 doi:10.20944/preprints202102.0207.v1

Article

Blockchain based trust model using tendermint in vehicular adhoc networks

Sandeep Kumar Arora [1], Gulshan Kumar[1*] and Tai-hoon Kim[2]

[1] Lovely Professional University; sandeep.16930@lpu.co.in
[2] Glocal Campus of Konkuk University, 268, Chungwon-daero, Chungju-si, Chungcheongbuk-do, 27478, SOUTH KOREA

*Corresponding Author: G. Kumar (gulshan3971@gmail.com), T.H. Kim (taihoonn@daum.net)

Abstract: : Blockchain is the consensus-based technology to resolve the conflicts in Byzantine environments. Vehicles validate the messages received from the neighboring vehicles using Gradient Boosting Technique (GBT). Based on the validation results the message source vehicle generates the ratings that are to be uploaded to Road Side Units (RSUs) through that trust offset value can be calculated. All RSUs maintain the trust blockchain and each RSU tries to add their blocks to trust blockchain. We proposed a blockchain-based trust management model for VANET based on Tendermint. It eliminates the problem of malicious nodes entering the network and will also overcome the problem of power consumption. Simulation results also show that the proposed system is 7.8% and 15.6% effective and efficient in terms of Packet Delivery Ratio (PDR) and End-to-End Delay (EED) respectively to collect the trusted data between the vehicles.

Keywords: blockchain; vehicles; trust; traffic; consensus

1. Introduction

The vehicular network helps to provide information about road accidents, traffic congestion, road conditions etc. and this helps the vehicles to timely aware of the critical situations hence improve transportation safety [6].

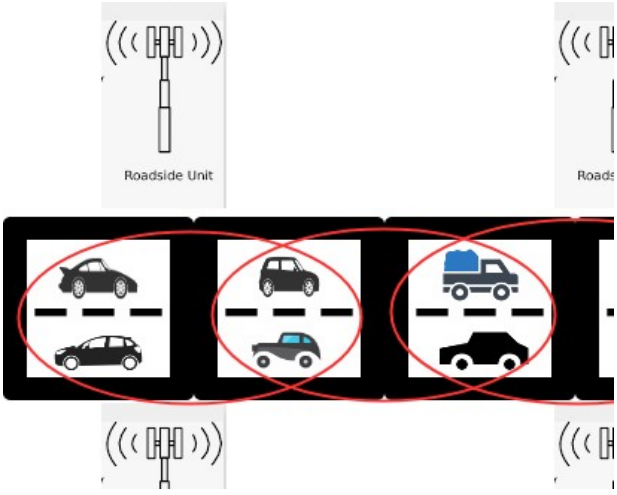

Figure 1. Architecture of VANET Networks

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

Vehicular communication is using onboard sensing and computation to communicate with each other [1] [2] as shown in Figure 1. Even smart vehicles want to communicate with each other and this is the basic key in the fifth-generation network (5G) [3] [4]. However, due to high mobility and dynamic network, we cannot trust every vehicle. The malicious nodes can enter the network and spread the false information in the network which leads to failure of the vehicular network. For example, a malicious node can broadcast a message that there is an accident on a road claiming the congestion but there was no accident and traffic congestion. These types of misbehavior produce the risk in the vehicular network. Therefore, trustworthiness is an important factor to deal with which is a critical issue in the network [3]. The trust management program allows vehicles to determine whether or not the received message is reliable [8] [9]. Normally, the vehicle's trust value can be determined based on the ratings produced by the vehicle's past behavior. Trust management can be categorized into two classes, i.e. centralized and decentralized [10] [11]. Centralized systems store confidence values on the central repository, e.g. the cloud repository. These central systems cannot fulfill the stringent quality of services (QoS) specifications because any time nodes have to ask the central server to test the trust value that increases the latency of the network. Trust management is to be conducted at a vehicle or RSU level in decentralized trust management systems so the task for interaction with the server is reduced too much extent which ultimately increases the efficiency of the system [12] [13] [14]. Moreover, we cannot rely on one node for trust management. Due to the dynamic network, it is difficult to trust each node for the ratings. Therefore, designing an effective decentralized network is still a challenge [14].

Blockchain is one of the new innovations in the financial sector that establishes a clear and tamper-proof ledger without centralized banks, so people can transact with absolute trust [17] [18] [22]. Due to its high security, blockchain has been commonly used in the non-financial market, i.e. content delivery [26], key management [23], decentralized storage [24] [25] etc. Therefore, due to the design of the blockchain trust management, it can be conveniently carried out between nodes with decentralized systems [19]. The block generation by the attacker is slow as compared to the normal RSUs due to trustworthiness. The proposed system works effectively by holding the trustworthiness between the nodes in vehicular networks. Internet of vehicles using big data is also a trending area and which is explored by game theory i.e. coalition games for spatio-temporal big data in internet of vehicles where the vehicles will be rewarded and penalized according to game rule [16]. Automated based contention aware data forwarding has also been proposed which is based on Baysian coalition game theory which improves the routing parameters of VANET [17] [20]. The contribution of this paper is summarized below:

(a) A decentralized trust management system has been proposed based on blockchain technology which permits all the vehicles and RSUs to update the trust value in decentralized manner and active participation of all vehicles and RSUs for the updation procedure.

