IJCRT.ORG ISSN : 2320-2882
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract

Arockia Sneha A[1], Kaviya B[2], Harini S[3], Vijayalakshmi C[4]

[123]*Student, Computer Science and Engineering,*

[4]*Professor, Computer science and engineering,*
[1234]*Panimalar Engineering College, Chennai, India*

Abstract—The Internet of Vehicles (IoV) provides the concept of coordination of vehicles for enhancing safety of both the driver and the vehicle and also increasing transportation performance. Vehicles are coordinated for avoiding collisions by communicating their positions when they become closer. The information about location is identified by their geographical positions or the ones in road maps. The system can also be made efficient by informing about traffic jams by sharing their locations and destination. In this way, traveling time can be reduced. However, IoV also have some security challenges, such as keeping safe from virtual hijacking. To avoid this, vehicles should detect and avoid the hijacked vehicles ignoring their communications. This system presents a technique for improving security by applying certain prioritization rules, using digital certificates, applying trust policies and incorporating them with block chain technology for detecting and avoiding hijacked vehicles. Based on trust values the corrupted messages are blocked by the system itself and broadcasting of fake messages is completely avoided, thereby enhancing the security.

Keywords— **Internet of Vehicles (IoV), VANET, Broadcasting messages, RSU, V2V communications**

I. INTRODUCTION

VANET is an enhancement of Internet of Things. In VANET, the vehicles can cooperate among each other 1) to avoid collisions 2) to estimate the routes with less traffic or 3) to arrange the best routes for avoiding waiting times in the charging stations for electric vehicles.

Vehicles in a VANET environment are supposed to broadcast messages when in need. But these messages and data should be transferred in a secure way that no one can hijack the network. So, this system provides authentication and sign on algorithm to verify the users and trust values to verify the originality of the messages broadcasted.

II. DESCRIPTION

A. METHODOLOGY:

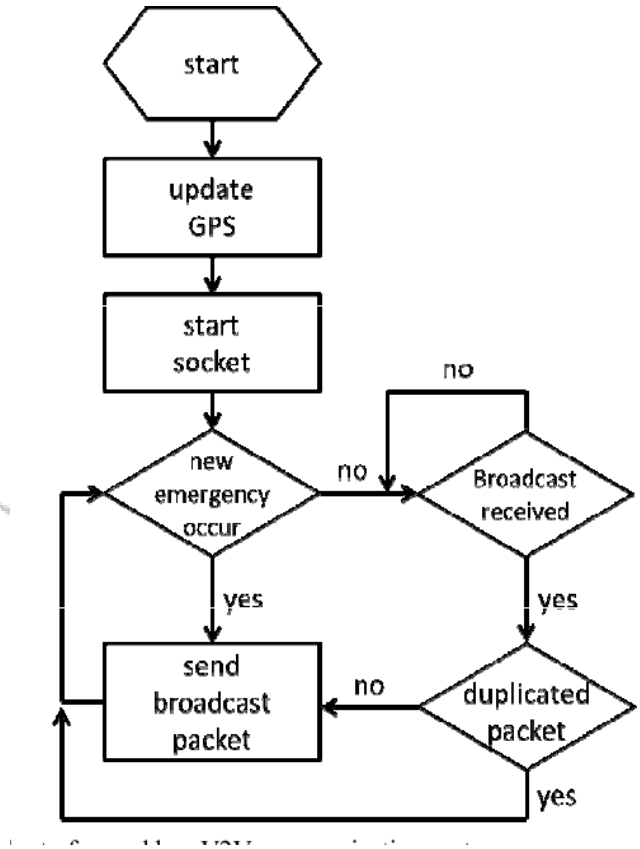

Fig 1: Flowchart of the system

The fig1. Shows working layout of the system from locating a vehicle to broadcasting the message. Emergency event here denotes partial brake, ambulance ahead, overtaking etc., Suppose a vehicle slows down suddenly, this information should be broadcasted to other vehicles in region of interest to avoid rear end collisions. Although the system of broadcasting the messages have been proposed earlier, this system proposes broadcasting messages in a secure way by managing trust values.

