Journal of Computer Science

Original Research Paper

Security Mechanism for Vehicle Identification and Transaction Authentication in the Internet of Vehicle (IoV) Scenario: A Blockchain Based Model

[1,2]Mirador Labrador and [1]Weiyan Hou

[1]School of Information Engineering, Zhengzhou University, Zhengzhou City, China
[2]College of Engineering, Samar State University, Catbalogan City, Philippines

Article history
Received: 31-10-2018
Revised: 06-01-2019
Accepted: 12-02-2019

Corresponding Author:
Mirador Labrador
Samar State University,
Catbalogan City, Philippines

Email: labradormirador@yahoo.com

Abstract: Internet of Vehicle (IoV) is now changing the landscape of Transportation System-paving the way of the so called Intelligent Transport System as it is being powered by the plethora of converging smart sensors and technologies. However, beyond its potential, this technology is still in a ground zero level considering the many facets of issues and concerns that needs to be addressed prior to its full implementation. One of the never ending and unresolved issues is on the area of Security and Privacy. In fact, security and privacy is always the prevailing concern not only of that of IoV but also in other areas of Communication and Network dependent systems. On this note, this paper directs the utilization of the Blockchain Technology Coupled with Public Key Cryptography as a security mechanism for Vehicle Identification and Transaction Authentication in IoV scenario. It lays down also the associated network model for a Blockchain based security processes. It also defines and describes the IoV Block and Blockchain requirements and conditions as the block are being propagated in the network.

Keywords: Blockchain, Security and Privacy, Internet of Vehicle, Ad hoc Network, Intelligent Transport System

Introduction

The importance of Technology goes beyond measures in the history of human life. This is because in today's reality, every aspect of our human endeavour is already anchored with that of technology – it seems that life without technology is meaningless. In fact, economic progress and sustainability can now be dictated by the extent of technology adoption, utilization and integration. With this, the interconnection of devices becomes prevalence giving rise to what is popular known as Internet of Things (IoT) which include the so called the Internet of Vehicle (IoV).

Internet of Vehicle is an open and integrated network system with high manageability, controllability, operationalization and credibility and is composed of multiple users, multiple vehicles, multiple things and multiple networks (Fangchun *et al*., 2014) IoV is now changing the landscape transportation system – paving the way of the so called Intelligent Transport System. From its basic concept, IoV requires the interconnection of a pervasive and mission-critical sensors and actuators which is often referred to as smart devices. Smart devices includes: (1) the vehicles on board units (OBU); (2) the road side units (RSU); (3) the traffic lights; (4) application units; (5) gateways and other electronic devices. The interconnection of these smart devices leads to the generations and access of the vast amount of information. Note that, the transfer and access of information implies significant privacy and security issues.

In fact, any smart device has an ability to collect sensitive and personal information. For this case, IoV creates a new security challenge which cannot be overcome by simply using a simple data security and privacy mechanism. In addition, smart devices in IoV prompted the introduction of "infotainment and telematics" applications which becomes a common application programs used by drivers themselves. Usually, these applications were built on vehicles on board units and driver's "brought-in" phone. And as such, if we consider the triangulation of data coming from this myriad of smart devices then the issues on privacy and security will truly exist.

Science Publications

© 2019 Mirador Labrador and Weiyan Hou. This open access article is distributed under a Creative Commons Attribution (CC-BY) 3.0 license.

Accordingly, due to IoV dynamic topological structures, huge network scale, non-uniform distribution of nodes and mobile limitation, it becomes prone to various forms of attacks such as authentication and identification attacks, availability attacks, confidentiality attacks, routing attacks, data authenticity and etc. It is on this reasons that IoV indeed requires security and privacy mechanisms (Sun *et al*., 2015).

On the other hand, blockchain is a technology that is argued to be robust and provide strong security solution. In fact, the block itself is time-stamped which contain all the transaction records (Schutzer and Comer, 2016). In other words, information in IoV operations can be provided by means of the so-called "trusted Timestamping". A timestamp is a sequence of characters or encoded information identifying when a certain events occurs, usually giving date and time of day, sometimes accurate to small fraction of second (Zheng *et al*., 2017). Further, blockchain is a distributed system which does not require central authority and third party intermediaries across programming. All of these blockchain characteristics make it ideal with that of IoV processes. In addition, all accounts created in blockchain system do not establish a direct relationship to the entities in the real world maintaining privacy and anonymity.

