Sana'a University Journal of Applied Sciences and Technology https://journals.su.edu.ye/index.php/jast

Vol. 17 | No. 2 | Page 276 – 283 | 2023 | ISSN : 2958-9568

Doi: 10.59628/jast.v1i3.370

Hierarchical Blockchain as Line Defense of Attacks to Messages Propagation in VANET

Malek Algabri[1] , Firdaus Alhrazi[1,*] and Abdualmajed Ahmed G. Al-Khulaidi [2]

[1] Department of Computer Science, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen.

[2] Software Engineering, Department of Computer Science, Faculty of Computer and Information Technology,
Sana’a University, Sana’a, Yemen.

Corresponding author:** ***firdaus.mansoor2024@gmail.com

ARTICLE INFO

Article history:
Received: April 21, 2023
Accepted: August 6, 2023
Published: August, 2023

KEYWORDS

1. Blockchain
2. Ad-hoc Network
3. Line Defense
4. UVA
5. Attacks
6. Propagation
7. VANET

ABSTRACT

The Vehicle Network (VANET) is a component of the Intelligent Transport System (ITS), for the exchange of messages between vehicles and roadside units (RSU). While due to the increase in the number of vehicles, there have been a lot of privacy, trust, and security challenges related to the Vehicle Network (VANET). The information exchanged between vehicles must be correct to achieve the CIA principle. Trust, privacy, and security solutions don’t apply to centralized networks. Most importantly, the lack of confidentiality, privacy, and availability. In this paper, solutions to solve security problems using hierarchical blockchain technology will be presented. Hierarchical blockchain has the advantages of unanimously emphasizing message credibility, decentralization, and immutable storage. All these advantages will provide solutions to those problems and challenges related to the security of VANETs. This paper seeks two main objectives. The first is to monitor malicious and no malicious vehicles by UAV, to validate the message before sending it via VANET. The second is a set of complex rules and specific calculations to verify the message. Consensus algorithms are also used to agree among vehicles on what is true, and to evaluate performance using the following metrics (Throughput, tolerance, latency).

CONTENTS

1. **Introduction:**

The Internet of Vehicles (IoV) is the most important field of the Internet of Things (IoT), which includes (IoV) communication between vehicles and things, such as communication between vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X). The main objective of the Internet of Vehicles (IOV) is to share information and spread messages between vehicles to ensure orderly traffic and safe journey [1]. In this study, solutions are developed for the problem of congestion and unorganized traffic, owing to the increased density of vehicles, which causes accidents, increased risks, and a great threat to the safety of individuals [2]. A blockchain is a digital, ever-growing list of data records. Such a list comprises many blocks of data, which are organized in chronological order, linked, and secured by cryptographic proofs. where acts as a decentralized, distributed, and public digital ledger responsible for keeping a permanent record (chain of blocks) of all previously confirmed transactions. A hierarchical blockchain contains parallel layers of blocks outside the chain, and all blocks are connected to the main block to improve the latency of nodes as well as to improve productivity, unlike the traditional blockchain ledger horizontal, where each block is connected to the previous block. The proposed blockchain-based decentralized authentication framework is organized into a multilevel or hierarchical structure. Bolckchain, as a Line Defense of attackes, contributes to Technology Bolckchain in the field of security, as it faces the challenges of a network attack, specifically the Vehicle Network (VANET), which makes the vehicular network safe from any attack from malicious and selfish nodes on the VANET network, as blockchain is a solution to protect against the attack of malicious nodes in the network vehicles (VANET).

Word count: 303 words, excluding references.

Funding Statement: The study was supported by grant NN from the Foundation of Basic Research. This work was carried out under research program NNN of NN University. Author NN was supported by grant NN from the Ministry of NN.

Ethical Compliance: All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.

Data Access Statement: Research data supporting this publication are available from the NN repository at located at www.NNN.org/download/.

Conflict of Interest declaration: The authors declare that they have NO affiliations with or involvement in any organization or entity with any financial interest in the subject matter or materials discussed in this manuscript.

Author Contributions: AB and MJ contributed to the design and implementation of the research, JK to the analysis of the results and to the writing of the manuscript. VK conceived the original and supervised the project.

