Implementing blockchain technology in the Internet of Vehicle (IoV)

Mirador Labrador
School of Information Engineering
Zhengzhou University
Zhengzhou City, PR China
https://orcid.org/0000-0002-3719-7279

Weiyan Hou
School of Information Engineering
Zhengzhou University
Zhengzhou City, PR China
houwy@139.com

***Abstract*— Vehicle Connectivity or the Internet of vehicle (IoV) is projected to be the solution of the pressing issue on traffic, enables a better traffic management system and reduce traffic accidents. On this, however, vehicular communication is a parameters that will ensure its realization. However, vehicular communication is not exempted of the never-ending issues on security and privacy. Thus, this study proposes a mechanism on the utilization of blockchain technology in ensuring authentic vehicle identification and data authentication as data packets are transmitted from one vehicle to another. The study utilizes the Simulation of Urban Mobility (SUMO) and the Objective Modular Network Testbed in C++ (OMNET++) coupled with the developed program and cryptographic algorithm integrated in OMNET++ for vehicle communication process. Results indicate that blockchain is can be used as a security mechanism in vehicle identification and data authentication in the Internet of Vehicle.**

I. Introduction

An automated vehicle system consists of vehicles and the associated networks in which vehicles, roadside units, and other road network infrastructures, coordinates and communicates with each other via the Dedicated Short-Range Communication (DSRC). DSRC are devices that are embedded as part of Road-Side Units (RSUs) and vehicles On-Board Units (OBUs) which facilitates the communications. DSRC governs Vehicular Communication which enables the operationalization of Vehicular Ad hoc Networks (VANET). VANET is the fundamental network structure of Internet of Vehicle (IoV)

IoV security requirement (VANETs in particular) – their challenges and security attacks has been identified and investigated in [2]. Further, in VANET, information is exchanged over a shared wireless medium with a limited communication range [7]. The exchanged of information are governed by smart devices that is being equipped with wireless communication systems. Unfortunately however, smart devices also captures critical vehicle data such vehicle ID, locations, registration number, etc., which at the macro level compromises data security and privacy. On this, studies on VANETs security mechanisms and approaches has been undertaken. However, most of the proposed VANET security approaches are primarily based on Public Key Cryptography (PKC) and Secret Key Cryptography (SKC) [8]. Note that PKC and SKC based security solutions has a large computational overhead and requires ubiquitous connectivity of the smart devices [1] making it ill-suited in VANET architecture. Thus, the main motivation of this study is to design a robust security and privacy solution based on blockchain technology and cryptographic functions considering the complimentary and decentralized features of both the blockchain and VANET architecture.

Implementing blockchain technology in the Internet of Vehicle (IoV) explores its applicability as a security solution in VANET. Particularly, it proposes the use of blockchain for vehicle identification and data authentication. In the context of this paper, vehicle identification is a mechanism to which a vehicle identifies other vehicle (i.e. vehicle registration number, plate number, etc.) and data authentication is a data verification process where only those authorized receivers would be able to decode or unpacked the message.

II. Related Works

The most common security mechanism and approaches for vehicular communications are the Public Key Cryptography (PKC) and Secret Key Cryptography [8]. PKC approach includes both the Traditional Public Key Infrastructure (PKI) and the group signature techniques. In [6], it argues that in a group signature, the unique cryptographic primitive is an important characteristic that matches the privacy and security requirements of VANETs. The study also pointed out that the different privacy and security requirements should be anchored on the types of VANET communication – the vehicle-to-vehicle (V2V) and the vehicle-to-infrastructure (V2I) and should be in accordance to the combination of group identity and signature (ID) techniques. Though the study enables a privacy-preserving and novel secure protocol for vehicular communication however, it creates a heavy overhead in signature verification. The scenario resulted to a failure in authentication and verification of the received messages. In the same context, the study in [12] an enhanced mechanism of a PKC-based signature using a cryptographic primitive called batch signature providing an efficient authentication protocol for vehicular communication has been developed. The study reduced the RSU message overhead verification. However, the proposed mechanism is found to be vulnerable to Denial of Service (DoS) attack when a false data is injected.

Conversely, the used of token as security mechanism in VANET has been also explored. In [7], a token-based trust vehicle in VANET was proposed. The method was found to be viable for secure and lightweight trusted communication. In [2 -3], a Trusted Ad-hoc On-demand Distance Vector routing protocol was proposed. The model uses a trust model that establishes a malicious free route in a multi-hope manner for every source node transmission. Studies of [9-11] also maximizes the potential of token-based approach in implementing a secure communication VANET.