In particular, this article deals on Blockchain Based Model in vehicle identification and transaction authentication with the main objective - strengthening data security and maintaining privacy. Alongside with this, significant IoV security mechanism are being explored, discussed and presented. Also, blockchain complementing features with that of IoV operations are being identified and discussed.

Related Works in IoV Security

At macro-level, it is important to point-out that security and privacy in IoV processes is one of the prevailing issues that need substantial consideration. In fact, security and privacy is always the prevailing concern not only of that of IoV but also in other areas of Communication and Network dependent systems. As noted previously, the heterogeneous and dynamic nature of IoV brings up several questions related to security and privacy, which must be addressed properly by taking into account its specific characteristics and the environment they operate in. Thus, this scenario entails an extensive review on IoV security and privacy implementation.

One of the classic security and privacy examples in IoV is the Message-linkable Group Signatures (MLGS) (Domingo-Ferrer and Wu, 2009). MLGS is a privacy-preserving system that thwarts Sybil attack and at the same time guarantees message authentication through both a priori and a posteriori countermeasures. However, in general perspective, Choi *et al*. (2011) categorizes IoV security and privacy into three groups: (1) cryptography based, (2) grouping based and (3) unlinkability based.

The main goal of cryptographic-based security and privacy mechanism is to hide the identity of the message sender using a key. Ming and Shen (2018) proposed a practical certificateless conditional privacy preserving authentication (PCPA) scheme integrating the concept of certificateless signature with message recovery (CLS-MR) which is based on certificateless cryptography and elliptic curve cryptography mechanism. Accordingly, aside from satisfying all security and privacy requirements, PCPA has a low computation and communication costs because it does not use the bilinear pairing and map-to-point hash operation. In a different context, Bouabdellah *et al*. (2016) proposed a trust cooperative transmission protocol for multiple-hops broadcast in Vehicular Ad hoc Network (VANET) which selects among all relays only the best ones minimizing a function of finite number metrics. The said protocol uses ciphertext-policy attribute based encryption – a primitive cryptography technique that ensures confidential communication between the source and the destination. Other cryptographic-based IoV security and privacy mechanism are presented in the paper of Choi *et al*. (2011) which includes: (1) Group Signature and Identity Signature (GSIS) – a protocol wherein a recipients uses the group public key to verify a message signature and (2) Location Privacy Preserving Authentication Scheme (LPPAS) – a protocol that adopts a blind signature to protect VANET privacy.

A Grouping-based protocol is a complementary approach to privacy preservation. The key idea of grouping-based protocols is to hide the vehicle's explicit identity and location in a group (Choi *et al*., 2011). The US Department of Transportation (2006) proposed a Group-based secure source authentication (GSA) protocol for VANETs. GSA makes use of group attributes as dynamic group key to protect data transmission in intra-group communication, which is dynamic changing with real-time environment and consistently updates among group members. Also, Kumar and Nayak (2013) proposed an efficient group-based safety message transmission protocol for VANET. The protocol aims to improve the safety alert message communication in VANET using grouping of vehicles. While Lloret *et al*. (2013) proposed a Group-based protocol and mobility model for VANETs where in each public transport vehicle forms a group of vehicles - each vehicle can access and allow access to internet through the public transport vehicle. Moreover, Khan *et al*. (2014) proposed a group based key sharing and management algorithm for vehicular ad hoc networks. The said algorithm utilizes a midia mixing algorithm that decides what information should be provided to each user and how to provide such information.

