Using Blockchain Technology for the Internet Of Vehicles

Conference Paper · May 2021

DOI: 10.1109/MIUCC52538.2021.9447622

Marianne A. Azer
National Telecommunication Institute, Egypt

2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) | 978-1-6654-1243-8/20/$31.00 ©2021 IEEE | DOI: 10.1109/MIUCC52538.2021.9447622

Using Blockchain Technology for the Internet Of Vehicles

Ahmed M. Eltahlawy
Information Security Department,
Nile University, Cairo, Egypt.
a.eltahlawy@nu.edu.eg

Marianne A. Azer
National Telecommunication Institute,
Nile University, Cairo, Egypt.
mazer@nu.edu.eg

Abstract—**The Internet of Vehicles (IoV) aims to connect vehicles with their surroundings and share data. In IoV, various wireless technologies like 5G, WIFI, DSRC, WiMAX, and ZigBee are used. To share data within wireless surroundings in a secure way, some security aspects need to be fulfilled. Blockchain technology is a good fit to cover these countermeasures. IoV uses a lot of technologies and interacts with different types of wireless nodes, and this increases the vulnerability to some attacks that could endanger lives. Using blockchain technology within the IoV architecture could provide efficient solutions to overcome these attacks. In this paper, we present the IoV security requirements and their countermeasures using blockchain technology. We also introduce some serious attacks over the IoV architecture and the different countermeasures to overcome these attacks.**

Keywords— **Attacks, Blockchain, Decentralized Network, IoV, Security, Wireless Ad Hoc.**

I. INTRODUCTION

The Internet of Vehicles (IoV) is a network under the Internet of Things (IoT) umbrella that connects vehicles, people, and smart devices together [1]. The IoV dynamic architecture and scalability allow vehicles to interact together through the internet and internal cloud. It also allows moving vehicles to communicate without having a fixed network infrastructure [2]. IoV is a complex dynamic architecture that is efficient for sharing data between vehicles and the surroundings [3], the communication could be Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I, Vehicle to Pedestrian (V2P), Vehicle to Cloud (V2C), Vehicle to Sensors (V2S), Vehicle to Road (V2R) nodes, and Vehicle to Network (V2N). In another way, it is a Vehicle to Everything (V2X) communication. Fig. 1 [4] illustrates the V2X communication.

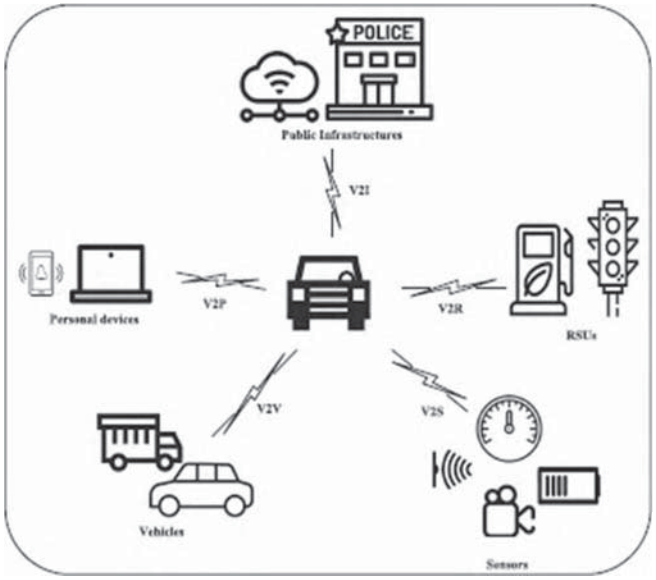

Fig. 1- Vehicle to Everything communication [4]

To be a part of the IoV network, vehicles should be equipped with some hardware parts to be fully functional. On-Board Unit (OBU) is an important part that is put inside the vehicle to be able to communicate with other OBUs and Road Side Units (RSUs) like traffic lights, gas stations, and toll stations. In addition, some sensors are needed to gather vehicle and road important data [5]. The communication is done through different well-known technologies like DSRC, WiFi, GSM, LTE, Bluetooth, Zigbee, WiMAX. Global Positioning System (GPS) is important for vehicle position localization. Communication between RSUs and OBUs has two types of messages. The first type is safety-relevant messages such as Basic Safety Messages (BSMs), Cooperative Awareness Messages (CAM), and Decentralized Environmental Notification Messages (DENM) in which the safety-relevant information should be included such as message timestamp, vehicle positions, vehicle speed, brakes status, and emergency alerts [6]. The safety messages should be highly secured and protected against attacks as they are critical information that needs to be highly protected also should be real-time. The second type is non-safety messages like

978-1-6654-1243-8/21/$31.00 ©2021 IEEE

infotainment messages which tolerate more delay and less security [7]. Typical IoV network elements are shown in Fig.2 [7] .