The different security approaches introduced above explores the utilization of PKC, SKC and token based methods. PKC and SKC method relies on encryption scheme where a key is used for data encryption and decryption. It

978-1-7281-3159-7/19/$31.00 ©2019 IEEE

defines public-key-infrastructure (PKI) –based approach for securing message sent in vehicle-to-vehicle and vehicle-to-infrastructure fashion. While a token-based security approach is based on trust-based management scheme as a mean to identify the trustee and the truster. In general, token based security approach uses certificates as a mechanism to identify and authenticate information.

On the contrary, this paper proposes blockchain based approach as security mechanism for IoV. Blockchain is a decentralized security solution that is complimentary to the characteristics of VANET network structure. In blockchain, data are in a form block which is being generated and transmitted by the vehicle itself. Thus the approach makes the data more secure and authentic.

III. THE BLOCKCHAIN APPROACH

Implementing blockchain technology in IoV requires network model and data set standard. On this, IoV network model has been proposed as described in figure 1. The network model in figure 1 is divided into two parts – (1) the backbone network and (2) the blockchain operated network [5].

The backbone network governs the network connection between the base station and the cellular network facility. It provides the internet connectivity and data requirement of IoV operations via the localized server serving as Wireless Base Station (WBS). Conversely, the blockchain operated network comprises of Vehicle-to-vehicle (V2V) communication (as defined by the ad hoc network), the vehicle-to-infrastructure (V2I) communication – the network connection between the vehicle in the ad hoc network to the RSU, and the I2I (infrastructure-to-infrastructure) communication as defined between RSU to RSU communication via wired or wireless connection governed by Wireless Base Station (Server).

In this proposed technique, detailed vehicle information is stored and controlled by the localized WBS and is only referenced in block-field. The main reason is the limited size of block-field and to reduce the bulk of data transmitted in the network, ensuring a faster transfer process. In other words, data blocks generated by vehicles are in small data size. However, a particular field in data block references the information stored in WBS such as vehicle information – vehicle registration number, vehicle owner, vehicle type and model, etc. [5].

Conversely, standard data set refers to the different data-fields that will form as block. Standardizing block-fields is necessary to ensure data consistency. Consistency of data is necessary in order to simplify data aggregation, avoid data redundancy, and reduce network data traffic. On this, two factors are being considered: (1) the standard block fields, and (2) the standard blockchain based transaction process.

On this study, the standard block fields includes: (1) the generic blockhash, (2) previous blockhash, (3) timestamp and (4) transaction records. Note that Transaction root is a hash function comprising the input message (if there is, a message can be null) and the private key used for encryption purposes which will enhance the transaction security as the block is in the network. Each block components are defined as follows:

- Generic Blockhash – The generic blockhash is a self-generated hash (an inherent hash function) of vehicle. The hash contains vehicle identification (ID) and block version.
- Previous Blockhash – this hash functions refers to the transaction records coming from the generating vehicle. The presence of this component in the block structure constitutes the blockchain process.