Message Propagation is a potential application of VANETs that contain emergency information related to highway accidents. To quantify how efficiently RSUs and vehicles disseminate information. A vehicular ad hoc network (VANET) is a technology that supports various types of communication. In the vehicle-to-vehicle (V2V) case, vehicles are allowed to communicate only with each other. Vehicle-to-infrastructure (V2I) systems can also communicate with roadside infrastructure if they are present. The most flexible solution, vehicle-to-everything (V2X) communication, does not impose any restrictions on communicating entities. With an increasing number of vehicles equipped with computing technologies and wireless communication devices, intervehicle communication has become a promising field of research, standardization, and development. VANETs enable a wide range of applications, such as collision prevention, safety, blind crossing, dynamic route scheduling, and real-time traffic condition monitoring. Another important application of VANETs is to provide internet connectivity to vehicular nodes. Message propagation in VANET shows its importance in regulating the traffic of vehicles, as incoming vehicles change their crossing path to avoid traffic congestion or accidents by receiving messages before crossing to a crowded place. This technology allows a safe journey for oncoming vehicles. A Dedicated Vehicle Network (VANET) may encounter many difficulties owing to the increase in the density of connected vehicles, as the dedicated vehicle network (VANET) includes a large number of nodes, which are the Roadside Unit (RSU) and vehicles, some of which may be malicious and may cause the transmission of messages to stop in emergency situations. Security and privacy are major goals in the communication between nodes, and it is not true that the central network (CA) is the central responsibility for this network, as failure of a point in it may disrupt the entire network. Therefore, in a network of dedicated vehicles, a decentralized network must be used, as this technology does not disrupt the entire network if a point fails, and this is an important point in the application of this technology. The aim of this paper is to present two main goals: the first is to monitor malicious and non-malicious vehicles by UAV, and to validate the message before sending it via VANET. The second is a set of complex rules and specific calculations for verifying the message. Consensus algorithms are also used to agree among vehicles on what is true and to evaluate performance using the following metrics (throughput, tolerance, and latency). Hierarchical clustering algorithms (cluster analysis) were used with the application of Hierarchical Blockchain, where adjacent nodes are grouped together into a block, and those nodes are not added before the generated information is validated, this information verification is done by Proof of Work (POW) aggregation algorithms, where this algorithm performs large arithmetic operations and complicated to verify the correctness of the information in the contract. These algorithms work together as an integrated approach as a line of defense against malicious attacks on the VANET network.

2. Related Work

The main goal of the intelligent transportation system (ITS) is to optimize traffic flow, safety, and driving conditions through vehicle communication. Complete vehicle communication, including communication between vehicles and between vehicles and other things. An Internet of Vehicles (IOV) system is an environment comprising vehicles, people, and things, as shown in Figure 1. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are the primary means by which an intelligent transportation system (ITS) distributes critical messages regarding driving and road conditions [3].

A. Vehicle Network System:

(VANET) As shown in Figure 2, the VANET system model consists of three components.

- Vehicular: A vehicle that contains units equipped with on-board unit sensors (OBU) and an Application Unit (AU). The vehicle can communicate with the next vehicle via a VANET [4].
- Road Side Unit (RSU): This fixed roadside node serves as a conduit for infrastructure network communications with vehicles, RSU, and CA. The Internet of Vehicles (IOV) may be connected through an RSU, which can also help with the transmission of critical messages [4].
- Central Authority (CA): Through a wired connection, the CA and RUS talk to one another. The role of CA is to distribute rewards, register nodes, uphold trust, and give or revoke cryptographic keys [4].

B. Communication in VANETS:

Vehicles often drive at a rapid pace [5]; thus, information transmission between two entities must be completed in a brief amount of time. A VANET uses dedicated short-range communication (DSRC) to interact with the network. It is necessary to build a specialized network and transport data during this short period. Along with security, human privacy must also be preserved, which may include complex computations such as key pair creation. As a result, with a VANET, several tiny networks are built, and information is transmitted quickly while also ensuring data security and user privacy. There are three different methods of communication, Vehicle-to-Vehicle Communication, Vehicle-to-Infrastructure Communication, and In-Vehicle Communication (On-Board Unit and Application Unit).

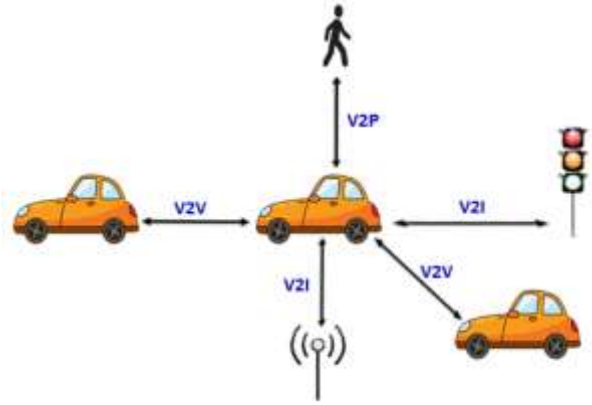

Fig. 1. IOV Communication

C. Security in VANETS: The main characteristic of VANETs is their security. The CIA offers three categories of security services. Most studies have focused on the results of this research to increase the security of VANETs. The CIA refers to availability, integrity, and confidentiality. These three services enhance the security triads. Other services are also responsible for maintaining VANET security. These services include nonrejection, authentication, and access control. These services have also been the focus of some studies [5]. Confidentiality, integrity, and availability (CIA) are the main aspects of security. Care must be taken to ensure that they are available to satisfy the security requirements of any system. Similarly, a secure connection between the VANETs and CIA must be achieved.