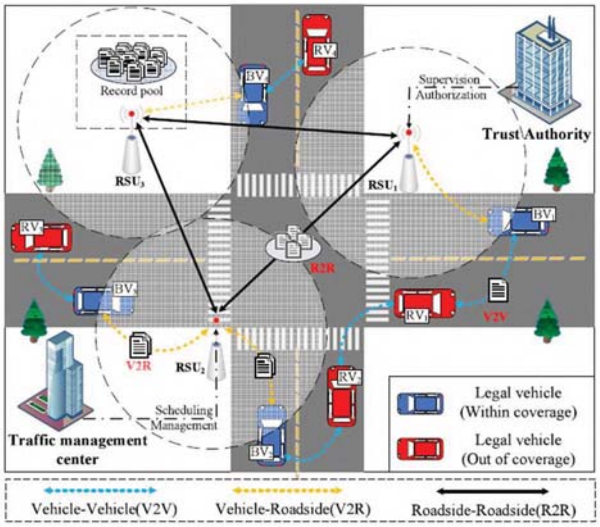

Fig.2- IoV network elements [7]

In this paper, we present the IoV security requirements and their countermeasures using the blockchain technology. We also introduce some serious attacks over the IoV architecture and the different countermeasures to overcome these attacks. The remainder of this paper is organized as follows. Section II introduces the blockchain technology and the process of consensus agreement between network nodes. In section III, we discuss the different security requirements needed for the IoV architecture, and the blockchain features that fulfill the needed network requirements. Section IV covers different frameworks and system designs for blockchain architecture based on blockchain technology. In section V, we explain different security attacks breaching the IoV network and the use of blockchain in mitigating these attacks. Finally, conclusions and future work are presented in section VI.

II. Background

In the IoV architecture, vehicles communicate with each other and with RSUs without any human interaction. To ensure that messages are transferred efficiently, assure message privacy, and control network performance; the blockchain is the best fit to be integrated with IOV architecture [8]. Blockchain technology is a powerful technology to make interactions and data sharing in a trusted and secure way. It uses peer-to-peer network concept, along with public key cryptography techniques beside distributed shared databases between all nodes [8].

Blockchain is a series of blocks that are linked together to form one big set of connected blocks. Each block holds information about the sender and some data. In the blockchain, each node has a full identical record of the blocks, this record is saved in a distributed manner in addition to a centralized way inside the network ledger. Once a new block is recorded into the ledger it is immutable to changes. Each block has a block header which is used to identify this block and refers to the previous block in the chain to link all blocks together in one long virtual chain of blocks [9].

To create a block, all active nodes must trust each other and have a consensus agreement to validate the block. To do so, there is a concept technique called the Proof of Work (PoW). In the PoW, the vehicle miners that try to create a new block race together, have a complex puzzle to solve based on the processing power. Afterward, they collect the network data together into one block and propose this block to the rest of vehicles on the IoV network. Then comes the role of network validators to validate this block. After having an agreement on one of the proposed blocks created by the miners, all nodes record this new block in their copy of the ledger and link it with the previous one, to encourage miners to continue creating new blocks all the time, they must be awarded for that. Many awarding mechanisms were proposed, but they are not covered in this paper. To have an agreement between all nodes, a set of rules are saved inside a smart contract to be able to make decisions.

The IoV architecture is a combination of RSU nodes, and each RSU is a part of multiple VANET networks. For communication inside a single VANET, the consensus and communication are decentralized, and the agreement is done between nodes without any central authority. After the agreement, a selected vehicle of the VANET sends a new block to the RSU [10]. Then, it becomes the responsibility of the centralized RSU leader to have a decision to update its ledger and verify the created blocks and then broadcast to the rest of VANET. It is the RSU's responsibility is to secure handover when a vehicle moves from one region to another as shown in Fig.3 [10].

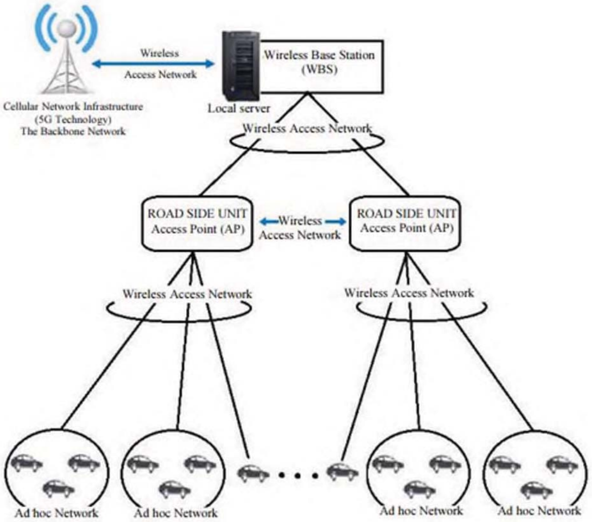

Fig.3- VANET network in IoV [10]

