Preparing for Vulnerable Attacks in the Vanet Through Block chain Method Utilizing the Reduplication Technique for Cloud Computing Data Storage Management

Mr. Manas Kumar Satapthy, Mr. Manoj Kumar Behera ,

Department of Master in Computer Application, College Of Engineering Bhubaneswar, Odisha, INDIA.

ABSTRACT: Another name for vehicular ad hoc networks (VANETs) is intelligent transportation systems. In order to increase traffic flow efficiency and road safety, VANET makes sure that vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are accurate and timely. VANET's high mobility and open wireless boundary make it susceptible to malicious nodes attempting to enter the network and launch serious medium access control (MAC) layer attacks, including replay, denial of service (DoS), impersonation, and Sybil attacks. This might compromise network security and privacy, impair legitimate nodes' ability to communicate information throughout the network, and increase the number of traffic fatalities. Consequently, a unique blockchain-based safe trust-based architecture

Keywords: VANET; trust model; blockchain; architecture; privacy; authentication; security

1. INTRODUCTION

Vehicle ad hoc networks (VANET) emerged as a subset of a mobile ad hoc network (MANET) application. VANET is considered a substantial approach for intelligent transportation systems (ITS) . VANET has recently been the focus of various researchers in the wireless mobile communication field. The aim of VANET is to provide inter-vehicle communication and roadside units to vehicle communication to increase road safety and improve local traffic flow and the efficiency of road traffic by providing accurate and timely information to road users .

There are two types of communications in VANET, which are vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications . The on-board units (OBUs) and road side units (RSUs) in VANET establish a connection among themselves with the help of dedicated short-range communication (DSRC) in a single or multi-hop communication .

VANET offers various services and applications to the users, most of which are concerned with the safety of the drivers, infotainment, and navigational aid . There are two types of information shared in VANET: safety (vehicle speed warning, curve warning) and non-safety information (value-added comfort application) . By default, safety information is given a higher priority in VANET as compared to non-safety information, since safety information notifies drivers of expected dangers to allow an vehicles enter and exit highways, they require certain safety information, such as traffic congestion and road conditions, to make decisions on which route to take to their destination. It is essential that this information be delivered in a timely manner; otherwise, it could lead to delays in reaching the destination safely . In certain scenarios, some malicious nodes refuse to relay or even intentionally modify the required safety messages before transmitting to the requesting user, which could result in longer delay or fatalities. Besides this, characteristics of VANET (e.g., high mobility, volatility) which are distinct

from other wireless communication networks have caused VANET to be susceptible to numerous internal and external attacks . Due to the decentralized structure and dynamic topology of VANET, the security of the vehicles, users, and data has become essential, since the identification of malicious or faulty nodes or users has become difficult . In VANET, vehicles exchange sensitive information and traffic changes with each other . However, a lack of authentication of this information can result in malevolent attacks which present harm to drivers . However, for messages to be authenticated, the vehicles in the network are tracked for their identification and whereabouts at any given time , compromising the privacy of the users. Hence, there must be a perfect balance between authentication and preserving the privacy of the users . Several researchers have developed various techniques for preserving privacy, such as pseudonyms and anonymous authentication , which could achieve the goal of preserving the privacy of the users, as long as the pseudonyms cannot be linked to the user. Nevertheless, these schemes may not be very secure, because reported traffic information can be utilized to link the pseudonyms to the users, as vehicles do not change their pseudonyms during information exchange . Not only that, the availability of abundant valid pseudonyms for each vehicle makes VANET vulnerable to attacks, such as Sybil attacks, as the pseudonyms could be used to correctly authenticate non-existing vehicles . Although solutions that can provide secure communication channels against external attacks are available, trust management and privacy protection for vehicles are still open issues for VANETs . Therefore, designing a secure VANET demands that three key elements be considered—security, privacy, and trust —to reduce or prevent any attacks in the network. This paper is organized as follows. Section 2 presents the related work. Section 3 explains the motivation of the proposed approach. In Section 4, the proposed blockchain in VANET is presented and the simulation environment is set-up in Section 5, followed by the performance and security analysis of the proposed solution under results and discussion in Section 6. Finally, Section 7 concludes the paper, along with future work.

2. PROPOSED BLOCKCHAIN IN VANET

Many academicians and researchers are drawn to blockchain technology for its enormous benefits to be gained in vast fields, including academics, finance, medicine, and banking. To be precise, blockchain is a technology that is technically comprised of an unlimited number of blocks that are connected in a sequential order to form a blockchain. As this technology is potentially beneficial for expertise in vast fields, it has also gained the interest of many in resolving critical information dissemination issues in VANETs. Bitcoin cryptocurrency is the underlying support of blockchain technology that emerges from the decentralization and distribution of a computing paradigm that has the ability to provide privacy and security in peer-to-peer (P2P) networks . In the VANET environment, this technology is a vital part that helps in managing the ground truth of information for automobiles due to the fact that any automobiles in the system can access the past event lists and its information if it is placed in the public blockchain.

