Trust Management Model for Secure Internet of Vehicles

Subjects: Computer Science, Information Systems

Contributor: Wenbo Ruan , Jia Liu , Yuanfang Chen , Sardar M. N. Islam , Muhammad Alam

The Internet of Vehicles (IoV) enables vehicles to share data that help vehicles perceive the surrounding environment. However, vehicles can spread false information to other IoV nodes; this incorrect information misleads vehicles and causes confusion in traffic, therefore, a vehicular trust model is needed to check the trustworthiness of the message.

Internet of Vehicles blockchain trust management

1. Introduction

With the popularity of 5G and 6G [1] and the application of programmable V2X environments and blockchain-based V2X (vehicle to everything) technologies [2], the IoV has embraced rapid development. In IoV, vehicles can share their perceived information with other nodes, including traffic safety information, weather information, road information, etc., and obtain services from other nodes [3], thus, improving traffic safety and efficiency.

However, vehicles can be unreliable, and we need to solve the problems of how to evaluate the reliability of the message sent by the vehicle and quantify an evaluation measure [4] (i.e., trust value) based on the historical behavior of the vehicle before utilizing IoV. For example, in IoV, vehicles may be controlled by attackers to spread false information for selfish reasons, thus, leading to false environmental perception and driving decision-making and thus, endangering the safety of drivers and causing serious traffic accidents [5].

In IoV, the basic principle behind the trust model is to ensure the reliable transmission of data by identifying and canceling malicious vehicles and the false news generated by them [6]. The trust management mechanism can help vehicles calculate the credibility of received messages [7] to improve the accuracy of vehicles in decision-making. In summary, the existing trust management mechanisms can be generally divided into centralized trust management and distributed trust management [8]. Centralized trust management has problems such as single points of failure, while distributed trust management has problems such as the delayed update of trust value.

Blockchain, as bitcoin's core technology, is a distributed ledger [9]. Due to its decentralized and immutable characteristics, blockchain can record and update vehicles' trust values. With blockchain, even if a small number of RSUs have storage errors or are controlled by attackers, the consensus results of the entire network can still be protected. Therefore, some researchers combine blockchain with trust management mechanisms to solve the above problems of centralized and distributed trust management.

However, there are still some problems in the research of trust management mechanisms based on the blockchain or single-layer blockchain. First of all, the vehicles need to store a complete blockchain ledger or send a request to the adjacent full node for verification every time the transaction is verified, which will undoubtedly increase the burden of the vehicle and waste the vehicle's resources. Secondly, because the number of blockchain nodes is very large and the coverage is active and wide, it is also difficult to conduct hierarchical management according to objective factors such as geographical location, communication traffic, and node density. Finally, because the importance of vehicle data is not the same, the data storage and data sharing between vehicles and RSUs is inefficient if the system does not distinguish the importance of messages. Therefore, how to enable the system to store and share data of different levels of importance is a problem.

2. Trust Management Model in IoV

2.1 Centralized Trust Management

Mahmoud et al. [10] adopted an incentive and punishment strategy (TRIPO) to prevent intentional packet loss attacks in rational cases and unintentional packet loss attacks in irrational cases. TRIPO uses small payments to reward rational nodes that correctly forward packets from other nodes. For irrational nodes, TRIPO uses a reputation system to measure, i.e., a new monitoring technique to monitor the nodes. However, all of these operations are centralized in the offline trusted party. Based on the malicious behavior detection system running on vehicles and RSUs, Bißmeyer et al. [11] proposed a centralized trust management model, which uses the malicious behavior report to establish trust relationships and reach the goal of identifying and removing attackers in IoV. Li et al. [12] proposed a reputable ad hoc network announcement scheme that consists of a centralized reputation server, access point (physical wireless communication equipment), and vehicle. The centralized reputation server's role is to collect and aggregate feedback to generate reputation and spread reputation. The access point acts as the communication interface between the vehicle and the reputation server, and the vehicle broadcasts and receives information from neighboring vehicles. The credibility of the received information is evaluated and then reported to the reputation server.

2.2 Distributed Trust Management

Huang et al. [13] proposed a distributed reputation management system (DREAMS), in which basic reputation management tasks are performed by local authorities (LA) in different locations. LA acts as the trusted authority and arranges the vehicle edge computing server for local reputation display and updates. Oluoch et al. [14] also proposed a reputation model to help vehicles in the network evaluate the reliability of other vehicles, that is, each receiving vehicle requests other vehicles within its communication range to give reliability to the sending vehicle, or the receiving vehicle obtains the corresponding results from the RSU. Raya et al. [15] proposed a data-centric trust management model, which calculates the trust of each data, aggregates multiple related but possibly contradictory data, and finally obtains the final trust value.

2.3 Combination of Blockchain and Trust Management

Yang et al. [16] proposed a decentralized trust management model for IoV based on blockchain technology. The receiving vehicle uses Bayesian inference to verify the results for the messages received from adjacent vehicles. Then according to this result, the receiving vehicle generates scores for each vehicle sending messages and uploads them to the nearby RSU, which is responsible for calculating the variation of trust value of each vehicle according to the scores and packaging these data into a “block”. RSUs compete to become miners using the POW Consensus algorithm. Zhang et al. [17] proposed a trust management system for the IoV based on blockchain, which solves the problem of calculating message credibility. Moreover, this system can detect vehicles sending malicious messages and reduce their credit value according to the rating mechanism. In addition, a combination of the consensus mechanisms of PoW and PoS is used to ensure that vehicles with significant changes in reputation can be updated to the blockchain more quickly. Kang et al. [18] proposed a credit-based data sharing scheme, which considers the three weights of interaction frequency, event timeliness, and trajectory similarity, adopting the three-weight subjective logic (TWSL) model to select more reliable data sources and improve data credibility. In addition, the alliance blockchain is utilized to establish a secure and distributed vehicle blockchain and smart contracts are deployed on the vehicle blockchain to realize safe and efficient data storage of RSUs and data sharing among vehicles.