III. Security Requirements of IoV and Blockchain

There is a need for authentication, confidentiality, availability, integrity, and access control in the IoV to be able to secure safety messages from being faked, altered, or sniffed, also to block non-authorized users or malicious nodes from being a part of the network. Blockchain technology is the best fit to cover the security requirements needed for the IoV architecture [11]. In a blockchain, any node must have an identification address. Shared data is signed to assure authentication, the data is encrypted by public-key encryption elliptic curve algorithm which assures confidentiality. The PoW consensus makes it almost impossible to alter the message content, this assures data integrity. For privacy, different privacy-preserving solution mechanisms are proposed to overcome this big challenge [11]. In the following, we present some of the main security requirements.

A. *Authentication*

Authentication ensures that the sender vehicle ID is well identified, and the message is from a genuine sender. To authenticate users in the IoV architecture using blockchain technology, the authors of [12] proposed a BC-based system in which blockchain is deployed and centralized at Road Side Unit (RSU), the credential manager is used to verify the user's authentication and authorization. Also, the RSU contains a ledger to store all vehicle authentication needed data. The authors of [13] proposed that instead of directly asking the RSU for certification, one leader of the authorized vehicles should send the request to nearby RSU. It is somehow a decentralized consensus system where authorized vehicles first validate the data and then share it within the network.

B. *Availability/Real-time Guarantees*

Availability ensures that the vehicle is always connected to the network and the critical data is available when needed even if the node is under attack. The vehicle should remain functional, and the network should be secure and fault tolerant. Real-Time Constraints are very sensitive and critical, having the right data within the right time boundaries is an important requirement. In addition, soft handover between different VANET networks without disconnecting from the network is needed.

Blockchain is a decentralized system that prevents a single point of failure and assures data availability, the problem exists when a vehicle cannot access any nearby RSUs, or the communication link is disconnected. To overcome this issue, the authors in [14] proposed a trust assurance system based on V2V communication, where a vehicle sends messages to nearby vehicles to create a V2V network until the RSU connection is returned.

C. *Data integrity*

Integrity means that the message is correct and has not been altered or dropped. To assure integrity, a sender signature with a hashing algorithm should be deployed. Blockchain enhances data integrity using a trustless consensus mechanism, as each node has its local ledger containing all network shared data and transactions. The Ledger is immutable and well trusted, where only valid transactions and data are stored after having PoW consensus to ensure data integrity. Also, transferred messages are signed and protected using a hashing algorithm, a combination between access control and authentication in addition to a hash algorithm increases the level of trust over the whole system.

D. *Non-repudiation*

Non-Repudiation means that the message sender cannot deny sending the message. This is important, especially in case of accidents, where the investigation unit checks the transmitted messages before the accident to identify the accident environment. In the blockchain, the consensus mechanism assures that no one can deny sending a message. The message is verified by different nodes and saved at the RSU ledger and replicated in all nodes. Every node can verify the other node transactions along with the sender signature and embedded timestamp for the whole block [15].

E. *Confidentiality*

Confidentiality plays an important role in ensuring that only legitimate users can read and access this message and other non-legitimate users do not have access. Confidential information is encrypted using public-key algorithms and only users with a decrypt key can access the needed information. Blockchain uses an elliptic curve public key Asymmetric cryptography algorithm to encrypt the messages before sending them to assure data confidentiality.

F. *Access control*

Access control means having different access levels and roles for nodes and applications to access some data inside the network or perform some operations. To ensure access control for the massive amount of data transferred, the authors of [16] proposed a vehicular management system where RSUs are blockchain nodes to ensure accessibility of the vehicles by checking the block header where there is a list of allowed applications that have access to this content. In addition, a load balancer is assured by spreading the load over different RSUs.

G. *Privacy*

The Vehicles' private data like location, plate number identity, and speed should not be revealed to any non-legitimate authority. Privacy preservation techniques should be used to protect private data from sniffing. To make sure of user anonymity, the authors of [17] proposed a blockchain-based privacy-preserving mechanism where an anonymous authentication trust scheme is used not to reveal private data and to use RSUs as a trusting authority.

H. *Scalability*

Due to the increased number of vehicles that are expected to reach two billion within the next ten years [26], high-speed mobility, and handover between IoV networks, the network should be scalable, and the number of vehicles should be dynamic without any disruption or limitation. Blockchain is based on a decentralized approach where it has no limit for the number of users and is flexible to frequent changes.

Table.1 concludes the security requirements of IoV architecture and the blockchain specifications to meet these requirements.

