ISSN 2278-3091

Volume 9, No.4, July – August 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse368942020.pdf

https://doi.org/10.30534/ijatcse/2020/368942020

# Secured Message Delivery in Vehicular Networks Based on Blockchain and FDRO Algorithm

**H.Prabavathi[1], Dr.K.Kavitha[2]**

[1]Research Scholar, Department of CSE, Annamalai University, Chidambaram, India
prabavathih@gmail.com
[2]Associate Professor, Department of CSE, Annamalai University, Chidambaram, India
kavithacseau@gmail.com

## ABSTRACT

Vehicular networks are faster moving networks that provide intelligent transport systems to passengers with the internet and ensures comfort and safety drive. Trustworthy of the messages transmitted over the vehicular networks is threatening as false messages received by the vehicle lead to a high risk of the passengers travelling in that vehicle. Therefore, security is a major constraint in vehicular networks to ensure a safer journey of the driver and the individuals. In this paper, we suggest a security-aware routing protocol (SARP) for vehicular networks based on blockchain technology. This SARP protocol speedily updates the status of abandoned vehicles in the OpenFlow switch layer and also reduces the communication and computation overhead by relieving dependency on the authority for trusted identity verification. In the proposed work, vehicles send and receive cryptographically encrypted messages created using the blockchain technology with a privacy-preserving algorithm. The authentication of the vehicles in VANET is given by the OpenFlow switch which applies falsy detect rule optimization algorithm (FDRO) to find the malicious vehicles which try to create false messages. The implementation of this SARP protocol and FDRO algorithm are performed in the Network Simulator tool (NS3) and the efficiency and performance of the algorithm have been validated using the NS3 simulation environment.

**Key words:** Blockchain, FDRO, SARP, Secured message delivery, Vehicular networks

## 1. INTRODUCTION

Vehicular networks are a type of ad-hoc network that are self-organized networks, this allows vehicles to form a network on the road. VANET may be created very soon without a central authority is an advantage. Drivers receive warning messages in the dashboard to quickly react to the condition that avoids accidents. In case of an accident, the information transmitted between the vehicles helps the traffic policeman to quickly reach the scene of the accident [1]. Vehicles receive navigation messages to select alternate routes. In these conditions, the reliability of the information and validity of the message should be ensured. Vehicles in VANETs can share navigation information without driver's intervention as VANET provide cooperative driving applications [2]. The self-organizing networks consist of Vehicle to Infrastructure node (V2I) and Vehicle to Vehicle communication (V2V) within the range of 500m with 5.9 GHz band and bandwidth of 75 MHz. The IEEE 802.11p model supports the wireless devices to communicate between speedy vehicles and the roadside units (RSUs). These standards support many applications, information communicated should be authenticated and anonymity of the source must be preserved [3].

The cloud servers in the VANET provide an excellent hurdle for the attackers but during single node failure, the entire situations become critical as this cloud server setup is centralized [4]. The falsy messages from the malicious node or alteration in original message dominate the driver behaviour and cause safety problems to the passengers while on road [5]. In our view, without high safety measures on security, the high-level intelligence transport system will fail. To improve the ITS (intelligent transport system) and also to maintain the profitability, effectiveness, and stability, there is a need to develop a secured decentralized framework to realize the smooth flow of data in ITS, thus building a high trusted ITS.

Blockchain technology gives an effective way of securing and storing data in the decentralized environment, it reduces the third party or middleman. The blockchain architecture is cryptographically secured and it applies consensus for authentication [6]. The distributed public ledger is maintained, a copy of which is maintained by all the nodes and the encrypted blocks are chained in chronological order. Each node has its private key and shared public key [7]. A block contains its own hash value, the signature of the block, nonce, and timestamp. Every message is encrypted by the sender with its public key of the receiver; the receiver decrypts the message with its private key. The advantages of the blockchain model are trust, collective maintenance, chronological order, decentralization, programmability, and security [8]. Blockchain is the perfect solution for the issues in ITS.