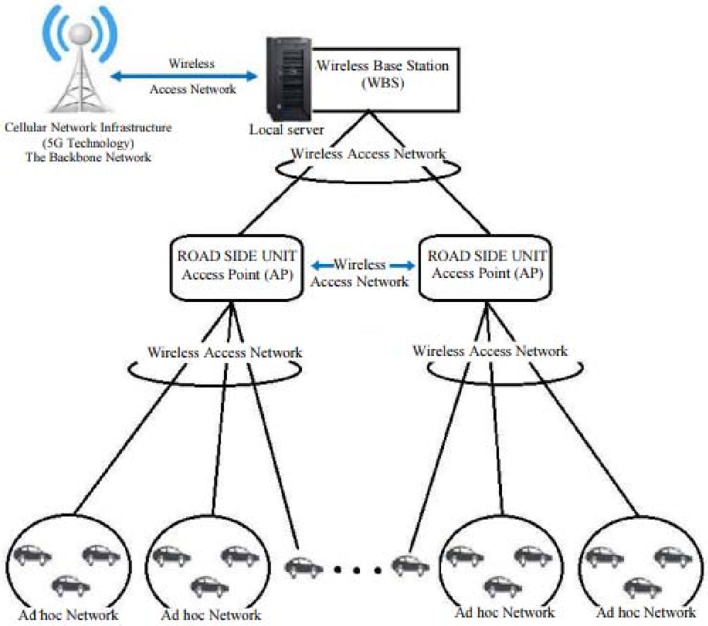


Figure 1. Blockchain based IoV network

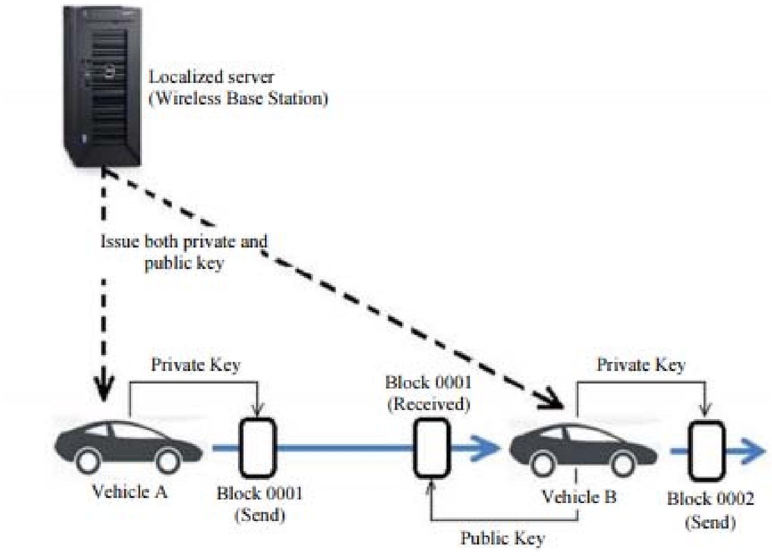


Figure 2. Blockchain based transaction

- Timestamp – timestamp refers to the actual time of block generation, the current speed of the vehicle, it current location and direction. Hash function generation for timestamp considers the relevant vehicle sensor such as the speedometer, GPS and others.
- Transaction Root/Records – this refers to the inputted message by the drivers (note that message may be null– in cases to which a driver opt to attached messages i.e. emergency needs and assistance, vehicle status, etc.) and the associated encryption algorithm (private key) in order to ensure authenticity of the transaction.

In reference to the different block fields defined above and in conformity with the existing block hashing algorithm, the block size of this proposed security mechanism is 256 bits which is based on SHA256 Cryptographic Hash Algorithm. In particular, however the hash value size for encryption is set to 4-bytes which is used as part of the component of transaction records where data are also incorporated.

Blockchain based transaction security encompasses both information security and transaction security. Information security refers to data authenticity, validity and confidentiality, while transaction security refers to transaction authenticity and confidentiality.

Note that all things written in the blocks are encrypted and approved by distributed anonymity participators for and in the case of vehicles. In fact, in a simplest context, the block itself represents a digital fingerprint. And that, in theoretical aspect, digital fingerprint is unique to each block which makes block data to be tamperproof – guaranteeing data authenticity.

Although the block itself is authentic in form, however in an IoV blockchain operation, the transaction (as the block is broadcasted and received) still needs to be validated and authenticated and as such, the use of public key cryptographic scheme as part of the block is incorporated. In Figure 1, it is assumed that a private and public key are being issued to each vehicle by the localized server. However on the context of this paper it is a prerequisite that the localized server as shown in figure 2 isued both the private and public key to each vehicle prior to operation and at the same time the vehicle unique ID and other relevant information are being generated and stored by the WBS itself. This process can be done during the time that the vehicle is being applied for registration immediately after purchase. In other words, the localized server is controlled and operated by the vehicle registering agency or the local traffic controller office of a certain area. Note that vehicle detailed information and public keys as generated by WBS can be shared also and into the other WBS via the backbone network to ensure continuity of vehicle communications as it jumps from one network domain (from one traffic controller to another) to another. In particular, the following steps define the blockchain based IoV transaction:

1. The localized server generates and store vehicle ID and other relevant information upon vehicle registration and issues both the private and public key needed in blockchain cryptographic requirements to the registering vehicle
2. Vehicle A, generates generate blockhash function for the block to be broadcasted in a network (inclusive of all the block components as defined in Figure 2
3. Vehicle A broadcast the block in the network
4. Vehicle B, receives the block, validates the transaction authenticity and block authenticity. When vehicle B

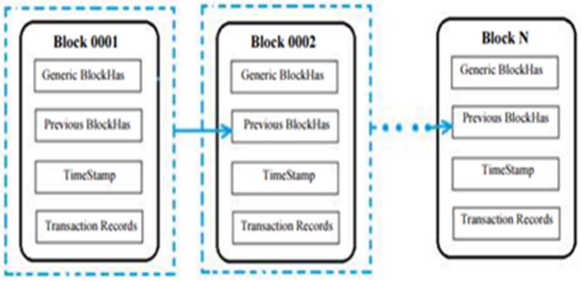


Figure 3. The IoV Blockchain Mechanism

rebroadcast the block in the network it will attach the previous block hash to its generated block – realizing the blockchain mechanism.