Table.1- Security Requirements of IoV and Blockchain

Security Requirement	Description	Blockchain Specifications
Authentication	ensures that the sender vehicle ID is well identified, and the message is from a genuine sender.	Blockchain systems can assure authentication by having a credential manager ledger to store all vehicle authentication needed data.
Availability/Real-time Guarantees	Availability ensures that the vehicle is always connected to the network and the critical data is available when needed.	Blockchain is a decentralized system that prevents a single point of failure and assured data availability.
Data integrity	Integrity means that the message is always correct and has not been altered or dropped.	Blockchain enhances data integrity using a trustless consensus mechanism, where only valid transactions and data are stored after having consensus to ensure data integrity.
Non-repudiation	Non-Repudiation means that the message sender cannot deny sending the message.	The consensus mechanism assures that no one can deny sending a message.
Confidentiality	Confidentiality ensures that only legitimate users can read, and access messages and other non-legitimate users do not have access.	Blockchain uses an elliptic curve public key Asymmetric cryptography algorithm to encrypt the messages before sending them to assure data confidentiality.
Access control	Access control means having different access levels and roles for nodes and applications to access some data inside the network or perform some operations.	Blockchain nodes ensure accessibility of the vehicles by checking the block header where there is a list of allowed applications that have access to this content.
Privacy	The vehicle's private data should not be revealed to any non-legitimate authority.	Blockchain assures anonymous authentication trust using a trusting authority.
Scalability	The network should be scalable, and the number of vehicles should be dynamic without any disruption or limitation.	Blockchain is based on a decentralized approach where it has no limit for the number of users and is flexible to frequent changes.

IV. BLOCKCHAIN SYSTEM DESIGN FOR THE IOV FRAMEWORK

To design a secure and highly performing IoV network structure using blockchain technology, there are some needed design principles to be considered. The network should not have a single point of failure. It should be easy for deployment within existing infrastructure and flexible for upgrades and future changes. Scalability is a must where IoV manages a lot of vehicles, and this number is rapidly increasing while taking into consideration the high-speed mobility of the vehicles. The security and reliability aspects are also a part of the network design choice [18].

Existing blockchain technology deals with cryptocurrency while the IoV network deals with vehicle information and road events such as accidents with all associated needed information. Therefore, to adapt the blockchain in the IoV network different proposals were presented in the literature.

The authors of [19] proposed an IoV system design based on blockchain. The key components are RSUs, Traffic Management Authority (TMA), Issuers, Law Enforcement Department (LED), and a group tracking system. For each geographical region, the role of the issuer is to issue vehicle credentials within this region, the group of trackers cooperates to know the identity of senders in case fake messages are discovered. TMA authority is used to hold the public key identifier for the whole system and cover it over, while LED is authorized for revealing the identity of the sender in case fake messages are found and needs for investigations arise. For each region, there is an auxiliary blockchain branch of the parent blockchain and only one parent blockchain including the smart contract to ensure consistency between the whole system. In [20], the authors proposed an ITS seven-layer framework model which is very similar to the open system Interconnection (OSI) networking model. The first layer is the Physical layer which includes all infrastructure and physical components like vehicles, sensors, OBUs, and RSUs. Then comes the data layer in which all blockchain data exists like data blocks, timestamps, and hashing algorithms. The third layer is the Network layer in which all data verifications and forwarding mechanisms are found. The fourth layer is the consensus layer including the Proof of Work (PoW) and Proof of Stake (PoS) algorithms needed for consensus. The following layer is the Incentive layer where all mining activities and rewards exist. The sixth layer is the contract layer where the smart contract needed conditions are found, and the last layer is the application layer where different applications could be deployed over the network. Fig.4 depicts the ITS seven-layer framework [20].

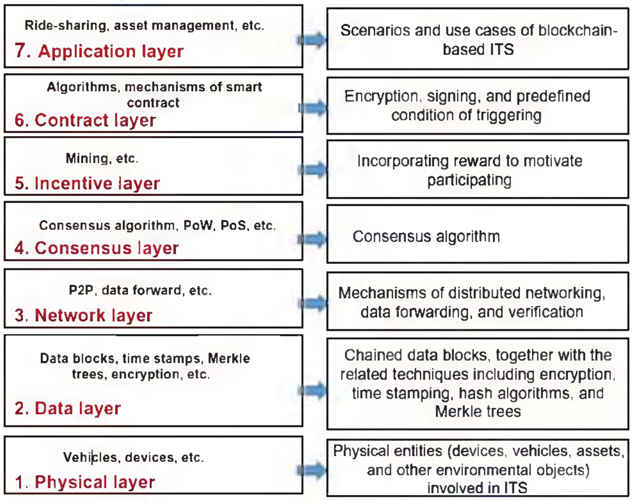
Ride-sharing, asset management, etc.
7. Application layer
Scenarios and use cases of blockchain-based ITS
Algorithms, mechanisms of smart contract
6. Contract layer
Encryption, signing, and predefined condition of triggering
Mining, etc.
5. Incentive layer
Incorporating reward to motivate participating
Consensus algorithm, PoW, PoS, etc.
4. Consensus layer
Consensus algorithm
P2P, data forward, etc.
3. Network layer
Mechanisms of distributed networking, data forwarding, and verification
Data blocks, time stamps, Merkle trees, encryption, etc.
2. Data layer
Chained data blocks, together with the related techniques including encryption, time stamping, hash algorithms, and Merkle trees
Vehicles, devices, etc.
1. Physical layer
Physical entities (devices, vehicles, assets, and other environmental objects) involved in ITS

