American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)

ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

© Global Society of Scientific Research and Researchers

http://asrjetsjournal.org/

Distributed Anonymity Based on Blockchain in Vehicular Ad Hoc Network by Block Size Calibrating

Farid Rezazadeh[a]*, Mehdi Agha Sarram[b], Kiarash Mizanian[c], Seyed Akbar Mostafavi[d]

[a,b,c,d]Department of Computer Engineering Yazd University Yazd 8915818411, Iran

[a]Email: rezazadeh@stu.yazd.ac.ir, [b]Email: mehdi.sarram@yazd.ac.ir

[c]Email: k.mizanian@yazd.ac.ir, [d]Email: a.mostafavi@yazd.ac.ir

Abstract

The network connectivity problem is one of the critical challenges of an anonymous server implementation in the VANET. The objective and main contribution of this paper are to assure the anonymity in VANET environments. In the proposed blockchain method, before packaging transactions into blocks, anonymity risk reduced through techniques such as k-anonymity, graph processing, dummy node, and silence period. This paper addresses the challenges of anonymous servers, such as update challenges and single point of failure, by exploiting append-only, distributed, and anonymity features. Although mounting the blockchain process with asymmetric cryptography solves the connectivity challenge, start-up delay and network overhead are severe. The significant feature of the proposed method solves this delay challenge by aggregating many transactions into a block and fixing constraint range of multicasting blocks. Also, aggregating transactions of various end-users into a block preserves the path anonymity. The asymmetric cryptography with ring public and private keys protects the identity anonymity as well as unlinkability. The robust anonymity mechanism existence and the traceability of all transactions constitute the main advantages of the proposed method. The simulation is running by the python to evaluate blockchain performance in VANET with connectivity failure and rapidly changing topology. The results indicate the stabilization of the proposed method in the VANET environment.

Keywords: blockchain; VANET; security; anonymity; cryptography.

----

* Corresponding author.

1. Introduction

The blockchain administration performed by swarm intelligence in distributed wisdom, information manipulation, and fraud prohibited in the data hierarchy. Blockchain technology has considered one of the most appropriate distributed applications. The distributed computational capability, encryption, and the anonymous data exchange are significant features in a combination of this technology and asymmetric cryptography with ring public and private keys. End-users consensus manages to store distributed data in a large number of blockchain members. Therefore, disconnecting the network does not stop this distributed database service. Hence, it is appropriate for transient systems like VANETS. The simultaneous proper of the end-users is inevitable. Each edit, insertion, or deletion operation generates a new transaction. The transaction log series provides numerous data recoveries through forwarding or backward operations. The database integrity in the absence of any central management provides a blockchain consistency database in unstable environments. Each end-user has a full version of the blockchain data, which must support by unlinkability methods to assure anonymity. All data stored in the blocks, consequently. The selected leader users use POW to add a new block. POW acts as a solution finding for a mathematical problem. Similar to finding the amount of n for data x, adding a hash (n) to x is less than specified amount of Y. Each block has a hereditary identifier constructed through HASH functions of combining the previous block’s id and current block’s context. One of the HASH functions benefits is mapping different data size to the fixed size HASH code. That assures the database integrity because any change in the content of a block will result in identifier HASH change, causing the loss of end user’s ensemble approval. The same HASH code for the same content considered a drawback of this method. The random volume named NONCE applied it, adding for making the same content not to have the same HASH. Transactions encrypted by asymmetric cryptography need not have any sensitive identify features; thus, meeting the sender's anonymity is available in the proposed method. High security, information maintenance, preventing any manipulation in data storage, and the possibility of tracing histories are key points of the proposed method. In the proposed method, each end-user has signed its transactions with one of the private keys, attach an owner identifier code, and then encrypts them applying one of the public keys. A transaction can request a money transfer or even sending a text message by first, broadcasting, assuring its authenticity consensus, and next aggregate in a new block with different users’ transactions. Although the proposed method has durable privacy protection, before the transaction packaged into blocks, this privacy may treat. Many transactions, such as financial transactions, require comprehensive security mechanisms. On the other hand, The exchange of end-users’ sensitive features in business firms, promotion, and sales is inevitable [1]. The stakeholders cannot guarantee end-users privacy. Sensitive feature propagation increases the risk of privacy protection. The network graph processing is powerful to solve this challenge. The network graph is expressed as $G = (v, e, L, \lambda)$ where, $V = \{v_1, v_2, \ldots, v_n\}$ is set of vertices. $E = \{e_1, e_2, \ldots, e_n\}$ is the edges set between the vertices consisting of network links. The λ is the vertices and edge labels mapping function to set L. in the proposed method, before the release of each message, the graph processing is running. The end user’s unique identifiers eliminated. Of course, each conscious attacker is capable of violating privacy with no need for any unique identifiers. To solve, must use to eliminate attributes, generate ambiguity and distortion. In this context, there exist three generic categories for end-user attributes [2] expressed as: Key features: The direct threat can disclose user id and needs to eliminate. Semi identifier: the attacker’s knowledge leads to identification deduction of sensitive attributes by Semi identifiers. A solution is increasing the degree of anonymity and controlling the number of repeating queries. One of the most critical stages of the anonymous process is choosing the right group of semi identifiers and the degree of anonymity. The latter depends on the density of end-users if the degree of anonymity not met, assisted by the deployment of the silence period, the dummy node, and the hidden region methods which follow using resources and network utility [3,4,5,6,7,8]. Sensitive features: Disclosing the private property is one of the main issues of preserving privacy to eliminate attribute, causing ambiguity and distortion, which related to the attacker's motives. The non-sensitive attribute is never beneficial for the attacker. For example, by applying an approximate location in contact queries, the direct inference of the vehicle‘s position has been prevented. Unfortunately, with enough repetition of these queries, indirect deduction becomes possible [9]. In the proposed method, before the transaction packaged into blocks, using graph processing and the right group of semi identifier selection, the degree of anonymity is determined. Of course, the local small area graph processing takes less time. The anonymity degree calibrated to reduce the anonymity risk in k-anonymity, dummy node, and silence period methods.

