BLOCKCHAIN-BASED TRUST MANAGEMENT MODEL FOR LOCATION PRIVACY PRESERVING IN VANET

DR. KARTHICK, M. (Assistant Professor)

AND

SATHISH KUMAR, P. (PG Scholar)
Department of Computer Science & Engineering,
Nandha College of Technology, Erode-52
Vailkaalmedu, Tamil Nadu 638052,
India

ABSTRACT

The intelligent traffic system (ITS) relies heavily on the vehicle ad hoc network (VANET), a distinct mobile ad hoc network (MANET). When we take advantage of the convenience provided by the location-based service (LBS), the security issues have not been sufficiently resolved due to the high mobility of VANETs. To preserve location privacy, we present a trust management model that is based on the blockchain. Vehicles can use the scheme to request LBS without disclosing any personal information by using a certificate. In order to guarantee the privacy and security of vehicles, we construct an anonymous cloaking region. To control and standardize the behavior of vehicles, we propose a trust management algorithm and use blockchain to implement vehicle data security. To test the hypotheses, we use a variety of data sets. Experiments and security analysis reveal that the system is resistant to a variety of trust model attacks, allowing vehicles' privacy and security to be better protected. The results of the simulations show that the proposed system can be used to collect

KEYWORDS: Blockchain-Based Trust Management Model, Location Privacy and Vanet

INTRODUCTION

VANET is a low-cost, self-organized, and simple-to-implement inter-vehicle communication network. On-board computing and communication technology have made it possible for vehicle networking to enter a rapid development phase in recent years. The vehicle and the traffic infrastructure together make up the vehicle network in vehicle networking. Through wireless communication technology, the vehicle's onboard equipment gathers dynamic information from other vehicles and infrastructure, such as the state of the road ahead, regardless of traffic congestion (Pokhrel & Choi, 2020). The vehicle node is able to assess the state of the road flow and plan the best driving route by collecting and analyzing the data. This improves transportation safety and efficiency. Taking the LBS as an illustration, VANETs are susceptible to attacks by external attackers in the LBS. The issue of trust and security between internal vehicles remains unresolved, despite the fact that some studies have designed secure communication channels to prevent attacks from the outside (Baza, Nabil, Lasla, Fidan, Mahmoud, and Abdallah, 2019; Shrestha, Nam, Bajracharya, & Kim, 2020). The malicious vehicles may make use of the high mobility of VANETs to gather and investigate sensitive vehicle data, inferring personal privacy such as driving patterns and activities performed. We

believe that a privacy-preserving VANET model should safeguard personal information security as well as users' data security. One of the most popular privacy-preserving algorithms is the K-anonymous algorithm, which has accurate query results and a low computational overhead. So, it can effectively stop personal information from being shared. The K-anonymous privacy-preserving scheme can be broken down into two groups: distributed and centralized [4]. The first has a reliable, anonymous central server that can safeguard user data security. However, there are performance bottlenecks and single-point failures. The latter resolves the performance issue, but users lack mutual trust. In order to address the trust crisis, we use the distributed k-anonymous algorithm and introduce trust management. With high mobility, vehicles can start LBS queries across a large geographic area. It is difficult to establish a reliable central server that can save and promptly update the historical trust information for all vehicles due to performance limitations. To address this issue, a decentralized trust management system is required. In addition, we hope that the trust information recorded by the system is tamper-resistant and consistent with the data. Blockchain is a decentralized data storage technology like that. The information regarding LBS queries and trust values can be publicly verified and traced thanks to the blockchain's role as an immutable ledger. Additionally, the blockchain's consensus mechanism contributes to vehicle trust. Therefore, we use blockchain to safeguard vehicle privacy. This paper's contribution is as follows: 1) In order to prevent real information from getting out, we use a digital certificate as a fake name when we communicate. The blockchain is used by the certificate authority to record users' real information and issue certificates. This safeguards users' privacy while maintaining the ability to locate malicious users. 2) To create an anonymous cloaking region, we present an RSU-dominant algorithm. In order to safeguard the privacy and security of vehicles, it reduces the computing load and allows direct vehicle communication. (3) To record trust information using blockchain and optimize the distributed k-anonymous algorithm, we present trust management. Our method, as demonstrated by experiments, is highly resistant to traditional trust attacks. The following is the structure of the remainder of this paper: We present related works on VANET trust management models and k-anonymity schemes in Section II. The system's architecture and the problem's definition are presented in Section III. Section IV offers a detailed plan for our trust management model, including the privacy-preserving algorithm and trust management strategies. The system analysis and experimental results are presented in Sections V and VI, respectively. In this section, we present our conclusion and future work.