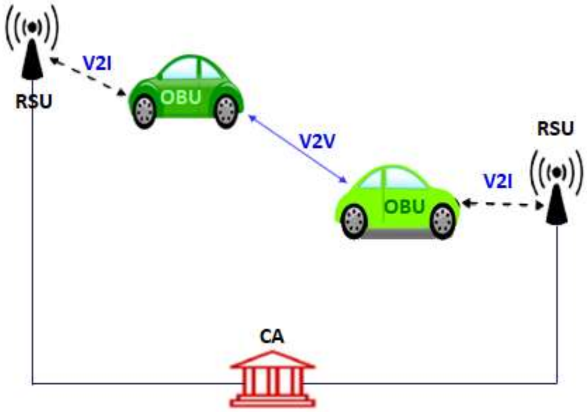

Fig. 2. The VANET System

D. Bolckchain as a Line of Defense in the Vehicle Network (VANET):

Technology contributes to Bolckchain effectively in the field of security, as it faces the challenges of network attacks, specifically the Vehicle Network (VANET), which makes the vehicular network safe from any attack from malicious and selfish nodes on the VANET network, as Bolckchain is a solution to protect against attacks from malicious nodes in network vehicles (VANET).

3. Methodology

This methodology is based on assumptions and the use of the CIA model to protect against malicious attack. Hierarchical Blockchain has been used in VANET with the application of some algorithms to ensure security in VANETs. The following is an explanation of the methodology used for this system. To build a vehicle network (VANET) that is secure against malicious attacks and provides a high level of security, the following methodology must be followed.

A. Step 1: Providing security:

Security is the defense of a vehicle network (VANET) against attacks and security risks posed by attackers (VANET) [6]. In this step, we explain the methodology used in the VANET.

• ***Reliability***

involves evaluating the message produced in three stages:

1) Message Prediction is Based on whether a node’s message is true or false and its private trust is categorized. The message sent by that node is rejected if the rating is below a certain level [7].

2) After the message is predicted, its authenticity is validated based on the number of votes from neighboring nodes under the supervision of a UAV [8].

3) In the final stage, the trusted node is involved in evaluating the message [9].

• *Availability*

This ensures that the network operates even in the presence of a malicious node. where the vehicle network should be (VANET) able to publish a number of messages within a certain time limit. In the event of an emergency on the road, all the relevant vehicles will have information. In addition, the message in the receiving vehicle must be able to select the appropriate relay node for this message, which can effectively forward the message to the largest number of vehicles or nodes. To reach a fast and reliable solution for disseminating messages on a vehicle network (VANET) [10]. Selecting incorrect relay nodes might prevent the message from spreading over the vehicle network or result in an unacceptable speed. The RSU central node sends messages to the vehicle network. The size and position of the RSU node are also important for system performance and require significant investment in the infrastructure. Obfuscation is a cybersecurity attack against availability features. This attack might result in a problem with message delivery between the sender and the receiver, keeping the message inaccessible to the network [11]. Therefore, an appropriate relay node must be selected to ensure availability. Messages must be protected from jamming and attack devices to provide availability to the vehicle network (VANET).

B. Step 2: Privacy

In this paper, word privacy refers to the idea that the node in the vehicular network that creates communication has the authority to grant the other nodes the right to access, distribute, or watch that message. Two additional privacy features include the following.

• *Anonymity*

Authenticating a node anonymously means keeping its original identity secret [12]. Public-key cryptography is one of the most common methods for concealing the original identity in a vehicle network (VANET), where pseudonyms are used to ensure privacy in the network [13]. Additionally, the central authority is the trusted person in charge of spreading encrypted keys (CA). In addition, because the central authority (CA) only needs to use a private key for authentication, an identity-based public key encryption mechanism is adopted. Here, reduces the burden on CA [14].

• *Confidentiality*

This means that the communication must be private and that the only person who should have access to it is the intended receiver. Encryption should be used to protect secrecy and defend against espionage and attacks.