The proposal is to generate a scheme whereby the trustworthiness of node and message passing in VANET is guaranteed by placing them in a public blockchain to act as a ground truth for other automobiles. The application of an existing blockchain to the VANET system is not sufficient, as event messages as a transaction form are adopted instead of the bitcoin transaction for the cryptocurrency feature. The reason for the variation made to the transaction is to ensure the suitability of features for the VANET system as an assurance of providing security for critical

information dissemination and resolving the VANET issues. The variation method adapted adds new blocks based on event messages, similar to transactions in bitcoin, apart from the hashing sequences of blocks to be connected in chronological order to the blockchain. The scalability and timeliness of message dissemination is ensured in this system by implementing a local blockchain with independent chains from different geographical regions. A public blockchain is considered to store and manage all the node and message trustworthiness information given in a geographical region. Based on the type of blockchain, which could be either public or private, a different set of blockchain consensus mechanisms are offered. Therefore, the security and scalability level of the blockchain also depends on the vital role played by the consensus mechanisms.

3. CONCLUSIONS

VANETs have received an enormous amount of attention from both researchers and the vehicular industry due to their potential in delivering information to provide safety and infotainment messages to drivers and passengers. Unfortunately, trust management for vehicles is still an open issue in VANETs. Therefore, this research proposed a secure trust-based blockchain architecture to effectively mitigate several network attacks while preserving the privacy and security of the users in VANET. The proposed solution was developed to mitigate networks attacks, such as message fabrication, impersonation, DoS attacks, and Sybil attacks, while maintaining the privacy of the users in VANET. The blockchain technology in the proposed solution uses timestamps and hashing techniques to maintain the freshness of the messages delivered. These techniques minimize message fabrication or modification attacks, as the timestamps record the time a message is delivered, while hashing secures the message against tampering by malicious nodes. Furthermore, the proposed solution also uses a message rating and credibility approach via the blockchain technology. The message rating and credibility approach ensures trust management among vehicles during information exchange in VANET. Any vehicle that communicates fake messages to other vehicles in the network will be rated with low values, decreasing its credibility. Vehicles with a lower trust value than the threshold value will be rejected from the network and their vehicle certificates will be revoked. The performance of the proposed solution was evaluated via simulation using the Veins simulation tool under two settings, which were without denial of service attacks and with denial of service attacks. From the simulation, the proposed solution was found to perform better than the benchmark algorithms in terms of the PDR against increasing number of nodes in the network. The simulations showed that the proposed solution experienced up to 98% of PDR when there were no attacks launched in the network, while during attack, the proposed solution incurred up to 94% of PDR. Interestingly, the proposed solution experienced a similar delay of 0.130 s over increasing number of vehicles in the network, with and without network attacks. Despite the improved performance of the proposed solution, this study was still bound to several research limitations. First, the proposed solution was only implemented and evaluated on one component of the intelligent transportation system—vehicular ad hoc network (ITS—VANET). Future works should include deployment of the proposed solution in autonomous vehicles and deployment in a multi-junction road network. Cooperative-ITS (C-ITS) is another component of ITS that supports connectivity and cooperative awareness of road users, which can be achieved with regular exchange of safety information among users . In the future, C-ITS will be a possible application to be integrated with the proposed solution and to investigate the performance of the

proposed solution in enabling cooperative awareness in VANET.