Fig.4- ITS seven-layer framework [20]

In [21], the authors proposed a four-layer system architecture where the application is the uppermost layer used by users to access the IOV network through web-based interfaces or mobile applications. The application layer interacts with the blockchain layer where smart contracts allow different organizations and service providers to deploy some rules and agreement protocols for successful transactions. It also includes artificial intelligence algorithms to predict and learn vehicle behavior and improve driving assistance. In addition, it holds the consensus algorithms for block validation to be saved inside the database ledger. It also includes the needed algorithms to provide different services. Registration authority should be involved in this layer to verify new registrations during the initial registration phase, location certificate authority is also needed to prove vehicle locations. In addition, vehicle service providers lay into this layer to provide services such as vehicle insurance. The following layer is the database layer, it provides the needed services and stores vehicle details and all transactions over the system. This database is divided into a primary big chain DB database for normal vehicle details and an interplanetary file system for large file storage like vehicle logs.

The lower layer is a peer-to-peer network layer that provides communication between vehicles and IoV network nodes.

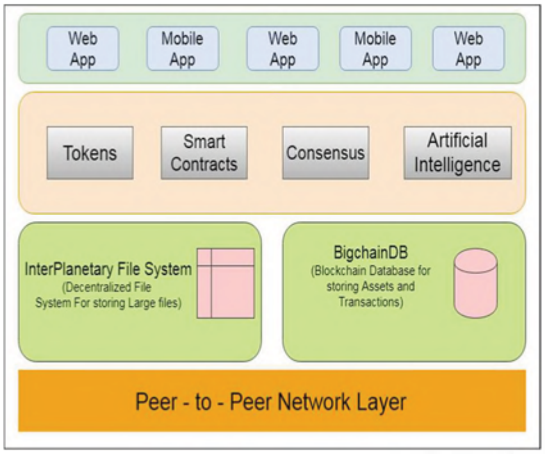
Web App
Mobile App
Web App
Mobile App
Web App
Tokens
Smart Contracts
Consensus
Artificial Intelligence
InterPlanetary File System
(Decentralized File System For storing Large files)
BigchainDB
(Blockchain Database for storing Assets and Transactions)
Peer - to - Peer Network Layer

Fig.5- Four layers blockchain architecture [21]

The authors in [22] proposed a system in which each layer has its own ledger and miners to reach consensus over two different layers. The proposal structure includes top-layer and ground-layer where each layer is completely independent. The ground layer consists of RSUs that are responsible for mining and holding the smart contract, and vehicles to transmit data with low effect range to RSUs, while the top layer is responsible for the data with a high affect range in which all transactions are transmitted by RSUs and Base stations (BS) to check the data validity and integrity then save the transaction over the network.

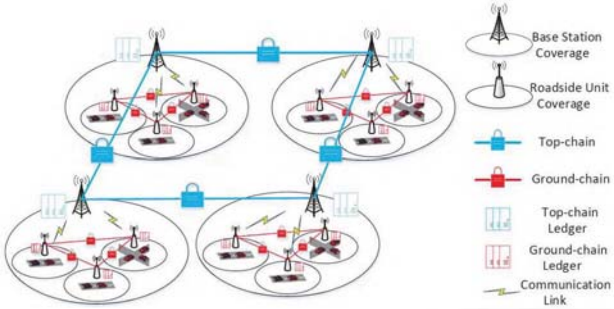

Fig.6- Hierarchical Blockchain Architecture [22]

V. IoV Security Attacks And Solutions based on blockchain TECHNOLOGY.

The IoV is vulnerable to different types of attacks due to the lack of infrastructure, and high mobility nodes with a strict security requirement. In this section, we present the different IoV security attacks and solutions using blockchain technology.

A. Sybil Attacks

In Sybil attacks, a vehicle attacker fabricates its identity and claims to be an authentic valid node using its ID in the network, which is called node impersonation. It can even pretend to be several vehicles with different identities and positions at the same time or in succession.