(b) We have proposed a Proof of Authority (PoA) which is better than Proof of Work (PoW) and Practical Byzantine Fault Tolerance (pBFT) because of high energy consumption and more overhead respectively.

(c) We have proposed a system model and conducted a simulation which proves that our proposed model is efficient in practical vehicular networks.

2. Related Work

2.1 Byzantine Consensus

The consensus is a part of distributed computing. An agreement is reached between a distributed number of processes [5] and a popular consensus scheme is called the Byzantine Fault Tolerant (BFT). This type of protocol is used to secure the network from node failure. Practical Byzantine Fault Tolerance (PBFT) [7] is one of the well-established BFT algorithms since it is based on three rounds prior to the actual agreement. This ensures that 3f+1 nodes are necessary to reach a consensus if we have f Byzantine nodes [7]. In [15] the author discusses well-known families of consensus algorithms for both permissionless and permissioned blockchain, which includes Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Burn (PoB), etc. Decentralized key management mechanism has been proposed which is light weight mutual authentication scheme used to prevent many network attacks [41].

The distributed consensus in the blockchain creates trust between multiple parties and is considered to be Byzantine Consensus [21]. Byzantine consensus is still a research field and is backed by recent advances in blockchain technology. The consensus is broadly divided into proof-based and voting based. Under proof-based bitcoin is the popular one that uses PoW that requires the miner to solve the difficult problem and it requires a large number of resources. Moreover, the transactions are very slow nearly seven transactions per second. PoS uses stake to determine the mining difficulty which can be determined as proof for the voting [21]. Proof based mechanism provides consistency in the network but

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

suffering from the lower transaction rate and large resource consumption. Novel VANET system model using edge computing is implemented and it uses individual session key for each vehicle to prevent interference [42] [39]. The RFID based mechanism provides better authentication and prevent many network attacks and it uses Elliptic Curve Cryptography to secure the session [37]. Moreover, Telecare medical information system also used ECC mechanism for preserving the anonymity of the user and it is found to be suitable in cryptography [38]. Even to secure the localization the same trust base mechanism is used in wireless sensors network which is based on decentralization [44].

The voting-based consensus is more useful for the permissioned blockchain customer because of knowing your customer methodology nodes will achieve a consensus over multiple rounds of collective voting. The popular project Hyperledger fabric [27] uses PBFT in its 0.6version, R3 Corda employs BFT-SMaRt [28] which is identical to PBFT. Blockchain architecture is used to prevent many network attacks due to its tamperproof environment and it provide more security to transactions. Moreover, these transactions are transparent on blockchain [43].

2.2 Centralized trust management

So many researchers have put up a lot of research work for centralized trust management in recent years. Central servers are used to collect, measure and store the trust value of all vehicles and are believed to be a fully trusted entity not compromised by an attacker [7] [10] [11]. Vehicles notice traffic-related incidents and issues notices to neighbors. Vehicle feedback is obtained from a centralized reputation-based server. Based on these results, the server is able to issue certificates based on their credibility values.

Simulation and punishment mechanisms are also shown [10]. In this, the concept of micropayment has been shown. Honest nodes can earn a certain amount of credits which they can spend on relaying the packets. If any node with more packet drop is identified by the receiver that will be evicted from the network.

With the evident increase in the number of vehicles, it is not possible to cope up with all nodes using centralized systems. Moreover, if the central system fails the entire system failure can be possible.

2.3 Blockchain based decentralized data management

Blockchain is a very recent technology that also provides the concept of decentralization. Blockchain-based crowdsourcing program introduced by [29] used to apply for court adjudication. [30] and [31] proposed blockchain-based crowdfunding that is a different form of crowdsourcing. In addition,[25] developed a distributed storage and keyword search based on blockchain. Public keys of the entire network are stored in this paper blockchain. Therefore, blockchain helps to design a trust-based decentralized and tamper-proof network for vehicular networks.

Therefore, it has summarized that PoW and PoS are the consenses that are widely used in permissionless blockchain. Tendermint is the open-source consensus protocol that can solve the problem of Byzantine fault tolerance.

3. Proposed Approach

The proposed system model consists of the following components as illustrated in Figure 2

3.1 Road Side Unit

Roadside units are used to communicate with the vehicles running on the road and give the information and updates about the route. This is acting as a bridge between trusted authority and end-users. Moreover, RSU is also responsible for some of the major tasks i.e. collection of ratings and trust value management.

3.2 On-Board Unit

This unit is used to broadcast the traffic-related information periodically. The information contains the speed, multimedia and updation of direction for the traffic movement.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

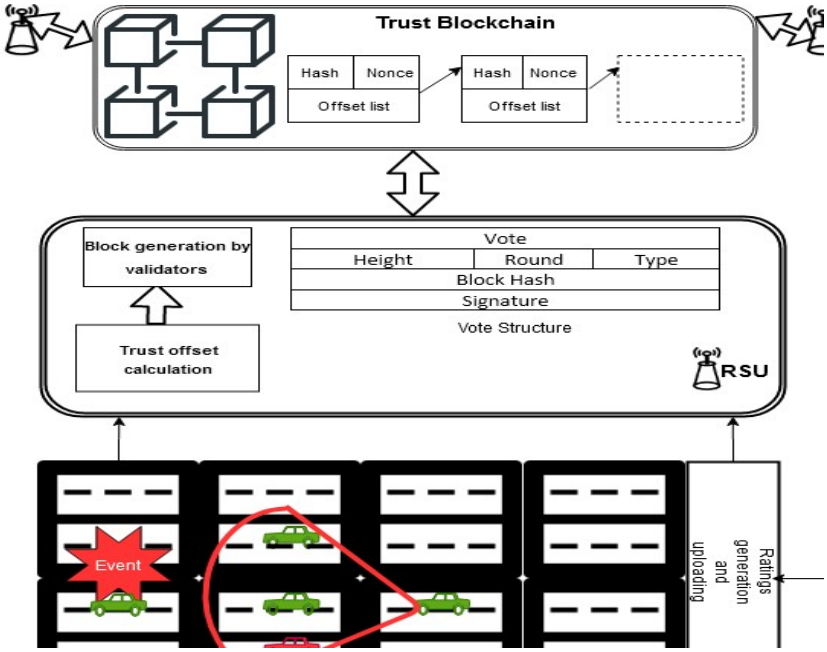

Figure 2. Proposed blockchain based system model for trust management system

3.3 Trust Value management

We assume that the RSUs are able to calculate the trust values by aggregation of the ratings received from the different vehicles. So, the credibility of the message is basically judged by the aggregated value of the rating and can be fetched from the trust value management servers [32].

3.1 Main Procedures

The proposed model procedure is divided into three parts as described in Figure 2.

Step 1 Rating generation and uploading

This is the first step towards the decentralization of trust management in a vehicular network. This is the procedure that has to be conducted on vehicles. Some specific rules are required to assess the credibility of the messages and to generate the ratings. Messages are divided into groups {*M1, M2, ……Mj*}, where M_j represents the group reporting event e_j. e.g. an accident happened in one road segment R. All messages are having different values of ratings calculated by the RSUs. The vehicle which is near to the event will have more rating value because it is close to the event elapsed and will exactly aware that the event happened or not. Therefore, the credibility of a certain message is defined as follows [32]

$$c_{k=}^{j} b + e^{-\gamma d_k^j} \quad (1)$$

Where c_k^j is the credibility of the message in group Mj by vehicle, d_k^j is the distance between the sender and the location of the event. b and γ are two preset parameters, which control the lower bound and the rate of change of message credibility. Moreover, c_k^j=0; if k does not report this event. The receiver can obtain a credibility set C^j for event e^j using Eq. (1), where $C^j = \{ c_1^j, c_2^j, \ldots \ldots \}$. Based on credibility set C, the receiver is able to calculate the aggregated credibility of event e using Gradient Boosting Technique [33].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

The Gradient boosting technique splits input space into T_m disjoint regions like $R_{1m}, R_{2m}, \ldots R_{Tm}$ and then predicts a vehicle with a lower trust value in each region. Here, T_m represent the number of leaves in a tree. Therefore, output of a gradient boosting. Thus, output of gradient boosting tree $h_m(x)$ for input x (x indicates the mobile node with trust value) and represented mathematically as follows:

$$h_m(x) = \sum_{T=1}^{T_m} b_{tm}\ I\ (x \in R_{Tm}) \tag{2}$$

From Eq. (2), b_{tm} denotes the predicted mobile nodes which consisting of lower trust value in tree. After that, the coefficients b_{tm} are multiplied by a random value γ_m in order to remove the lower trust value mobile nodes in VANET scenario. So, the updated model is described below:

$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x) \tag{3}$$

$$\gamma_m = \arg\min_{\gamma} \sum_{i-1}^{n} L\ (y_i, F_{m-1}(x_i) + \gamma_m h_m(x_i) \tag{4}$$

Using Eqs. (3) and (4) the lower trust values from the vehicular network will be removed by RSU. Finally, the nodes with higher trust values will be retained by the given formula,

$$F_m(x) = F_{m-1}(x) + \sum_{T=1}^{T_m} \gamma_{T_m} I(x \in R_{Tm}) \tag{5}$$

$$\gamma_{T_m} = \arg\min_{\gamma} \sum_{x_i \in R_{Tm}}^{n} L(y_i, F_{m-1}(x_i) \tag{6}$$

RSU may have differences in ratings produced by similar messages, e.g. 9 positive and 3 negative ratings. The former is a majority group and the latter is a minority group. In the proposed methodology, weighted aggregation solves the problem of ranking conflicts. The offset is between-1 and + 1 (normalized value), which is positively associated with the positive rating ratio in this message. The estimation of the offset value of the trust is shown in Eq.7.

$$\sigma_k^j = \frac{\theta_1 . m - \theta_2 . n}{m + n} \tag{7}$$

Where σ_k^j is the trust value offset of vehicle k based on message j and $\sigma_k^j \in [-1,1]$. m and n are the number of positive and negative ratings, whose weights are θ_1 and θ_2, respectively. θ_1 and θ_2 are determined using Eq. 8 and 9.

$$\theta_1 = \frac{F(m)}{F(m) + F(n)} \tag{8}$$

$$\theta_2 = \frac{F(n)}{F(m) + F(n)} \tag{9}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

Where $F(.)$ controls the sensitivity of the minority group of ratings, e.g., $F(x) = x^2$ is less sensitive to the minority group of ratings compared with $F(x) = x$.This strategy has been carried out under the premise that the intruder cannot dominate the majority group. The proposed weighted aggregation is therefore in a position to boost the reliability of the trust value offsets.