4. REFERENCES

1. Ghori, M.R.; Zamli, K.Z.; Quosthoni, N.; Hisyam, M.; Montaser, M. Vehicular ad-hoc network (VANET): Review. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 11–12 May 2018.
2. Gillani, S.; Shahzad, F.; Qayyum, A.; Mehmood, R. A survey on security in vehicular ad hoc networks. In *Communication Technologies for Vehicles. Nets4Cars/Nets4Trains 2013. Lecture Notes in Computer Science*; Berbineau, M., Jonsson, M., Bonnin, J., Cherkaoui, S., Aguado, M., Rico-Garcia, C., Ghannoum, H., Mehmood, R., Vinel, A., Eds.; Springer: Heidelberg/Berlin, Germany, 2013; pp. 59–74. [CrossRef]
3. Abbasi, I.A.; Khan, A.S. A review of vehicle to vehicle communication protocols for VANETs in the urban environment. *Future Internet* **2018**, *10*, 14. [CrossRef]
4. Junaid, M.A.H.A.; Syed, A.; Warip, M.N.M.; Azir, K.N.F.K.; Romli, N.H. Classification of security attacks in VANET: A review of requirements and perspectives. In Proceedings of the Malaysia Technical Universities Conference on Engineering and Technology, Penang, Malaysia, 6–7 December 2017.
5. Malik, N.; Nanda, P.; Arora, A.; He, X.; Puthal, D. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In Proceedings of the 2018 17 th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, New York, NY, USA, 1–3 August 2018.
6. Hasrouny, H.; Bassil, C.; Samhat, A.E.; Laouti, A. Group-based authentication in V2V communications. In Proceedings of the 2015 5th International Conference on Digital Information and Communication Technology and its Applications, Beirut, Lebanon, 29 April–1 May 2015.
7. Patel, N.J.; Jhaveri, R.H. Trust based approaches for secure routing in VANET: A survey. *Pro. Comp. Sci.* **2015**, *45*, 592–601. [CrossRef]
8. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [CrossRef]
9. Bhoi, S.K.; Khillar, P.M.; Singh, M.; Sahoo, M.M.; Swain, R.R. A routing protocol for urban vehicular ad hoc networks to support non-safety applications. *Digital Commun. Networks* **2018**, *4*, 189–199. [CrossRef]
10. Azees, M.; Vijayakumar, P.; Deborah, L.J. Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intell. Transport Syst.* **2016**, *10*, 379–388. [CrossRef]

11. Ghaleb, F.A.; Razzaque, M.A.; Zainal, A. Mobility pattern based misbehavior detection in vehicular adhoc networks to enhance safety. In Proceedings of the 2014 International Conference on Connected Vehicles and Expo, Vienna, Austria, 3–7 November 2014.
12. Qu, F.; Wu, Z.; Wang, F.Y.; Cho, W. A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *10*, 2985–2996. [CrossRef]
13. Lai, C.; Zhang, K.; Cheng, N.; Li, H.; Shen, X. SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 1559–1574. [CrossRef]
14. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]
15. Begum, R.; Raziuddin, S.; Prasad, V.K. A survey on VANETs applications and its challenges. In Proceedings of the International Conference on Advanced Computer Science & Software Engineering, Hyderabad, India, 11 March 2016.
16. Xi, Y.; Sha, K.; Shi, W.; Schwiebert, L.; Zhang, T. Enforcing privacy using symmetric random key-set in vehicular networks. In Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, Phoenix, AZ, USA, 21–23 March 2007.
17. Defrawy, K.E.; Tsudik, G. ALARM: Anonymous location-aided routing in suspicious MANETs. *IEEE Trans. Mob. Comput.* **2016**, *10*, 1345–1358. [CrossRef]
18. Chaubey, N.K. Security analysis of vehicular ad hoc networks (VANETs): A comprehensive study. *Int. J. Secur. Appl.* **2016**, *10*, 261–274. [CrossRef]
19. Florian, M.; Finster, S.; Baumgart, I. Privacy-preserving cooperative route planning. *IEEE Internet Things J.* **2014**, *1*, 590–599. [CrossRef]
20. Li, J.; Lu, H.; Guizani, M. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 938–948. [CrossRef]
21. Rabieh, K.; Mahmoud, M.M.E.A.; Younis, M. Privacy-preserving route reporting schemes for traffic management systems. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2703–2713. [CrossRef]
22. Rabieh, K.; Mahmoud, M.M.E.A.; Guo, T.N.; Mohamed, M. Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs. In Proceedings of the 2015 IEEE International Conference on Communications, London, UK, 8–12 June 2015. [CrossRef]
23. Zhang, Y.; Zheng, D.; Deng, R.H. Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE Internet Things J.* **2018**, *5*, 2130–2145. [CrossRef]
24. Lu, Z.; Qu, G.; Li, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 760–776. [CrossRef]
25. Ying, B.; Nayak, A. Anonymous and lightweight authentication for secure vehicular networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10626–10636. [CrossRef]
26. Wazid, M.; Das, A.K.; Kumar, N.; Odelu, V.; Reddy, A.G.; Park, K.; Park, Y. Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. *IEEE Access* **2017**, *5*, 14966–14980. [CrossRef]
27. Rajput, U.; Abbas, F.; Eun, H.; Oh, H. A hybrid approach for efficient privacy-preserving authentication in VANET. *IEEE Access* **2017**, *5*, 12014–12030. [CrossRef]
28. Tangade, S.; Manvi, S.S. Scalable and privacy-preserving authentication protocol for secure vehicular communications. In Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, Bangalore, India, 6–9 November 2016. [CrossRef]
29. Cui, J.; Zhang, J.; Zhong, H.; Xu, Y. SPACF: A secure privacy-preserving authentication scheme for VANET with CUCKOO Filter. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10283–10295. [CrossRef]
30. Lim, K.; Manivannan, D. An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. *Veh. Commun.* **2016**, *4*, 30–37. [CrossRef]
31. Raya, M.; Jungels, D.; Papadimitratos, P.; Aad, I.; Hubaux, J.-P. *Certificate revocation in vehicular networks*; Laboratory for computer Communications and Applications (LCA), School of Computer and Communication Sciences, EPFL: Lausanne, Switzerland, 2006.
32. La, V.H.; Cavalli, A.R. Security attacks and solutions in vehicular ad hoc networks: A survey. *Int. J. AdHoc networking Syst.* **2014**, *4*, 1–20.
33. Abbasi, I.A.; Khan, A.S.; Ali, S. A Reliable Path Selection and Packet Forwarding Routing Protocol for Vehicular Ad hoc Networks. *EURASIP J. Wirel. Commun. Networking* **2018**, *1*, 236. [CrossRef]