Figure 2 reflects the graphical representation of the IoV blockchain based network transaction in an Ad hoc network manner. Note that the same mechanism holds true for V2I communications, the only difference is that some parameters in the generic hash may not be the same with that of vehicle (i.e., Roadside Unit ID instead of Vehicle ID; RSU status instead of Vehicle status, etc.).

Although generic information are embedded within the block through the generic block hash, the public key cryptographic services is also essential to ensure the privacy-preserving communication demand of communicating vehicles as noted earlier. It also provides the proof of authenticity of every transaction. In a much better perspective, when vehicle A attaches an encryption in the block transaction component, it is as if, that the vehicle itself is attaching a token to the block so that only those vehicles that knows and have the token (in a form of a public key) are allowed to receive the block. In other words, the public cryptographic service in the blockchain operation serves also as a handshake mechanism between the transmitting and receiving vehicle. Note that the receiving vehicle requires the previous block hash function so that it would be able to generate a new block containing the information of the previous block satisfying the blockchain mechanism as shown in Figure 3.

On the different context, when the block is received by vehicle that does not have a public key, then it could not validate the transaction and as such it could not decrypt the message, could not append the transaction records and at the end it could not use the block. In other words, the block becomes useless. In particular only those that has a public key may continue to use the block and re-forward it again in the network (as part of the new block and as the case maybe). This process ensures transaction anonymity, privacy and confidentiality.

In this proposed technique, vehicle can authenticate transactions itself without the intervention of RSU or the centralized sever. This mechanism is in conformity with the decentralized network characteristics of V2V communications, although the role of a central server (CS) in the operation could not be denied. The CS is the central traffic controller of a certain area, the one that control the traffic light units, manages RSU and allocates blocks for each vehicle with the provision of cryptographic keys [5].

IV. Experimental set-up

Proposed approach was tested using 2 platforms, the Simulation for Urban Mobility (SUMO) and the Objective Modular Network Testbed in C++ (OMNET++). The SUMO was used in simulating the road set-up scenario, OMNET++ in simulating the visual communication and transaction authentication between vehicles-vehicles and vehicles-RSUs via blockchain mechanism.

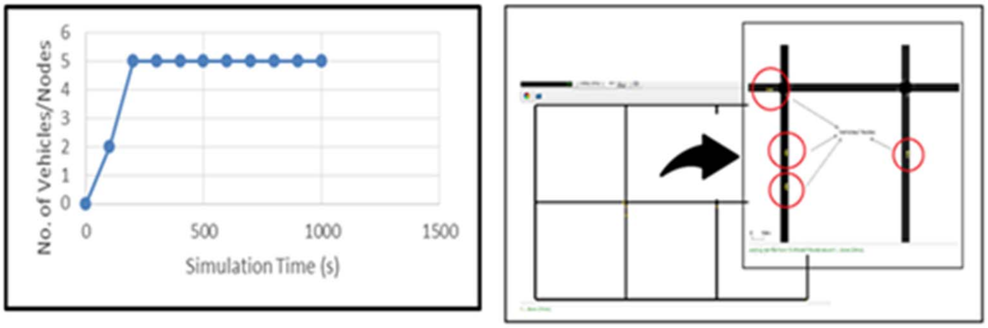
In SUMO, a 2 x 3 Manhattan grid with segment length of 300m with the same priority was used. Every intersection follows the right-before-left priority rule and each road segment has one lane in each direction. For all simulation the Krauss car-following model was used for vehicle with a predefined parameters generated by SUMO. Each trip has a source and destination chosen at random as defined by the generated trips.trips.xml file of randomTrips.py SUMO function. The route for each trip is computed using duarouter defined and generated also by randomTrips.py function. The simulation set-up uses a fixed number of 5 vehicles and the simulation stop when the simulation time is over set 10000 seconds.

