Obstacle Detection and Mapping in Vehicle-to-Vehicle Networks

Subjects: Computer Science, Hardware & Architecture
Contributor: Rubén Juárez, Borja Bordel

Vehicle-to-Vehicle (V2V) networks, specifically Vehicular Ad Hoc Networks (VANETs), are central to enhancing road safety by improving vehicle visibility, particularly when traditional onboard sensors fall short. The crucial role that VANETs play in modern transportation systems is increasingly being recognized, with the ability to facilitate real-time communication between vehicles, improving situational awareness, and thereby enhancing road safety. However, the accuracy, integrity and security of these data are of paramount importance, as any inaccuracies or compromises could lead to incorrect hazard perception and possibly catastrophic consequences. Hence, substantial effort is required to maintain these data characteristics while enabling efficient and rapid data exchange.

Keywords: VANET ; security

1. Introduction

In a digitally evolving world, the role of vehicles as communicators within the technological matrix has given rise to Vehicle-to-Everything (V2X) communications. This new communication paradigm, among other innovations, has birthed the Internet of Vehicles, which enables data exchange among vehicles, infrastructure, and the environment [1]. In fact, data exchange among vehicles is the most relevant and promising technology. Therefore, it receives a specific name: Vehicle-to-Vehicle (V2V) communications. Different authors [2] proposed that V2V communication will be essential to improve road safety and traffic efficiency.

V2V communications cannot create fixed networks (as vehicles are mobile) but rather ad hoc networks whose structure evolves dynamically according to the vehicles' movement. Specifically, Vehicular Ad Hoc Networks (VANETs) and related systems, similar to Mobile Ad Hoc Networks (MANETs), consist of vehicles, Roadside Units (RSUs), and a Trusted Authority (TA) acting as mobile nodes [1] and exchanging data about traffic, each vehicle's status, etc. These networks, among other advantages, enhance autonomous vehicle decision making by providing environmental data for proactive hazard measures [3].

2. Obstacle Detection and Mapping in Vehicle-to-Vehicle Networks

Vehicle-to-Vehicle (V2V) networks, specifically Vehicular Ad Hoc Networks (VANETs), are central to enhancing road safety by improving vehicle visibility, particularly when traditional onboard sensors fall short [4][5]. The crucial role that VANETs play in modern transportation systems is increasingly being recognized, with the ability to facilitate real-time communication between vehicles, improving situational awareness, and thereby enhancing road safety [6]. These networks are fundamentally built upon the exchange of obstacle map data, providing valuable information about potential road hazards, enabling advanced warning systems, and fostering overall safer driving conditions. However, the accuracy, integrity and security of these data are of paramount importance, as any inaccuracies or compromises could lead to incorrect hazard perception and possibly catastrophic consequences [7][8]. Hence, substantial effort is required to maintain these data characteristics while enabling efficient and rapid data exchange [9].

The investigation of obstacle detection for vehicles has a rich history, dating back to the 1980s and 1990s, before the advent of autonomous driving technology [10][11]. Initial techniques focused primarily on obstacle detection to avoid collisions, often neglecting the crucial aspect of data exchange between vehicles. However, technological advances have reshaped this domain. High-resolution cameras and sophisticated sensors such as LIDAR have elevated detection methods, considerably enhancing their reliability and accuracy [12][13]. Consequently, evolved detection methods provide a more comprehensive understanding of the driving environment, contributing significantly to reducing collision incidents [1].

Despite these advances, challenges remain to secure an efficient exchange of obstacle data, which is crucial for the comprehensive functionality of V2V networks. Thus, blockchain technology, known for its security and the decentralization advantages, has seen its application in the V2V communication space. But, still, its potential to enable coordinated obstacle mapping, a significant aspect of VANETs, is often neglected [14][15]. Nevertheless, blockchain has been successfully employed in other VANET subsystems mostly as enabling technology for secure data transmissions or key exchange.

Expanding on exciting and innovative research in blockchain-enabled V2V communication systems, several researchers have presented promising methods and architectures to enhance security and efficiency within VANETs. Shrestha et al. [16] introduced a novel blockchain system that ensures secure message exchange within VANET. The system utilizes blockchain's immutability and transparency features to validate the authenticity of transmitted messages, thereby improving the trustworthiness of VANET communications. Furthermore, Ma et al. [17] proposed a decentralized key management mechanism that provides robust security in VANET. Leveraging the blockchain's decentralized nature, the authors built a system that eliminates single points of failure, thereby enhancing the robustness and reliability of key management in VANET. Additionally, Luo et al. [18] present a blockchain-enabled trust-based location privacy protection scheme in VANET. This scheme uses blockchain to create a decentralized, trust-based model that protects user privacy while ensuring secure V2V communication. But none of these solutions is designed to protect obstacle information or ensure efficiency or scalability.

