INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN MULTIDISCIPLINARY EDUCATION
ISSN(print): 2833-4515, ISSN(online): 2833-4531
Volume 02 Issue 04 April 2023
DOI: 10.58806/ijirme.2023.v2i4n02
Page No. 143-146

A Blockchain Based Secure Communication in Vehicular Ad Hoc Network

Dhivya K[1], Dr. R Rajesh Kanna[2]
[1]Department of Computer Science, Dr.N.G.P Arts and Science College, Coimbatore
[2]Assistant Professor, Department of Computer Science, CHRIST (Deemed to be University), Bangalore - 560029

ABSTRACT: Efficiency can be a significant drawback in Blockchain technology, especially in resource-constrained environments such as vehicular communication networks. We proposed Adaptive Proof of Driving (APoD) consensus algorithm is designed specifically for Blockchain based Vehicular Communication Networks (VCN) operating in resource-constrained environments. By combining the First Come First Serve (FCFS) and Priority (Reputation) schemes, this algorithm aims to improve the energy and cost efficiency of Blockchain systems in vehicular networks while maintaining a secure and reliable communication environment. Proposed APoD consensus algorithm has the potential to make a significant contribution to the development of secure and reliable communication vehicular environments.

KEYWORDS: Blockchain technology, Consensus vehicular communication, intelligent transportation system

INTRODUCTION

Blockchain technology is used in several fields. Blockchain can trace the possession of real time data and forbidding fraudulence. Blockchain can also revolutionize the IoV communication. Within the next 10 to 20 years, there could be two billion vehicles registered worldwide. In order to increase transportation efficiency and guarantee the safety of both vehicles and drivers, a vehicular ad hoc network (VANET) has been proposed as the basis of an intelligent transportation system (ITS). For effective road traffic control and safety, researchers are focusing on the recent development of information communication technology (ICT), vehicular networks (VN), and their communication architecture. For efficient road traffic and safety, vehicles with advanced communication systems are used. Vehicle to vehicle (V2V), vehicle to road (V2R), and vehicle to infrastructure (V2I) communication types make up the majority of the vehicular ad hoc network (VANET) [1]. VANET uses wireless access in vehicular environments and dedicated short-range communication (DSRC) as its communication methods (WAVE). Designing or creating more effective communication techniques is currently the subject of research. VANET communication, however, faces a number of challenges, including scalability, flexibility, security, and limited programmability [2]. As a result, SDN, a new networking technique, was developed. The ability to separate the control plane from the data plane and control and manage the network in a programmable manner in order to increase network performance is a new technology. Furthermore, the fundamental idea of the SDN separates hardware switches from control logic. In order to effectively use system resources and lengthen the lifespan of networks, SDN's core concept is to address limitations by separating the hardware's operating system and application. SDN divides data plan from control plan using centralised network controllers to flow traffic throughout the entire network [3]. Application programming interfaces (APIs) are provided by the aforementioned technology, SDN, to facilitate new business analysis. SDN offers centralised communication with dynamic control and is efficient, distinctive, adaptable, and programmable. Due to these benefits of the SDN, the researchers combined the SDN and vehicular ad hoc network VANET for efficient vehicle communication. The combined infrastructure is known as "SDVN" [4], [5]. Effective vehicle communication on the road is made possible by SDN. Unwanted behaviors like theft and security can increase when there is less traffic and movement. In order to prevent any danger from occurring to passengers or tourists, the vehicle message must be sent to the monitoring system (i.e., the police) in this case [6].

CONTRIBUTIONS

- To decrease communication delays between vehicles in the vehicular ad hoc network VANET, a novel architecture based on SDVN is proposed in which an edge server is used for local processing rather than cloud computing.
- Edge computing is validated and verified using blockchain in order to offer secure services to moving vehicles. The Blockchain, which is built into the cloud server, registers the edge server by issuing the smart contract to provide secure services to the requesting device when the edge server asks the cloud server to provide a service required by the IoV vehicle.
- To avoid message-related task failure, a message failure fault-tolerance mechanism is also suggested.

RELATED WORK

This section provides a thorough literature review on the vehicular ad hoc network (VANET) model that has been suggested. An advanced communication system for vehicles on the side of the road to exchange information is known as an intelligent transportation system (ITS). Its most sophisticated variety is VANET, which can link thousands of roadside vehicles or wireless nodes. Currently used by intelligent transportation systems, VANET is a type of advanced vehicle ad hoc network.

Pankaj Kumar, Chakshu Goel &Inderjeet Singh Gill[2017][7]To improve the quality of service in VANET architecture, the author proposed a model with safety and non-safety messages. The ability to defend against the various security and privacy attacks that are present in VANETs is essential to the network acquisition and delivery system's success. They employed a variety of protocols, including AODV, Q-Learning, and cryptographic, and their effectiveness was assessed by offering a real-time environment on NS2.

Xia Feng, Kaiping Cui, Haobin Jiang & Ze Li [2022][8] In order to facilitate secure communication in VANET, the author proposed a powerful blockchain-based authentication system (EBAS). By using transactions built using the UTXO model, the entities in this method are able to verify each other. The message's sender's identity is confirmed by the verifier by examining the accuracy of the transaction's single input to ensure its validity. The transaction pseudonym is created to enable users to take part in the authentication process anonymously while maintaining privacy, and it is based on the asymmetric key encryption technique. Furthermore, this approach ensures the scalability of EBAS by putting forth a transaction update mechanism that can maintain data storage and retrieval efficiency at a constant level rather than undergoing near-linear growth. In terms of protecting privacy and fending off frequent VANET attacks, this method is more thorough, according to the security analysis. The simulations regarding the proposed authentication scheme reveal that it outperforms the current schemes with an average computational cost of about 0.942 ms. Moreover, a simulation experiment to assess the authentication overhead and communication delay must be implemented.

Mohiuddin Ahmed, Nour Moustafa, A. F. M. Suaib Akhter & Ahmet Zengin [2022][9]In this paper, a Proof of Concept (PoC) for the EMT protocol using the Ethereum blockchain is presented. In order to demonstrate the effectiveness of the suggested method, performance analyses are presented for both the EMT and GMT. While GMT throughput, PDR, and delay analysis are presented to show the improvements of the proposed method over conventional MAC protocols, performance of the EMT is evaluated according to the computational and storage consumption.

PROPOSED METHODOLOGY

Proposed Proof of Driving (APoD) Methodology

With the help of Blockchain technology, we have created a decentralised distributed reputationbased vehicular communication network (VCN) that fosters trust between vehicles. The new consensus algorithm Adaptive Proof of Driving (APoD), which boosts performance and throughput by lowering miner congestion, is the foundation of the proposed Blockchain technology for vehicular communication. By combining the First Come First Serve (FCFS) and Priority (Reputation) schemes, as shown in steps 1 and 2 of Fig.1.our proposed algorithm provides a secure, reliable, and scalable consensus mechanism for vehicular networks. Lower timestamps and well-known vehicles are given preference in the FCFS scheme's priority system, which maintains the timestamp list using a blockchain server.

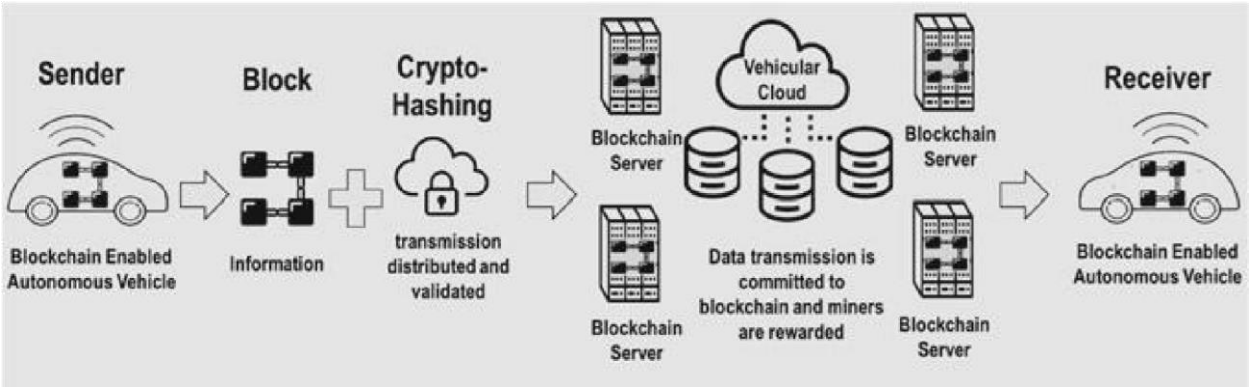

FIG. 1Process of Blockchain based secure vehicular communication networks

Vehicle Reputation Point (VRP), a cryptographic ID that has been issued specifically for each vehicle and is used to enable the flow of reputation points, which serve as a reputation value for vehicles to participate in information exchange between vehicles, has been introduced to validate the reputed vehicles. We are utilising blockchain technology in the intelligent transportation system (ITS), which stores all VRP information for each vehicle and is accessible by all vehicles, for the management of VRP data [10].

Proof of Driving (APoD) Consensus Algorithm

We suggest an Adaptive Proof of Driving (APoD) consensus algorithm that employs First Come First Serve (FCFS) and Priority to reduce miner congestion and boost performance.

First Come and First Serve (FCFS): First Come and First Scheme makes use of timestamps to lessen miner traffic in the vehicular communication network. Vehicle Vi is added to the miner list as it has a lower timestamp if its timestamp ti is less than that of vehicle Vj's timestamp tj.

Priority scheme: In this priority scheme, the blockchain server is maintaining a miner list that is based on the Vehicular Reputation Points (VRP) of each vehicle. The higher the VRP of a vehicle, the higher priority it will be given in the miner list. Furthermore, vehicles that have higher VRP are considered more trustworthy and are incentivized with additional VRP. Specifically, if a vehicle with higher VRP receives a broadcasted message, it is considered trusted and is awarded some reward points. Overall, this priority scheme aims to encourage good behavior and incentivize trustworthiness among vehicles in the network by rewarding those with higher VRP.

Pseudocode of APoD Consensus Scheme

For timeline &size instant ts
If (Vi (t_s)) < (Vj (t_t))
Minerlist ← V_m return Minerlist
Priority(Miner list (VRP))
For Vehicular Reputation Points VRP
If (V RP[V_m]) >(V RP[V_n])
V RP[V_m]← V RP[V_n] + Reward Points return V RP[V_m] else V RP[V_n] ← V RP[V_n] + Reward Points return V RP[V_n]

Intelligent Vehicle Communication Use Case Scenario

There are two schemes used by the APoD algorithm

First Come First Serve (FCFS): The FCFS scheme ensures that vehicles are allowed to cross the intersection in the order in which they arrive, which is a fair and simple approach.

The Priority scheme: it enables certain vehicles to be given priority over others based on specific criteria, such as emergency vehicles or vehicles carrying passengers with urgent medical needs. This approach can be particularly useful in situations where time is of the essence.

Overall, our proposed APoD algorithm appears to be a promising solution for managing traffic flow at intersections in a way that is energy-efficient, cost-efficient, and reliable.

CONCLUSION

Proposed Adaptive Proof of Driving (APoD) consensus algorithm for Blockchain-based Vehicular Communication Networks (VCN). This algorithm combines two schemes, First Come First Serve (FCFS) and Priority (Reputation), to provide a secure and reliable consensus mechanism for vehicular networks. The use of the FCFS scheme and Priority scheme seems like a sensible approach to manage the flow of vehicles in a fair and efficient manner. Vehicle Reputation Points (VRP) are used to enable the flow of reputation points, which serve as a reputation value for vehicles to participate in the information exchange between vehicles. VRPs were introduced to validate the reputed vehicles and are issued as unique cryptographic IDs for each vehicle. In the future, we will use simulations and actual experiments to put our consensus algorithm for Blockchain-based secure decentralised reliable vehicular communication networks into practice.

REFERENCES

1) Shin, M.K.; Nam, K.H.; Kim, H.J. Software-defined networking (SDN):"A reference architecture and open APIs" In Proceedings of the IEEE 2012 International Conference on ICT Convergence (ICTC), Jeju Island, Korea, 15–17 October 2012.
2) D. Kreutz, F. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, ''Software-defined networking: A comprehensive survey,'' Proc. IEEE, Jan. 2015.
3) S. Singh and S. Agrawal, ''VANET routing protocols: Issues and challenges,'' in Proc. Recent Adv. Eng. Comput. Sci. (RAECS), Mar. 2014,
4) E. Borcoci, ''From vehicular ad-hoc networks to Internet of Vehicles,'' in *Proc. NexComm Conf.*, Venice, Italy, 2017
5) M. O. Kalinin, V. Krundyshev, and P. Semianov, ''Architectures for build- ing secure vehicular networks based on SDN technology,'' *Autom. Control Comput. Sci.*, vol. 51, no. 8, pp. 907–914, Dec. 2017.

6) W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, ''ComplementingIoT services through software defined networking and edge computing: A comprehensive survey,'' *IEEE Commun. Surveys Tuts*Quart., 2020.
7) P. Kumar, C. Goel, and I. S. Gill, ''Performance evaluation of network aggregation techniques in VANET,'' *IJIREEICE*, Jan. 2017
8) Xia Feng, Kaiping Cui, Haobin Jiang & Ze Li "EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network" https://doi.org/10.3390/sym14061230, 2022
9) Mohiuddin Ahmed, Nour Moustafa, A. F. M. Suaib Akhter & Ahmet Zengin," A Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET" IEEE TRANSACTIONS, 2022, Doi:10.1109/TITS.2021.3115245
10) M. Singh, S. Kim, Branch based blockchain technology in intelligent vehicle. Comput. Netw. (2018). ISSN 1389-1286. https://doi.org/10.1016/j.comnet.2018.08.016
11) M. Singh, S. Kim, Crypto trust point (cTp) for secure data sharing among intelligent vehicles,in *The 2018 International Conference on Electronics, Information and Communication (ICEIC2018)*, Sheraton Waikiki Hotel, Honolulu, Hawaii, USA, 24–27 Jan 2018. https://ieeexplore.ieee.org/document/8330663/
12) B. Leiding, P. Memarmoshrefi, D. Hogrefe, Self-managed and blockchain-based vehicular adhocnetworks, in *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2016, pp. 137–140. https://dl.acm.org/citation.cfm?id=2971409
13) S. Kim, Blockchain for a trust network among intelligent vehicles. Adv. Comput (2018).ISSN0065-2456. https://www.sciencedirect.com/science/article/pii/S0065245818300238