C. Step 3: Confidence

In a Vehicle Network (VANET), trust is utilized to maintain security and evaluate the authenticity of messages.

This methodology suggests using a comprehensive approach based on value and reputation to improve agreement and identify harmful conduct in a vehicle network (VANET). The contribution contract is funded by the creator of the message, to be effectively sent via the network. where the cost is a confirmation of the message’s veracity. This mechanism serves as a stimulant for negative and self-serving nodes, encouraging them to join and help prevent malicious and negative node fraud. The approach outlined in this paper is the practice of imposing fines to deter malicious nodes from disseminating malicious messages [15]. To solve the above points, a hierarchical blockchain was used with the application of consensus algorithms in addition to the general supervision by UAV, where the need for harmonious algorithms with the hierarchical blockchain comes in order to detect defective and malicious nodes in the vehicle network, by means of a set of complex calculations and agreement between vehicles on what is true of the information that will be sent to the vehicle network (VANET). The performance of the consensus algorithms was also evaluated using metrics such as Tolerance, Latency, and Throughput. In addition, in this methodology, a Hierarchical Blockchain is used for speed and improved block latency as well as for better productivity. The Hierarchical Blockchain contains parallel layers of blocks, all of which are connected to each other by a master block. Moreover, miners were pioneers in hierarchical blockchains. In this study, the blocks in a Hierarchical Blockchain are classified into two types: micro and key, where small blocks are added in parallel to achieve decentralization. In this methodology, hierarchical clustering algorithms (cluster analysis) have been used with the application of hierarchical blockchain, where adjacent nodes are grouped together in a block, and these nodes are not added before the information generated is validated. This information is verified by proof-of-work (POW) clustering algorithms, which perform large and complex calculations to verify the correctness of the information contained in the contract. These algorithms work together as an integrated approach as a line of defense against malicious attacks on the VANET network.

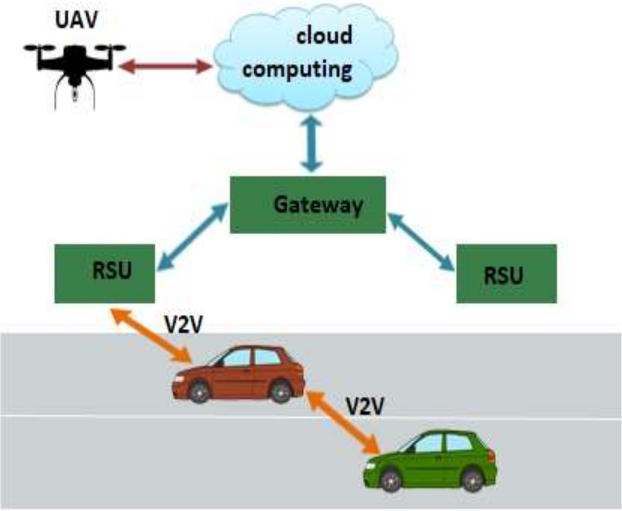

Fig. 3. VANET environment that has been proposed

UAVs are an important component of VANET vehicle networks. This will play a significant and effective role in the security of networks to monitor malicious nodes and ensure the correctness of information before sending it to the VANET vehicle network. The most important benefit of having a UAV as an essential element in the VANET vehicle network is that in the event of an accident and the infrastructure of the VANET vehicle network is destroyed, the role of UAV in the rescue process and the general supervision of information on the network to get rid of any kind of malicious attack at the time of the accident, and the UAV must be connected to each other via satellite, and its security information is stored via cloud computing to provide the highest degree of security and confidentiality, availability, and integrity to achieve CIA. Figure 3 shows the VANET environment proposed in this methodology.

3. Discussion And Results

This study presents the trust, privacy, and security requirements for publishing messages on VANET vehicle networks. It has been concluded that the Hierarchical Blockchain offers solutions to many challenges in VANET, particularly in the dissemination of messages on the vehicle network. Blockchain hierarchical results work with the POW consensus algorithm, hierarchical clustering algorithm, and UAV as an integrated approach to providing decentralization, security, privacy, and trust in VANET, as well as to achieve the CIA principle. As displayed in Table I Challenges associated with spreading messages via VANET and correspondingly showcases the solutions offered by the Hierarchical Blockchain. One of the disadvantages of using the traditional blockchain is that the mobile nodes contain an updated ledger, which leads to a split state in which case forks are excluded. Therefore, using a traditional blockchain has become difficult in VANET. In this study, the solution to this problem is the use of a Hierarchical Blockchain, as the results of using this method are positive and effective and ensure security and protection from attacks launched on the VANET network.

