A Voting Blockchain based Message Dissemination in Vehicular Ad-Hoc Networks (VANETs)

Ferheen Ayaz, Zhengguo Sheng, Daxin Tian†, Guan Yong Liang*, and Victor Leung‡
Department of Engineering and Design, University of Sussex, UK
† School of Transportation Science and Engineering, Beihang University, China
* School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore
‡ Department of Electrical and Computer Engineering, University of British Columbia (UBC), Canada
Email: F.Ayaz@sussex.ac.uk

***Abstract*—Secure message dissemination is an important requirement of intelligent transportation systems (ITS). Existing solutions, such as broadcasting, are effective in flooding a message to a wider area, however, they are inherently unreliable and bandwidth inefficient. Furthermore, it is difficult to both assess the authenticity of a message and maintain the privacy of sender in a single solution. Moreover, as a practical solution, there is a need of economic modeling to incentivise vehicles for safe driving and cooperation. This paper proposes a blockchain based message dissemination approach which utilises incentive distribution and reputation management to overcome these challenges. Specifically, with the proposed voting based consensus algorithm, it can assess the authenticity of a message and select the most suitable relay node for its dissemination in a completely decentralised fashion. Meanwhile, the blockchain based integrated incentive and reputation scheme encourages the cooperation among vehicles and strengthens its ability to deliver authentic messages. The security capacity of the proposed solution is demonstrated by a game theoretic analysis. Simulation results show that the proposed approach can save average consensus time by 11% and improve success rate of authentic message dissemination by 17% with less number of hops as compared to the existing solutions.**

***Index Terms*—blockchain, reputation, incentive, VANET**

I. Introduction

A prominent feature of Intelligent Transportation Systems (ITS) is using vehicle-to-everything (V2X) communications to disseminate messages in emergency situations, such as traffic jam and accident, thereby leading to improved road safety and driving conditions [1]. It is important for vehicles in Vehicular Ad-Hoc Network (VANET) to authenticate messages [2]. Moreover, due to increasing privacy concerns, the identity of a vehicle must not be revealed if it originates or forwards a message. Although message dissemination, trust management, privacy and security in VANETs are widely discussed in the literature [3], [4], there is a need to develop an integrated approach in which efficient and trusted V2X communications can be managed without a central authority.

To further maintain the sustainability of message dissemination, economic modeling is needed to strategise incentives, encourage cooperation and punish negative behaviour. Generally, there are two types of incentive strategies: price based and reputation based. An integrated strategy leveraging advantages of both price and reputation based schemes is more effective in encouraging cooperation and detecting malicious behaviour in Mobile Ad-hoc Networks (MANETs) [5]. Another challenge associated with message dissemination is broadcasting storm. It occurs when multiple vehicles send the same message simultaneously, which is highly bandwidth inefficient and may result in packet collision. VANET must be able to select appropriate relay nodes which can effectively forward a message to a large number of vehicles [6].

In this paper, we propose a voting based blockchain for message dissemination to overcome the discussed challenges in VANET. A blockchain is an encrypted and decentralised peer to peer system in which transaction data is maintained in a ledger as immutable timestamped blocks [7]. It is able to solve issues related to privacy and authentication. The consensus protocol is the core of a blockchain. It is an agreement to validate a transaction. Proof-of-Work (PoW) consensus is known for its high computation cost and large propagation delay. An alternative of PoW is Proof-of-Stake (PoS) which selects miner to commit block on the basis of highest stakes owned. However, it is unfair to other members in blockchain possessing smaller stakes [8]. Some blockchains use Practical Byzantine Fault Tolerant (PBFT) protocol which requires a certain number of votes to validate a transaction [9]. A novel PBFT protocol known as Yet Another Consensus (YAC) requires votes for not only transaction validation but also selection of miner [10]. A comparison of basic consensus protocols is summarized in Table I, which indicates that PBFT is the most promising consensus protocol for VANETs.

For vehicular networks, Kang *et al.,* [11] proposes a blockchain enabled reputation management based on the consensus protocol of PoS where reputation is the stake of vehicles. The vehicles report their reputation opinions of other vehicles to a nearby Road Side Unit (RSU). To carry out consensus protocol, a miner is elected on the basis of highest reputation. The vehicle is considered malicious if its reputation value is below a certain threshold. A similar work is presented by Yang *et al.,* [12] where RSUs store the reputation of vehicles and maintain blockchain. The consensus is completed by participating RSUs. In [13], a blockchain of reputation is managed by each vehicle and messages are authenticated based upon the sender's reputation. Apart from reputation, Li *et al.,* [14] proposes a blockchain based incentive announcement

978-1-7281-5089-5/20/$31.00 ©2020 IEEE

TABLE I: Performance comparison of consensus protocols

Feature	PoW	PoS	PBFT
Energy saving	No	Yes	Yes
Time saving	No	Yes	Partial
Discriminatory	Yes[a]	Yes[b]	No
Example	Bitcoin [7]	Ethereum(Serenity) [8]	Hyperledger [9]

[a]Towards computational power
[b]Towards stakes owned

network which uses virtual credits, known as, CreditCoin, as a reward for forwarding message. Transactions of CreditCoins are managed by blockchain, whereas VANET communication is implemented separately. The contributions of this paper are summarised as follows:

- We propose a blockchain based VANET by economically modeling an integrated price and reputation based incentive strategy for message dissemination. Using game theory analysis, the proposed strategy is proved to be secure against malicious vehicle behaviour.
- We design a voting based consensus algorithm for vehicles. Simulation results show that it saves 11% of time in finalising transactions compared to another voting based consensus protocol, CreditCoin [14].
- We develop a novel relay selection as a part of the consensus algorithm. Simulation results show that the proposed approach improves the success rate of message dissemination by 17% with less number of hops than the reputation based blockchain approach [11], [12].

The remainder of this paper is organized as follows. Section II explains the proposed blockchain design. Section III presents game theoretic analysis of proposed solution. Section IV includes results and discussion. Section V concludes the paper.

II. Proposed Solution

A. Components Definition

The system components are described as follows.

a) Central Authority (CA): Before joining the blockchain network, a vehicle needs to be registered with CA. It assigns a wallet address and a pair of public and private keys to vehicle for communications and records its original identity. The role of CA is to grant vehicles an access to a permissioned blockchain system.

b) Originator (ORG): It is the vehicle which is involved in an incident and originates a $transaction\ proposal$.

c) Transaction Proposal: It is an unendorsed message sent by ORG including incident details, its location and time.

d) Endorsement: An $endorsement$ is a vote confirming that a $transaction\ proposal$ is authentic. A minimum number of $endorsements$, N^{min}_{END}, is required to consider a $transaction\ proposal$ as an endorsed message.

e) Endorsers at hop i ($\overline{END}(i)$): At each hop i, it is a set of vehicles which vote for a relay node. When $i = 0$, $\overline{END}(i)$ are vehicles adjacent to ORG. They vote for a relay node and also endorse a $transaction\ proposal$, if they have witnessed the incident.

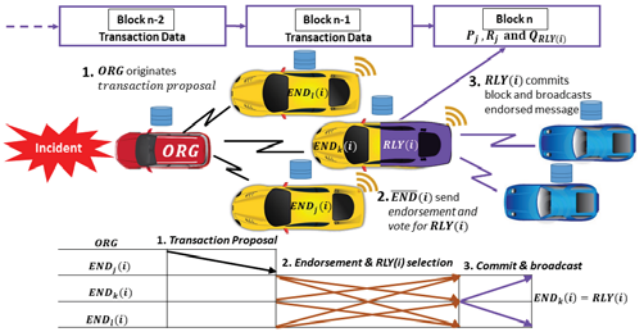


Fig. 1: Voting based consensus protocol.

f) Relay node at hop i ($RLY(i)$): It is the vehicle which forwards an endorsed message. It is mutually selected by voting of $\overline{END}(i)$. It is also one of the $\overline{END}(i)$ and may vote for itself. It also commits block to record transfer of virtual credits and reputation updates at each hop i.

g) Credit Wallet: Each vehicle possesses a credit wallet in which virtual credit is stored.

h) Reputation (R_j): It is a reputation value of vehicle j. A vehicle is only eligible to endorse a $transaction\ proposal$ if $R_j > R_T$, where R_T is the reputation threshold.

i) Transmission charge (TC): It is a fee deducted from a vehicle's credit wallet when it originates or endorses a $transaction\ proposal$ or further disseminates an endorsed message. This fee is deposited to CA. The purpose of introducing TC is to demotivate vehicles to make a fake $transaction\ proposal$ or $endorsement$, as it is generated at the expense of their virtual credit.

j) Call compensation (CC): As a compensation of causing an incident, CC is the amount deducted from the credit wallet of ORG. It is inversely proportional to R_{ORG}.

B. Voting based Consensus Protocol

The proposed consensus protocol based on YAC is illustrated in Fig. 1. When an incident occurs, ORG originates a $transaction\ proposal$. Upon receiving a $transaction\ proposal$, a vehicle j that can confirm the incident becomes an endorser, i.e. $j \epsilon \overline{END}(0)$, broadcasts its cryptographically encrypted signature as a part of $endorsement$ and votes for a suitable $RLY(0)$, as shown in Algorithm 1. If N^{min}_{END} endorsements are obtained within the time limit, t^{max}_{END}, the $transaction\ proposal$ is considered to be an endorsed message. Then $RLY(0)$ will further disseminate it and generate a block. Voting based selection of $RLY(i)$ for $i > 0$ continues until it reaches a maximum number of hops, that is, $i > N^{max}_{HOP}$ or the endorsed message has been disseminated until a time limit, t_{max}. It is noted that $\overline{END}(i)$ need to send $endoresements$ for a $transaction\ proposal$ only when $i = 0$. At $i > 0$, $\overline{END}(i)$ only take part in consensus of $RLY(i)$ selection, because they already receive an endorsed message instead of a $transaction\ proposal$.

C. Relay selection mechanism

$\overline{END}(i)$ vote for the most appropriate $RLY(i)$ which then further disseminates an endorsed message. In this work, we assume that each vehicle j shares its location coordinates, channel quality parameter, CQ_j, collision probability, CP_j, receiving antenna gain, G_j^r, transmitting antenna gain, G_j^t, maximum transmitting power, TP_j, and transmission range, TR_j, during their regular beacon message exchange. The parameters of $RLY(i)$ are stored in the blockchain and are regularly audited by CA to detect and investigate potential fraud if a vehicle cheats by sending fake parameters. $j \epsilon \overline{END}(i)$ computes the quality factor, Q_j, from the information received in beacon messages and determines its own choice of $RLY(i)$ with the highest Q_j, that is,

$$RLY(i) = index(max(Q_{\overline{END}(i)})), \tag{1}$$

and

$$Q_j = \alpha_1 df_j + \alpha_2 CQ_j(1 - CP_j) + RSSM_j. \tag{2}$$

where $j \, \epsilon \, \overline{END}(i)$, df_j is the distance factor of vehicle j, $RSSM_j$ is the received signal strength matrix, α_1 and α_2 are corresponding weights. df_j is defined as follows

$$df_j = \begin{cases} \frac{d_{j,ORG}}{d_{HOP}^{min}}, & \text{if } d_{j,ORG} \geq d_{HOP}^{min},\ i = 0, \\ \frac{d_{j,RLY(i-1)}}{d_{HOP}^{min}}, & \text{if } d_{j,RLY(i-1)} \geq d_{HOP}^{min},\ i > 0, \\ 0, & \text{otherwise}, \end{cases} \tag{3}$$

where d_{HOP}^{min} is the minimum distance a message should be disseminated per hop to restrict $RLY(i)$ selection outside a distance limit. CQ_j and CP_j depend upon internal statistical parameters of medium access control (MAC) as described in [15]. CQ_j is defined as follows

$$CQ_j = \begin{cases} \frac{N_j^s}{N_j^o}, & \text{if } N_j^o > 0, \\ 0, & \text{otherwise}. \end{cases} \tag{4}$$

where N_j^s is the number of successful transmissions and N_j^o is the number of total transmissions in a time window. CP_j is estimated as likelihood of collision occurrence if a message is forwarded by vehicle j. It is the ratio of accumulated time at which the channel is occupied, t_j^{occ}, and a fixed time window, t_w, i.e. $CP_j = \frac{t_j^{occ}}{t_W}$. The Received Signal Strength, RSS_j, as defined in [16], can be calculated from a distance between locations of vehicle j and j', where $j' \, \epsilon \, \overline{END}(i)$, as

$$RSS_j = \frac{G_j^r \times G_j^t \times TP_j}{(4\pi d_{j,j'}/\lambda)^2}. \tag{5}$$

where λ is the wavelength used in VANET. The threshold of received signal strength, RSS_T, is defined as

$$RSS_T = \frac{G_j^r \times G_j^t \times TP_j}{(4\pi \times 0.9054 TR_j/\lambda)^2}. \tag{6}$$

The range of antennas is assumed as the circular area of radius TR_j. From [15], it shows that the average distance between two random mobile nodes in a circular region of radius TR_j is $0.9054 \cdot TR_j$. The purpose of using RSS_T as a threshold parameter is to estimate the reliability of connection with vehicle j. If $RSS_j \geq RSS_T$, the connection can successfully be maintained for a certain time period. Otherwise, the connectivity may be lost before completing a voting consensus [17]. The $RSSM_j$ is calculated as

$$RSSM_j = \begin{cases} 1 - \frac{RSS_T}{RSS_j}, & \text{if } RSS_j \geq RSS_T, \\ 0, & RSS_j < RSS_T. \end{cases} \tag{7}$$

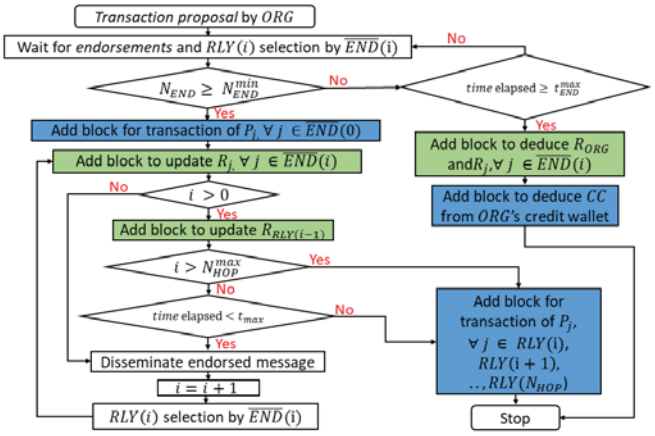


Fig. 2: Flowchart of the proposed message dissemination solution.

Algorithm 1 *Endorsement*

1: **if** $i == 0$ & $R_j > R_T$ **then**
2: **if** $validity(transaction\ proposal) == true$ **then**
3: $transaction\ proposal \leftarrow sign(\overline{END}(i))$
4: $RLY(i) = index(max(Q_{\overline{END}(i)}))$ //defined in (1)
5: **end if**
6: **else**
7: $RLY(i) = index(max(Q_{\overline{END}(i)}))$
8: **end if**

D. Block generation

After the consensus, $RLY(i)$ is responsible for block generation. The flow of its actions is displayed in Fig. 2. A block is generated at each hop to record parameters associated with $Q_{RLY(i)}$, transaction of virtual credits and update in reputation. Each vehicle in the network possesses the distributed ledger of blocks. Committing of transaction is announced by $RLY(i)$ to vehicles in its transmission range. Each vehicle is responsible for updating its blockchain regularly in order to avoid forks and discrepancies.

1) Distribution of CC: CC is used as a monetary incentive in the proposed solution. It is divided into two parts with ratio $w_1 : w_2$, where w_1 and w_2 are corresponding weights

Fig. 3: Simulation map of University of Sussex campus.

Algorithm 2 CC Distribution and Reputation Update

while $i \leq N_{HOP}^{max} + 1$ **do**
  if $i == 0$ **then**
    if $N_{END} \geq N_{END}^{min}$ **then**
      $Broadcast(Endorsed\ message)$
      $Block[w_1 CC, R_{\overline{END}(i)}, Q_{RLY(i)}]$ //Add block
      $i = i + 1$
    else if $time\ elapsed \geq t_{\overline{END}}^{max}$ **then**
      $Block[R_{ORG}, CC]$
      if $N_{END} > 0$ **then**
        $Block[R_{\overline{END}(i)}]$
      end if
    end if
  else if $i \leq N_{HOP}^{max}$ & $time\ elapsed < t_{max}$ **then**
    $Broadcast(Endorsed\ message)$
    $Block[R_{\overline{END}(i)}, R_{RLY(i-1)}, Q_{RLY(i)}]$
    $i = i + 1$
  else
    $Block[R_{\overline{END}(i)}, R_{RLY(i-1)}, Q_{RLY(i)}, w_2 CC]$
  end if
end while

to divide the share of CC among $\overline{END}(0)$ and $RLY(i), i = 1, 2, ..., N_{HOP}$, respectively. The profit, P_j, of a vehicle j is

$$P_j = \begin{cases} \frac{w_1 CC}{N_{END}^{min}}, & \text{if } j \,\epsilon\, \overline{END}(0), \\ \frac{w_2 CC}{N_{HOP}}, & \text{if } j = RLY(i). \end{cases} \tag{8}$$

As shown in Algorithm 2, transactions for $\overline{END}(i)$ are committed as a block at each hop by $RLY(i)$ and transactions for $RLY(i)$, $RLY(i+1)$,..., $RLY(N_{HOP}^{max})$ are committed as a block at last hop by $RLY(N_{HOP}^{max} + 1)$. If N_{END}^{min} $endorsements$ are not obtained for a $transaction\ proposal$ until t_{END}^{max}, it is considered as fake and CC is transferred to CA as a penalty to ORG. This penalty is recorded as a transaction by $RLY(i)$ which is selected by ORG itself while originating a $transaction\ proposal$. No share of CC is paid to $\overline{END}(0)$ if a fake $transaction\ proposal$ is endorsed.

2) Reputation Update: Reputation is affected by the behaviour of vehicles. Honest behaviour of $\overline{END}(i)$ and $RLY(i)$ is recognised as successful action performed during message dissemination. Malicious behaviour refers to a fake $transaction\ proposal$ initiated by ORG or endorsed by $\overline{END}(i)$ and an endorsed message not forwarded by a selfish $RLY(i)$. If a vehicle j behaves honestly, its reputation is updated as $R_j = R_j + \beta$, where β is the reputation reward. If it behaves maliciously, then $R_j = R_j - \gamma$, where γ is the reputation penalty.

III. Game Theory Analysis

We apply game theory to analyse the performance of proposed system against collusion of $RLY(i)$, $RLY(i+1)$,..,$RLY(n)$, where n is the number of colluding relay nodes. The message dissemination game is described as follows:

a) Players: This game has N_{END}^{min} number of $\overline{END}(0)$ and one $RLY(i)$ at each hop i. The number of hops is N_{HOP}.

b) Actions: At each hop i, every player j has two possible actions, honest (H) and selfish (S). If player j follows the protocol, it is honest. If it does not take part in message dissemination, it is selfish. We denote the action of player j by ACT_j. Then ACT_j is either H or S.

c) Utilities: Without colluding with its neighbours, the utility, U_j, at i^{th} hop is

$$U_j = \begin{cases} P_j - TC, & \text{if } ACT_j = H, \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

Proposition 1. *In the message dissemination game, playing honest is the best response action of all players if* $TC < P_j$.

Proof: According to (9), if $TC > P_j$, U_j will be negative. In that case, the best response action of players is playing selfishly. Therefore, TC must be set such that the action results in positive U_j for all players, so that they are motivated to play honestly. □

Theorem 1. *CC distribution mechanism is resistant against the collusion of* $RLY(i)$, $RLY(i+1)$,...,$RLY(n)$ if $TC \geq 0$.

Proof: Lets consider the case with one conspired $RLY(i)$. Suppose $CG = \{RLY(i), RLY(i+1)\}$ is a collusion group. CG forges a bogus path with one additional hop, i.e., $ORG \rightarrow RLY(i) \rightarrow RLY(i+1)$ instead of the most appropriate path, i.e. $ORG \rightarrow RLY'(i+1)$. Let p be the probability with which $RLY(i)$ encounters and $p \,\epsilon\, [0, 1]$, it has a probability of p^2 to encounter both ORG and $RLY(i+1)$. The expected utility sum of CG, $E(U_{CG})$, is

$$E(U_{CG}) = p^2(U_{RLY(i)} + U_{RLY(i+1)}) + (1-p^2)(U_{RLY'(i+1)}). \tag{10}$$

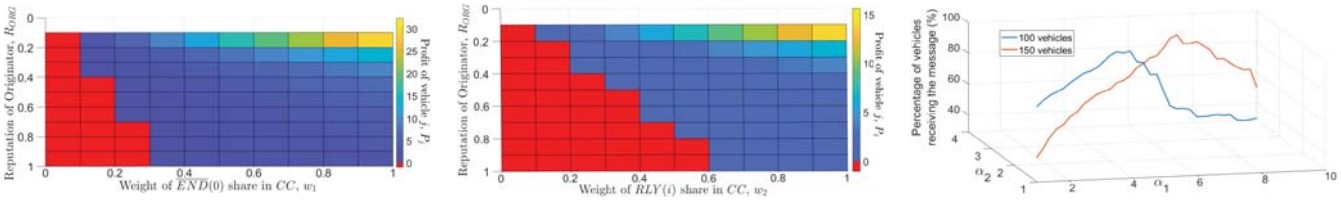
Since $N_{HOP} = 2$ in collusion and $N_{HOP'} = 1$ otherwise,

$$E(U_{CG}) = p^2\Big(w_2 CC - 2TC\Big) + (1-p^2)(w_2 CC - TC), \tag{11}$$

or,

$$E(U_{CG}) = w_2 CC - TC - p^2 TC. \tag{12}$$

To avoid collusion of relay nodes, we want $E(U_{CG}) \leq U_{RLY'(i+1)}$, i.e., $w_2 CC - TC - p^2 TC \leq w_2 CC - TC$, which leads to $p^2 TC \geq 0$. By generalizing cases when $n > 2$, we can derive the collusion resistant condition, i.e., $p^n TC \geq 0$. Hence, for any $p \,\epsilon\, [0, 1]$, we prove that the mechanism is relay node collusion resistant if $TC \geq 0$. □



(a) Profit of $\overline{END}(0)$, P_j, $\forall\ j\,\epsilon\,\overline{END}(0)$. (b) Profit of $RLY(i)$, P_j, $\forall\ j = RLY(i)$. (c) Effect of α_1 and α_2 on message delivery.

Fig. 4: Setting of simulation parameters.

TABLE II: Simulation Parameters

Parameters	Values	Parameters	Values
Simulation Time	1000 s	Protocol	IEEE 802.11p
No. of vehicles	[50, 200]	Encryption	SHA-256
Area	12.5 km x 12.5 km	Average speed	40 km/hr
t_{END}^{max}, t_{max}	600 ms, 4 s	t_W	10 s
N_{END}^{min}, N_{HOP}^{max}	3, 6	CC	$10/R_{ORG}$
w_1, w_2	0.35, 0.65	β, γ	0.1, 0.2
TC	1	R_j	[0,1]
R_T	0.5	α_1	[1, 10]
α_2	[1, 4]	d_{HOP}^{min}	100m

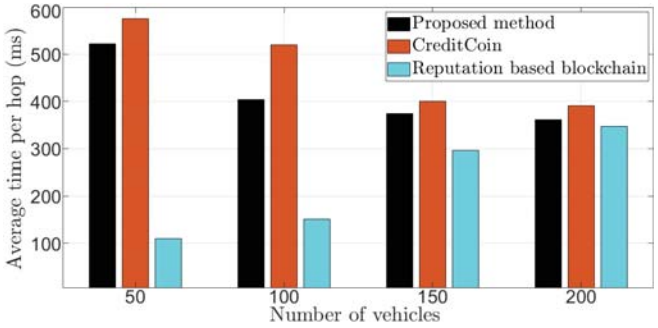


Fig. 5: Average time per hop with respect to No. of vehicles.

IV. Simulation Results and Discussion

In this section, we analyse the performance of our proposed solution through extensive simulations using OMNeT++ integrated with SUMO (Simulation of Urban Mobility) which can be seen in Fig. 3. The simulation parameters in Table II are set so that Proposition 1 holds true regardless of the value of CC. In our simulations, we have arbitrarily set $CC = 10/R_{ORG}$. Higher R_{ORG} leads to lower amount of CC, thereby resulting in less P_j. However, it must be ensured that the message dissemination protocol results in profit gain in credit wallets of all, despite of deduction of TC. As shown in Fig. 4(a) and Fig. 4(b), $w_1 > 0.3$ and $w_2 > 0.6$ would always result in positive P_j, irrespective of the value R_{ORG}. Therefore, in order to ensure profit gain, we have set $w_1 = 0.35$ and $w_2 = 0.65$ in simulation. Fig. 4(c) shows percentage of vehicles which received messages within a specified period of time, t_{max}, with respect to α_1 and α_2, under different traffic densities. It shows that the selection of α_1 and α_2 depends upon the number of vehicles and affects $RLY(i)$ selection defined in (2). Thus in our simulation, we choose α_1 and α_2 such that they achieve maximum reception rate.

Fig. 5 shows the average time consumption per hop over 100 simulation runs. The reputation based blockchain [11], [12], only allows vehicles with reputation above a certain threshold to disseminate messages. CreditCoin is a witness-based blockchain, in which ORG requires a certain number of witnesses for message authentication [14]. The latency is increased in this approach because it relies on ORG to wait for witnesses before generating an announcement packet. On the contrary, our proposed solution saves an average of 56 ms (or 11%) of the time consumed as it does not include waiting time of ORG. Fig. 5 also shows that the reputation based method takes the least time to complete one hop as it does not involve waiting time for $endorsements$. However, the average time increases with raising number of vehicles because more time is needed to access reputation of a vehicle. In the proposed approach, the average time decreases with raising number of vehicles. To support a completely decentralised message dissemination solution, each vehicle in the reputation based blockchain has the whole copy of blockchain in order to find reputation of any vehicle whenever needed. Therefore, the storage complexity of reputation based blockchain is $O(B)$, where B is the total number of blocks in a blockchain [18]. On the other hand, our proposed solution does not require each vehicle to store the whole copy of blockchain for $RLY(i)$ selection and message dissemination and therefore its storage complexity is $O(1)$. In terms of communication, the conventional PBFT requires at least N_{END}^{min} signatures both during $endorsement$ and committing a block, therefore resulting in an overall communication complexity of $O((N_{END}^{min})^2)$ [9], whereas our proposed solution requires N_{END}^{min} signatures only during $endorsement$ and hence results in communication complexity of $O(N_{END}^{min})$.

With 50 vehicles, our solution consumes 522 ms for completing one consensus. Given the average speed of vehicle is 40 km/hr, it only incurs a moving distance of approximately 5 m, which can be easily mitigated within 300 m coverage of typical IEEE 802.11p radio. The worst case scenario is presented in Fig. 6, where low vehicle density, i.e. 50 and 100, cannot successfully complete a consensus at the speed beyond 100 km/hr and 110 km/hr, respectively, within the time limit of 600 ms which is used as a delay threshold for message authentication in VANETs [19]. However, in practice, it is unlikely that a vehicle can travel with more than 100 km/hr

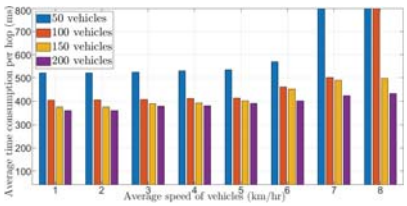


Fig. 6: Time consumption per hop with respect to speed.

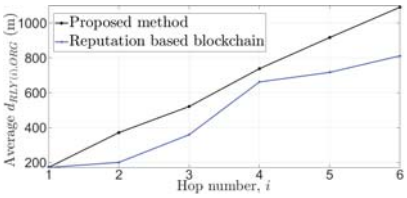


Fig. 7: Average distance of $RLY(i)$ from ORG.

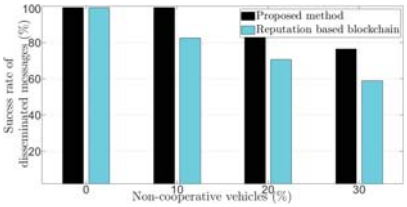


Fig. 8: Success rate in presence of non-cooperative vehicles.

on a road affected by an incident or traffic jam. Overall, it shows that the proposed approach is suitable for VANETs, particularly for high density traffic with lower speed.

Fig. 7 shows average distance of $RLY(i)$ from ORG with respect to number of hops over 100 simulation runs. An appropriate $RLY(i)$ cannot be selected on the basis of its reputation only. Therefore, we have proposed the selection process as a part of consensus protocol. It shows that the proposed solution can be used to propagate message to a longer distance in less number of hops as compared to the reputation based approach, because a reputation based blockchain does not consider position of $RLY(i)$, transmission range and other channel parameters during consensus. The average difference between two approaches is 148 m.

Fig. 8 shows average success rate of message dissemination over 100 simulation runs in presence of non-cooperative vehicles. We have considered non-cooperative vehicles as those vehicles whose reputation fall below R_T. Different to the reputation based system which does not allow such vehicles to originate $transaction\ proposals$, our consensus algorithm conducts voting based authentication. The trust among vehicles can still be maintained since a message cannot be further disseminated without getting $N_{END}^{min}\ endorsements$. Our proposed approach disseminates averagely 17% more authenticated messages than the reputation based blockchain approach in presence of non-cooperative nodes.

V. Conclusion

In this paper, we have proposed a voting based blockchain for message dissemination in VANETs. The proposed approach can save averagely 11% of time in disseminating a message as compared to other voting based methods. The integration of relay selection with consensus can improve the success rate of transmission by 17%. As a trade-off, it requires more time to generate block. However, latency difference is negligible with increasing traffic density. The economic model of integrated price and reputation-based incentive strategy makes it stronger against collusion attacks, which can be potentially used to calculate annual road tax. A vehicle which is involved in less number of incidents would have spent less credit, leaving higher balance in its credit wallet which can be redeemed into road tax.

References

[1] R. Chen, W. Jin and A. Regan, "Broadcasting safety information in vehicular networks: issues and approaches," *IEEE Netw.*, vol. 24, no. 1, pp. 20-25, Jan./Feb. 2010.

[2] T. Gazdar, A. Belghith, and H. Abutair, "An Enhanced Distributed Trust Computing Protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, Oct. 2017.

[3] Y. He, F. Yu, Z. Wei and V. Leung, "Trust management for secure cognitive radio vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 86, pp. 154-165, Apr. 2019.

[4] O. Rehman and M. Ould-Khaoua, "A hybrid relay node selection scheme for message dissemination in VANETs," *Future Gener. Comp. Sy.*, vol. 93, pp. 1-17, Apr. 2019.

[5] Z. Li and H. Shen, "Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 8, pp. 1287-1303, Aug. 2012.

[6] A. Yanez, S. Cespedes, and J. Rubio-Loyola, "CaSSaM: Context-aware System for Safety Messages Dissemination in VANETs," *Proc. of IEEE COLCOM*, Colombia, May 2018.

[7] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf.

[8] A. Baliga, "Understanding blockchain consensus models," *Pune, India, Persistent Syst. Ltd.*, White Paper, Apr. 2017.

[9] B. Choi, J.-Y. Sohn, D.-J. Han, and J. Moon, "Scalable Network-Coded PBFT Consensus Algorithm," *Proc. of IEEE International Symposium on Information Theory,* France, Jul. 2019.

[10] F. Muratov, A. Lebedev, N. Iushkevich, B. Nasrulin, and M. Takemiya, "YAC: BFT Consensus Algorithm for Blockchain," *arXiv preprint arXiv:1809.00554*, Sep. 2018.

[11] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906-2920, Mar. 2019.

[12] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based Decentralized Trust Management in Vehicular Networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495-1505, Apr. 2019.

[13] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," *Proc. of IEEE 28th Annual International Symposium on PIMRC*, Canada, Oct. 2017.

[14] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "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, Jan 2018.

[15] C. Iza-Paredes, A. Mezher, M. A. Igartua, and J. Forné, "Game-Theoretical Design of an Adaptive Distributed Dissemination Protocol for VANETs," *Sensors*, vol. 18, no. 1, Jan. 2018.

[16] S. Chatterjee and S. Das, "Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network," *Inform. Sciences*, vol. 295, pp. 67-90, Feb. 2015.

[17] C. Bettstetter, H. Hartenstein, and X. Pérez-Costa, "Stochastic Properties of the Random Waypoint Mobility Model," *Wirel. Netw.*, vol. 10, no. 5, pp. 555-567, Sep. 2004.

[18] A. Ahmad, M. Saad, L. Njilla, C. Kamhoua, M. Bassiouni, and A. Mohaisen, "BlockTrail: A Scalable Multichain Solution for Blockchain-Based Audit Trails," *Proc. of IEEE ICC*, China, Jul. 2019.

[19] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711-1720, Mar. 2016.