Increasing the number of fake vehicles in the network could lead to a majority and break the consensus mechanism if gained more than 50 percent of the number of existing nodes in the network. In [17], the authors proposed a three-phase system architecture based on blockchain technology. It consists of registration servers, service providers, blockchain, and a trusted central. These components are responsible together for the verification of vehicle's identification and offering different services if the vehicle is authorized. First, the vehicle must register using its unique identifier then the authentication is done inside the network infrastructure. Afterward, if the vehicle is authorized, it can access the offered services and shared data based on the allowed permission that was predefined by the service provider. Fig. 7 [17] illustrates the three-phase system.

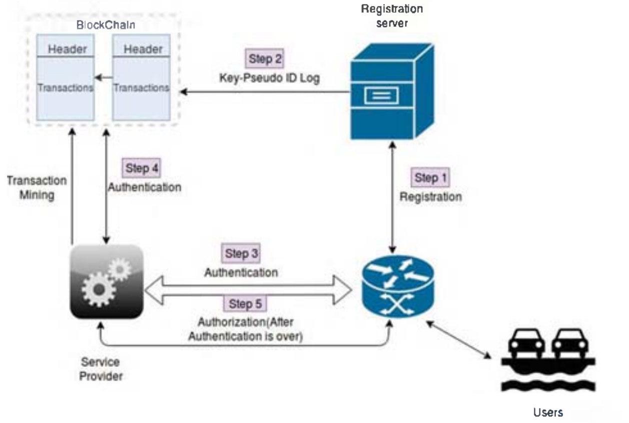

Fig.7- Overview of three-phase system architecture [17]

B. *Denial of Service Attacks*

The Denial of Service (DoS/DDoS) attack is used to consume the target system's resources and disrupt the communication to make some services or resources unavailable or at least reduce network performance by flooding the system with a coordinated massive number of requests until the service becomes unavailable. DDoS attackers control some innocent nodes and use them to launch attacks from different locations at the same time to affect availability. There are some types of DoS attacks in IoV like Jellyfish, intelligent cheater, flooding, and jamming attacks. The authors in [22] proposed a defensive architecture to DDoS attacks, the defense mechanism design is divided into three layers,

1. The first layer is Software-Defined Networks (SDN) in which traffic analysis and security policies are deployed,
2. The second layer is Network Function Virtualization (NFV) where virtualized functions like packet inspection and firewalls are used in response to attacks,
3. The third layer is the blockchain layer that uses smart contracts to provide trusted consensus agreements.

Black and white list addresses are shared among the blockchain network and saved inside the blockchain ledger. The smart contract runs an authentication script so that only certified and authentic nodes are allowed inside the IoV network. The authors in [23] used the Ethereum model and integrated this technology over the IoV network. Ethereum uses the Proof-Of-Stake (POS) concept in which each transaction consumes some stakes (ex. bitcoin), and after consensus, the consumed stakes are restored. However, in case of bad behavior like sending invalid transactions, the stakes will be lost forever as a punishment and the node will be considered unauthorized in the blockchain ledger. In addition, each node has a predefined gas limit value to ensure that it will not exceed the gas limit value while requesting a resource inside the network. If the maximum value is reached no more resources will be consumed. This protects the system from malicious nodes as it will consume its predefined stakes and gas limit before overloading the bandwidth. In case of a planned attack, in which all malicious nodes try to consume the bandwidth within the available gas limit, the bandwidth will not be exhausted as the RSU server node also has a maximum bandwidth for the whole network that should not be exceeded. Fig. 8 [23] depicts the DDoS prevention.

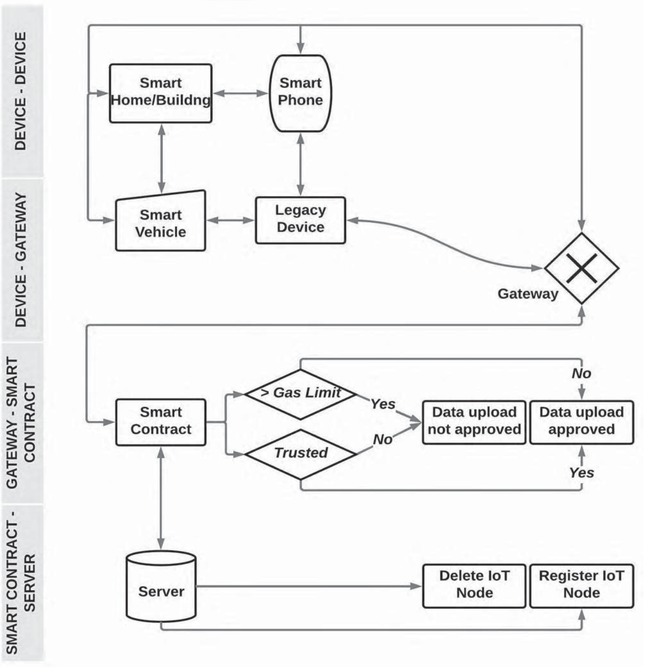

Fig.8- DDoS prevention with gas limit approach [23]