B. *Components in VANET:*

Usually, the interaction between vehicles and the RSUs is done via wireless technology called as wireless access in vehicular environment (WAVE). This technology ensures the safety of passengers by providing vehicle information and traffic flow. The VANET architecture comprises units such as RSUs, OBUs and TA.

i. Roadside units:

RSU, stands for Roadside unit, is a DSRC transceiver built along a road or pedestrian passageway or at the intersection or in the parking area. It can also be built on a vehicle or be carried in hand. But RSU operates only when the vehicle or hand-carried unit remains stationary. RSUs broadcasts messages or information to OBUs in its communication zone.

ii. Onboard units:

OBU stands for Onboard Units, is a GPS based tracking device. It is equipped with many components like processor, sensor devices, user interface, read/write storage for getting storage information etc., that facilitates vehicles to share information between RSUs and OBUs. The connection between RSUs and OBUs is established wirelessly. The communication with RSUs and OBUs is done in the form of messages.

iii. Trusted Authority:

TA, stands for Trusted Authority, is responsible for registering RSUs, OBUs and vehicle users. It is also responsible for generating keys and distributing secure services in the VANET environment. TA authenticates the identity vehicle OBUs or the identity of user vehicles to avoid malicious attack into the system.

C. *System architecture:*

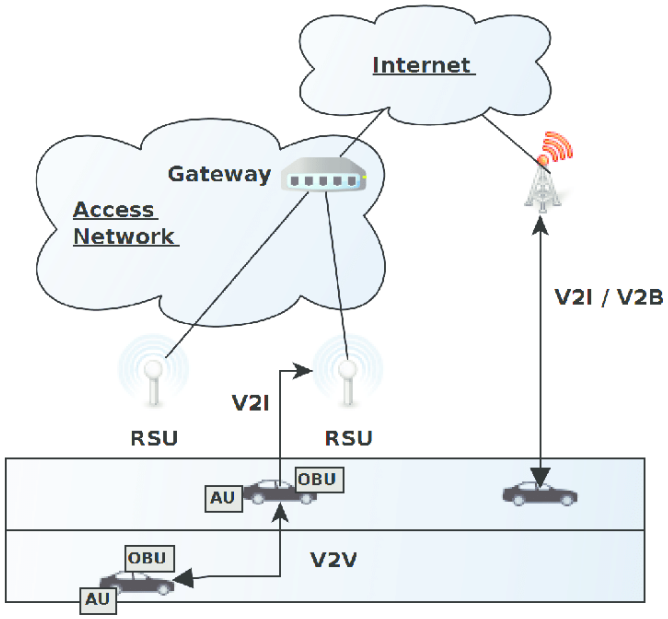

Fig 2: System architecture diagram

The fig 2. Shown above depicts the architecture diagram of the VANET system. The architecture can be explained clearly by going through the below mentioned modules. The modules are

i. User registration and authentication.
ii. Node creation.
iii. Neighbour node calculation.
iv. Broadcasting the messages.

i. User registration and authentication.

The first and foremost thing in the VANET environment is that the user has to register himself/herself with the system with valid information. Once the user is done with the registration, he/she is supposed to login into system every time he/ she wishes to use the system. Authentication is done every time the user logins into the system to avoid some attackers penetrating the network. Sign up and authentication here ensures the first level of security of the VANET environment. This acts as a security layer before the nodes begin to communicate with each other.

ii. Node creation

Once the user registered himself in the system, he needs to locate himself in the network to get connected with RSUs and other OBUs so that the user can receive or throw messages within the region of interest of communication. The OBU deployed in a vehicle is responsible for providing essential details of vehicle to the RSU. Vehicle is located with the help of

latitude and longitude values provided by Onboard unit.

iii. Neighbour node calculation.

We have to determine our neighbour nodes to create a network and broadcast the message. To create a network, we have to get information about vehicles' speed, distance among the vehicles, destination comparison between next hop. These are the important requisite of a VANET system. The speed and distance among the vehicles are provided by the GPS in the Onboard Unit. GPS plays a vital role in limiting the network. This method is called position-based routing. This method is chosen since it has more efficiency in urban environment than any other methods.

iv. Broadcasting the messages.