Only a very few authors have reported blockchain-enabled secure obstacle mapping solutions in VANETs. The Starling system [19] is probably the most promising and popular. Starling is an innovative solution designed to improve road safety. This system leverages the strengths of blockchain technology, offering secure storage and retrieval of road obstacle data [20]. The system design aims to minimize the traditional problems associated with obstacle data exchange [21], paving the way for safer and more efficient V2V communications. The proposed Starling system is built on an open-layered architecture that encompasses six autonomous subsystems in three hierarchical layers (see **Figure 1**). This layout provides a structured and efficient network for communication, making the system capable of handling complex V2V communications with ease [22].

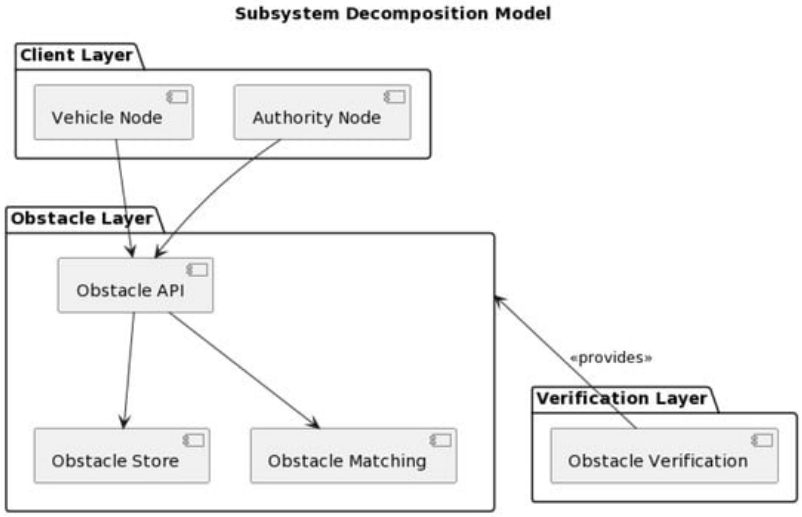

Figure 1. Subsystem decomposition model of the standard Starling system.

The Starling system involves three central actors: vehicles, vehicle owners, and enforcement authorities. Each actor has unique roles and requirements within the network, which dictates their unique interaction with the system [23]. **Figure 2** represents those interactions. Vehicles communicate with the system via the VehicleClient interface, which is situated within the system's topmost layer, the Client Layer. This interface allows vehicles to access the Obstacle Repository located in the Obstacle Layer, enabling them to record and retrieve obstacle data [24]. This feature allows for a more dynamic and adaptive navigation system, thereby improving traffic efficiency and safety. An additional utility provided by the VehicleClient interface is the VehicleIdentifier. Enforcement authorities can solicit this identifier during investigations, instilling accountability and encouraging responsible driving behaviors [25]. This accountability measure serves to protect the integrity of the system and enhance the safety it provides.

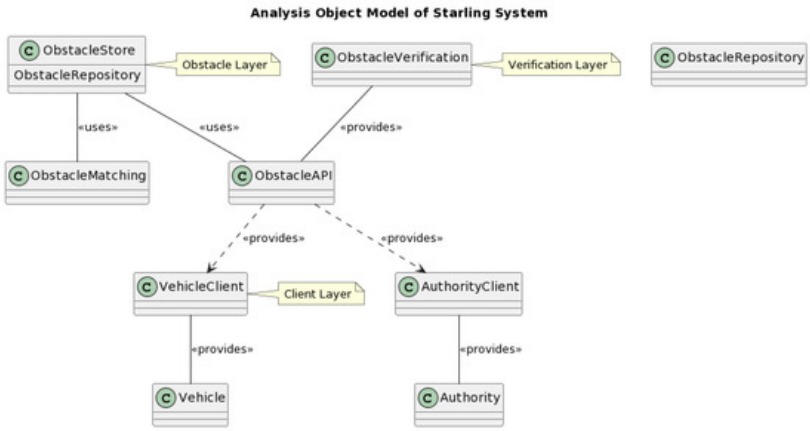

Figure 2. Analysis object model of Starling system.

But Starling and the other prior solutions encountered issues such as high latency in alias generation, inefficient V2V and Vehicle-to-RSU communication due to the limited presence of Roadside Units (RSUs), and increased computational costs from nodes vying to add blocks to the blockchain [26][27]. All these open problems result in a very poor scalability and efficiency, which prevents the implementation of these novel schemes in real transportation applications.