2.4. Combination of Double-Layer Blockchain and Trust Management

Lee et al [19] proposed a two-layer blockchain trust management model for the Internet of Vehicles, which is composed of the local one-day message blockchain and the global vehicle reputation blockchain. The data in the global vehicle reputation blockchain are generated by RSUs located in different regions, which consist of the vehicle’s reputation score based on the vehicle’s historical behavior. Therefore, each vehicle’s reputation is updated and permanently stored in the global vehicle reputation blockchain for further query. In the local one-day message blockchain, vehicles and RSUs store and share local traffic information in a short period of time. RSUs and vehicles in the same region act as blockchain nodes. This blockchain creates a new block at a set time every day and deletes the previously recorded blockchain data. Kandah et al [20] also proposed a two-layer blockchain trust management model composed of platoon blockchain and global blockchain. The participating nodes of a platoon blockchain are a group of vehicles with a small gap in proximity and speed. They store the localized trust consensus (trust value of vehicles), while the global blockchain stores the trust factors of all vehicles in the system, that is, the data in the platoon blockchain is added to the global blockchain through mining. In the mining stage, RSU mines the block using the trust bidding system.

References

1. Vaezi, M.; Azari, A.; Khosravirad, S.R.; Shirvanimoghaddam, M.; Azari, M.M.; Chasaki, D.; Popovski, P. Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G. IEEE Commun. Surv. Tutor. 2022, 24, 1117–1174.

2. Noor-A-Rahim, M.; Liu, Z.; Lee, H.; Khyam, M.O.; He, J.; Pesch, D.; Moessner, K.; Saad, W.; Poor, H.V. 6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities. Proc. IEEE 2022, 110, 712–734.
3. Mohanty, S.K.; Tripathy, S. SIoVChain: Time-Lock Contract Based Privacy-Preserving Data Sharing in SIoV. IEEE Trans. Intell. Transp. Syst. 2022, 23, 24071–24082.
4. Ahmad, F.; Kurugollu, F.; Kerrache, C.A.; Sezer, S.; Liu, L. Notrino: A novel hybrid trust management scheme for internet-of-vehicles. IEEE Trans. Veh. Technol. 2021, 70, 9244–9257.
5. Tian, Z.; Gao, X.; Su, S.; Qiu, J. Vcash: A novel reputation framework for identifying denial of traffic service in internet of connected vehicles. IEEE Internet Things J. 2019, 7, 3901–3909.
6. Mahmood, A.; Sheng, Q.Z.; Siddiqui, S.A.; Sagar, S.; Zhang, W.E.; Suzuki, H.; Ni, W. When trust meets the internet of vehicles: Opportunities, challenges, and future prospects. In Proceedings of the 2021 IEEE 7th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 13–15 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 60–67.
7. Yang, Z.; Wang, R.; Wu, D.; Yang, B.; Zhang, P. Blockchain-enabled trust management model for the Internet of Vehicles. IEEE Internet Things J. 2021. Early Access.
8. Singh, P.K.; Singh, R.; Nandi, S.K.; Ghafoor, K.Z.; Rawat, D.B.; Nandi, S. Blockchain-based adaptive trust management in internet of vehicles using smart contract. IEEE Trans. Intell. Transp. Syst. 2020, 22, 3616–3630.
9. Misra, N.; Dixit, Y.; Al-Mallahi, A.; Bhullar, M.S.; Upadhyay, R.; Martynenko, A. IoT, big data, and artificial intelligence in agriculture and food industry. IEEE Internet Things J. 2020, 9, 6305–6324.
10. M. E. Mahmoud and X. Shen An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks. *IEEE Transactions on Vehicular Technology* **2011**, *60*, 8.
11. Bißmeyer, N.; Njeukam, J.; Petit, J.; Bayarou, K.M Central misbehavior evaluation for vanets based on mobility data plausibility. *In Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications, Low Wood Bay Lake District* **2012**, *73*, 82.
12. Li, Q.; Malip, A.; Martin, K.M.; Ng, S.L.; Zhang, J A Reputation-Based Announcement Scheme for VANETs. *IEEE Transactions on Vehicular Technology* **2012**, *61*, 9.
13. Huang, X.; Yu, R.; Kang, J.; Zhang, Y Distributed reputation management for secure and efficient vehicular edge computing and networks. *IEEE Access* **2017**, *5*, 25408 - 25420.
14. Oluoch, J A distributed reputation scheme for situation awareness in vehicular ad hoc networks (VANETs). *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)* **2016**, *1*, 1.

15. Raya, M On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications* **2008**, *0*, 0.
16. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C Blockchain-Based Decentralized Trust Management in Vehicular Networks. *IEEE Internet of Things Journal* **2018**, *6*, 1495 - 1505.
17. Zhang, H.; Liu, J.; Zhao, H.; Wang, P.; Kato, N Blockchain-Based Trust Management for Internet of Vehicles. *IEEE Transactions on Emerging Topics in Computing* **2020**, *9*, 1397 - 1409.
18. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal* **2018**, *6*, 4660 - 4670.
19. Lee, S.; Seo, S.H Design of a Two Layered Blockchain-Based Reputation System in Vehicular Networks. *IEEE Transactions on Vehicular Technology* **2021**, *71*, 1209 - 1223.
20. Kandah, F.; Huber, B.; Skjellum, A.; Altarawneh, A A Blockchain-based Trust Management Approach for Connected Autonomous Vehicles in Smart Cities. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* **2019**, *0*, 0.