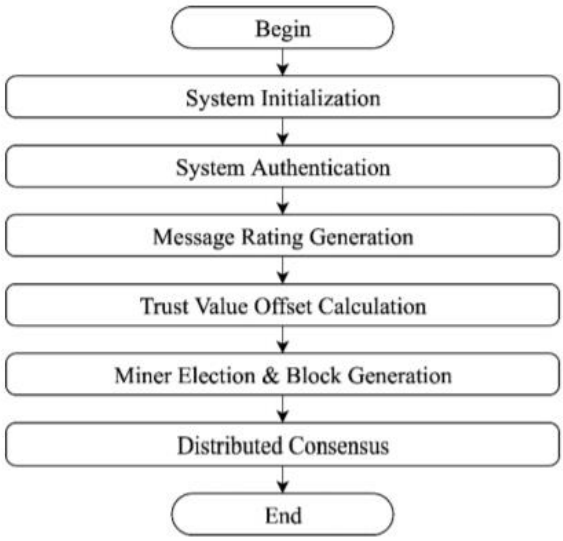

Fig.3: Flowchart of Message Broadcasting

Once a node detects an emergency event has occurred, it has to inform other nodes in that network about the event to avoid accidents. The emergency event can be partial break, sudden slow down of vehicle, Ambulance crossing, road mending works, etc., The message before getting broadcasted has some steps to be done to avoid malicious attacks on the communication.

When an emergency occurs, a node detects that will develop an alert message. To ensure the trustworthiness of that alert message, message rating generation is implied for providing rating for the messages sent by the communicating nodes. Following this, Trust value offset calculation is done to calculate the trustworthiness of each and every node in the network. After this phase, the system evaluates the messages for miner election and block generation, that implements blockchain technology for tracking nodes efficiently in the network.

If the calculated trust value of node ensures trustworthiness of the message, it will be broadcasted to the neighbour nodes or else the message is blocked or gets displayed as message corrupted.

III. Conclusion

In this paper, we proposed mechanisms that manage trust using blockchain in IoV. We proposed a blockchain-based decentralized approach in which CA/TA deployed the smart contract, and all RSUs work in a distributed manner to maintain consistent vehicular trust database and enhance reliability, availability, and consistency. We also introduced the idea of maintaining shared blockchains, that will not only reduce the propagation delay of transactions but will also increase the throughput and efficiency of the entire system. We also introduced incentive strategy for the vehicle participating in event detection, i.e., their contribution in the detection of a true event and its accurate reporting helps them to get rewards, which they can redeem for various services and payments. The proposed incentive mechanism encourages participating peers to perform well and get wallet points.

IV. Future Enhancement

As future work, we will try to integrate the misbehaviour detection process and the privacy part. We will look for the role of AI in the misbehaviour detection and efficient consensus algorithms in the RSU plane of IoV for decentralized trust management. In blockchain system, the decentralized approach addresses large amount of networking overhead than the centralized approach. So, more efforts have to be taken to improve networking performance by combining networking and computing technologies as well as decentralized consensus algorithms.

V. References

[1] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social Internet of Vehicles: Architecture and enabling technologies," Comput. Elect. Eng., vol. 69, pp. 68–84, Jul. 2018.

[2] G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," Future Gener. Comput. Syst., Jan. 2018.

[3] R. Kasana et al., "Location error resilient geographical routing for vehicular ad-hoc networks," IET Intell. Transp. Syst., vol. 11, no. 8,pp. 450–458, Oct. 2017.

[4] S. D. Khalid et al., "Location information verification using transferablebelief model for geographic routing in VANETs," IET Intell. Transp.Syst., vol. 11, no. 2, pp. 53–60, Oct. 2017

[5] A. Mansoori and C. Achar, "Smart roads using IoT devices," Int. Res.J. Eng. Technol., vol. 5, no. 6, pp. 1526–1529, 2018.

[6] E. Karaaslan et al., "Modeling the effect of electric vehicle adoptionon pedestrian traffic safety: An agent-based approach," Transp. Res. CEmerg. Technol., vol. 93, pp. 198–210, Aug. 2018.

[7] K. Małecki, "A computer simulation of traffic flow with on-street parking and drivers' behaviour based on cellular automata and a multi-agentsystem," J. Comput. Sci., vol. 28, pp. 32–42, Sep. 2018.

[8] I. García-Magariño, G. Palacios-Navarro, and R. Lacuesta,"TABSAOND: A technique for developing agent-based simulation apps and online tools with nondeterministic decisions," Simulat.Model. Pract. Theory, vol. 77, pp. 84–107, Sep. 2017.

[9] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the ratee: A trust management system for social Internet of Vehicles," Wireless Commun.Mobile Comput., vol. 2017, Dec. 2017, Art. no. 7089259