The third approach referred as unlinkability approaches which deal on addressing the linkability issues that is caused by the same certificate being issued repeatedly. Unlinkability is an approach that uses a concept of ephemeral in issuing the identifications and certificates. On this aspect, the identification of the message is made open to the public but then uses a different approach in identification of two messages coming from the same vehicle. Also, Weerasinghe *et al*. (2011) proposed a synchronized pseudonyms changing protocol based on the concept of forming groups among neighboring vehicles which aims to enhance unlinkability in vehicular ad hoc networks. Among of the key identified advantage of the said protocols are (1) it makes larger anonymity set and higher entropy; (2) it reduces the tracking probability; (3) it can be used in both safety and non-safety communications: and (4) vehicles need not suspend regular communication for changing pseudonyms. Jiang *et al*. (2014) proposed an Efficient Ticket Based Authentication Protocol with Unlinkability for Wireless Access Network. Accordingly, the said protocol is found to be effective in protecting the weakness identified by Hsieh and Leu (2014) wherein they proposed the anonymous authentication protocol based on elliptic curve cryptography. Other protocols falls under this approach includes: (1) Raya and Hubaux protocol called Huge Anonymous Certificate Protocol (HAP) which installs a large number of certificates at about 43,8000 in advance and randomly selects one of them to sign a message (Raya and Hubaux, 2007); (2) Ming and Shen (2018) proposed a protocol similar to HAP, the exception being its use of short-lived anonymous certificate; (3) Identity-Based Encryption (IBE) cryptography as proposed by Zhang *et al*. (2008) is another protocol for VANET wherein a vehicle's identification is set to its public key and the vehicle keeps changing its ID quickly to avoid being tracked; and (4) the Efficient Conditional Privacy Preservation Protocol (Lu *et al*., 2008) which sought to solve the storage requirement by using the RSU to manage the vehicle's certificate. And at the same time of authentication, the RSU issues only ephemeral certificates for valid vehicles, eliminating the need for vehicles to manage the certificates and RL.

The Blockchain Technology

Blockchain is to be taught as an innovation for managing digital society, which provides fundamental principles to support democratically distributed application complementing with that of the characteristics of IoV operations. Blockchain guarantees that all written in blocks are encrypted and approved by distributed anonymity participator which is very ideal in IoV operation considering the mobility characteristics of vehicle-to-vehicle communication while ensuring the accuracy of messages in every transaction/operations. In fact, blockchain provides an unchangeable distributed system with strong security measures. Blockchain structure is shown in Fig. 1.

Generally, blockchain is divided into two parts as indicated in Fig. 1(a). One is the block headers of the blockchain and the other is all transaction stored in the existing blocks. Block header includes block version, parent block hash value, Merkle root, timestamp, difficulty and nonce.

Block version store the relevant version number of the blockchain system and protocol. In other words, it indicates which set of block validation rules to follow. Parent Block Hash Value records the hash value of the previous block. Note that all blocks in the parent block hash value can be joined together to form a blockchain, which makes it also more difficult to be tampered. It is because the new blocks are constantly being superimposed on the old blocks, the hash values of old pieces will continue to be passed to the latest piece. The more stacking of the hash value the harder it is to modify the earlier. Merkle Root refers to the hash value of all the transactions in the block. The hash value of Merkle tree root in blockchain can be used to quickly check the correctness of all stored transaction on current block. Note that fundamentally, a merkle are data structure trees where each non-leaf node is a hash of its respective child nodes. The leaf nodes are the lowest tier of nodes in the tree (Curran, 2018). Timestamp records the block generation time in year, month day, hour and second. Difficulty refers to the target threshold of a valid block hash. And a nonce which is an arbitrary number (bits code) that are added as part of the block which further makes the block more different.

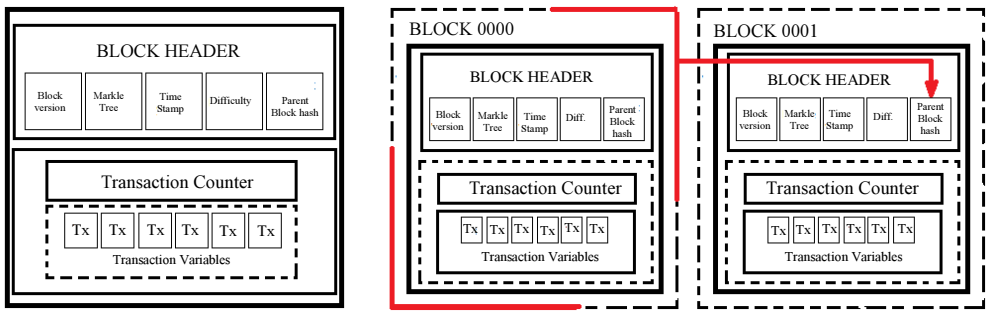

Fig. 1: (a) The Block Structure (b) The Blockchain Mechanism

Blockchain is a sequence of blocks, which holds a complete list of transaction record like conventional public ledger. Figure 1(b) illustrates an example of a blockchain with a previous block hash contained in the block header. Note that when using blockchain to record transactions, it is typical that only a relatively small amount of data associated with a particular transaction is stored directly in the blockchain ledger itself. Other data associated with the transaction, which might be much larger, is stored separately from the entry in the blockchain ledger, but is referenced by the entry. This approach is desirable to avoid overwhelming the blockchain ledger with large volumes of data.