Step 2 BFT based consensus for transaction between vehicles

PoW cannot deter the participants from performing selfish mining [40]. If we choose the PoS we can remove the problem of energy consumption and speed can also be increased. Joint proof of work and a method for creating a block that takes the number of absolute offsets as a stake and the complexity of completing the proof of work depends on the stake. RSU has more stakes and can quickly locate the nonce and win the mining election [32]. It will publish the block faster as compare to alone PoW but PoW and PoS both are the mechanisms used for permissionless blockchain which is more vulnerable to network attacks. So, we want to introduce here the permissioned blockchain consensus in our proposed model which is more secure than the permissionless blockchain. The proposed block generation method is based on validators and voting power i.e. Tendermint [consensus without mining]

A. Validators Every node has the same weight in the BFT process. In Tendermint, nodes with a non-negative sum of voting power and nodes with a positive voting power are considered as validators. Such participants participate in the consensus through the transfer of signatures and votes to the next generation of blocks.

B. System Model Tendermint consists of three steps- *Propose, Prevote, Precommit* and two special steps *Commit and NewHeight*.

Obtaining more than 2/3 of commit requires obtaining commitments from a total of 2/3 validators. When commitments for this block have been signed and transmitted by 2/3 validators so block is said to be dedicated by network. Vote structure is shown in Figure 3.

Vote		
Height	Round	Type
Block hash		
Signature		

Figure 3. Vote structure

The three steps which we mentioned takes one-third of the total allocated time. Every round is longer span of time as compare to the previous round so that consensus achieves and block generates.

The proposer is chosen in round-robin fashion in each round, so that validators are chosen in proportion to their voting power with frequency. The structure of proposer as shown in Figure 4.

Proposal	
Height	Round
Block	
Proof of Lock	
Signature	

Figure 4. Proposal Structure

The first step is Proposal step in which the proposer transmits a proposal by gossiping to his peer. When a proposer is locked into a prior process then the initiative proposes a proof-of-lock.

The next step is Prevote where each validator determines. If validator is locked on to any previous block proposed, it will sign and broadcast a locked block prevote. If no block has been sent by the validator then it sends null prevote.

Each validator makes the decision in the beginning of Precommit phase. Validator signs and transmits a precommit for that block if it has received more than 2/3 prevotes for a similar appropriate block. If the node receives 2/3 null votes then it simply unlocks the block.Each node makes the decision at the end of Precommit phase. If more than 2/3 of precommits have been received by the node than entered for the Commit stage. Otherwise it will start with Propose

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

next round stage.The Commit step is very important step here in which two parallel conditions needs to be checked before finalizing the round. First, the node will obtain the block that the network has committed. Second, once received and signed by validator broadcasts a commit for that block. All this work flow is shown in Figure 5. This is the one round of consensus for the generation of block by the RSUs. In this way RSUs can handle the malicious node if any present in the network.

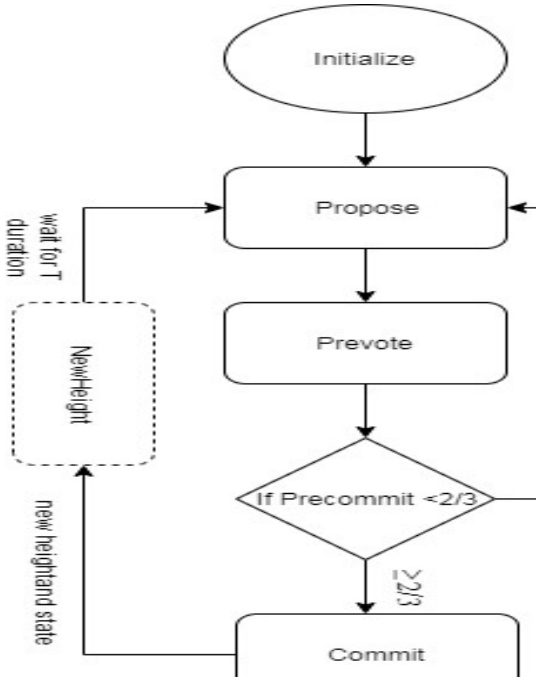

Figure 5. Consensus algorithm without mining used by Tendermint

4. Simulation Parameters

To analyze the proposed approach network performance analysis is selected. The proposed consensus scheme performance was also compared with the existing consensus scheme implemented on VANET network. SUMO simulator has used for the vehicular setup and the simulator parameter are as described in Table 1.

Table 1. Simulation parameters

Parameter	Value
No. of Nodes	50
Maximum Vehicle Speed	40 m/s
Length of Vehicle	3 m
Width of Vehicle	2 m
Number of RSUs	7
RSU coverage	1 Km

5. Implementation and Results

Performance of the Tendermint by considering the different number of nodes is shown in Figure 6. In this, we have considered four scenarios in which 50 nodes are considered at the maximum and it is also shown that Tendermint can process thousands of transactions per second which ultimately increases the throughput level and the delay of the system reduces.

5.1 Performance metrics

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

This section reflects the theoretical study and the feasibility of the consensus suggested in the VANET networks. The network output is measured in terms of the packet delivery ratio, the end-to-end delay. Evaluation of the results is achieved by running the simulation and statistical analysis is conducted by averaging the collected values to a mean value.

5.2 *Packet Delivery Ratio (PDR)*

This applies to the amount of packets received successfully to the cumulative amount of packets transmitted across the network [35]. Mathematically, it is given by:

$$PDR = \frac{P_r}{P_s} \tag{10}$$

Where P_r is the total number of packets received and P_s is the total number of packets sent.

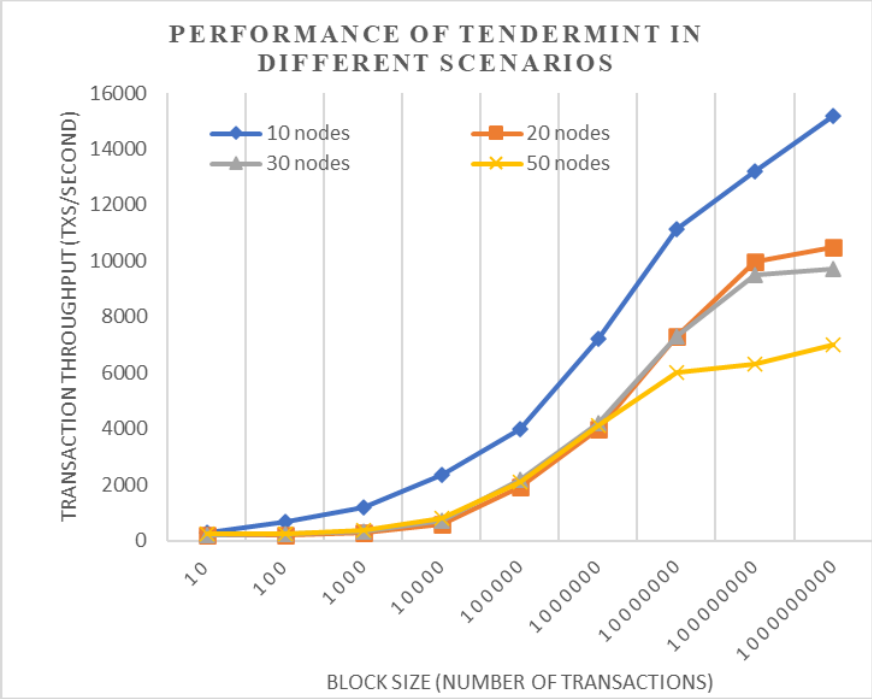

Figure 6. Performance of Tendermint

Figure 7 illustrates the packet delivery ratio for the proposed consensus scheme i.e. tendermint incurred higher PDR, with a difference of 7.8%, 5.6% and 2.4% as opposed to PoW, PoS and Hybrid respectively.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

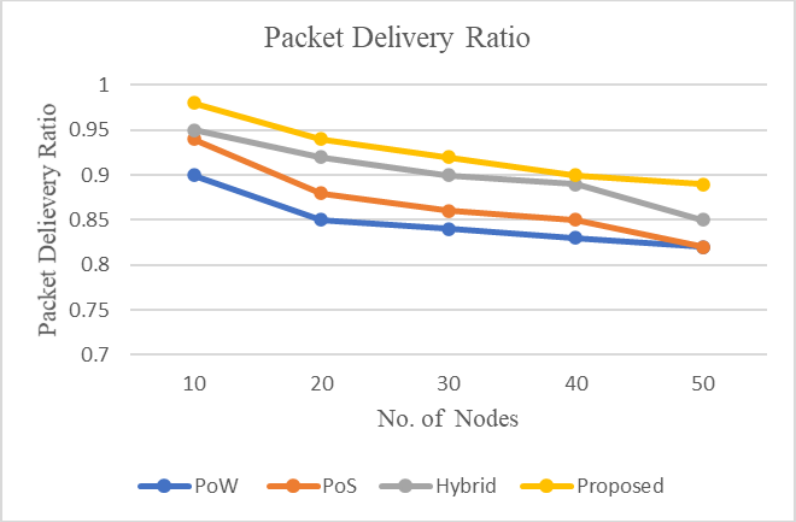

Figure 7. Packet Delivery Ratio

5.2 End-to-End Delay

End-to-end delay (EED) is defined as the time it takes for a packet to get from the source to the destination [36] [39]. End-to-end delay is impacting the PDR significantly on the network. Mathematically, it is given by:

$$EED = \sum T_A - T_S \tag{11}$$

where T_A is arrival time of packet and T_S denotes the sent time of packet.

Figure 8 shows the simulation results and proposed solution incurred low end-to-end delay with a difference of 15.60%, 3.60% and 11.80% as compared to PoW, PoS and Hybrid. The average delay in the case of the proposed scheme is 0.15 seconds which is far better than other schemes and compared in Figure 8.

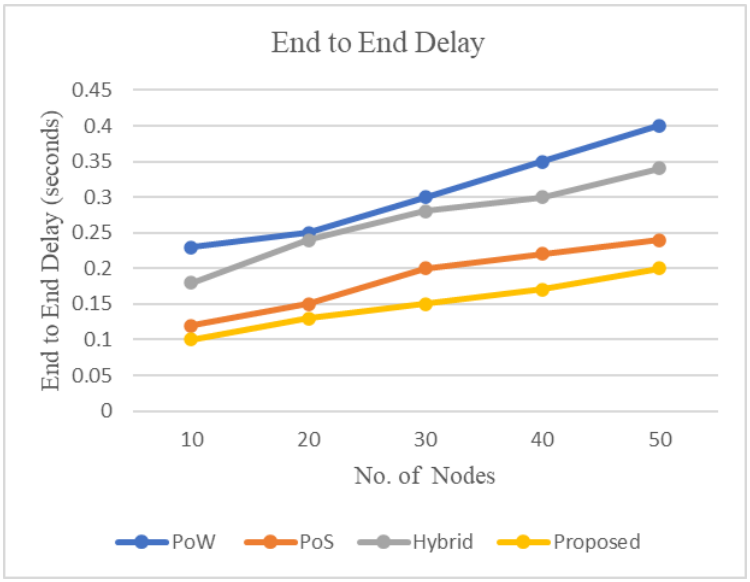

Figure 8. End-to-End delay

5.3 Performance Analysis of ratings

As we have already shown the end-to-end delay is more in the case of PoW i.e also reflected in the rating calculation. The latency has been shown in Figure 9 and it is incurred low with a difference of 0.48s, 0.44s, and 1.46s as compared to PoW, PoS and Hybrid.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2021 doi:10.20944/preprints202102.0207.v1

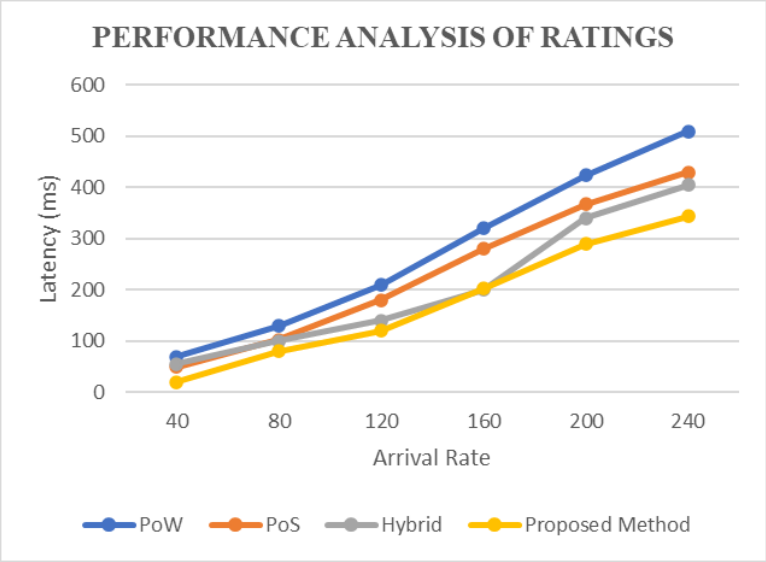

Figure 9. Performance analysis of ratings

5.4 Performance Analysis of ratings

As we have already shown the end-to-end delay is more in the case of PoW i.e also reflected in the rating calculation. The latency has been shown in Figure 9 and it is incurred low with a difference of 0.48s, 0.44s, and 1.46s as compared to PoW, PoS and Hybrid.

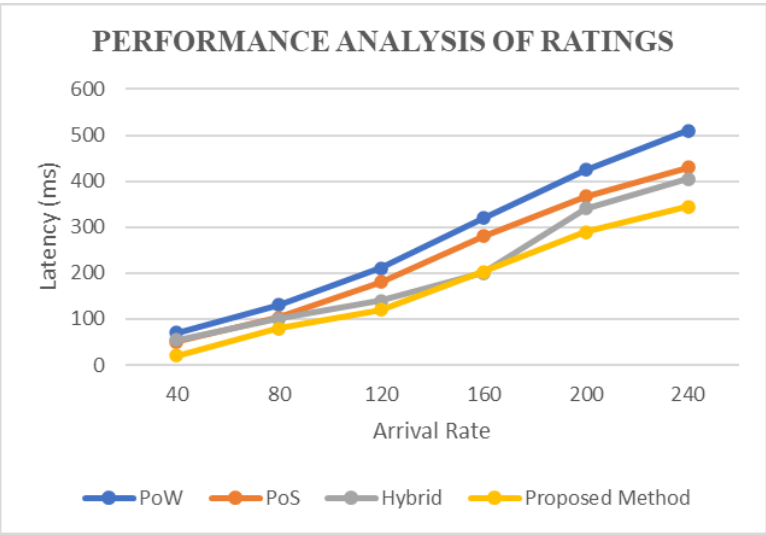

Figure 9. Performance analysis of ratings

6. Theoretical Analysis

6.1 Free from deadlock

It means no node at any point in time will wait for another node. No node will wait for a separate node to transmit or accept a request or vote, start to validate a block or add a block to its line.

6.2 Message spoofing attack

When a malicious vehicle enters into the system and tried to send the fake messages of accidents on the road but there was no accident. This is called message spoofing. We proposed the double layer mechanism here to defend against this kind of attack. First layer will use the Gradient Boosting Technique (GBT) based on machine learning mechanism able to provide trustworthiness between the vehicles. The credibility of the message has been checked by the receiver which analyze the different messages and their ratings broadcasted in the network. Tendermint based on Byzantine

fault tolerance acts as a second layer using the permissioned blockchain which is very less vulnerable as compared to permissionless blockchain.

6.3 Overwriting proposed blocks

When the nodes clash to reject the existing block, and suggest their own new block. To resist this form of attack, after consensus has been achieved, all nodes must agree on the same block to connect to the chain.

6.4 Temperproof environment

It is difficult to change or tamper the messages stored by the RSUs using blockchain. All the RSU's store the same blockchain version and continuously add new blocks to the blockchain. Compromised RSU's will create fake blocks and broadcast them. They do need to contend with the other blocks included in the blockchain, however. Therefore, the amount of compromised RSU's in this case is negligible due to the use of permissioned blockchain.

6.5 Strong privacy

Tendermint uses BFT consensus algorithm where appointed nodes send and receive messages and agree on blocks. It includes Propose, Prevote and Precommit messages. These messages included the signature of the node created the message. A block will generate after the consensus contains a Precommit signature of the node that agreed on block. Hence it maintains the privacy among the nodes.

7. Conclusion

In this paper, we have proposed a blockchain-based decentralized system that maintains the trust between the vehicles and that trust value is aggregated in the RSU's to share the data without tampering because of each RSU's stores the same version of blockchain. Simulations are carried out to check out the performance of the proposed technique and it shows that the proposed technique is providing fast transactions per second, high throughput and efficient PDR values. In future, the work on scalability can be performed when the number of vehicles grows rapidly. It is believed that by applying a blockchain based system the vehicles can communicate with neighbors safely and it also helps to build the intelligent transportation system.

Author Contributions: Sandeep Kumar Arora designed and performed the experiments, derived the models, and analyzed the data. He also wrote the manuscript in consultation with Gulshan Kumar.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhou H., ChainCluster: Engineering a cooperative content distribution framework for highway vehicular communications. *IEEE Trans. Intell. Transp. Syst.* **2014**, Vol. 15, pp. 2644–2657.
2. He, S; Shin, D.H.; Zhang, J.; Chen, J.; Sun, Y. Full-view area coverage in camera sensor networks: Dimension reduction and near-optimal solutions. *IEEE Trans. Veh. Technol.* **2016**, Vol. 65, pp.7448–7461.
3. Zheng, K.; Zheng, Q.; Chatzimisios, P.; Xiang, W.; Zhou, Y. Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions. *IEEE Commun. Surveys Tuts.* **2015**, Vol. 17, pp.2377–2396.
4. Wasef, R.; Lu, X.L.; Shen, X. Complementing public key infrastructure to secure vehicular ad hoc networks. *IEEE Wireless Commun.* **2010**, Vol. 17, pp.22–28.
5. Angelis, S. et al. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain. Italian Conference on Cyber Security, 2018, pp.1-11.
6. Zhang, K. et al. Security and privacy in smart city applications: Challenges and solutions. *IEEE Commun. Mag.* **2017**, Vol.55, pp.122–129.
7. Castro, M.; Liskov, B. Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.* **2002**, Vol. 20, pp.398–461.

8. Roosta, M.; T.; Meingast, M.; Sastry, S. Distributed reputation system for tracking applications in sensor networks, Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst. San Jose, CA, USA, 2006; pp.1–8.
9. Li, S.; Wang, X. Quickest attack detection in multi-agent reputation systems. *IEEE J. Sel. Topics Signal Process.* **2014**, Vol. 8, pp. 653–666.
10. Mahmoud, M.E.; Shen, S. An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks. *IEEE Trans. Veh. Technol.* **2011**, Vol. 60, pp.3947–3962.
11. Lai, C.; Zhang, K.; Cheng, N.; Li, H.; Shen, X. SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs. *IEEE Trans. Intell. Transp. Syst.* **2017**, Vol. 18, pp.1559–1574.
12. Gurung, S.; Lin, D.; Squicciarini, A.; Bertino, J. Information oriented trustworthiness evaluation in vehicular ad-hoc networks Int. Conf. Netw. Syst. Security, 2013; pp. 94–108.
13. Li, Z.; Chigan, C.T. On joint privacy and reputation assurance for vehicular ad hoc networks. *IEEE Trans. Mobile Comput.* **2014**, Vol. 13, pp. 2334–2344.
14. Huang, X.; Yu, R.; Kang, J.; Zhang, Y. Distributed reputation management for secure and efficient vehicular edge computing and networks. *IEEE Access.* **2017**, Vol. 5, pp. 25408–25420.
15. Mattila, J. The blockchain phenomenon. Berkeley Roundtable of the International Economy **2016.**
16. Kumar, N.; Misra, S. et.al. Coalition Games for Spatio-Temporal Big Data in Internet of Vehicles Environment: A Comparative Analysis. *IEEE Internet of Things.***2015**, Vol. 2, pp. 310-320.
17. Kumar, N.; Misra, S. et.al. Bayesian Coalition Game for Contention-Aware Reliable Data Forwarding in Vehicular Mobile Cloud. *Future generation computer systems*. **2015**, Vol. 48, pp. 60-72.
18. Kim, T. H; Kumar, G. et. al. A Privacy Preserving Distributed Ledger Framework for Global Human Resource Record Management: The Blockchain Aspect. *IEEE access.* **2020**, Vol. 8, pp. 96455-96467.
19. Goyat, R.; Kumar, G. et. al. Blockchain Powered Secure Range-Free Localization in Wireless Sensor Networks. *Arabian journal for science and engineering*. **2020**, Vol. 45, pp. 6139-6155.
20. Kumar, N.; Iqbal, R. et. al. An intelligent approach for building a secure decentralized public key infrastructure in VANET. *Journal of Computer and System Sciences.* **2015**, Vol. 81, pp.1042-1058;.
21. Zyskind, G.; Nathan, O.; Pentland, A.S. Decentralizing privacy: Using blockchain to protect personal data, Security and Privacy Workshops (SPW). *IEEE Access.* **2015**, pp.180–184.
22. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the Internet of Things. *IEEE Access.* **2016,** Vol. 4, pp. 2292–2303.
23. Lei A. et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet Things Journal.* **2017**, Vol. 4, pp. 1832–1843.
24. Cai, C.; Yuan, X.; Wang, C. Towards trustworthy and private keyword search in encrypted decentralized storage. IEEE Int. Conf. Commun. (ICC), 2017; pp. 1–7.
25. Cai, C.; Yuan, X.; Wang, C. Hardening distributed and encrypted keyword search via blockchain, IEEE Symp. Privacy Aware Comput. (PAC), 2017; pp.119–128.
26. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surveys Tuts.***2016**, Vol. 18, pp. 2084–2123.
27. Cachin, C.; Vukolic, M. Blockchains consensus protocols in the wild. arXiv preprint arXiv, **2017**,1707.01873
28. Clique. https://github.com/ethereum/EIPs/issues/225 (accessed on 2 July 2020)
29. Federico, A.S. The crowdjury, a crowdsourced justice system for the collaboration era, 2015.

30. Jacynycz, V.; Calvo, A.; Hassan, S.; Sanchez-Ruiz, A.A. Betfunding: A distributed bounty-based crowdfunding platform over Ethereum, Distributed Computing and Artificial Intelligence, 13th International Conference. 2016; pp. 403–411.
31. Zhu, H; Zhou, Z.Z. Analysis and outlook of applications of blockchain technology to equity crowdfunding in china. *Financial Innovation*.**2016**, Vol. 2(1), pp. 1- 29.
32. Yang, Z. et al. Blockchain-Based decentralized trust management in vehicular networks. *IEEE Internet of Things*.**2019**, Vol. 6, pp. 1495-1505.
33. Sangeetha, S. et al. Self-organized gradient boosting key authentication for secured data communication in mobile adhoc network. *International Journal of Applied Engineering and Research*. **2017**, Vol. 12, pp. 7823-7832.
34. Study on LTE-based V2X services, V1.0.0: TSG RAN, 3GPP, Sophia Antipolis, France, Rep. TR 36.885,2016.
35. Draz, U. et al. Evaluation based analysis of packet delivery ratio for AODV and DSR under UDP and TCP environment, International Conference on Computing, Mathematics and Engineering Technologies, 2013.
36. Shorfuzzaman, M. et al. Characterizing end-to-end delay performance TCP using an analytical model. *International Journal of Advance Computer Sci. Appl.* **2016**, Vol.7, pp. 406–412.
37. Kumar, N.; Kaur, K.; Misra, S; Iqbal, R. An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud. *Peer to Peer networking and applications.* **2015**, Vol. 9, pp. 824-840.
38. Amin, R. et. al. An Efficient and Practical Smart Card Based Anonymity Preserving User Authentication Scheme for TMIS using Elliptic Curve Cryptography. *Journal of medical systems*. **2015**, Vol. 39, pp. 525-533.
39. Pukale, P; Gupta, P. Analysis of end-to-end delay in vehicular networks. *Int. J. Sci. Res.* **2015**, Vol. 5, pp. 1122–1125.
40. Thin, W.Y. et al. Formal Analysis of a Proof-of-Stake Blockchain, International Conference on Engineering of Complex Computer Systems, 2018; pp.105-115.
41. Ma, Z et.al. An efficient decentralized key management mechanism for VANET with Blockchain. *Int. J. of Vehicular Technology*. **2020,** Vol. 69, pp. 5836-5849.
42. Tan, H; Chung, I. Secure authentication and key management with blockchains in VANETs. *IEEE access*. **2019**, Vol.8, pp. 2482-2498.
43. Khan, A.S et.al. Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors*.**2019**, Vol. 19, pp. 1-27.
44. Kim, T.H.; Goyat, R.; Kumar, G. A Novel Trust Evaluation Process for Secure Localization Using a Decentralized Blockchain in Wireless Sensor Networks. *IEEE access.* **2019**, Vol. 7, pp. 184133-184144.