Most of the researchers in VANETs focused on security aspects but they focused on authentication and privacy, they are lacked in focusing on the malicious behavior of the trusted node in the network. All the nodes in the network are not trusted as a malicious attacker may enter into the network and can communicate falsy messages to divert nodes on the road [9]. In our proposed work, vehicles are registered with the RSUs with (ECC) elliptic curve cryptography private key and public key. Blockchain technology is used to maintain authentication, security and a decentralized environment. The malicious node which creates false messages in the network is investigated using the FDRO algorithm which is applied in the OpenFlow switch layer. The other sections of this paper are the section 2 gives the related works, section 3 depicts the system model, section 4 covers the proposed falsy detect rule optimization algorithm, section 5 gives the implementation and results, and section 6 gives the conclusion.

## 2. RELATED WORKS

Many security algorithms have been proposed to solve the security issues in VANET. Most recent works for those challenges are summarized in this section. Lingyun Zhu et al [10] presented a symmetric masquerade security scheme (SMSS) to achieve security requirements with low system overhead. The model is provided with symmetric encryption to maintain the consistency of messages. However, this protocol only focuses on vehicle to vehicle communication only. Shiang-Feng et al [11] proposed an improved identity based batch verification scheme that provides security and privacy needed by vehicle. The scheme provides security in random oracle model. Small number of pairing is taken to prove the security, but the throughput and delay is not taken into consideration. Chun-Ta Li et at [12] used a light weight authenticated key establishment scheme with privacy preservation to secure the communication between vehicle to vehicle and vehicle to roadside unit in a vehicular networks. This scheme allows vehicles to interact with road side units securely using blind signature techniques. Privacy preservation is the major consideration in this scheme which considers the computational cost for comparison. Kiho Lim et al [13] suggested a protocol that ensures fast distribution of authentic messages in VANETs. RSUs energy is well utilized in this phenomenon for message dissemination and to verify the secrecy of the user vehicle. Redundant messages, message integrity are the major considerations in this scheme. ChakerAbdelazizKerrache et al [14] proposed an adaptive detection threshold. This gives solution to the unmanned ariel vehicles to face the detection process. The model proposed here evaluates the honest of the vehicles during the whole process. However throughput is not considered here for comparison. Romaincoussement et al [15] proposed a protocol in VANET to detect the malicious node with decision support mechanism. The protocol alerts the neighbouring vehicle when an attack occurs. Vehicles are grouped and headed by cluster heads.

## 3. SYSTEM MODEL

The blockchain-based architecture ensures secure message transfer in vehicles in the decentralized environment. This blockchain reduces the contribution of certificate authority in VANET. Private blockchain gives complete access of ledger to all the nodes [20]. The figure 1 shows the complete architecture of the system, Security aware routing protocol (SARP) in which the vehicles on road is authenticated by the RSU to ensure non-repudiations in the network. The trusted vehicles are only provided with group key to receive and send messages in the network. The RMS system is provided to maintain the blockchain with necessary data without any duplicates. All the functions like handover, retransmission in the VANET are controlled by the SDN layer.

### 3.1 Vehicle registration

This architecture focuses on reducing the dependency on centralized authority in vehicular networks. The vehicle initialization is the first step to proceed. The RSU builds the system with ECC based public and private key pairs. The ECC parameters are (G, a, b, p, n, and h) for the curve C in the field F. Integer p defines the field, here the field is integer modulo p, a and b are the parameters which define the curve, G is the base point generated by the base point generator which is the random initial coordinate position in the curve. A cyclic group Zp is generated with the order of G n, and h is the cofactor of the curve C given by h=E(Z/pZ)/n, E(Z/pZ) determines the number of coordinate points in the curve.
During registration of vehicle the parameters and the hash function are stored in on-board unit fixed permanent in the vehicle. The following model gives the security aware routing protocols that authenticates the vehicle based on blockchain verification and securely transfer the message using cryptographic ECC algorithm.

The blockchain network between RSU, resource management unit (RMU) and SDN Controller is initialized by the RSU with its public key. The public key is used to address and verify each other for transactions. When entering into the range of a RSU, it generates a public private key pair ($P_{ki}$and $Pr_{ki}$) to the new vehicle and it assigns a $RID_i$ (random ID). The RSU digitally sign the $RID_i$and forms the transaction block in the ledger, the block here is noted as β. The input of the transaction is verified by the RSU’s public key hash address. The output of the transaction is verified by the hash value generated with the RSU and with the hash value generated with the OBU. This matching provides authenticity of the vehicle. The RSU returns the assigned ID, public-private key pair ECC($P_{ki}$, $Pr_{ki}$), Hash $pointer_B$, transaction ID $TID_{Bi}$, to the OBU. The figure 2 gives the detailed description about the vehicle registration.