The Blockchain Based Model for IoV

Blockchain Based Network Model

Blockchain is based on P2P network and inherited the decentralized characteristics. In P2P's decentralized protocol, all nodes are not only playing the role of the clients but also the playing the role of the servers. And in conformity with the decentralized network characteristics, third party is no longer needed in blockchain which is in conformity to the nature of Ad-hoc network characteristics with that of IoV. In particular Fig. 2 depicts the network model for Blockchain Based IoV operation.

Basically, network set-up is one of the key requirements in order to analyze the exchange of messages from one node to another. And as such the Blockchain enabled IoV Operations must be defined in conformity with the defined network model of Fig. 2. At the macro-level the network set-up model is divided into (1) backbone network and (2) the Blockchain Operated Network.

The backbone network is either wired or wireless connection between wireless base station and the cellular network facility. Although this is not the concern of this paper, however, the backbone network provides the internet connectivity and data requirements of IoV operations via the localized server serving as Wireless Base Station (WBS). On the other hand, the blockchain dependent operation includes the Vehicle-to-vehicle (V2V) communication (as defined by the ad hoc network), the Vehicle to Infrastructure (V2I) communication as defined by the communication 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 communication as being governed by Wireless Base Station (server).

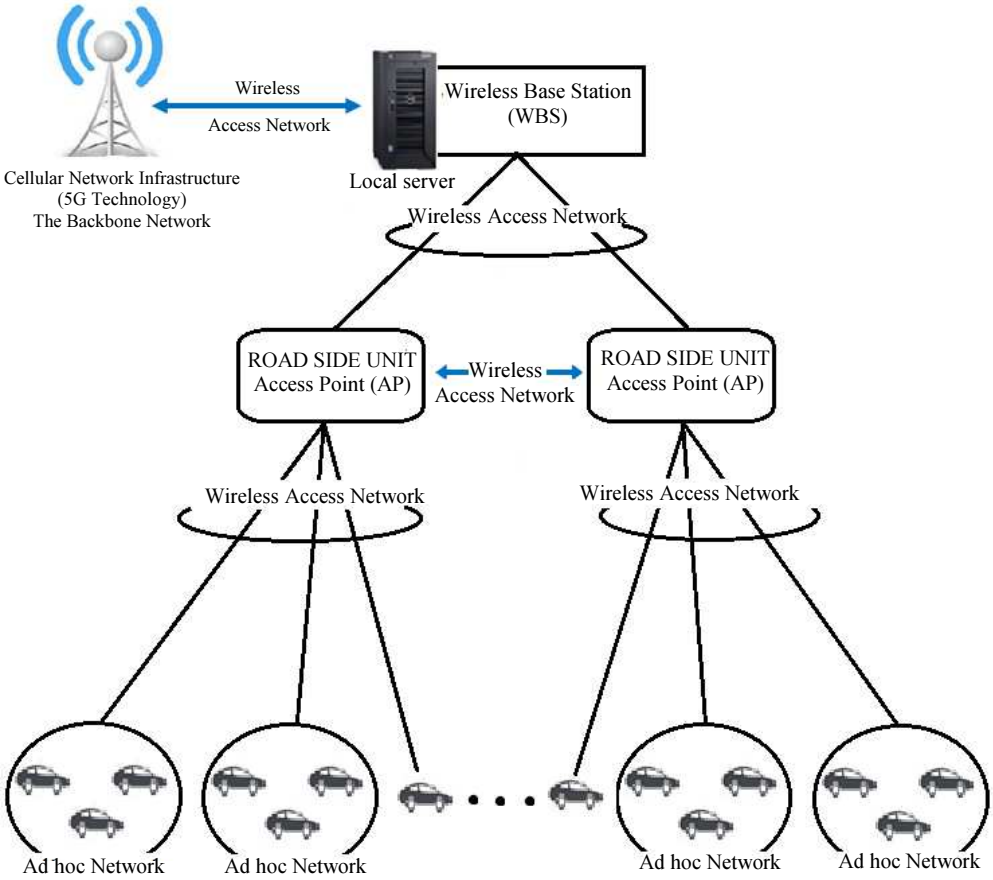

Fig. 2: Blockchain Based IoV Network Model

What is compelling with the blockchain network model is that, detailed vehicle information as being referenced in the block are all stored and can be controlled by the localized WBS. Note that the WBS only aims to minimize the size of the block data that are generated by vehicles. The main purpose is as to reduce bulk data transmission in the network, making network transaction faster, efficient and effective. This scenario should not be construed with that of a centralized network model. In other words, the blocks that are being generated by each vehicle come only in small sizes. And some information in the block (in a form of blockhash) directs or references only to information stored in the WBS. Such information may include the details of the vehicle such as vehicle owners, Vehicle licence, etc. Detailed discussion for this is described in succeeding section of this paper.