LITERATURE SURVEY

Federated Learning with Blockchain for Autonomous Vehicles: Analysis and Design Challenges

This system was proposed by Shiva Raj Pokhrel et al. We propose an autonomous blockchain-based federated learning (BFL) design for efficient and privacy-aware vehicular communication networking. In this design, local on-vehicle machine learning (oVML) model updates are distributed, exchanged, and verified. Utilizing the consensus mechanism of the blockchain, BFL makes it possible to implement oVML without the need for centralized training data or coordination. We develop a mathematical framework that takes a renewal reward approach and includes the controllable network and BFL parameters (like the retransmission limit, block size, block arrival rate, and frame sizes) to show how they affect system-level performance. More

importantly, the end-to-end delay is quantified with BFL by our thorough analysis of the dynamics of the oVML system. This provides important insights into how to determine the optimal block arrival rate by taking into account communication and consensus delays. Numerous non-trivial findings and insights for adaptive BFL design are highlighted by our numerical and simulation findings. Specifically, we show that the proposed idea of tuning the block arrival rate is able to drive the system dynamics to the desired operating point and minimize the system delay by exploiting channel dynamics based on analytical results. For a given set of channel conditions, retransmission limits, and frame sizes, it also identifies the improved dependence on other blockchain parameters. 1 However, a number of challenges—knowledge gaps—must be filled before these changes can be realized. In particular, we provide potential research directions and key bottleneck challenges that call for additional investigation (Ayvaz and Cetin, 2019).

Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles

This system was proposed by Mohamed Baza et al. Recently, autonomous vehicles (AVs) have received a lot of attention from industry and academia. As a complicated system with a lot of subsystems, antivirus software is a common target for hackers. As a result, the manufacturer needs to bring the firmware of the various subsystems up to date so that bugs can be fixed and new features can be added, such as by using security patches. Using blockchain and smart contract technology, we propose a distributed firmware update scheme for the AVs' subsystems in this paper. To guarantee the authenticity and integrity of firmware updates, a consortium blockchain created by various AV manufacturers is utilized. We enable AVs, or distributors, to participate in the distribution process rather than relying on centralized third parties, and we take advantage of their mobility to guarantee high availability and quick delivery of the updates. A reward system that maintains a credit reputation for each distributor account in the blockchain is established to encourage AVs to distribute the updates. In a trustless environment, the update is exchanged for a proof of distribution using a zero-knowledge proof protocol. In addition, we make use of an attribute-based encryption (ABE) scheme to guarantee that only authorized antivirus programs will be permitted to download and utilize a new update. According to our investigation, neither the exchanged transactions nor the additional cryptography primitives have any effect on how the AVs network functions. Additionally, our security analysis demonstrates that our plan is secure and effective against a variety of attacks.

Evolution of V2X Communication and Integration of Blockchain for Security Enhancements

This system has been proposed by Rakesh Shrestha and co.: Intelligent and self-driving vehicles will soon be on the market thanks to the rapid advancements in wireless communications and autonomous vehicles. In vehicular networks, Vehicle-to-Everything (V2X) communications offer driving safety, traffic efficiency, and road information in real time. By incorporating cellular 5G and New Radio (NR) access technology into V2X communications (i.e., 5G NR V2X), V2X has developed. It is able to meet the ever-changing requirements of connected vehicles for vehicular applications, communication, and services, such as extremely low latency, extremely high bandwidth, extremely high reliability, and security. However, deployment and management are experiencing a backlash as a result of scalability, inadequate security, and a lack of

flexibility in response to the growing number of intelligent and autonomous vehicles and the safety requirements associated with them. Reduced scalability and flexibility are achieved by bringing cloud services closer to vehicular nodes through multi-access edge computing (MEC). Additionally, blockchain has developed into a useful technology enabler for resolving a number of security, privacy, and networking issues that the current 5G-based MEC systems in vehicular networks face. In addition to MEC, blockchain can be incorporated as a robust security mechanism for managing and securing 5G V2X. The state-of-the-art V2X and its development on the basis of cellular 5G and non-cellular 802.11bd technology are the subject of an in-depth discussion in this survey. For the purposes of content caching, security, and privacy, we investigate the incorporation of blockchain into 5G-based MEC vehicular networks. After outlining the issues and obstacles that are currently present in edge computing and 5G V2X, we also shed some light on possible future research directions for these integrated and newly developed technologies.