References

1. Li, S.; Da Xu, L.; Zhao, S. The internet of things: A survey. Inf. Syst. Front. 2015, 17, 243–259.
2. Rosen, P.; Underwood, S.; Zacharias, G. Autonomous Vehicle Technology: A Guide for Policymakers; Rand Corporation: Santa Monica, CA, USA, 2015.
3. Rawashdeh, Z.Y.; Mahmud, S.M. A novel algorithm to form stable clusters in vehicular ad hoc networks on highways. EURASIP J. Wirel. Commun. Netw. 2012, 2012, 15.
4. Dwivedi, S.K.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.K.R.; Vollala, S. Blockchain-based vehicular ad-hoc networks: A comprehensive survey. Ad Hoc Netw. 2022, 137, 102980.
5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Business Review. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 9 August 2023).
6. Baras, S.; Saeed, I.; Tabaza, H.A.; Elhadef, M. VANETs-based intelligent transportation systems: An overview. Adv. Comput. Sci. Ubiquitous Comput. CSA-CUTE 2018, 17, 265–273.
7. Daeinabi, A.; Rahbar, A.G. Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks. Multimed. Tools Appl. 2013, 66, 325–338.
8. Liao, S.; Wu, J.; Bashir, A.K.; Yang, W.; Li, J.; Tariq, U. Digital twin consensus for blockchain-enabled intelligent transportation systems in smart cities. IEEE Trans. Intell. Transp. Syst. 2021, 23, 22619–22629.
9. Benslimane, A.; Taleb, T.; Sivaraj, R. Dynamic clustering-based adaptive mobile gateway management in integrated VANET—3G heterogeneous wireless networks. IEEE J. Sel. Areas Commun. 2011, 29, 559–570.
10. Nakrani, N.M.; Joshi, M.M. A human-like decision intelligence for obstacle avoidance in autonomous vehicle parking. Appl. Intell. 2022, 52, 3728–3747.
11. Aggarwal, C.C. Neural Networks and Deep Learning; Springer: Berlin/Heidelberg, Germany, 2018.
12. Levinson, J.; Askeland, J.; Becker, J.; Dolson, J.; Held, D.; Kammel, S.; Zico Kolter, J.; Langer, D.; Pink, O.; Pratt, V.; et al. Towards fully autonomous driving: Systems and algorithms. In Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 5–9 June 2011; pp. 163–168.
13. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography 2019, 3, 3.
14. Lin, J.; Shen, Z.; Zhang, A.; Chai, Y. Blockchain and IoT based food traceability for smart agriculture. In Proceedings of the 3rd International Conference on Crowd Science and Engineering (ICCSE), Singapore, 28–31 July 2018.
15. Kim, S. Impacts of mobility on performance of blockchain in VANET. IEEE Access 2019, 7, 68646–68655.
16. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. Digit. Commun. Netw. 2020, 6, 177–186.

17. Ma, Z.; Zhang, J.; Guo, Y.; Liu, Y.; Liu, X.; He, W. An efficient decentralized key management mechanism for VANET with blockchain. IEEE Trans. Veh. Technol. 2020, 69, 5836–5849.
18. Luo, B.; Li, X.; Weng, J.; Guo, J.; Ma, J. Blockchain enabled trust-based location privacy protection scheme in VANET. IEEE Trans. Veh. Technol. 2019, 69, 2034–2048.
19. Miehle, D.; Pfurtscheller, A.; Bruegge, B. Starling: A Blockchain-based System for Coordinated Obstacle Mapping in Dynamic Vehicular Environments. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2020; pp. 4033–4042.
20. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE Commun. Surv. Tutor. 2011, 13, 584–616.
21. Saad, M.; Khan, M.K.; Ahmad, M.B. Blockchain-enabled vehicular ad hoc networks: A systematic literature review. Sustainability 2022, 14, 3919.
22. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. IEEE Internet Things J. 2016, 3, 637–646.
23. Papadimitratos, P.; De La Fortelle, A.; Evenssen, K.; Brignolo, R.; Cosenza, S. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE Commun. Mag. 2009, 47, 84–95.
24. Rakesh, G.; Belwal, M. Vehicle collision avoidance in a vanet environment by data communication. In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 238–242.
25. Zheng, D.; Jing, C.; Guo, R.; Gao, S.; Wang, L. A traceable blockchain-based access authentication system with privacy preservation in VANETs. IEEE Access 2019, 7, 117716–117726.
26. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. Veh. Commun. 2022, 34, 100458.
27. Xue, K.; Ma, C.; Hong, P.; Ding, R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. J. Netw. Comput. Appl. 2013, 36, 316–323.