Another consideration to be established in a blockchain based network model is to consider a wired connection system between RSUs and that of WBS. Note that, a wired connection model for the WBS and RSU will free up some of the RSU wireless sensor technology (WSN) physical layer operation considering that the primary purpose of the RSU-WSN technology is to laid down and ensure the wireless system network connection as required in V2I and I2I communication. Note further that when WSN physical layer operation be reduced the corresponding, network transaction speed is expected to increase. Also, the mechanism will perhaps reduce communication bottle-neck occurrence on the part of RSU considering the number of vehicle communications that might exist in a particular period of time. And considering the nature and characteristics of RSUs a Field-bus wired connection system can be employed.

Although wired network on its original structure, a Fieldbus systems is a Distributed Computer Controlled System (DCCS) communication that are used to connect various industrial system. Fieldbus systems makes the data exchange between the nodes in the deterministic time deadline, which means that it can grants the stringent real-time property (Hou *et al*., 2003). This characteristic of fieldbus system complements the speed-time requirement of V2I communication. Moreover, fieldbus system can also be integrated with that of wireless network requirement of RSUs and WBS. Integration can be implemented via integration pattern explored in the study of Wang et..al.(Wang *et al*., 2010).

The IoV Block Structure and Blockchain Transaction

It is to be underscored however, that in blockchain transaction (V2V, V2I, V2X and I2I communications) there is a need to establish a common consensus transaction model to be followed. It is because of the varying wireless sensors technology utilized in a network infrastructure. Moreover, a consensus transaction model is necessary to ensure data consistency in a decentralized ad hoc network of Fig. 2. On this case, two things must be considered: (1) IoV Data Standardization or the Block structure Standardization and (2) the blockchain based transaction security process.

Figure 3, defines the IoV standard block structure. Primarily, the components of the IoV standard block includes: (1) Generic BlockHash, (2) Previous BlockHash, (3) Timestamp and (4) Transaction Records. These components define the IoV standard data set.