The following challenges arise in the VANET anonymous by applying an anonymous server:

- Updating server overhead [10]
- Vehicle mobility needs quick server update [11]
- The network failure and transient connections [10]
- The dichotomy of the network and the anonymity graph [11,12]
- More network Structural overhead [13]
- The rapid change cause lack of confidence [12]

The blockchain advantages related to the above challenges:

- Immutable
- Hacking resistant
- Data stability even after connectivity losses
- None single point of failure
- The blocks’ unique id hierarchy structured

A simple comparison of the proposed method advantage vs. VANET anonymous challenges consists of:

- Immutable means solving update challenges.
- Data stability is responsible for network connectivity failure.
- Resistance against hacking replaces graph-processing challenges.
- The unique Id of blocks is an appropriate alternative to the confidence challenge.

2. Innovation

Only applying the blockchain consensus model does not increase anonymity. Here, the transaction owner is identified by asymmetric cryptography, which does not need to Identify and disclose the sensitive fields, which supports the sender's identity anonymity. On the other hand, the unlinkability supported by the ring signature method, which implemented by an array structure, included pairs of public and private keys. Aggregation of different end user’s transactions in one block will hide its target between several blocks’ transactions [14]. Then, the transaction’s path anonymous related block size to provide path anonymity. On the other hand, multicasting blocks with size calibration algorithm with local small area constraint range, reduce the delay and setup overhead significantly.

Applications, to reach the agreement based on consensus models, are time-consuming, these delays consisting:

- The delay time of generating some transactions to complete the block’s capacity: By applying the dummy nodes, a few generation transactions are enough. Preparation delays will be adjustable with threshold values.
- The consensus approval delay: Using big blocks and multicasting them with local small area constraint range and propagating by area’s edge vehicles to everywhere of VANET, the consensus time and overhead reduced.

Blockchain stability and less start-up delay is the proposed method’s key point. The financial transaction fee is the miner motivation for spending its resources. According to the presence of both the dummy and real nodes’ transactions, the blocks’ fees obtained by counting the actual transactions per block. Of course, if this percentage is low, the risk of path anonymity disclosing will be high[15]. The proposed method fee calculates on successful transaction received in the target. Here, the graph processing applied to address end-users privacy breach, omitted the sensitive, key features, ambiguity, and distortion before had been collected transactions in blocks. These innovations applied by designing the traffic model, choosing the routing protocol, area handling, node, and blockchain configuration, proved by the simulation results.

3. Related Works

Ralph Merkel (1979) introduced the HASH tree. The main application of this tree encryption is expressed in the Lamport signature [16]. The blockchain approach used to authenticate the documents by [17]. The main advantage of this method is its ability to verify the production and editing time and intellectual property. All documents sent to the storage server, stored in the secure chest, to provide trace changeability. The owner's privacy violation and likely damage while submitting the document to the mark server is the primary disadvantage. The HASH functions used to design id hierarchy [18]. Any change in a document would make a different identifier. The HASH identifier represents the sole of the document context [19]. The digital currency mechanism introducing a distributed integrated approach named Bitcoin applied in [20].

The blockchain objects defined in three-part by [20]:

Blockchain: some blocks chained linear and time order. Transaction: each block includes many transactions of different end-users actions. Mining: Collecting transactions of different users in a new block and obtaining consensual approval by POW(a secure, distributed consensus voting mechanism [21][22]) is the main miner work. A safety method presented to support financial services in VANET environments [23] based on *Road Side Unit* (RSU), which is not applicable in many VANET situations. The main challenges of data routing and loss in frequent network failures not considered in this study. The connectivity between a million vehicles in the VANET environment to estimate the amount of latency and storage overhead in exchanging messages assessed in [14]. The consensus delay acceptability based on vehicle count in the blockchain process assessed in [24]. Two hundred vehicles are the minimum counts to make the process effective. If vehicle counts exceed 200, the delay and network efficiency will become better than normal VANET. There exists a direct relation between vehicle count and profitability. By clustering in VANETs and running blockchain functions in the cluster heads, the lightweight, scalable designed to support the vehicle's privacy. The pressing challenge of this approach placed in the cluster heads' privacy preservation. If an attacker gets control of the cluster heads, all in vehicles, VANET will undergo a significant crisis [25]. The method assuring the anonymity identity in the communication between vehicles is proposed in [26], where the asymmetric key encryption, ultrasonic and optical channels to support VANET connectivity are applied [27]. The business centers and factories provided the V&V connection outside the blockchain process, which is the source of privacy violations. The diversity l method with k degrees applied to protect the data structure and end-user features [28]. The k-anonymity assures that each end-user cannot identify from at least more the k -1 [29]. An end-user has diversity l, if and only if, there is at least l alternative for all end user's sensitive attributes [30].

4. Proposed Method

Our blockchain algorithm proposed to solve anonymous challenges in VANE requiring a distributed approach relating to devising the chain of immutable blocks, is proper for customization in a vehicular ad hoc network. Propagation of a transaction in VANET needs to define the security scheme.

The following algorithm runs before sending each transaction by focusing on the anonymity graph processing:

- The similarity area classifies by vehicles' speed, direction, and position in the road. According to the mobility model features vector stored in the vehicle routing table. Some vehicles chose to form an area by the Eq. (1).

$$d(V_i, V_j) = \sum_{l=1}^{m} |x_{i_l} - x_{j_l}| \qquad (1)$$

- Devise the area anonymity graph
- Remove all graph vertices and edges of unique value. The graph processing delay is when the scope is limited to the minor areas.
- Devise vehicles' neighbor list from the graph of cars left behind.
- Each vehicle sensitivity determines the k value
- If k > neighbor list's count, the vehicle enters the silence period
- If the silence period > the time threshold value, then the dummy node method applied. Devise ample

virtual vehicles to add on the neighbor list and the anonymity graph. The virtual vehicle mapped on the mean of all neighbor list's feature vectors, in a sense that the two virtual machines produced simultaneously will have different feature vectors. Where the feature of the virtual vehicle x_{*_l} obtained as Eq. (2).

