Non Repudiation
SMT	Information Disclosure	MAC (Message Authentication Code)	Authentication
NDM	Information Disclosure Location Tracking	Asymmetric Cryptography	Privacy
SEAD	DoS Routing Attack Resource Consumption	One Way Hash Function	Availability Authentication

TABLE 2. Comparison Table

V. MODULE DESCRIPTION

Wireless mobile network devices in the spontaneous - - vehicle ad-hoc network (VANETs) vehicles. Where network created by applying the principle of mobile ad hoc networks (MANETs) domain, can be formed and information may be relayed one of the car. The results show that in VANETs this vehicle to vehicle and vehicle-to-roadside communications architecture will co-exist to provide traffic safety, navigation and other roadside services. VANET is an important part of the Intelligent Transportation Systems (ITS) architecture. Sometimes, VANETs is called Intelligent Transportation

Network. To deploy VANETs, there must be some commercial applications, benefit from them. VANET application which can play a major role can be divided into two categories.

A. Safety Related Application

These applications are used to increase the safety on the roads. These applications can be further categorized in following way.

- **Collision Avoidance:** According to some studies, 60% accidents can be avoided if drivers were provided a warning half a second before collision If a driver get a warning message on time collision can be avoided.
- **Cooperative Driving**: Drivers can get traffic-related warnings, such as curve signal Cooperation and safe driving speed warning, lane change warning system, and these signals can be non-stop, and the driver.
- **Traffic optimization:** Optimizing the transmission by using the traffic jam and the like signals, Accidents and other vehicles, so that they can choose their own alternate path, you can save time.

B. User Based Application

These applications are used to increase the safety on the roads. These applications can be further categorized in following way.

- **Peer to peer application**: These applications provide a useful service like sharing Music, each vehicle network in the movies
- **Internet Connectivity**: People always want to connect with the Internet all the time. Hence VANET provides the constant connectivity of the Internet to the users.
- **Rapidly changing network topology**: Optimizing the transmission by using the traffic jam and the like signals, Accidents and other vehicles, so that they can choose their own alternate path, you can save time.
- **Unbounded network size:** VANET can be implemented as a city, or several cities. For the country. In VANET, this means that the network size is unlimited geographically.
- **Frequent exchange of information**: Temporary excitation of VANET nodes. To collect information from other vehicles and roadside units.
- **Wireless Communication**: VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore

some security measure must be considered in communication.

- **Time Critical:** The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.
- **Sufficient Energy:** The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power.
- **Better Physical Protection**: The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack.
- **Other services:** It provides the constant connectivity of the Internet to the users. VANET can be utilized in other user based application such as payment service to collect the tall taxes, to locate the fuel station, restaurant etc.

VI. CONCLUSION AND FUTURE WORK

We investigated main aspects of vehicular ad hoc networks (*i.e.*, the communication protocols V2V and V2I, differences from MANETs, main applications), and the main technologies, and sensors, used to support emerging inter and intra-vehicle communications. We also implemented the block chain to transparency of the vehicle authentication and published by the perform efficiently block chain technology. In future, we will simulate our proposed framework mechanism on real-time traffic data of vehicle information sharing scenarios as well as analyze with multiple use cases with a solution.

ACKNOWLEDGEMENT

The authors would like to thank the V.S.B Engineering College management and faculty members for their support .

REFERENCES

[1] A J. Li, K. K. Raymond Choo, W. Zhang et al., “EPA-CPPA: an efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” Vehicular Communications, vol. 13, pp. 104–113, 2018.

[2] J. Li, H. Yuan, and Y. Zhang, “Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks,” Cryptology ePrint Archive, 2018

[3] A J. Li, K. K. Raymond Choo, W. Zhang et al., “EPA-CPPA: an efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” Vehicular Communications, vol. 13, pp. 104–113, 2018.

[4] J. Li, H. Yuan, and Y. Zhang, “Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks,” Cryptology ePrint Archive, 2018

[5] J. Cui, J. Zhang, H. Zhong, and Y. Xu, “SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter,” IEEE Transactions on Vehicular Technology, vol. 66, no. 11, pp. 10283–10295, 2017.

[6] Song C., Zhang M., Peng W. Efficient pairing-based batch anonymous authentication scheme for VANET. J. China Univ. Posts Telecommun. 2018.

[7] Shao J., Lin X., Lu R., Zuo C. A Threshold Anonymous Authentication Protocol for VANETs. IEEE Trans. Veh. Technol. 2016.

[8] Lee J.L., Hwang J., Park H., Kim D. On latency-aware tree topology construction for emergency responding VANET applications; Proceedings of the IEEE INFOCOM 2018.

[9] A M. AbdelmagidElsadig and Y. Fadlalla, "VANETs Security Issues and Challenges: A Survey", Indian Journal of Science and Technology, vol. 9, no. 28, 2016.

[10] Y. Ming and X. Shen, “PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks,” Sensors, vol. 18, no. 5, p. 1573, 2018.

[11] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, “Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks,” International Journal of Distributed Sensor Networks, vol. 13, no. 3, Article ID 155014771770089, 2017.

[12] E. Eze, S. Zhang and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward", 2014 20th International Conference on Automation and Computing, 2014.

[13] A.S. Al Hasan, Md. ShohrabHossain, and Mohammed Atiquzzaman, “Security threats in vehicular ad hoc networks," Conference on Advances in Computing, Communications and Informatic, pp. 21-24, Sept.2016.

[14] Analytic model on data security in VANETs", 2017 17th International Symposium on Communications and Information Technologies (ISCIT), 2017.

[15] "Efficient privacy preserving security protocol for VANETs with sparse infrastructure deployment", 2015 IEEE International Conference on Communications (ICC), 2015.

[16] R. Kaur and U. Kaur, "Various Techniques to detect DOS attack in VANET: A Review", International Journal of Computer Applications, vol. 164, no. 8, pp. 38-41, 2017.