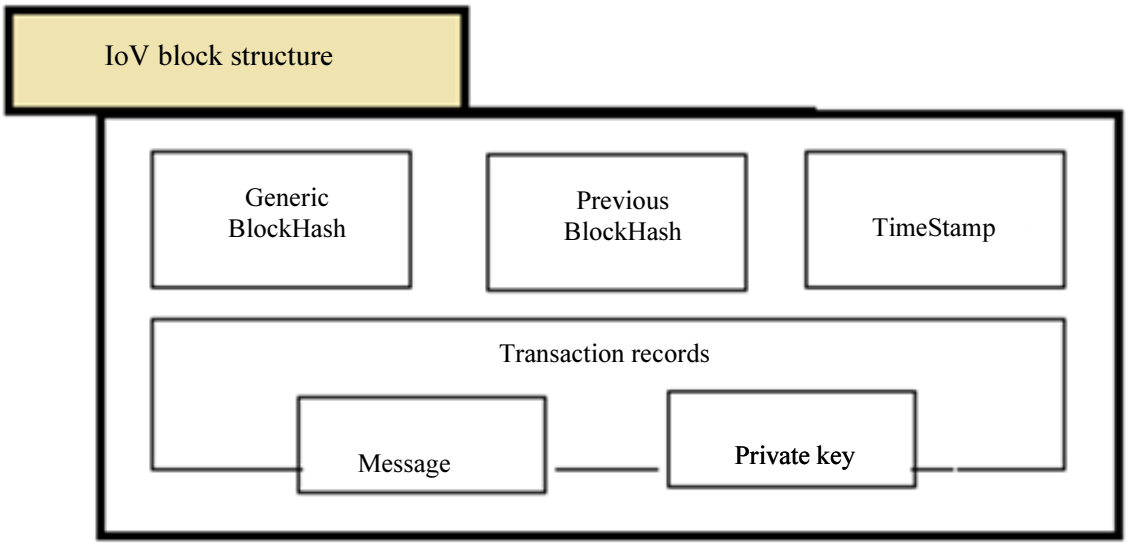

Fig. 3: The IoV Block Structure

And as such, all IoV transaction data are in a form of block comprising of the four components. 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. In other words, this hash function is point to the block which has been forwarded in the network and has been received by a particular vehicle. The presence of this component in the block structure constitutes the blockchain process.
- 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 must consider relevant vehicle sensor such as the speedometer, GPS and others which information varies relative to time.
- 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. The inclusion of private key encryption in the transaction records serves in two functions. One is that it encrypt the inputted message of the driver ensuring data privacy and secondly it will serve as a handshake token for the receiving vehicle ensuring that the block received are authentic and comes from a legitimate vehicle

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 would be 256 bits which is based on SHA-256 Cryptographic Hash Algorithm. In particular, however the hash value size for encryption is set to be at 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 Fig. 2, it is assumed that a private and public key are being issued to each vehicles by the localized server. However on the context of this paper it is a prerequisite that the localized server in figure 4 provides the private and public key of each vehicle prior to operation and at the same time vehicle identification and other relevant information are being generated and stored by the WBS itself. The 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 traffic management agency 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 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 Fig. 4
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 rebroadcast the block in the network it will attach the previous block hash to its generated block – realizing the blockchain mechanism

Figure 4 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.).

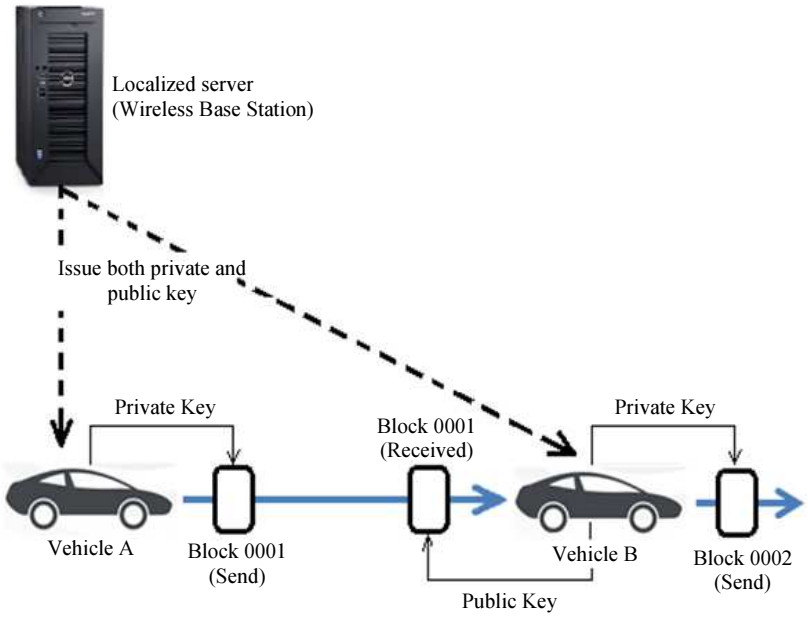

Fig. 4: IoVBlockchain based transaction

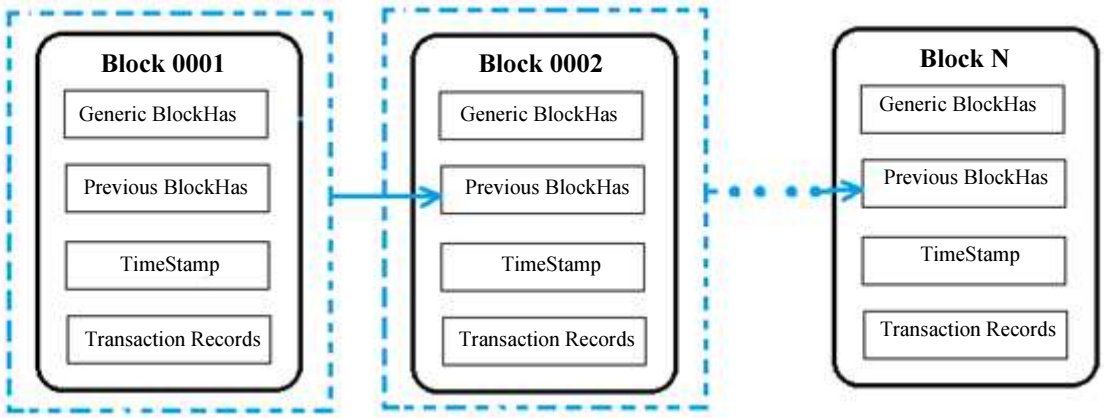

Fig. 5: The IoV Block Mechanism

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 that vehicle that knows the token in a form of a public key are allowed to receives 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 Fig. 5.

