Secured Communication in Vehicular Adhoc Networks (VANETs) using Blockchain

Shivaprasad More¹, Rahul Sonkamble², Dr. Udaykumar Naik³, Dr. Shraddha Phansalkar⁴, Priyanka More⁵, Dr. Baljit Singh Saini⁶

¹,²Assistant Professor, Department of Computer Science and Engineering, Sanjay Ghodawat University Kolhapur, Maharashtra, India
³Professor, Department of Electronics & Communication, KLE Dr. M.S. Sheshgiri College of Engineering & Technology, Belagavi, Karnataka, India
⁴Professor, Symbiosis Institute of Technology, Lavale, Pune
⁵Research Scholar, School of Computer Science and Engineering, Lovely Professional University, Punjab
⁶Professor, School of Computer Science and Engineering, Lovely Professional University, Punjab

shivaprasadmore@gmail.com, rahulgsonkamble@gmail.com, naikudayl@gmail.com, shraddhap@sitpune.edu.in, priyanka.bhosale@gmail.com, baljitsaini28@gmail.com

Abstract. In the last decade, the vehicular ad-hoc network (VANET) field is growing drastically. In VANET the communication is the most important aspect through which the data transmission is taking place. Data transmission is maybe related to data in the form of multimedia messages, notifications, announcements, or some warning messages that are involved in VANETs. Data transmission among different vehicles would lead to an exchange of audio-video files in the formed network. These multimedia messages should be transmitted in the fraction of second as this network is built for temporary communication. Vehicles involved in this communication should be trustworthy otherwise other vehicles those who are part of this network would be misguided due to intruder present in the network. To achieve security and integrity in the constituted network, system has proposed the blockchain security environment as a part of this proposed system. Blockchain induces high-end communication in the ad-hoc network. It also enhances the overall security aspect of the constituted network. In this paper, we have proposed blockchain-based security system for vehicular communication that handles this communication securely in a well efficient manner. The performance of the
The proposed system will be measured based on parameters like end-to-end delay, reliability, and packet delivery ratio.

1. Introduction

VANETs are typically composed of few vehicles those who can capable to form the network through wireless sensor networks (WSN) and they can exchange some multimedia data. Vehicles are equipped with a wide range of sensors to broadcast the messages among the network. This kind of communication would be useful to avoid serious accidents on the road or to make some announcements, warning messages, line change assistance, emergency vehicle notification etc. This communication also extends to convey natural calamities among the ad-hoc network. Two categories of communication are possible in the VANETs depicted as Vehicle to vehicle (V to V) and vehicle to infrastructure (V to I). In both categories of communication, the Road Side Unit (RSU) plays a vital role to initiate and accomplish the task. For instance, suppose a bridge is broken down on some road around one kilometer ahead and this kind of natural calamities can be shared among the network through neighbors so that they can take some preventive measures to avoid accident. Such emergency messages system need to distribute among the network. But there are some exceptions for this scenario as an intruder or any malicious node (vehicle) wants to share the fake message in the network to mislead the entire network. To avoid this, strong base of data authentication with security is required for vehicle communication. By attaining blockchain-based security the authenticity of the messages would be achieved among the network which will enhance the overall data exchange capability of the VANETs. We can deploy smart contracts that will ensure the authenticity of the messages. With the help of smart contracts only registered vehicles will be able to communicate in the VANETs. Vehicles in the network can share some multimedia files among the constituted network by secured way with the help of blockchain architecture.

2. Existing work

L.Zhang et.al. in [1] proposed the privacy mechanism vehicular communication system in a cloud environment. Hierarchy is defined in this network for efficient communication among the formed network. Hassan et.al in paper [2] suggested that blockchain is a viable solution for decentralized networks. Blockchain-based Internet-of-Things (IoT) system all transactional details and encrypted keys are accessible to all in the network. In [3-5] proposed trustworthy, safest, and privacy-preserving networks in vehicle-to-vehicle communications. Dedicated Short-Range Communication (DSRC) standard in VANET is used for safety message exchange that is involved in multi-hop data dissemination and routing [6]. For video transmission in VANETs, As the video files are bulky, they are encoded with the High Efficient Video Coding (HEVC) encoding scheme to form the bitstream [7]. Traffic safety and the efficiency of the VANET can be improved by broadcasting some warning or alert messages among the constituted network. Finding a single trusted entity to store and distribute such messages can be challenging, and vehicles may not be involved in the network [8]. An intruder cannot spoil a trusted network by concept using apriori countermeasure which mainly prevents the broadcasting of fake messages into the network [9].

3. Challenges

3.1 The problems that deteriorate the video streaming quality in VANET are the packet loss and the transmission delay. Many causes can lead to these problems such as high vehicles density, high speed of vehicles, environment obstacles, etc.[10]

3.2 The delivery of video flows in the best perceived video quality is big challenge as the nodes are endowed with high mobility [11].
3.3 The most important challenges of video streaming on VANETs is how to reduce the time for video streaming. The Peak Signal-to-Noise Ratio (PSNR) of video streaming on wireless networks is very low, because of the high packet loss probability caused by the fading, interference and collision. It is even worse in VANETs, because of the fast changing network topology caused by the high movement speed. The video streaming protocol do not possess reliability techniques, because reliability is considered to be useless in video streaming [12].

3.4 Video streaming in urban VANETs is a desired application, which is more complicated than others since it has strict QoS limitations and a greater amount of information to be transferred. An adaptive geographic routing scheme posing dynamic nature of urban VANETs was developed, in which the lifetimes of the discovered routes are limited and is insufficient for transferring all the packets of a large video file. Furthermore, the discovered routes need enough connection probabilities to satisfy the required QoS limitations including end-to-end delay, freezing delay and packet delivery ratio. [13]

3.5 The environment reliable data dissemination to the destination nodes is one of the biggest challenges as there may be a congestion in the network due to blind flooding of messages to their final destination, called as broadcast storm which may lead to the performance degradation with respect to the metric such as-message delivery, reliability and response time.[14]

3.6 The fair resource allocation in the vehicular environment and to ensure a best perceived video quality while switching from RSU coverage to another still remains big challenge [15].

4. System architecture

The proposed system mainly focuses on transaction among the V to V or V to I network in secured way. There are a lot of storage architectures and are used for different purposes. Blockchain is a distributed architecture that uses encryption and hashing algorithms. These characteristics of blockchain make it a very secure technology in the existing era. Due to such characteristics, various researchers have proposed ideas with the help of blockchain technology in different sectors like healthcare, government documents, stock markets, financial institutions. In the blockchain, there are different platforms exists listed as Ethereum, Hyperledger Fabric, Hydrachain, Multichain [16]. Ethereum [17-18] is a Type 2 platform where programmer can able to write and deploy his logic programmatically. These programs are called smart contracts. Nodes can communicate with each other in the ethereum blockchain using smart contracts. In the existing VANET system, the cloud can be used to store audio and video messages sent by the vehicles through RSU. In the cloud, privacy and security issues have been observed [19]. On the other hand, blockchain also suffers from some issues like cost and less storage space [20]. By collaborating the blockchain with cloud the system could able to achieve both storage and security issues in well efficient manner. In [21], paper presents validation of indoor wireless local area network (WLAN) propagation model for varying rectangular receiver node geometry. Moth-Whale Optimization Algorithm proposed to identify the best optimal path among different available multipath in the VANETs [22]. Large amounts of data storage on the blockchain will degrade the performance of the VANETs. Storing only transaction records, hash values of all required transactions, and off-chain data storage will be effective. The drawbacks of blockchain and cloud can be overcome by integrating these two technologies. This paper proposed a Blockchain-Cloud integrated VANET system as shown in Figure 1. In this proposed system, the possibility of generating fraudulent messages will be reduced and messages can be securely buffered on to the cloud system. The messages are forwarded among vehicles that are part of this network.
Figure 1: Blockchain-Cloud Integrated VANET System

Figure 2: Detailed Working of Blockchain & Cloud
The hexagonal network partitioning would be considered while forming the VANETs. In the network, each vehicle is provided with unique id for verification. The authenticated vehicle can able to transfer and receive the data frame sent by another vehicle which is part of that network. Within the network data frame transmission and dissemination is the challenging job. To accomplish this task network has to identify a vehicle which is a good forwarder and disseminator depending upon the past history of that vehicle by considering dissemination and transmission parameters. The message format is given in figure 3.

| Vehicle ID | Message No | Vehicle Position | Message Length | Expiry Duration | Vehicle Speed |
|------------|------------|------------------|----------------|----------------|---------------|

**Figure 3: Message Format**

As shown in above diagram message consist of vehicle unique id, message number, vehicle position, message length and expiry duration of the message.

\[
\text{Vehicle Speed } = \frac{\sum_{x=1}^{N(w)} |SP_x - SP_y|}{\text{Number of adjacent vehicles (w)}}
\]  

(1)

From equation(1) vehicle speed of the vehicle is computed by comparing speed of the adjacent vehicle. ‘x’ and ‘w’ are two adjacent vehicles in the network. Speed of the two adjacent vehicles is given by ‘SP_x’ and ‘SP_w’. Vehicle position is calculated by using equation (2) as follows

\[
u_p = u + \text{Vehicle Speed} \times (t_2 - t_1) \times \cos \theta
\]

(2)

\[
v_p = v + \text{Vehicle Speed} \times (t_2 - t_1) \times \sin \theta
\]

(3)

Where, ‘u_p’ and ‘v_p’ are the current positions detected by RSU and ‘u’, ‘v’ are the previous positions of the same vehicles. Time ‘t_2’ and ‘t_1’ are the current time and previous time respectively. \(\theta\) is given by

\[
\theta = \tan^{-1} \left(\frac{h_2 - h_1}{k_2 - k_1}\right)
\]

(4)

where, (h2, k2) is the current position, and (h1, k1) is the previous position of the vehicle.

The detailed working of the proposed VANET system is shown in Figure 2. When a traffic situation is observed by any vehicle among the network, then a message regarding the same is sent to RSU. This message may be in the form of audio or video. RSU needs to send the same message to blockchain for verification. The message will be verified based on the message format as given in figure 3. But before that system needs to confirm whether the received message is authentic or fraudulent. If a message is sent by a registered vehicle then it will be considered as an authentic message. This authenticity will be verified by a smart contract. This smart contract is written in solidity language. The smart contract will compare vehicle ID with registered vehicle IDs. If the vehicle ID is matched then, the message sending vehicle will be an authentic one. Then that message will be encrypted with the (Elliptic Curve Cryptographic) ECC algorithm. The hash value of the message will be saved on the blockchain. Then the encrypted message will be saved on the cloud. Then this message will be forwarded to RSU. RSU will forward the same message to the nearby
vehicle that is part of the network. That particular vehicle forward and broadcast the message to all other vehicles for acknowledgment of the particular event or any emergency condition. The broadcasting vehicle will be chosen based on the following equation (5).

$$\sum_{j=1}^{n} P_j = \text{Number of Adjacent Vehicles}_j + \text{Current Position}_j + \text{Speed of vehicle}_j$$  (5)

where ‘$P_j$’ may be any vehicle in the network that is in the communication range of RSU.

5. Experimental details

The experiment is performed by using a computer machine which consists of window 10 operating system and implementation is carried out by using the NS2 simulator for effective results.

6. Comparative Analysis

This section indicates the different results obtained by considering parameters like end-to-end delay, reliability and packet delivery ratio, etc. By examining this we can able to prove that our results are better than existing results. The proposed system is compared with existing protocols like Position-Based Seamless Connectivity Routing (PB-SCR), Adhoc On-demand Distance Vector (AODV), Reliability Aware Intelligent Data Dissemination (ReIDD), Greedy Perimeter Stateless Routing (GPSR), and Multi-Channel Error Recovery for Video Streaming (MERVS).

![Figure 4: End-To-End delay](image-url)
7. Conclusion and Future work

The proposed system will improve the performance of the VANET network through secure transmission and avoid unauthorized access to a fraudulent vehicle. The hash value stored on the blockchain and other communication messages are stored on the cloud. The hash value of each communication is stored in the form of 256 bits. This system will reduce the overall percentage of road accidents by sequencing communication strategies. This system also improves the overall
reliability, packet delivery ratio, and minimizes the end-to-end delay between two communicating vehicles. Security is the main concern in the VANETs is resolved by using this proposed system. In the future, by implementing some other distributed storage structures and security technologies can be apply to improve the overall mechanism of VANETs system.