$$x_{*_l} = \frac{\sum_{i=1}^{n} x_{i_l}}{n} \qquad (2)$$

- If k ≤ neighbor list's count, then first the transaction signed by a digital signature, next multicast to vehicles in there own area.
- When transactions received, add to the vehicle's transaction pool [31]
- If a transaction pool size reaches the block size, a new block will generate and broadcast to obtain consensus on its approval or rejection. Each block contains many transactions, the HASH identifier constructed from the parent blocks, and new block content. The private and public keys are designed based on the WIF[a], which comprises combined letters and huge numbers. The end-user signature approved with his private keys. Eq. (3) indicates the cryptography action in the sender.

$$C = E\left(PU_r, \left(s, E(PR_s, T_s)\right)\right) \qquad (3)$$

Where T_s is a transaction, s is the sender identify, PU_r is the public key, PU_s is the private key, and C is the encrypted transaction that is ready to multicast.

- Each block attached to the main chain, when obtained the consensus approval,
- Each vehicle contributes to the block miner to apply the proof of work functions. The motivation based on the financial transactions fee by counting the actual transactions per block receiving in destinations successfully. The fee calculation based on the successful individual transactions in the target.
- Each transaction will transmit to the destination through the public key, where each receiver has its public keys and has the list of all the related members' private keys. By applying Eq. (4): the destination's public key used to decrypt the sender id; then, the sender id will search in the destination's customer list to find the sender's private key.

$$s = D(PU_r, C) \qquad (4)$$

$$T_s = D\left(PU_r, \left(D(PR_s, C)\right)\right) \qquad (5)$$

By applying Eq. (5): the sender's private key decodes the encrypted transaction text.

Algorithm 1 proposed to add a new block to the main chain**.**

[a] Wallet Format

Algorithm 1 Mining a Block

Table 2

```
Input: Index, Previoushash, Timestamp, Data, HASH, NONCE

If (PreviousBlock.Index + 1 == NextBlock.Index) And
(PreviousBlock.Hash == NextBlock.PreviousHash) And (NextBlockHash == NextBlock.Hash) And
 IsValidHashDifficulty(NextBlockBash)) Then
 Begin
 Hash(Index, Previoushash, Timestamp, Transactions, Nonce);
 GenerateNextBlock(Data);
 ADDBlock(Index, Previoushash, Timestamp, Data, HASH, NONCE);
 End

Output ADD a New Block to BlockChain
```

The architecture and the manner of signing the transaction are flow charted in Figure 1.

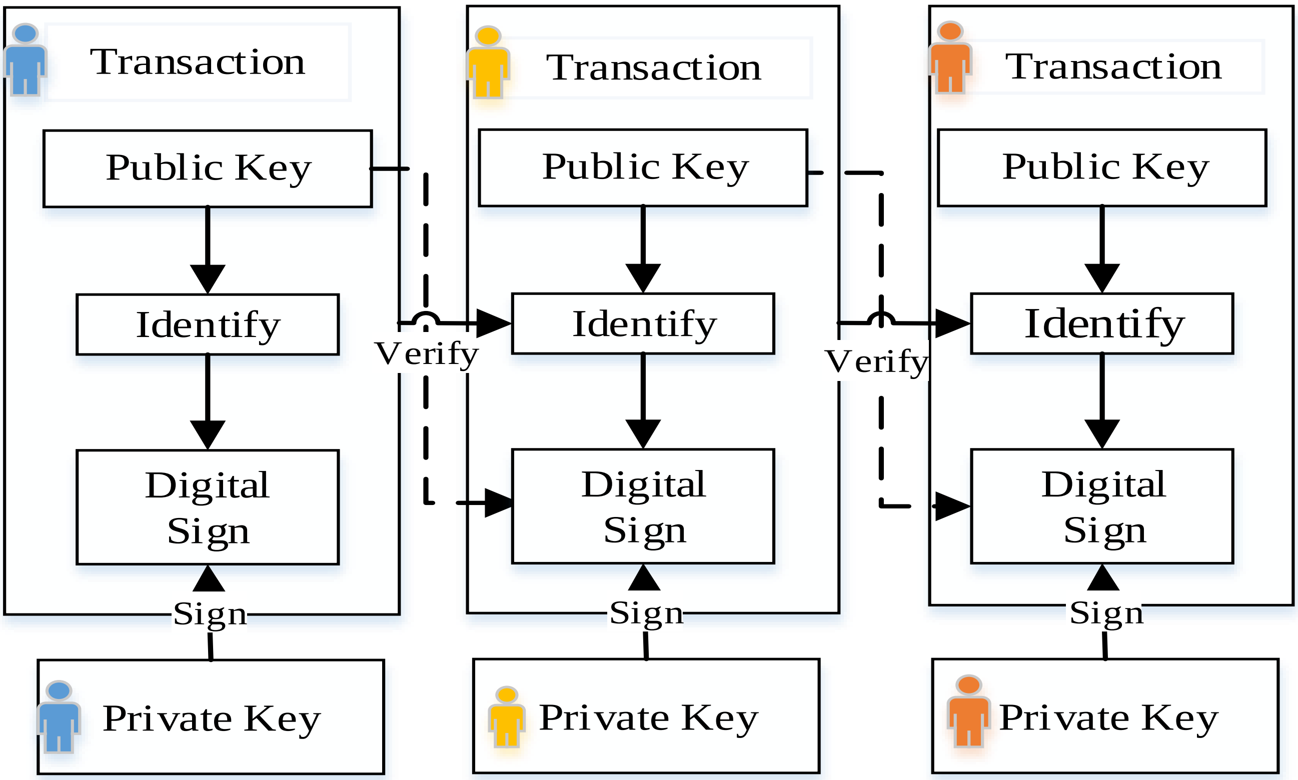

Figure 1: Transaction digital sign architecture

The Vehicles' operational flow chart illustrated in Figure 2. Many blocks and transactions receive from other vehicles. All verified transactions will add to the transactions pool to collect some anonymous transactions and prepare to build a new block.