Vehicular communication was analysed using OMNET++ coupled with the SUMO. In particular, vehicles (nodes) transmission parameters are being predefined and are uniform so as to remove transmission biases. Nodes mobility are defined by SUMO via veins-plexe module. Two vehicles (nodes) are pre-programmed as unregistered while three vehicles (nodes) are pre-programed as registered vehicles and one of the pre-programmed registered vehicle are further pre-programmed to re-forward all received messages to simulate the blockchain process. Pre-programming of this node are done in OMNET++ environment which becomes one of the function libraries of the project. The success of authentication are measured by tabulating the rate of success of authenticating valid messages and the rate of success of rejecting un-valid messages by the registered vehicle.

V. Results and Discussion

A. *Road and Traffic Scenario*

Road and Traffic Scenario are defined via SUMO. Parameters are set in accordance to the description described



(a) (b)

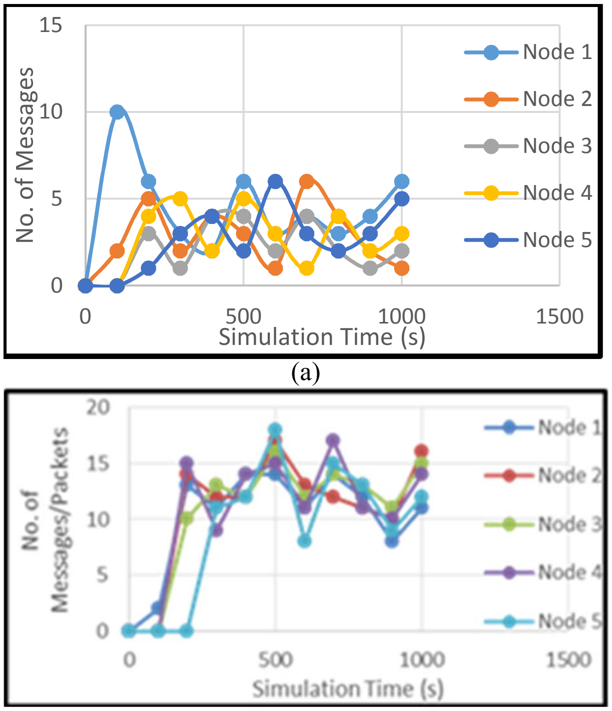
Figure 4. Vehicle Mobility Characteristics (a) No. of Vehicle v. Simulation Time
(b) Vehicle Actual Scenario in SUMO

in the experimental set-up. Vehicle movements i.e. speed, accelerations, etc., are automatically generated with the use of druarouter. Duarouter imports different demand definitions, computes vehicle routes using the shortest path algorithm. Figure 1 shows the number of vehicles in the scenario over a period of time. Only a single vehicle enters to the scenario in particular time as pre-set by duarouter via the randomTrips.py function.

Figure 4(a) shows the number of vehicles that are moving in a 2x3 manhattan grid road network as shown in figure 4(b). Further, as indicated in the figures, all numbers of nodes already enters in the simulation environment at approximately after 200 seconds. The actual positions of 4 nodes are highlighted in Figure 4(b).