C. *Blackhole/Wormhole Attacks*

In blackhole attacks, the attackers claim that they have the best routing path. Subsequently, they do not re-transmit the message, so the data is lost forever or only sent to other malicious nodes and not forwarded to the rest of the network. In wormhole attacks, the attacker claims to be the best routing path, then after receiving the message instead of dropping it like in a blackhole attack, the intruder encapsulates the message to disorder the hop count, it then forwards the encapsulated message to another malicious node through a private tunnel. The other node decapsulates and re-transmits the message. In [24], the authors proposed using the Euclidean distance method for validation. This method uses signal strength in addition to the sender vehicle's coordinates as an indication for the message travel distance. This could be a validation check for the blockchain network to identify wormholes inside the network in which all nodes are aware of the current position of others. When a malicious node is detected, a consensus agreement is held to decrease the sender ratings and drop the received message or even reject all incoming messages from this malicious node. Another proposed solution in [25] was to use a cluster-based method where each VANET is divided into clusters, and each cluster elects a cluster head internally. This election may be round-robin or based on a random timer. The cluster head's responsibility is to route information among all cluster members. This head is an acceptor, and all other nodes are proposers like in the Paxos consensus agreement [27].

D. *Bogus Information Attack*

Attackers broadcast meaningless or fake information to manipulate other vehicles for evil intentions. This fake information could be false position information to mislead other vehicles about the true position. Illusion attacks send fake information like sensor readings. Other attacks include GPS spoofing attacks in which the attacker uses GPS simulators to generate signals about GPS coordinates, which are more powerful than the satellite signals to mislead innocent vehicles.

E. *Replay/Timing attacks*

Also known as playback attack. Receiving the needed information within the correct time is important in the IoV network. In this attack, malicious nodes add some delay time slots to the transmitted message without any change in the message content. It follows that neighboring vehicles receive time-sensitive messages at a future time when they are no longer needed.

F. *Eavesdropping/sniffing attacks*

A passive attack is used to monitor and analyze the network traffic and steal vehicle confidential and sensitive information like location and vehicle's identity.

G. *Man in the Middle (MiMA) Attacks*

In this attack, the attacker gains access to confidential information and even deletes or alters its content. A malicious vehicle stands between two innocent nodes (V2V or V2I), receives the message from the transmitter node, changes its content, and then forwards the wrong message to the receiver.

H. *Unauthorized access attacks*

In this type of attack, network resources and different services are being accessed by unauthorized nodes which have no privileges or rights to do so.

I. *Brute-force attacks*

Malicious nodes try to steal sensitive information from innocent nodes like ID, or private security keys. They make many trials based on the security algorithm and encryption technique used to secure the information. In blockchain technology, any transmitted message is encrypted using public-key encryption technique, which is unbreakable within a reasonable time, the moving vehicles and frequently changed network nodes increase the difficulty to have such an attack within the blockchain network.

VI. Conclusions and Future Work

The Internet of vehicles is a promising architecture for vehicle connectivity and data sharing among nodes. It has some security requirements and known attacks. Therefore, it is important to integrate the blockchain technology within the IoV network to fulfill the needed requirements and overcome the security attacks. In this paper, we introduced the IoV network architecture and the needed security requirements, we also mentioned how to reach these requirements through the integration of blockchain technology within IoV. In addition, we presented different types of possible attacks over the IoV and the solutions proposed in the literature to overcome these attacks using blockchain. In the future, we plan to propose solutions to other attacks using blockchain technology.

Acknowledgments

This work is fully supported and funded by Valeo Egypt Research and Software Development Center.

References

[1] Sheng Ding and Maode Ma. Springer Nature Singapore Pte Ltd. 2021. An Attribute-Based Access Control Mechanism for Blockchain-Enabled Internet of Vehicles.

[2] Nishant Sharma, Naveen Chauhan, and Narottam Chand. 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC). Security challenges on the Internet of Vehicles (IoV) environment.

[3] Harsha Vasudev and Debasis Das. 978-1-7281-1217-6/19/$31.00 2019 IEEE. An Efficient Authentication and Secure Vehicle-to-Vehicle Communications in an IoV.

[4] Xinshu Ma, Chunpeng Ge, and Zhe Liu. Springer Nature Switzerland AG 2019 J. K. Liu and X. Huang (Eds.): NSS 2019, LNCS 11928, pp. 336–351, 2019. Blockchain-Enabled Privacy-Preserving Internet of Vehicles: Decentralized and Reputation-Based Network Architecture.