Intelligent Resource Allocation for Video Analytics in Blockchain-Enabled Internet of Autonomous Vehicles with Edge Computing

This system was suggested by Xiantao Jiang et al. Video surveillance in intelligent transportation systems (ITS) is growing quickly, and video analytics could help make the Internet of Autonomous Vehicles (IoAV) safer. However, vehicular networks face an enormous burden due to the massive amount of video data that must be transmitted and the computationally intensive video analytics. In addition, the video data is not always reliable because of the unstable network connection, making data sharing in IoAV unsecure and unscalable. In order to improve the blockchain system's transaction throughput and decrease the MEC system's latency, we first propose a video analytics framework that incorporates both blockchain and multi-access edge computing (MEC) technologies. In addition, the asynchronous advantage actor-critic (A3C) algorithm is used to solve the joint optimization problem, which is modeled as a Markov decision process (MDP) using deep reinforcement learning. The results of our simulations show that our method can significantly boost the performance of blockchain-enabled IoAV with MEC through rapid convergence.

Witness of Things Blockchain-based distributed decision record-keeping system for autonomous vehicle

This system has been suggested by Serkan Ayvaz et al. Purpose: The goal of this paper is to create a model for self-driving cars to establish trusted parties by combining distributed ledgers and self-driving cars in traffic to provide a single version of the truth and thus build public trust. Design, methodology, and approach: The model, which the authors call Witness of Things, relies on vehicular networks and vehicle-to-vehicle/vehicle-to-infrastructure (or vice versa) communications to store autonomous vehicle decision logs in distributed ledgers. The model provides a single version of the truth, making it easier for the autonomous vehicle industry, organizations related to it, and government agencies to determine the true causes of road accidents and the consequences of those accidents in investigations. Results: In this paper, the authors looked into one way that the blockchain protocol could affect autonomous vehicles. The framework offers a means of operating autonomous vehicles without the need for a central authority in an unreliable setting. Additionally, the model can be extended to include other intelligent unmanned systems. Originality and value: A blockchain

protocol-based record-keeping model is proposed in this study for autonomous cars to protect a single version of the truth and establish trustworthy parties in traffic. Keywords: blockchain, autonomous driving and communication, self-driving cars, autonomous cars, and vehicular communication networks.

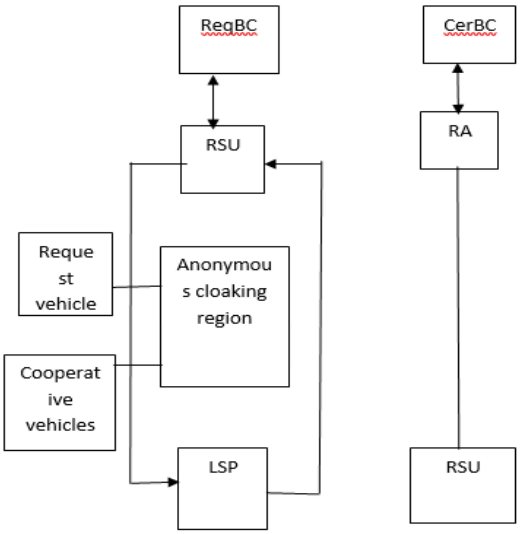
EXISTING SYSTEM

The technology that underpins many real-time applications and their data is called blockchain. Distributed ledger technology's potential for use in autonomous vehicles or systems and for enhancing products, customer satisfaction, and other valuable experiences is one area in which automakers are eager to accept its benefits. Autonomous Electric Vehicles (AEV), Autonomous Underwater Vehicles (AUV), Autonomous Guided Vehicles (AGV), Autonomous Aerial Vehicles (AAeV), and Autonomous Driving are all topics that will be examined in this research. A comparative analysis of blockchain-integrated autonomous vehicle systems is examined in this work to identify current and future obstacles. The uses and significance of sensors, architectures and infrastructure requirements, vehicle types, driving modes, strategies for targeting and tracking vehicles, intelligent contracts, intelligent data handling, and industry-specific use cases are also investigated. The investigation of the most recent methods and technologies forms the basis of this study. This paper examines recent advancements in autonomous vehicles and systems, as well as the ways in which blockchain can assist in enhancing user experiences and enhancing industry practices, in light of the expectation that autonomous vehicles will be the intelligent transportation of the future. Finally, the issues and limitations of various autonomous vehicles and systems, as well as directions for future research, are discussed.