B. Communication Scenario

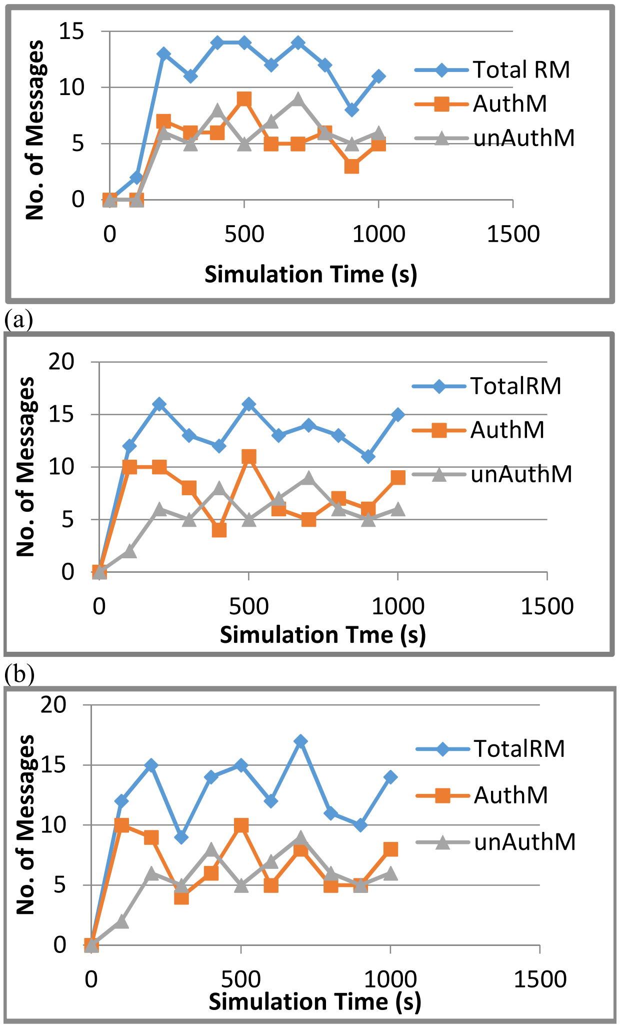
Vehicle communication has been defined via OMNET++. However additional source codes consolidated as Bloackchain Approach are being developed which includes: (1) Blockchain.cc; (2) Blockchain.h; and (3) Blockchain.ned. The sources codes define the Blockchain approach as proposed on this study. On this, results characteristics of individual vehicle/nodes data transmission and reception are indicated in figure 5. Node 0 has the greatest number of transmissions from the start of simulation period up to 200 seconds. This is because node 0 is the first node that enters in the scenario and made significant number of data transmission which was received by the defined Road Side Unit (RSU) in the OMNET++ environment. On average, each node was able to transmit of around 4 data packets for every 200 seconds. Comparatively analyzing the nodes messages transmission characteristics with that of nodes message reception characteristics as described by figure 5 (a) and (b), it can be seen that though there is a number of transmitted of messages between 0 -200 seconds period, however only few messages are received. This situation is due to the fact that only a single node is in the scenario transmitting a message on that particular period (nodes/vehicle enters the scenario in different periods) and that there are no available nodes that captures or received such messages.



(a)

(b)

Figure 5. Individual Vehicle/Nodes (a) data transmission (b) data reception characteristics



(a)

(b)

(c)

Figure 6. Vehicle/Nodes Data Authentication Performance (a) Vehicle/Node 0, Vehicle/Node 2,

Figure5 also indicate that each node receives more data than it has been able to transmit data. This is because as nodes transmit messages all other nodes would be able to receive such transmitted messages (note that the transmission range set for each node covers the entire simulation areas). When one node is on transmission mode, all other nodes are on data reception mode as defined by the broadcast protocol used in simulation.

C. Vehicle/Node Identification and Data Authentication

Vehicle identification and data authentication follows the privacy-preserving communication as described in section III and IV of this paper. In addition, specific identification and authentication processes are integrated as functionalities in the developed Blockchain Approach codes (Blockchain.cc;

blockchain.h and blockchain.ned). Results are shown in figure 6 (a), (b) and (c). In particular, only registered nodes 0, 2 and 3 are set to undertake nodes identification and data authentication.

Figure 6 (a), (b) and (c) depicts the nodes identification and data authentication performance of registered nodes 0, 2, refers to received data transmitted by registered nodes as verified during identification and authentication process while unathenticated Messages (unAuthM) refers to received data transmitted by unregistered nodes. unAuthM are data received but unrecognized by the receiving nodes (unrecognized data are lost along the process as it could not be identified and authenticated).

D. *The blockchain mechanism*

As noted earlier, blockchain mechanism was realized by setting one of the registered nodes as a re-forwarding node. In particularly, node 3 was pre-programmed to function as a re-forwarding node. Re-forwarding means that received messages would then be rebroadcasted again into the network after proper node identification and authentication. Re-forwarded messages contain the original data as received however, additional information from the re-forwarding nodes are added to it. The process constitutes with that of blockchain mechanism as described in figure 2 and 3

Figure 7 shows the nodes characteristics of re-forwarding nodes in terms received messages, authenticated messages and messages categorized as Blockchain Messages (BChainM). Note however that, the message re-forwarding node is set not to broadcast its own message but was preset only to capture messages and once the said messages have been authenticated it will be re-forwarded again into the network (when it is already allowed to transmit data).