Algorithm 2 K-Anonymity Method

Table 3

```
Input: sender_anonymity_degree, sender_featurevetor

Set feature vector as $\{f_j\}0<j<m+1$
Set Open list    as $\{o_i\}0<i<n+1$
Set Closed list   as $\{c_i\}0<i<k+1$
Set Key vector   as $\{PU_i,PR_i\}$ $0<i<21$
For i := 1 To area_vehicle_count Do
If distance(sender.f, $o_i$.f) is less than 200 meter, same direction and near speed Then add(Closedlist, $o_i$)
For j :=1 to feature count do
Create G = (V,E) with making edges as $c_i.f_j$ to $o_i.f_j$
Graph processing is decided to prune G
Delete $\forall$ $c_i$ where is mutual exclusive
Delete $\forall$ $c_i.f_j$ to $o_i.f_j$ connection where is sensitive
Create neighbor list from $\forall$ $c_i \in G$
if Anonymity_degree > count(neighbor list) then
 if silence_counter > Silene_mode_max_time then
   Add dummy nodes to link the neighbor list & G
  Else Wait and keep silence for random time
n := n + 1
If n > 20 then n := 1
Create and sign the transaction with $PUr_n$ & $PRs_n$
multicast the transaction in range of area

Output multicasting transaction
```

Algorithm 2 proposed to define the security scheme before sending each transaction by focusing on the anonymity graph processing. This scheme is capable of calibrating the anonymity degree related to vehicle sensitivity needs. The K-anonymity, dummy node, and silence mode methods configured with anonymity degree to support vehicles’ privacy for sending transactions. All vehicles must perform algorithm2 to decide between waiting and multicasting its transaction.

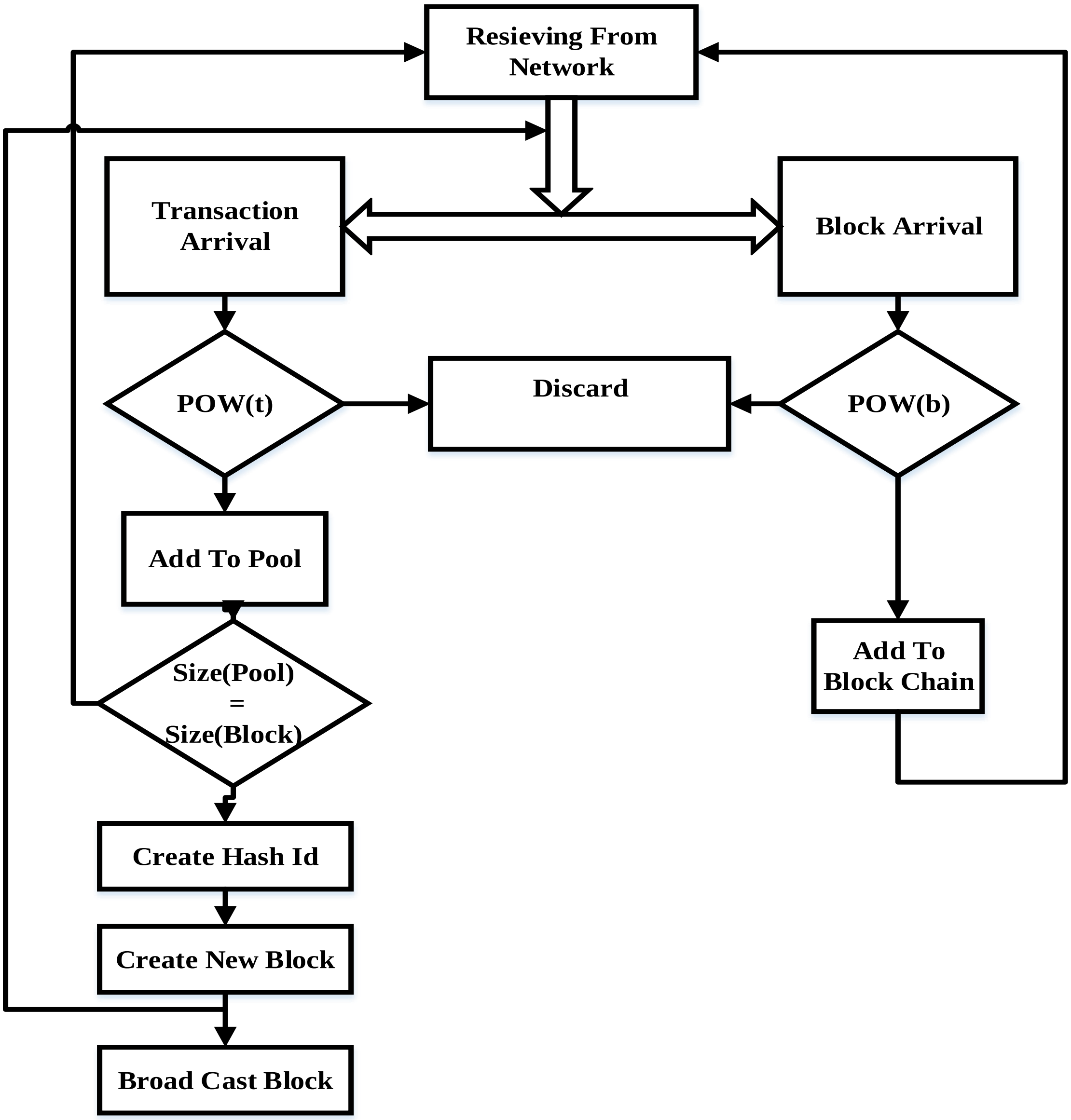

Figure 2: Vehicles' Operational Flow Chart

5. The simulation Results

The simulation in this proposed method run by applying python 3.7. The blockchain performance evaluated in VANET with connectivity failure and rapidly changing topology. Here, the end-to-end routing is not Applicable; thus, the hop by hop routing is an alternative that and one hop delays its related criteria. The spent bandwidth is another critical criterion, which can measure by the ratio message carrier. The user acceptance rate and network coverage are other comparable criteria. In this implementation, the epidemic based routing chosen, with the main advantage of having reliable message propagation in the VANET environment.The Intelligent Driver Mobility (IDM) mobility model applied with usual traffic scenarios, full velocity, and location diversity distribution. The mobility model's parameters set concerning the available findings in the related literature, as in Table 1.