References

[1] L.Zhang, C.Hu, Q.Wu, J.Domingo-Ferrer, B.Qin, Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response, IEEE Trans. Comput. 65(8) (2016) 2562-2574.
[2] M.Raya, J.Hubaux, Securing vehicular ad hoc networks, J.Comut. Security. 15(1) (2007) 39-68.
[3] D.Boneh, X.Boyen, H. Shacham, Short group signatures, in: CRYPTO, in: Lect. Notes Comput. Sci., vol.3152,2004, pp.41-55.
[4] L.Zhang, Q.Wu, A.Solanas, J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communication, IEEE Transactions on Veh. Technology.59(4)(2010) 1606-1617.
[5] X. Lin, X.Sun, P.H.Ho, X. Shen, GSIS: a secure and privacy-preserving protocol for vehicular communication, IEEE Transactions on Vehicular Technology 56(6)(2007) 3442-3456.
[6] Shivaprasad More, and Udaykumar Naik,” A Novel Technique in Multihop Environment for Efficient Emergency Message Dissemination and Lossless Video Transmission in VANETS”, Journal of Communications and Information Networks, vol.3, no.4, December 2018.
[7] Shivaprasad More, and Udaykumar L. Naik, "Optimization driven Multipath Routing for the video transmission in the VANET", In proceedings of 2nd IEEE Global Conference on Wireless Computing and Networking (GCWCN), November 2018.
[8] Lei Zhang, MingZing Luo, Jingtao Li, Man Ho Au, Kim-Kwang Raymond Choo, Tong Chen, Shengwein Tian “Blockchain-based secure data sharing system for internet of vehicles: A position paper” https://doi.org/10.1016/j.vehcom.2019.03.003.
[9] Q.Wu, J. Domingo-Ferrer, U. Gonzalez- Nicolas, Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications, IEEE Transactions on Vehicular Technology.59(2)(2010) 559-573.
[10] Zaidi, S., Bitam, S. and Mellouk, A., "Enhanced user datagram protocol for video streaming in VANET," In proceedings of IEEE International Conference on Communications , pp. 1-6, IEEE, May 2017.
[11] Smida, E.B., Fantar, S.G. and Youssef, H., "Video streaming challenges over vehicular ad-hoc networks in smart cities" In proceedings of International Conference on Smart, Monitored and Controlled Cities, pp. 12-16, February 2017.
[12] Hengheng Xie, Azzedine Boukerche, Antonio A.F. Loureiro “MERVS: A Novel Multi-channel Error Recovery Video Streaming Protocol for Vehicle Ad-hoc Networks”, IEEE Transactions on Vehicular Technology, pp 1 – 14, 2015.
[13] Mostafa Asgharpoor Salkuyeh, Bahman Abolhassani, “An Adaptive Multipath Geographic Routing for Video Transmission in Urban VANETs,” IEEE Transactions on Intelligent Transportation Systems, pp 1 – 10, 2016.
[14] AmitDua, Neeraj Kumar, Seema Bawa1,“ReIDD: reliability-aware intelligent data dissemination protocol for broadcast storm problem in vehicular ad hoc networks”, Springer, Telecommunication System, 2016.
[15] Smida, E.B., Fantar, S.G. and Youssef, H., "Video streaming challenges over vehicular ad-hoc networks in smart cities" In proceedings of International Conference on Smart, Monitored and Controlled Cities, pp. 12-16, February 2017.
[16] Toshendra Kumar Sharma, “Top 10 Blockchain Platforms You Need To Know About”, https://www.blockchain-council.org/blockchain/top-10-blockchain-platforms-you-need-to-know-about/, 2019.

[17] “Ethereum”, https://ethereum.org/en/

[18] Bina Ramamurthy, “Blockchain Basics”, online 4 week course, https://www.coursera.org/learn/blockchain-basics

[19] Kaur, H., Alam, M.A., Jameel, R. et al. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J Med Syst* 42, 156 (2018) https://doi.org/10.1007/s10916-018-1007-5

[20] Chen, Y., Ding, S., Xu, Z. et al. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *J Med System* 43, 5 (2019) https://doi.org/10.1007/s10916-018-1121-4

[21] Udaykumar Naik, Vishram N. Bapat “Aspect Ratio of Receiver Node Geometry based Indoor WLAN Propagation Model” J. Inst. Eng. India Ser. B (August 2017) 98(4):369–375, DOI 10.1007/s40031-016-0272-2.

[22] Shivaprasad More, and Udaykumar L. Naik, “Optimal Multipath routing for video transmission in VANETs” Springer, Wireless Personal Communication, ISSN: 0929-6212 (print); 1572-834X (web).