34. Wu, Q.; Liu, Q.; Zhang, L.; Zhang, Z. A trusted routing protocol based on GeoDTN+Nav in VANET. *China Commun.* **2014**, *11*, 166–174. [CrossRef]
35. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 31 October 2008).
36. Hammad, B.T.; Jamli, N.; Rusli, M.E.; Z'aba, M.R. A survey of lightweight cryptographic hash function. *Inter. J. Sci. Eng. Res.* **2017**, *8*, 806–814.
37. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.K.; Zhang, J.Z.C. "What Will 5G Be?". *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082. [CrossRef]
38. Cheng, N.; Lyu, F.; Chen, J.; Xu, W.; Zhou, H.; Zhang, S.; Shen, X. Big Data Driven Vehicular Networks. *IEEE Network* **2018**, *32*, 1–8. [CrossRef]
39. Chen, S.; Hu, J.; Shi, Y.; Peng, Y.; Fang, J.; Zhao, R.; Zhao, L. Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G. *IEEE Commun. Stand. Mag* **2017**, *1*, 70–76. [CrossRef]
40. Farooq, S.; Hussain, S.; Kiran, S.; Ustun, T. Certificate based security mechanisms in vehicular ad-hoc networks based on IEC 61850 and IEEE WAVE standards. *Electronics* **2019**, *8*, 96. [CrossRef]
41. Balan, K.; Khan, A.S.; Julaihi, A.A.; Tarmizi, S.; Pillay, K.S. RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks. *Inter. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 298–304. [CrossRef]
42. Draz, U.; Ali, T.; Yasin, S.; Shaf, A. Evaluation based analysis of packet delivery ratio for AODV and DSR under UDP and TCP environment. In Proceedings of the 2018 International Conference on Computing, Mathematics and Engineering Technologies, Sukkur, Pakistan, 3–4 March 2018. [CrossRef]
43. Shorfuzzaman, M.; Masud, M.; Rahman, M.M. Characterizing end-to-end delay performance of randomized TCP using an analytical model. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 406–412. [CrossRef]
44. Pukale, P.; Gupta, P. Analysis of end-to-end delay in vehicular networks. *Int. J. Sci. Res.* **2013**, *5*, 1122–1125.
45. Luo, J.; Gu, X.X.; Zhao, T.; Yan, W. A mobile infrastructure based VANET routing protocol in the urban environment in Communications and Mobile Computing (CMC). In Proceedings of the 2010 International Conference on Communications and Mobile Computing, Shenzhen, China, 12–14 April 2010.
46. Samundiswary, P.; Sathian, D.; Dananjayan, P. Secured greedy perimeter stateless routing for wireless sensor networks. *Inter. J. Ad hoc. Sens. Ubiquitous Comput.* **2010**, *1*, 9–20.
47. Lyamin, N.; Vinel, A.; Jonsson, M.; Bellalta, B. Cooperative awareness in VANETs: On ETSI EN 302 637-2 performance. *IEEE Trans. Veh. Technol.* **2018**, *67*, 17–28. [CrossRef]
48. Lyamin, N.; Vinel, A.; Jonsson, M. Poster: On the performance of ETSI EN 302 637-2 CAM generation frequency management. In Proceedings of the 2014 IEEE Vehicular Networking Conference, Paderborn, Germany, 3–5 December 2014. [CrossRef]