Table 1: set up the scenario

Feature	Value
The length of the road in meter	20000
The flag indicates the two directions	true
Lane width in meter	3
The number of lanes per direction	3
Length of a vehicle in meter	5
Total simulation time in second	3000
Scenario flag	Freeway Free

The challenges posed by blockchain approaches, such as network overhead, have been addressed by the proposed method in the primary simulation presented in Figures 3 and 4. The blockchain process requires a lot of data synchronization, which will undoubtedly bring a vast network overhead. The proposed method replaces broadcast with multicast the big blocks that calibrated in size; then, the network overhead decreased significantly.

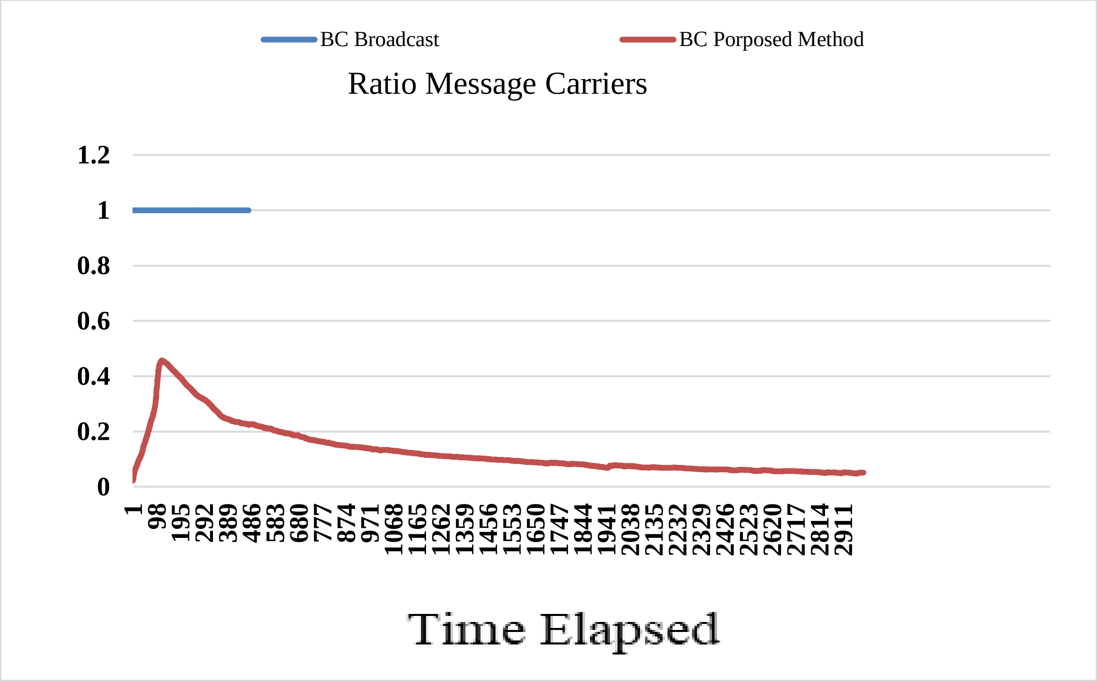

Figure 3: Message Carrier Rate

The bandwidth and one hop delay compare in Figures 3 and 4. After 475-second broadcasting big block in VANET, the memory error acquired, and the process stopped and crashed. Also, 100% of bandwidth spent, one hop delay increased significantly. These events happen in the corei7 system with an 8-gigabyte ram, which runs the python 3.7.2 to simulate our experiments. When multicasting in a range of small local areas, one hop delay, and bandwidth spending replaces, broadcasting decreased significantly.

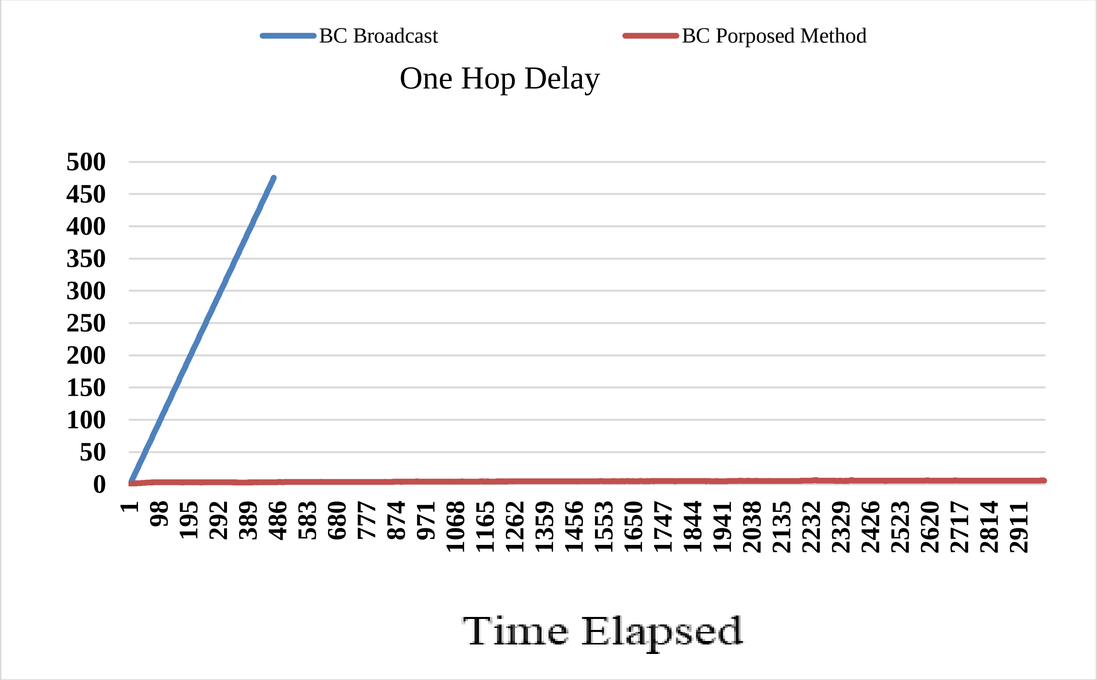

Figure 4: One Hop Delay

The result of this experiment explains that multicast is the first key point in VANETs. We prove that the next key point is the size of blocks, which propagated to achieve consensus in the VANET environment. Some block size selected in our implementation compare the simulation result for changing block size. The comparisons between these simulations are run and presented in Figure 5 to 8. In comparing Figure 5, it observed that new vehicle acceptance observed as blockchain member starts after the initial gap when the block size is 10, 30, or 100 transactions in a block. The interesting point is the deletion of early delay when the block size set to 20.

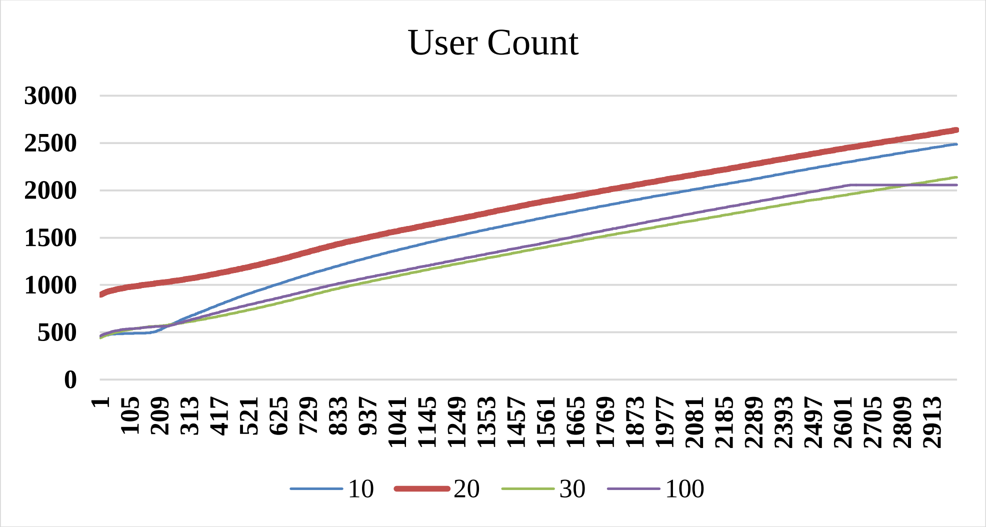

Figure 5: End-user Count Rate

The proposed method with gathering twenty transactions in a block takes nearly results with the VANET only case and solves the start-up delay. Of course, processing and storing big blocks will consume several hardware resources. If the vehicles' hardware resources strengthened, then the initial gap will reduce.