[5] Alberto Marroquin, Marco Antonio To RLICT, Cesar A. Azurdia-Meza, Sandy Boluf`e. Conference: IEEE XXXIX CONCAPAN 2019, At Guatemala City, Guatemala. A General Overview of Vehicle-to-X (V2X) Beacon-Based Cooperative Vehicular Networks.

[6] Chaitanya Yavvari. 2019 published by ProQuest LLC. USING VEHICULAR DYNAMICS TO ENHANCE SAFETY AND SECURITY IN CONNECTED AUTONOMOUS VEHICLES.

[7] HAIBO ZHOU, WENCHAO XU, JIACHENG CHEN, AND WEI WANG. 0018-9219 2020 IEEE. Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities.

[8] V. Dedeoglu, R. Jurdak, A. Dorri, R. C. Lunardi, R. A. Michelin, A. F. Zorzo and S. S. Kanhere. Springer Nature Singapore Pte Ltd. 2020. Blockchain Technologies for IoT.

[9] Priyanka Rathee. Springer Nature Singapore Pte Ltd. 2020. Introduction to Blockchain and IoT

[10] Mirador Labrador, Weiyan Hou. (2019) International Conference on Intelligent Computing and its Emerging Applications (ICEA) Implementing blockchain technology on the Internet of Vehicle (IoV).

[11] Leo Mendiboure, Mohamed Aymen Chalouf, Francine Krief. https://doi.org/10.1016/j.compeleceng.2020.106646 0045-7906/ 2020 Elsevier Ltd.Survey on blockchain-based applications on the internet of vehicles.

[12] Noureddine Lasla, Mohamed Younis, Wassim Znaidi, and Dhafer Ben Arbia. 978-1-5386-3662-6/18/$31.00 2018 IEEE. Efficient Distributed Admission and Revocation using Blockchain for Cooperative ITS.

[13] van der Heijden RW, Engelmann F, Modinger D, Schonig F, Kargl F. In: Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. ACM 2017. p. 4. Blockchain: Scalability for resource-constrained accountable vehicle-to-x communication.

[14] Wagner M, McMillin B. 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC). IEEE; 2018. p. 64–73. Cyber-physical transactions: A method for securing VANETs with blockchains.

[15] Philip Asuquo, Chibueze Ogah, Waleed Hathal and Shihan Bao. Springer Nature Singapore Pte Ltd. 2020. Blockchain Meets Cybersecurity: Security, Privacy, Challenges, and Opportunity

[16] Rohit Sharma, and Suchetana Chakraborty. 978-1-5386-4920-6/18/$31.00 2018 IEEE. BlockAPP: Using Blockchain for Authentication and Privacy Preservation in IoV.

[17] Li M, Zhu L, Lin X . IEEE 2019;6(3):4573_84. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing.

[18] Tigang Jiang, Hua Fang, and Honggang Wang. IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 3, JUNE 2019. Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis.

[19] LeiZhang, Mingxing Luo, JiangtaoLi, Man HoAu, Kim-Kwang RaymondChoo, TongChen, ShengweiTian. 2214-2096/2019 Elsevier Inc. Blockchain-based secure data sharing system for the Internet of vehicles: A position paper

[20] Shiho Kim. 2018 Elsevier Inc. https://doi.org/10.1016/bs.adcom.2018.03.010. Blockchain for a Trust Network Among Intelligent Vehicles.

[21] R. Ramaguru , M. Sindhu , and M. Sethumadhavan. Springer Nature Singapore Pte Ltd. 2019. Blockchain for the Internet of Vehicles.

[22] Haoye Chai,Supeng Leng,Ming Zeng, and Haoyang Liang. 978-1-5386-8088-9/19/$31.00 2019 IEEE. A Hierarchical Blockchain Aided Proactive Caching Scheme for Internet of Vehicles.

[23] Uzair Javaid, Ang Kiang Siang, Muhammad Naveed Aman, and Biplab Sikdar. CryBlock'18, June 15, 2018, Munich, Germany, Association for Computing Machinery, ACM ISBN 978-1-4503-5838-5/18/06. Mitigating IoT Device based DDoS Attacks using Blockchain.

[24] Snehal Deshmukh-Bhosalea, and Santosh S. Sonavane. 2351-9789 2019 Elsevier Ltd under responsibility of the 12th International Conference Interdisciplinarity in Engineering. A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things.

[25] Maliheh Shahryari, and Hamid Reza Naj. 2015 Journal of Advanced Computer Science & Technology. A cluster based approach for wormhole attack detection.

[26] Sperling, D., and D. Gordon. Two Billion Cars: Driving Toward Sustainability. Oxford University Press, 2009.

[27] Aleksey Charapko, Ailidani Ailijiang, and Murat Demirbas, Bridging Paxos and Blockchain Consensus, 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber.