JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Adding Blockchain To Enhance Security in VANET

[1]Himanshu Bhoir, [2]Rushikesh Sasamkar , [3]Prasad Pansare , [4]Aarti Yadav

[1] B.E Scholar, [2] B.E Scholar, [3] B.E Scholar, [4] B.E Scholar
[1,2,3,4]Information Technology,
Sandip institute of Technology And Research Center, Nashik, India

Abstract :
The number of automobiles has been increased on the road in the past few years. Due to high density of vehicles, the potential threats and road accident is increasing. Wireless technology is aiming to equip technology in vehicles to reduce these factors by sending messages to each other. The vehicular safety application should be thoroughly tested before it is deployed in a real world to use. Simulator tool has been preferred over out door experiment because it simple, easy and cheap. VANET requires that a traffic and network simulator should be used together to perform this test. Many tools exist for this purpose but most of them have the problem with the proper interaction. In this thesis, we aim at simulating vehicular networks with external stimulus to analyze its effect on wireless communication but to do this job a good simulator is also needed. So we will first debate on the shortcoming of current simulators and come up with our own recommendations to perform our simulation.

IndexTerms **– VANET, Blockchain, etc.**

I. INTRODUCTION:

Traffic congestion on the roads is today a large problem in big cities. The congestion and related vehicle accommodation problem is accompanied by a constant threat of accidents as well. Absence of road traffic safety takes a toll of precious human lives and poses a dire threat to our environment as well. Other negative consequences are related to energy waste and environmental pollution. According to National Highway Traffic Safety Administration, the following figures indicate some of the consequences of recent car accidents .The communication platforms in the vehicle-to-vehicle area (V2V). Almost ten years back from initial research or advanced procedure function [3]. THE latest V2Y1 network surveys last year had more than a thousand quotes on the reference sheet. V2X is nothing but it is the type of VANET such as V2V (Vehicle to vehicle), V2I that's mean Vehicle to infrastructure. In the Current era, Strong radio communication management problems because of to its decentralization and its strong quality of service (QoS) specifications for transport safety apps force the production of potential vehicle-on-vehicle (V2V) and vehicle-on -infrastructure wireless communications networks (V2I) systems [4]. Vehicles will communicate their location as well as the speed for surrounding vehicles on even a regular basis utilizing IEEE 802.11p to prevent conflicts with road traffic [4].V2Y is a component of intelligent transportation networks (ITS) is the main reason for this. The ITS scope is larger than V2X because it still involves road, ground, and air transport networks. However, the focused scientific work just started to evolve after the public and private sectors revealed the services. Enhanced network performance ("green"), decreased traffic delays, economic development, passenger content, but most specifically, health is the driving factor for all of ITS. This is more apparent in V2X as traffic crashes in major developing countries already take millions of lives every year. While we are constrained to V2Y only, that zone's width is large. For few years V2V mechanism has already been known after work on the V2V mechanism because it varies from those of other conventional communication systems. The closest approximation may be between cellular as well as I antenna heights each of the transmitter (Ty) and receiver (Ry) are small, and both Ty and Ry are mobile, and V2V can be distinguished from either the V2V channel. While there is a protocol for V2V communications (5.9 GHz UNII band;particular-range committed communications, DSRC, Traditional). Traditional wireless local area networking (WLAN) for all devices might not be enough [5]. Throughout the Wi-Fi Standard, the lowest two levels of the networking routing protocol are the transmitting scheme[5]. However, when modern V2V technologies grow, such technologies can have to be supported by modern standards. It may be Standard Wireless Metropolitan Area (WMAN). A broad range of implementations of the 802.16 specifications are also assigned to as WiMAX by energy sector established technology.V2V technologies provide higher bandwidth speeds, rapid comment channel structured disappearing, or smarter FEC encoding to boost efficiency. For potential V2V environments, it is also feasible to add certain specifications. Whatever the transfer method, wireless channels information is important for the optimum development and efficiency of any V2V network. It should be well established that perhaps the effects of the computational channel evaluation offer basic information in the data link-form architecture or study among all communications systems.

2.Objective:

The work in this thesis has been divided into two parts:

1. A survey of various traffic simulators, network simulators and VANET simulators resulting in the selection of a preferred recommended choice.

2. Practical implementation and use of a VANET simulation based on the preferred choice, with NS3 network simulation.

3.The main objective of this paper is to study how to securely deliver trustworthy event messages by applying blockchain technology in VANETs. We will deal with a local blockchain that is independent of chains from other countries to improve the scalability and timeliness of message dissemination in the VANET. We consider a public blockchain that independently manages and stores all node trustworthiness and message trustworthiness in a given country. We also present different types of blockchain consensus mechanisms based on a private or public blockchain.

3.Proposed System:

Vehicular Ad-Hoc Networks (VANETs) have great potential in improving traffic control and mitigating road accidents. This is done by sending messages or basic safety messages (BSMs) between vehicles (V2V communication) or between vehicles and road side units (RSUs) (V2I communication).

Security is one of the main challenges in VANET. This is crucial because it directly affects the lives of the commuters or incurs a substantial financial loss to them. As discussed in section there are many security concerns and different potential attacks that could take place in VANET. Authentication is one of these security requirements that is very crucial for validating the messages from a sending vehicle. It is important to improve the efficiency of the authentication scheme so that a higher number of messages can be validated by the vehicles, which will, in turn, ensure that critical safety messages are not dropped due to the delay in the authentication.

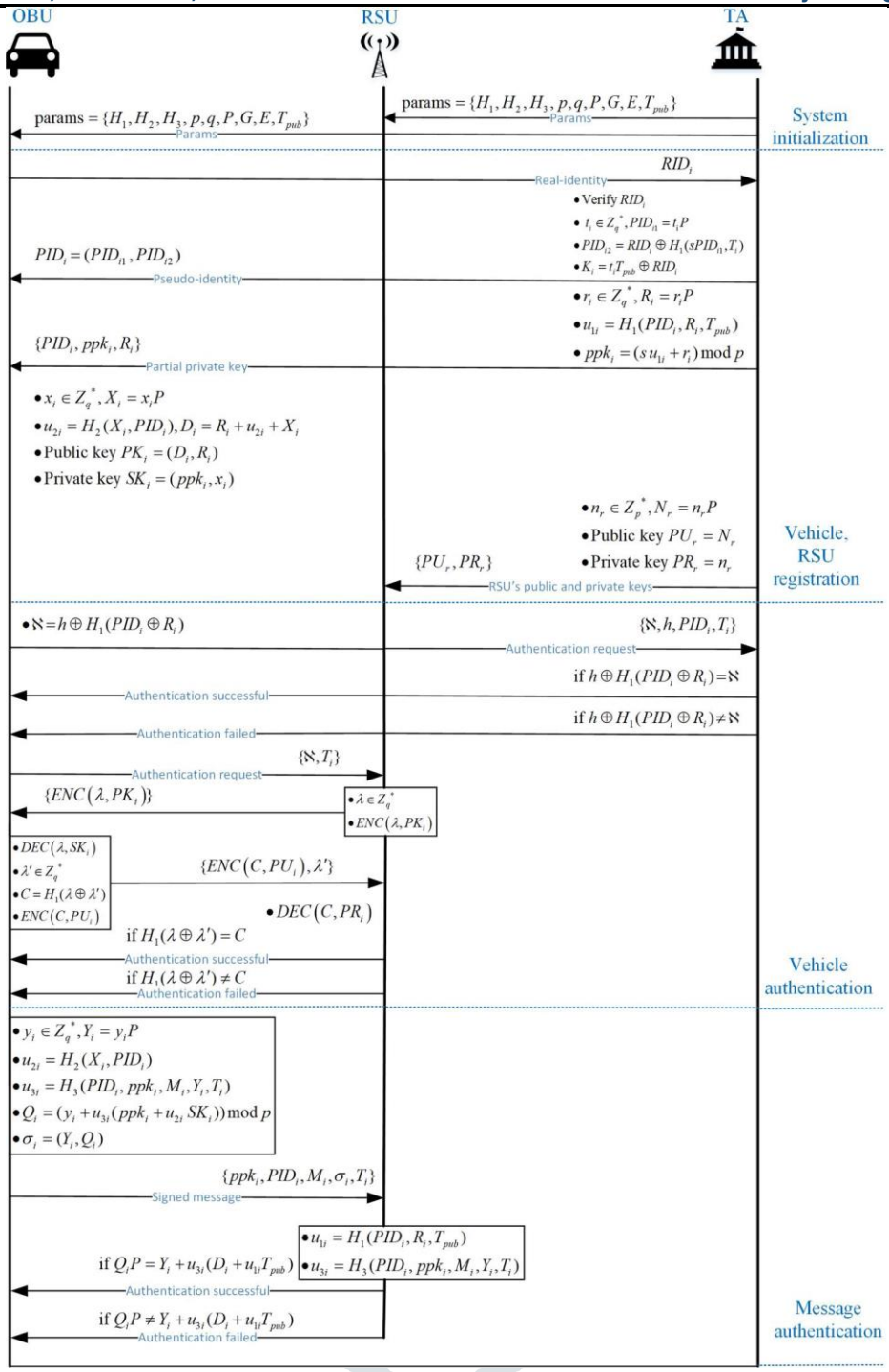
Operation	**Sender**	**Transaction**
Registration	Authentication Party	<VIN, PID> <PID, PK, Status, Misbehavior Report>
Misbehavior Report	Authentication Party	<PID, RSUID, ++Misbehavior Report>
Revocation	(automatically invoked)	<PID, Status>
Readmission	Authentication Party	<*VIN, PID> <PID, PK, Status, Misbehavior Report>
Query_Valid_Vehicles	RSU	<select the vehicle with a PID and ‘valid’ status>