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 in the end it could not used 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 reforward it again in the network (as part of the new block and as the case maybe). This process ensures transaction anonymity, privacy and confidentiality.

Critical to IoV blockchain operation is the transaction record hash function generation and the associated

cryptographic process. Figure 3 indicates that transaction records contain two elements – the message and the cryptographic services. Note, that the rule of the transaction component of the block is crucial in every blockchain transaction. In fact, the transaction record is the block communication interface. It is through this to which transaction and information authentication are being guaranteed. Thus defining the transaction records and public key cryptographic process is necessary. These definitions are described by equations Equation 1 and 2:

$$T_R = V_M \hat{} V_{PK} \quad (1)$$

Initial transaction record in the block is defined by Equation 1 Transaction (TR¬) is defined as a function of the two elements-the VM which is the vehicle message as keyed-in by the driver itself and the VPK which is the Vehicle Private Key as issued by the localized server. And once the block is being broadcasted in the network and consequently received by other vehicles, the succeeding transaction record is then defined in Equation 2:

$$T_R = [V_{PP} \mid V_{\overline{PP}}(V_{PK1}, V_{PK2}, ...V_{PKn})] V_{PK1} \hat{} [V_{PK} \hat{} V_M] \quad (2)$$

In Equation 2, transaction record would become the function of the V_{PP} which is the public key used in the decryption process provided that public key is as a function of the Private Keys issued by the localized server, the V_{PK}, which is the private key of the receiving vehicle and the V_M, the new message of the new vehicle. The definition ensures that all present and previous transactions are all recorded.

Conclusion

From the above discussion, a blockchain based network model for IoV operations are being laid down as a requisite for the implementation of blockchain based security mechanism of IoV. The network model as described is hybrid in form – it captures the decentralized ad hoc network requirements of V2V communication and the distributed network features of V2I and I2I communication. In addition it also laid down the network implementation strategy between RSU and WBS – using the Fieldbus systems. The complimentary characteristics of Fieldbus system with that of decentralized ad hoc requirement of V2V and V2I communication together with its operational capabilities complements also with that of Blockchain technology.

Anchored to its main objectives, the blockchain based security model as defined on this paper addresses the issues on security and privacy associated in the implementation of IoV. Particularly, the used of blockchain technology coupled with public cryptographic services model as describe on this paper ensures communication privacy as transaction are being recognized first and afterwards authenticated and validated via the public cryptographic service model that are embedded within the structure of transaction component of the block or the blockchain. Also, all transaction information is constantly preserves and tamper-proof as the transaction and records are all governed by blockchain technology mechanisms.

Acknowledgement

The authors acknowledges Zhengzhou Unversity for the full scholarship it has granted to the corresponding author to which this research work has come to realized. Also, the authors acknowledges the Samar State University for alowing the him to pursue advanced studies.

Author's Contributions

Mirador Labrador: Contributed substantially in the formulation of the orginal concept of the paper, drafted the article, undertake literature review and perform all other research works.

Weiyan Hou: Conceptualizes the topic direction, provided research materials and resources. Undertakes checking and validations of all key information of the paper.

Ethics

This research manuscript is original and has not been published elewhere. The corresponding author confirms that all of other authors have read and approved the manuscript and there were no ethical issues involved.

References

Bouabdellah, M., F. El Bouanani and H. Ben-Azza, 2016. A secure cooperative transmission model in VANET using attribute based encryption. Proceedings of the International Conference on Advanced Communication Systems and Information Security (ACOSIS), IEEE Xplore press, pp: 1-6.

Choi, H.K., I.H. Kim and J.C. Yoo, 2011. Secure and efficient protocol for vehicular ad hoc network with privacy preservation. EURASIP J. Wireless Communications Networking, 2011: 716-794. DOI: 10.1155/2011/716794

Curran, B., 2018. What is a Merkle Tree? Beginer's Guide to this Blockchain Component.