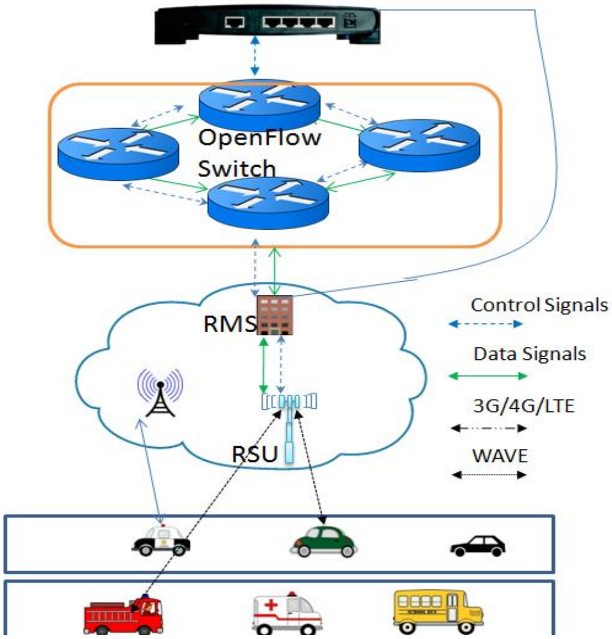


**Figure 1:** System architecture

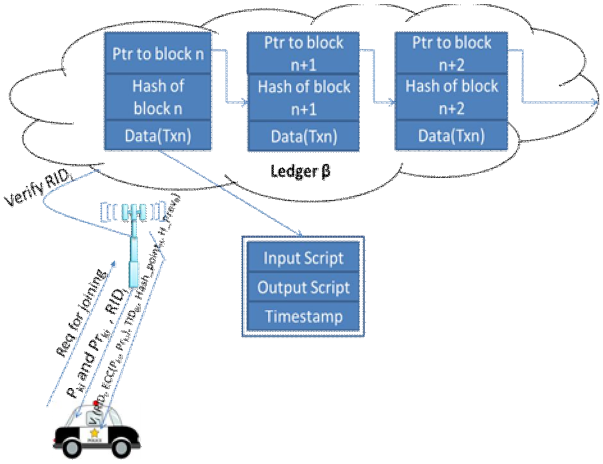


**Figure 2:** Vehicle registration

### 3.2 Identity based authentication

While on road the OBU is active and it tries to become part of the group of vehicles in the range of RSU [23]. It identifies that it has all the parameters of the RSUs and tries to connect with the nearest RSU. The OBU originates a message consists of Hash_point$_B$, TID$_{Bi}$, encrypted with the RSU's public key $P_{RSU}$, RSU receives the message and decrypts with its private key $Pr_{RSU}$, it also gets the pointer to the block, corresponding ledger entry with the message.

**Table 1: Vehicle Registration in RSU**

| | |
|---|---|
| 1. | $V_i$→ RSU (Vehicle enters into RSU range) |
| 2. | RSU * RID (Verify RID) |
| 3. | RSU # T (input→(RID$_i$))<br>(output→H(RSU) with H(OBU))<br>If matches provide authenticity |
| 4. | RSU # β (ledger updation) |
| 5. | RSU → $V_i$ (RID$_i$, ECC($P_{ki}$, $Pr_{ki}$), TID$_{Bi}$, Hash_point$_H$, H_Prev$_B$) |

Now, RSU enquires with the blockchain ledger with the RID$_i$ as the index, if RID$_i$ index found in the ledger with the transactions, then RSU confirms the OBU with a challenge message *'n'* encrypted with its private key and wait for the response, if the OBU decrypts the message with the public key of the RSU and it generates the response with the next positive integer *'n+1'*, now OBU is authenticated with the RSU. OBU receives a group key from the RSU and OBU will post and receive messages in group of vehicles and it also receives emergency messages from the RSU in the network, this will continue with all the RSUs when the vehicle is moving on the road.