Blockchain operations

4.Mathematical Model:

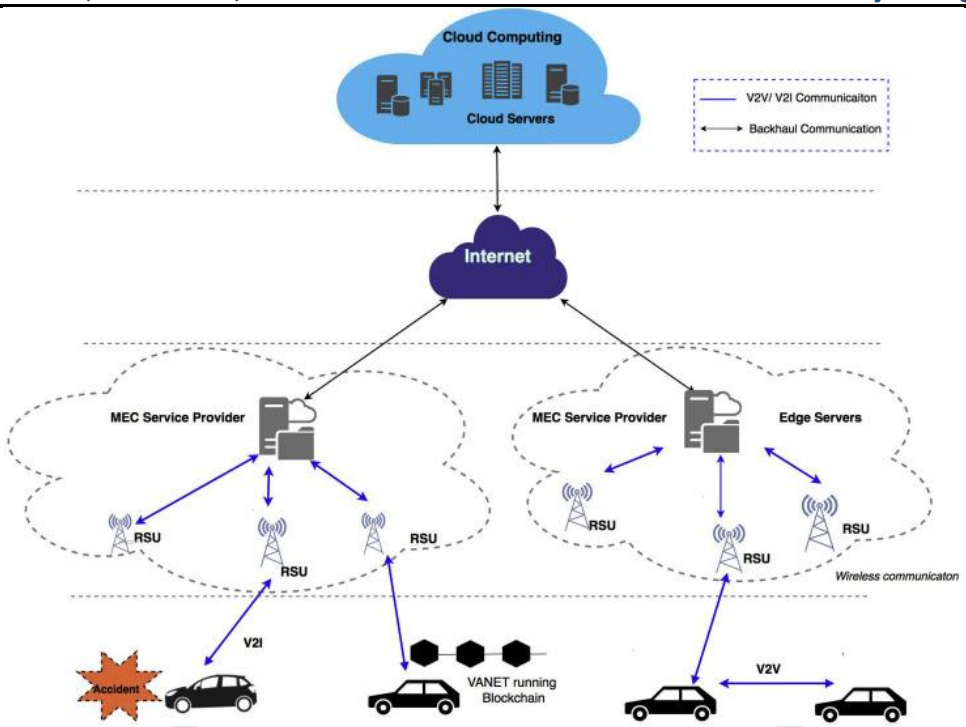
- Check the sender vehicle's previous trust level from the main blockchain
- Check the PoL based on the location certificate
- Check if it is first-hand information
- Check the timestamp

If the received event message is valid and trustworthy based on the verification policy, then its trust level will be updated. The trust level is defined as the fraction of true event messages m sent by vehicle Vi to the total event messages m + n, i.e., TL = m/ m + n , where n is the number of false event messages. The trust level varies over time, depending upon true or false messages. The trust level of a vehicle increases as the number of true messages increases.



5.Future Work:

As for the future perspective, we have introduced edge computing for the blockchain, which can reduce the delay of block generation by offloading the high computational PoW to the edge servers to mine the blocks by the miner vehicles. Furthermore, the block propagation delay can be reduced by using the edge cloud computing. The Mobile Edge Computing (MEC) can provide edge cloud service at the edge for the VANET nodes and offload resource-intensive work from vehicular nodes to the edge servers [39,40]. he application of the MEC in the VANET. blockchain is shown in Fig. 8. The MEC can be used to propagate block messages between the miner nodes that can reduce the propagation delay. In addition to this, the vehicular nodes offload the mining process to the MEC servers to speed up the mining process that helps in frequent block generation, which is suitable for the VANET. As we are dealing with emergency event messages, timeliness of message dissemination is of high priority. The edge computing can be used to mine the blocks faster in our proposed scheme



We assume that the MEC service providers deploys their edge servers for vehicular minernodes. The miner can offload the computational intensive PoW to the MEC servers and the service provider charge the miner nodes for providing their services. The miner node has to pay a small amount offee to the edge service provider which will be less than the reward gained when a new block is mined. The miner nodes request for edge service and offload the PoW computation. The MEC servers accept and compute the PoW, and provide solutions to the miner nodes. The minernodes then broadcast the PoW solution to the network. If a miner is successful in mining a block, then it will receive an incentive in the form of rewards. The MEC also handles other resource intensive tasks

6.CONCLUSION:

The motivation to provide a light weight authentication framework that was computationally efficient compared to the traditional PKI architecture, is realized using the blockchain framework. In our proposed framework, we validate the PID and PK of the vehicles sending messages using the RSU services. The vehicles also maintain a short list of recently validated vehicles (PID and PK) with an expiration time. After validating the PID and the PK of the sending vehicle, we then validate the digital signature of the BSM along with the timestamp that the message was send. The RSUs will have access to the blockchain and will query it to validate the PID and PK of the vehicles.

Our proposed method reduces the computational time for authentication, but this is done by sacrificing the channel busy time. Our proposed method will require additional messages to be transmitted to the RSUs and further, from the RSUs to the vehicles. Hence, this results in the additional channel busy time. However, we were able to reduce the delay due to authentication by half of that in the PKI framework. Further, using blockchains will enable a decentralized and distributed system for VANET, avoiding single point of failure.

The performance of the algorithm for VANET was evaluated in terms packet delivery ratio, end-to-end delay, packet loss, and packet overhead using the selected Veins simulation tool. Each performance analysis was run 10 times in the simulator and then a statistical analysis was performed by averaging the values obtained to a mean value of the reading to be compared with the benchmark protocols, as well as the confidence interval (CI) of the results obtained for each evaluation metric, both with and without the presence of a denial of service attack, which was simulated using NETwork Attacks (NETA). 6.1. Packet Delivery Ratio (PDR) PDR refers to the ratio of the number of packets that were successfully received to the total number of packets sent in the network [42]. PDR was obtained by determining the ratio of total number of packets received, Pr , to the total number of packets sent, Ps , in the network, as shown in

(1): PDR = (Pr /Ps) × 100%

7.REFERENCES:

[1] "Global status report on road safety 2018.," 2019, June 27.

[2]"First of its kind CAA study identifies Canada's worst traffic bottlenecks.," 2017, January 11.

[3] S. Yousefi, M. M. S. and M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," 6th International Conference on ITS Telecommunications, pp. 761-766, June 2006.

[4] "VANET [jpg]," 2015.

[5] R. Abassi, "VANET security and forensics: Challenges and opportunities," Wiley Interdisciplinary Reviews: Forensic Science, 1(2), e1324, 2019.

[6] M. N. Mejri, J. Ben-Othman and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Vehicular Communications, 1(2), 53-66, 2014.

[7] N. Malik, P. Nanda, A. Arora, X. He and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 674-679, August 2018.

[8] X. Liu, Z. Fang and L. Shi, "Securing Vehicular Ad Hoc Networks," in IEEE, 2007.

[9] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, p. 217–241, August 2012.

[10] B. Cronin, "Vehicle Based Data and Availability," October 2012. [Online]. Available: https://www.its.dot.gov/itspac/october2012/PDF/data_availability.pdf. [Accessed 12 July 2019].

[11] J. Pan, J. Cui, L. Wei, Y. Xu and H. Zhong, "Secure data sharing scheme for VANETs based on edge computing," EURASIP Journal on Wireless Communications and Networking, December 2019.

[12] N. Bauerle, "What is the Difference Between Public and Permissioned Blockchains?,"Coindesk,[Online].Available: https://www.coindesk.com/information/what-is-the-difference-between-open- and-permissioned-blockchains. [Accessed 06 November 2019].

[13] "Introduction–HyperledgerFabric,"2019.[Online].Available:https://hyperledger-fabric.readthedocs.io/en/release 1.4/blockchain.html. [Accessed 10 August 2019].