Domingo-Ferrer, J. and Q. Wu, 2009. Safety and privacy in vehicular communications. In: Privacy in Location-Based Applications, Bettini, C., S. Jajodia, P. Samarati and S.X. Wang (Eds.), Springer, Berlin, Heidelberg, pp: 173-189.

Fangchun, Y., W. Shangguang, L. Jinglin, L. Zhihan and S. Qibo, 2014. An overview of internet of vehicles. China Communications, 11: 1-15.

Hou, W., H. Adamczyk, C. Koulamas and L. Rauchhaupt, 2003. Performance evaluation of the RFieldbus system. IFAC Proceedings Volumes, 36: 117-123. DOI: 10.1016/S1474-6670(17)32473-4

Hsieh, W.B. and J.S. Leu, 2014. Anonymous authentication protocol based on elliptic curve Diffie–Hellman for wireless access networks. Wireless Communications Mobile Computing, 14: 995-1006. DOI: 10.1002/wcm.2252

Jiang, Q., J. Ma, G. Li and L. Yang, 2014. An efficient ticket based authentication protocol with unlinkability for wireless access networks. Wireless Personal Communications, 77: 1489-1506. DOI: 10.1007/s11277-013-1594-x

Khan, Z.S., M.M. Moharram, A. Alaraj and F. Azam, 2014. A group based key sharing and management algorithm for vehicular ad hoc networks. Scientific World J., 2014: 1-8. DOI: 10.1155/2014/740216

Kumar, A. and R.P. Nayak, 2013. An efficient group-based safety message transmission protocol for VANET. Proceedings of the International Conference on Communication and Signal Processing, Apr. 3-5, IEEE Xplore press, India, pp: 270-274. DOI: 10.1109/iccsp.2013.6577057

Lloret, J., A. Canovas, A. Catalá and M. Garcia, 2013. Group-based protocol and mobility model for VANETs to offer internet access. J. Network Computer Applications, 36: 1027-1038. DOI: 10.1016/j.jnca.2012.02.009

Lu, R., X. Lin, H. Zhu, P.H. Ho and X. Shen, 2008. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. Proceedings of the 27th Conference on Computer Communications IEEE INFOCOM, Apr. 13-18, IEEE Xplore press, USA, pp: 1229-1237. DOI: 10.1109/INFOCOM.2008.179

Ming, Y. and X. Shen, 2018. PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks. Sensors, 18: 1573. DOI: 10.3390/s18051573

Raya, M. and J.P. Hubaux, 2007. Securing vehicular ad hoc networks. J. Computer Security, 15: 39-68. DOI: 10.3233/JCS-2007-15103

Schutzer, D. and C.T. Comer, 2016. What is blockchain and why it is important. FSRoundtable

Sun, Y., L. Wu, S. Wu, S. Li and T. Zhang *et al*., 2015. Security and privacy in the internet of vehicles. Proceedings of the International Conference on Identification, Information, and Knowledge in the Internet of Things, Oct. 22-23, IEEE Xplore press, China, pp: 116-121. DOI: 10.1109/IIKI.2015.33

US Department of Transportation, 2006. Vehicle safety communication. National Highway Traffic-Safety Administration–Final Report.

Wang, H., W. Hou, Z. Qin and Y. Song, 2010. Integration Infrastructure in Wireless/Wired Heterogeneous Industrial Network System. Li, K., M. Fei, L. Jia and G.W. Irwin (Eds.)., Life System Modeling and Intelligent Computing. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg.

Weerasinghe, H., H. Fu, S. Leng and Y. Zhu, 2011. Enhancing unlinkability in vehicular ad hoc networks. Proceedings of the IEEE International Conference on Intelligence and Security Informatics, Jul. 10-12, IEEE Xplore press, China, pp: 161-166. DOI: 10.1109/ISI.2011.5983992

Zhang, C., R. Lu, X. Lin, P.H. Ho and X. Shen, 2008. An efficient identity-based batch verification scheme for vehicular sensor networks. Proceedings of the 27th Conference on Computer Communications IEEE INFOCOM 2008, Apr. 13-18, IEEE Xplore press, pp: 246-250. DOI: 10.1109/INFOCOM.2008.58

Zheng, Z., S. Xie, H. Dai, X. Chen and H. Wang, 2017. An overview of blockchain technology: Architecture, consensus and future trends. Proceedings of the IEEE International Congress on Big Data (BigData Congress), Jun. 25-30, IEEE Xplore press, USA, pp: 557-564. DOI: 10.1109/BigDataCongress.2017.85