The parallel addition of small blocks when using a Hierarchical Blockchain also does not disturb the main linear ledger, and forks are accepted as transactions. In other words, the results of using a Hierarchical Blockchain are a solution to security attacks. The performance of the consensus algorithms was also evaluated using the following metrics [4]:

• Latency: The time required for a transaction's propagation and validation.

• Throughput number of blocks produced per second.

• Tolerance: The maximum number of malicious nodes that can manage a transaction simultaneously without affecting its initial validity status, together with the ability to handle forks and stop cheating.

Table i: issues and using blockchain in vanet

Issues in VANET	Hierarchical Bolckchain solutions
Message validation	Proof-of-Word algorithm
Trust without depend on a third party	Decentralised ledger
Incentive distribution	Miner incentives
Relay selection	Miner election by consensus
Privacy requirement	Cryptographic hashes

4. Conclusion And Future Work

The focus of this study is to devise solutions to disseminate messages on the vehicle network (VANET) and secure messages using a Hierarchical Blockchain. Here, the important contributions to privacy, trust, and security in the Vehicle Network (VANET) are highlighted by supporting the Hierarchical Blockchain with Hierarchical clustering and POW consensus algorithms with UAV connected to each other via satellites to provide a high level of security on the vehicle network. This study uses low-volume, flexible-mobility UAVs to assist the Vehicle Network (VANET) in mission-critical security implementation. An example is disaster rescue services when the network is very weak or infrastructure is not available when disasters occur. Therefore, the integration of connected drones with a Vehicle Network (VANET) is a promising solution to improve connectivity, in addition to addressing all the challenges of trust, security, and privacy in the Vehicle Network (VANET). Future research should continue to recommend the use of low-volume UAVs that are flexible in mobility in order to participate in the voting process to remove malicious nodes and malicious security attacks, as well as surveillance via satellites from any security attacks harmful to the vehicle network, to provide a higher level of security to meet all security challenges.

5. REFERENCES

[1] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," IEEE access, vol. 4, pp. 5356–5373, 2016.

[2] A. Aldegheishem, H. Yasmeen, H. Maryam, M. A. Shah, A. Mehmood, N. Alrajeh, and H. Song, "Smart Road traffic accidents reduction strategy based on intelligent transportation systems (tars)," Sensors, vol. 18, no. 7, p. 1983, 2018.

[3] A. R. Khan, M. F. Jamlos, N. Osman, M. I. Ishak, F. Dzaharudin, Y. K. Yeow, and K. A. Khairi, "Dsrc technology in vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) iot system for intelligent transportation system (its): a review," Recent Trends in Mechatronics Towards Industry 4.0, pp. 97–106, 2022.

[4] F. Ayaz, "Blockchain based secure message dissemination in vehicular networks," Ph.D. dissertation, University of Sussex, 2022.

[5] M. Balu, G. Kumar, and S.-J. Lim, "A review on security techniques in vanets," International Journal of Control and Automation, vol. 12, no. 4, pp. 1–14, 2019.

[6] T. Gazdar, A. Belghith, and H. Abutair, "An enhanced distributed trust computing protocol for vanets," IEEE Access, vol. 6, pp. 380–392, 2017.

[7] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (vanet)," Wireless Networks, vol. 24, no. 2, pp. 373–382, 2018.

[8] F. Ayaz, Z. Sheng, D. Tian, G. Y. Liang, and V. Leung, "A voting blockchain based message dissemination in vehicular ad-hoc networks (vanets)," in ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020, pp. 1–6.

[9] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," IEEE

Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1314–1345, 2018.

[10] A. Yanez, S. C ´ espedes, and J. Rubio-Loyola, “Cassam: Context-aware ´ system for safety messages dissemination in vanets,” in 2018 IEEE Colombian Conference on Communications and Computing (COLCOM). IEEE, 2018, pp. 1–6.

[11] Z. Lu, G. Qu, and Z. Liu, “A survey on recent advances in vehicular network security, trust, and privacy,” IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760–776, 2018.

[12] A. R. Prasad, S. Arumugam, B. Sheeba, and A. Zugenmaier, “3gpp 5g security,” Journal of ICT Standardization, vol. 6, no. 1, pp. 137–158, 2018.

[13] R. Al-Ani, B. Zhou, Q. Shi, and A. Sagheer, “A survey on secure safety applications in vanet,” in 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE, 2018, pp. 1485–1490.

[14] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, “Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles,” IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2204–2220, 2018.

[15] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, “Trust and exclusion in vehicular ad hoc networks: an economic incentive model-based approach,” in 2013 Computing, Communications and IT Applications Conference (ComComAp). IEEE, 2013, pp. 13–18.