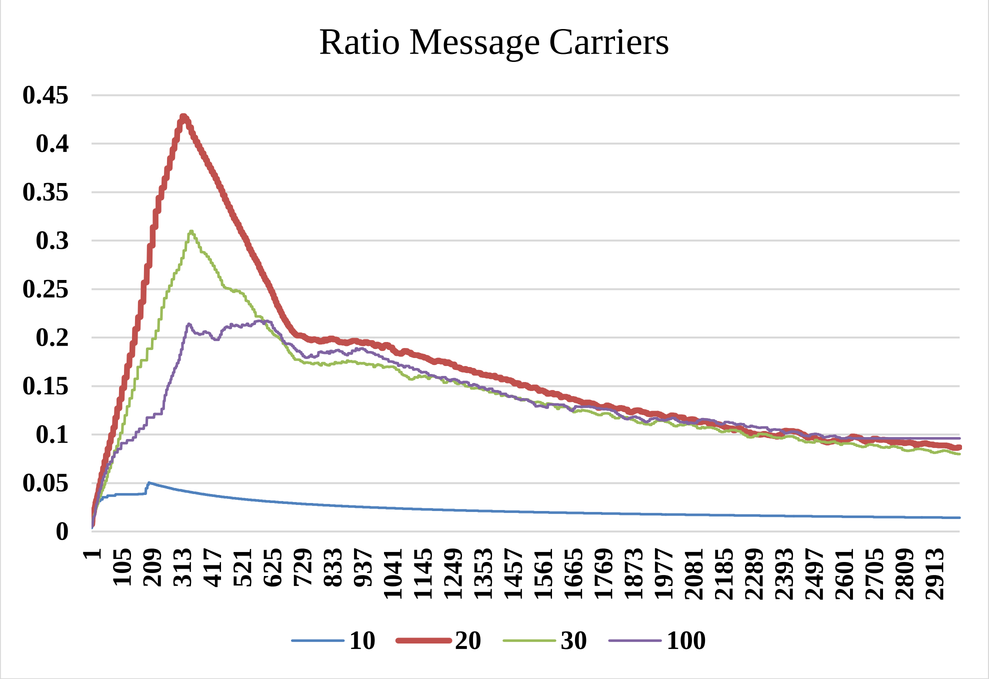

Figure 6: Message Carrier Rate in Deferent block size

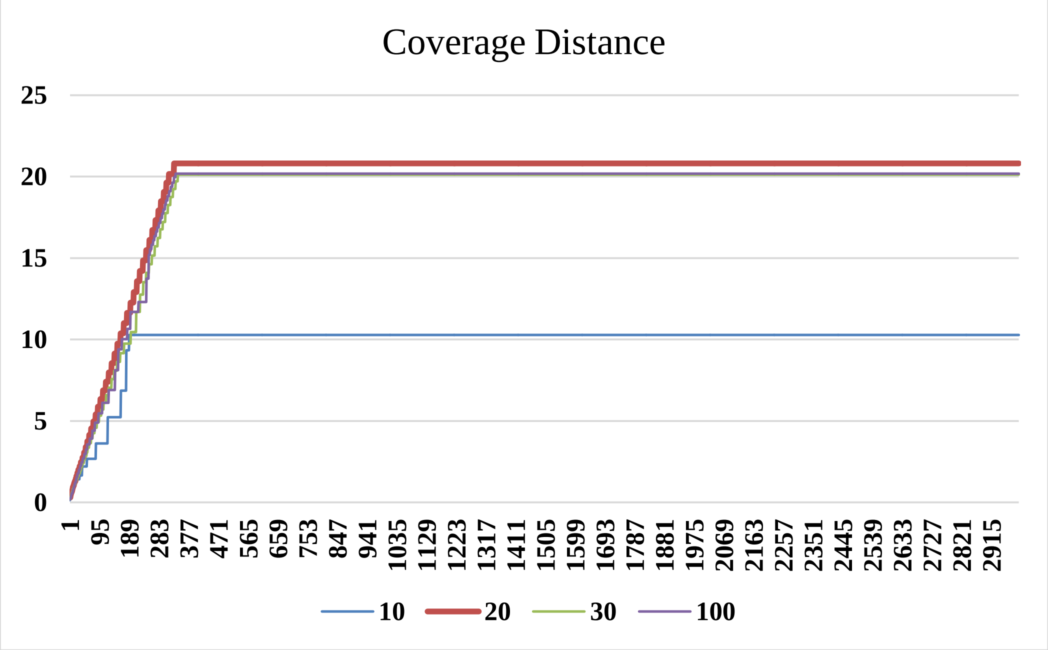

Figure 7: Coverage Distance

In comparing Figure 6, observed that first, the message carrier rate follows a rapid growth and then a gradual decrease due to stabilize routing protocol and increase the data coverage in VANET.The blockchain synchronization spends much bandwidth, and the block propagation is more in the proposed method. One of the proposed method's key points is the decreasing bandwidth consumed due to the time elapsed. Defiantly, if bandwidth spending makes significant delay reduction, then the proposed method is successful. In figure 8, the one-hop delay investigated. In comparing Figure 7, it observed that the coverage distance increases when the road continues. The coverage distances follow a rapid linear growth for the first time and remain fixed as the road continues, in the proposed method. On the other, the coverage distance constrained to road length. That reduces resource consumption and supports the privacy preserve instructions to implement the least privileges method. The small block size cannot cover at least 50% of road coverage. As observed in Figure 8, the first one-hop delay follows a rapid growth, and then a gradual decrease due to full road coverage happens. The proposed method is the best in initial one-hop delay management. The whole data distribution throughout network space, discard many unnecessary message exchanges. In VANET without blockchain approach, one hop delay increases slowly and never decreases. Updating delay and storing space increase when vehicle counts increase. The proposed method discards the start-up one-hop delay rapid growth. Although the big-block transition consumes the network resources, the one-hop delay will remain near to VANET without blockchain. According to the above four comparisons, the proposed method preferred to one-hop delay, coverage, and user acceptance management. When each transaction delivered, the identity and path anonymity becomes available in full. In this process, one possible privacy violation is the traceability on broadcasting transactions.

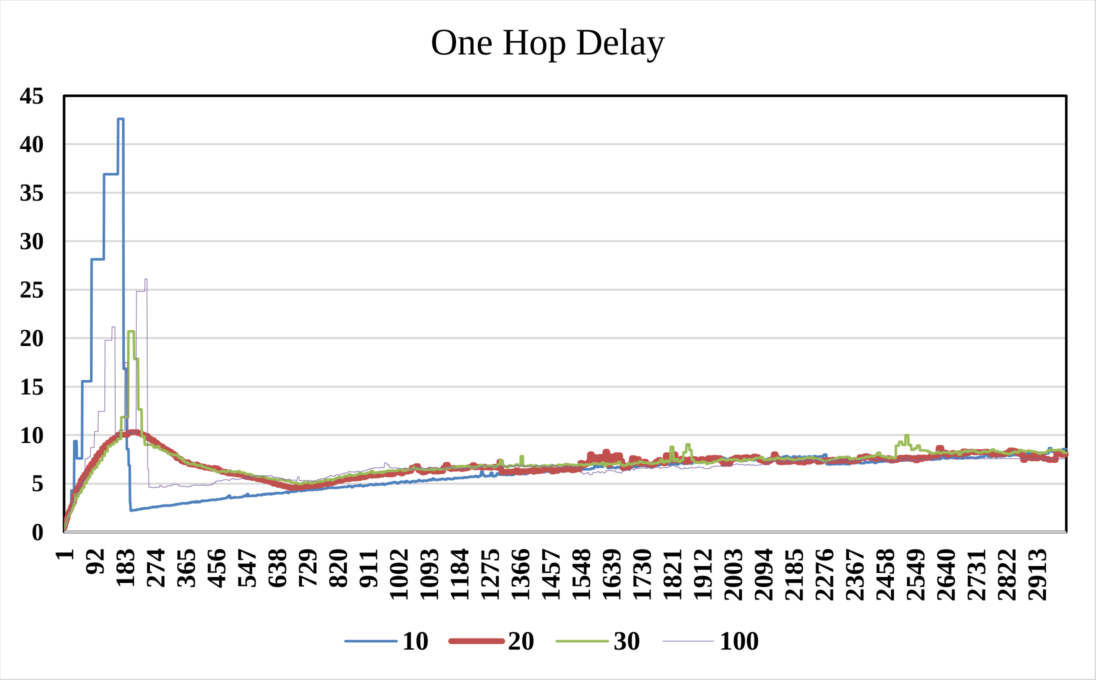

Figure 8: One Hop Delay

Because having anonymous public keys corresponding to user anonymity, it is not just enough. One type of anonymity an irrelevance or unlinkability. When seen some messages signed with the same private key, realized that the messages' sender is the same; then an anonymous challenge exacerbating by giving much more data to all members. The one-time password method can solve that, which requires a centralized server. On the other hand, the multiple messages exchanging between the senders and destinations to determine the next public and private keys, along with the nature of the frequent loss in VANET, renders this method unworkable in the absence of the RSU. The proposed method uses a circular array of public and private keys pairs. Each message sending uses one of the array rows according to the circular pointer of the array.

6. Conclusion

The objection of the proposed method is to determine the anonymity of VANET environments. The rapid vehicle movement faces many challenges. The blockchain approach implementation is to overcome many challenges while stability and anonymity privacy-preserving in these networks. The risk of privacy breach is high before connecting and collecting transactions in a new block. By k-anonymity, the local graph processing, dummy node, and silence period methods reduce the anonymity risk. Moreover, this proposed method allows the vehicle to manage its privacy. By collecting all minor area graphs, the advantage of the global anonymity graph yielded. Here, the proposed method with gathering many transactions in one block takes the nearest results in the VANET only case, of course, in block size equal to the 20-transaction constraint. The findings here have several important implications for future studies with the possibility of contribution in this respect. A blockchain is a proper tool for implementing the distributed anonymity in VANET. This process is capable of pinpointing the anonymous vehicle’s location and path, without any ambiguity and distortions.

7. Author Contributions

Farid Rezazadeh presented writing, research, original draft, simulations, and conceptualization. Mehdi Agha Sarram and Kiarash Mizanian performed leading and conceptualization. Seyed Akbar Mostafavi conceptualization.

References

[1]. B. Zhou, J. Pei, and W. Luk, “A brief survey on anonymization techniques for privacy preserving publishing of social network data,” ACM Sigkdd Explor. Newsl., vol. 10, no. 2, pp. 12–22, 2008.

[2]. P. Shi, L. Xiong, and B. Fung, “Anonymizing data with quasi-sensitive attribute values,” in Proceedings of the 19th ACM international conference on Information and knowledge management, 2010, pp. 1389–1392.

[3]. X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, “Traffic-aware multiple mix zone placement for protecting location privacy,” in INFOCOM, 2012 Proceedings IEEE, 2012, pp. 972–980.

[4]. K. Miura and F. Sato, “Evaluation of a hybrid method of user location anonymization,” in Proceedings 8th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA, 2013, pp. 191–198.

[5]. R. Al-Dhubhani and J. M. Cazalas, “An adaptive geo-indistinguishability mechanism for continuous LBS queries,” Wirel. Networks, pp. 1–19, 2017.

[6]. A. K. Tyagi and N. Sreenath, “Location privacy preserving techniques for location based services over road networks,” in International Conference on Communications and Signal Processing (ICCSP), 2015, pp. 1319–1326.

[7]. I. Memon, L. Chen, Q. A. Arain, H. Memon, and G. Chen, "Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks," Int. J. Commun. Syst., vol. 31, no. 1, 2018.

[8]. Q. A. Arain et al., "Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks," Wirel. Pers. Commun., vol. 95, no. 2, pp. 505–521, 2017.

[9]. S. Zakhary and A. Benslimane, "On location-privacy in opportunistic mobile networks, a survey," J. Netw. Comput. Appl., vol. 103, pp. 157–170, 2018.

[10]. G. P. Corser, A. Banihani, J. Cox, R. Hoque, H. Fu, and Y. Zhu, "Location Privacy, Application Overhead and Congestion in VANET Location Based Services," in Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2017 IEEE 3rd International Conference on, 2017, pp. 243–248.

[11]. P. Mahapatra and A. Naveena, "Enhancing Identity Based Batch Verification Scheme for Security and Privacy in VANET," in Advance Computing Conference (IACC), 2017 IEEE 7th International, 2017, pp. 391–396.

[12]. K. Logeshwari and L. Lakshmanan, "Authenticated anonymous secure on demand routing protocol in VANET (Vehicular adhoc network)," in Information Communication and Embedded Systems (ICICES), 2017 International Conference on, 2017, pp. 1–7.

[13]. C. Zuo, K. Liang, Z. L. Jiang, J. Shao, and J. Fang, "Cost-effective privacy-preserving vehicular urban sensing system," Pers. Ubiquitous Comput., vol. 21, no. 5, pp. 893–901, 2017.

[14]. Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for vanets," IEEE Access, vol. 6, pp. 45655–45664, 2018.

[15]. R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new-type of blockchain for secure message exchange in VANET," Digit. Commun. Networks, 2019.

[16]. S. Alboaie, D. Cosovan, L.-D. Chiorean, and M. F. Vaida, "Lamport n-time signature scheme," in 2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 2018, pp. 1–6.

[17]. S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in Conference on the Theory and Application of Cryptography, 1990, pp. 437–455.

[18]. D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," in Sequences II, Springer, 1993, pp. 329–334.

[19]. A. Kiayias and A. Mitrofanova, "Financial Cryptography and Data Security," Lect. Notes Comput. Sci., vol. 3570, pp. 109–124, 2005.

[20]. E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," in Proceedings of the Future Technologies Conference, 2018, pp. 1037–1058.

[21]. L. Baird, M. Harmon, and P. Madsen, "Hedera: A Governing Council & Public Hashgraph Network." 2018.

[22]. L. Baird, "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance," Swirlds, Inc. Tech. Rep. SWIRLDS-TR-2016, vol. 1, 2016.

[23]. B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in Proceedings of the 2016 ACM International Joint Conference on Pervasive and

Ubiquitous Computing: Adjunct, 2016, pp. 137–140.

[24]. L. Li et al., "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 7, pp. 2204–2220, 2018.

[25]. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, 2017.

[26]. S. Rowan, M. Clear, M. Huggard, and C. Mc Goldrick, "Securing vehicle to vehicle data sharing using blockchain through visible light and acoustic side-channels," arXiv preprint arXiv:1704.02553. eprint.

[27]. M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," arXiv Prepr. arXiv1708.09721, 2017.

[28]. M. Yuan, L. Chen, S. Y. Philip, and T. Yu, "Protecting sensitive labels in social network data anonymization," IEEE Trans. Knowl. Data Eng., vol. 25, no. 3, pp. 633–647, 2013.

[29]. P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," technical report, SRI International, 1998.

[30]. N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on, 2007, pp. 106–115.

[31]. X. Wang et al., "Survey on blockchain for Internet of Things," Comput. Commun., 2019.