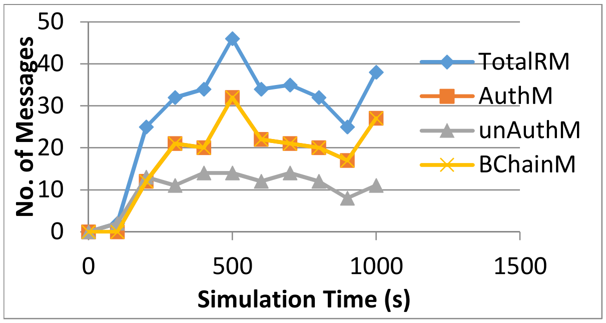


Figure 7. Data transmission characteristics of re-forwarding nodes

Considering the random data transmission assignment among the nodes, therefore not all received messages would be re-forwarded back to the network. Figure 7, shows the number of messages categorized as Blockchain Messages (BChainM). BChainM are data packets that have been transmitted by the re-forwarding node back to the network. This data is identified and authenticated by the node itself. The figure indicates that 12% of the received and authenticated data constitute to that of Blockchain Messages.

VI. Conclusion

The used of blockchain technology as a security solution – particularly on vehicle identification and data authentication was realized on this paper via the used of SUMO and OMNET++ simulator. Results indicate that in Vehicular communication, blockchain technology can be implemented with the associated cryptographic functions through the implementation of the Blockchain Approach as coded in OMNET++ environment. The proposed method enables vehicular identification and data authentication. Therefore, with the 100% nodes identification and data validation the mechanism can be used as a security solution in the implementation of IoV.

Note that the proposed security model was implemented in SUMO and OMNET++ coupled with the developed blockchain based communication algorithm. However, the paper did undertake encryption and decryption performance evaluation. Likewise, it did not undertake comparative authentication performance analysis as compared to existing algorithms and methods.

Acknowledgment

This is to acknowledge the Zhengzhou University and Samar State University for the opportunity being provided to the author.

References

[1] Sharma, K., Chaurasia, B. K., Verma, S., &Tomar, G. S. (2016). Token Based Trust Computation in VANET. International Journal of Grid and Distributed Computing, 9(5), 313-320

[2] Mokhtar, B., & Azab, M. (2015). Survey on security issues in vehicular ad hoc networks. Alexandria Engineering Journal, 54(4), 1115-1126.

[3] Shilpa, P., &Patil, R. B. (2015) COOPERATIVE MESSAGE AUTHENTICATION AND RESISTING FREE RIDING ATTACKS IN VANETs. International Journal of Research in Engineering and Technology, Volume 04

[4] Claeys, T., Rousseau, F., &Tourancheau, B. (2017, September). Securing Complex IoT Platforms with Token Based Access Control and Authenticated Key Establishment. In International Workshop on Secure Internet of Things (SIoT).

[5] Labrador, M. & Hou, W. (2019). Security Mechanism for Vehicle Identification and Transaction Authentication in the Internet of Vehicles (IoV) Scenario: A Block Chain Based Model, Journal of Computer Science, 15(2), 249-257

[6] Shilpa, P., & Patil, R. B. (2015). Cooperative message authentication and resisting free riding attacks in VANETS. Int J Res Eng Technol, 4(5), 127-131.

[7] Lin, X., Sun, X., Wang, X., Zhang, C., Ho, P. H., & Shen, X. (2008). TSVC: Timed efficient and secure vehicular communications with privacy preserving. IEEE Transactions on Wireless Communications, 7(12), 4987-4998.

[8] Zhang, C., Lu, R., Lin, X., Ho, P. H., & Shen, X. (2008, April). An efficient identity-based batch verification scheme for vehicular sensor networks. In IEEE INFOCOM 2008-The 27th Conference on Computer Communications (pp. 246-250). IEEE.

[9] Sharma, K., Chaurasia, B. J., Verma, S., & Tomar, G. S. (2016). Token Based Trust Computation in VANET. International Journal of Grid & Distributed Computing, 9(5), 313-320

[10] Debasish, R., & Das, P. (2017). Trusted and Secured Routing Protocol for Vehicular Ad-Hoc Networks, Indian Journal of Science and Technology, 10(17)

[11] Vaze, B. A., Shende, R., & Sahare, V. (2017). A New Token Based Scheme For Privacy Preserving Security in VANET, Proceedings, of WRFER-IEEEFORUM International Conference

[12] Yue, X., Chen, B., Wang, X., Duan, Y., Gao, M., & He, Y. (2018). An Efficient and Secure Anonymous Authentication Scheme for VANETs Based on the Framework of Group Signatures. IEEE Access, 6, 62584-62600.