PROPOSED SYSTEM

A traffic management system that makes use of the communication between vehicles to improve traffic flow and reduce congestion is one example of a proposed system that makes use of VANET. A central traffic management system and other vehicles can share information about their location, speed, and traffic conditions with vehicles equipped with communication devices. After that, this system is able to make use of this data to improve traffic flow, provide drivers with real-time traffic updates, and even reroute vehicles to avoid congestion. Blockchain can be used in VANETs to manage trust and privacy among vehicles in a secure and decentralized manner. A system based on the blockchain, for instance, can be used to verify the identity of vehicles and ensure that only authorized vehicles have access to certain services and information. Additionally, due to its decentralized nature, blockchain can offer a tamper-proof method for storing and exchanging data, assisting in the prevention of attacks, and guaranteeing the privacy of location data. This is especially useful in situations like autonomous vehicles and emergency services, where secure and dependable communication is essential.

ARCHITECTURE DIAGRAM



ROAD SIDE UNIT

A roadside unit (RSU) is a module in a blockchain-based autonomous vehicle system that communicates with vehicles to provide real-time traffic data, safety warnings, and other information. The RSU uses blockchain technology to securely record and verify data related to traffic flow and vehicle behavior, allowing for more efficient and safe transportation.

CERTIFICATE AUTHORITY

A certificate authority (CA) module is a trusted entity that issues digital certificates to authenticate the identity of vehicles and other network participants. These certificates are used to secure communication and transactions between vehicles and other components of the system. The CA is responsible for verifying the authenticity of the certificates and ensuring that they are not compromised. In some cases, the CA may also be responsible for revoking certificates if they are no longer valid.

BLOCKCHAIN

Blockchain can help secure the communication and data exchange between autonomous vehicles and infrastructure by creating an immutable record of all transactions and communications, making it more difficult for hackers to breach the system.

VEHICLE SENDER

A node or device on the network that is responsible for sending data or transactions to other nodes or devices. This can include data about the vehicle's location, speed, and other relevant information, as well as requests for information or transactions with other nodes or devices on the network. The blockchain technology allows for secure and transparent communication and transaction recording between the vehicle sender and other nodes, ensuring that all data is properly authenticated, validated, and recorded on the distributed ledger.

VEHICLE RECEIVER

The vehicle receiver uses blockchain technology to securely and transparently receive and process this information, ensuring that all data is properly authenticated, validated, and recorded on the distributed ledger. The receiver may also use the data received from other nodes to make informed decisions about vehicle operations, such as route planning, speed adjustments, or other actions.

CONCLUSION

A trust model for location privacy protection based on the blockchain is proposed in this paper. In this model, the vehicle requesting the location sends a location query to a nearby RSU, which is in charge of collecting collaborative vehicles to create anonymous hidden areas. The query result is then delivered to the vehicle that requested it. This paper uses a pseudonym for the certificate in order to reduce the likelihood of privacy disclosure and prevent vehicles from communicating directly with one another. Additionally, anonymous camouflage zones safeguard vehicle privacy from LSP. The consensus mechanism for the blockchain is a thermal reactor in our plan. It uses fewer resources and performs computations more efficiently than PoX. Finally, an algorithm for trust management is proposed, and its effectiveness is demonstrated through experiments. In general, incentive models with trust incentives and token incentives are used in general trust models. In addition, this paper does not discuss token incentives. The trust incentive model works well to stop malicious vehicles from doing bad things, but we need a token incentive to get honest vehicles to do good things. In future work, we will combine two incentive models to create a trust model that is better.

REFERENCES

Ayvaz, S. & Cetin, S. (2019). *Witness of Things*. Distributed decision-making and record-keeping system for autonomous vehicles based on blockchain technology, Intell. J. Automated System, 7(2) Pp. 72–87.

Baza, M., Nabil, M., Lasla, N., Fidan, K., Mahmoud, M. & Abdallah, M. (2019). *Blockchain-based firmware update scheme tailored for autonomous vehicles*, in Proc. Wireless Communication, IEEE Netw. Conf. (WCNC), pages in April 2019, 1–7.

Pokhrel, S. & Choi, J. (2020). *Federated learning with blockchain for autonomous vehicles*: by Problems with analysis and design, IEEE Trans. Commun., 68(8), Pp. 4734–4746.

Shrestha, R., Nam, S., Bajracharya, R. & Kim, S. (2020). *Evolution of V2X communication and integration of blockchain for security enhancements* Electronics, 9(9) Pp. 1338.

Xiantao Jiang, X., Richard, F., Song, T. & Victor, C. (2022). Intelligent resource allocation for video analytics in blockchain-enabled internet of autonomous vehicles with edge computing, *IEEE Internet Things Journal.*