**Table 2:** Identity authentication

| | |
|---|---|
| 1. | OBU$_i$*M$_i$ : OBU generates message M |
| 2. | OBU$_i$→RSU$_i$: M is transmitted to RSU |
| 3. | RSU$_i$*M : RSU decrypts M, |
| 4. | RSU$_i$*β : RSU verifies RID$_i$ |
| 5.<br>6. | RSU*T :RSU verifies Transactions<br>If false, do not authenticate the vehicle |
| 7. | RSU→OBU : RSU transmits n |
| 8. | OBU →RSU : OBU transmits n+1 |
| 9. | RSU → OBU : group key |

## 4. FALSY DETECT RULE OPTIMIZATION ALGORITHM

The control (manager) and data planes are separated in the software-defined network, so the network devices are not having forwarding rules and they do drop the packets as per the instructions given by the controller. In this paper, a module is suggested in which the SDN controller act as an arbitrator which monitors the data flow in the network. The behaviors of malicious nodes are classified as data centric malicious node behavior and node centric malicious node behavior. In node centric detection malicious nodes are identified based upon the security credentials and digital signatures. In data centric detection the data disseminated by the network nodes are analyzed and compared. The SDN controller maintains the network by providing identity to the nodes and monitoring the misbehavior nodes. Network nodes are provided with two lists of nodes. One is a white list which has trusted nodes provided by the RSU, next list has the blacklisted malicious nodes that are provided by the SDN controller.

### 4.1 Algorithm description

Three basic concepts are there to find the misbehavior node using the falsy detect rule optimization algorithm (FDRO).

i. A vehicle is considered as malicious node if it drops packets or duplicate packets while it routes packets in transmission.
ii. For a vehicle, if its distrust value $D_v$ exceeds the threshold value $T_v$ then it is identified as a malicious node.
iii. Normal vehicles motivate good transmission by forwarding the message.

### 4.2 FDRO Algorithm

The source node is the message creator and destination is the receiver of the message with the intermediate nodes as relay nodes. When a node $N_r$ is identified as a relay node then nodes that are adjacent to $N_r$ will act as a monitor node for $N_r$. The number of packets received by the node $N_r$ is assigned as parameter a, and the number of packets dropped monitor duplicated by the node $N_r$ which is monitored by the monitor node $N_m$ is assigned as parameter b. After a particular time $T_p$, if the node $N_r$ does not send the packets or added more packets or send multiple copies, these behaviors are monitored by $N_m$ and identified as abnormal behavior. This malicious behavior of $N_r$ is accounted and node $N_m$ increases the parameter b by 1. The distrust value $D_v$ of node $N_r$ is updated. The updated $D_v$ is broadcasted to all the adjacent nodes and they updated the list accordingly. Nodes with lower $D_v$ are placed in the white list, if the $D_v$ exceeds the threshold value $T_v$ then the ID of the vehicle is reported to the SDN controller, then the controller informs the ID as a malicious vehicle to all the nodes connected in the network.

In the proposed FDRO algorithm, for a node $N_r$ in the network, the monitor node is identified based on the weight (Wt), length (Lt), and distrust value ($D_v$). The nodes with the decision parameter $D_p$ lesser than $T_v$is selected as the monitor node compared to all the adjacent nodes in the region r(RSU, $N_r$). This method optimizes monitor node selection and improves network performance. The nodes under the region r are considered for monitor node selection. The region r is the intersection area of RSU and vehicular node $N_r$.

$$\text{Area}\ (N_r) = T_r(N_r)\text{-}T_p(S_{max}– S_{min})$$

Where,
$T_r(N_r)$ – transaction range of $N_r$
$T_p$ – latency time in vehicles
$S_{max}$ – Maximum vehicle speed
$S_{min}$ - Minimum speed of the vehicle
Monitor nodes are selected based on the following parameters.

Weight (Wt) – refers to the number of nodes that are verified by the monitor node. Node with less weight will have a greater chance to be a monitor node.

Distrust Value ($D_v$) – A vehicle with less $D_v$increases its trust value. Abnormal behaviour increases the $D_v$ and it is compared with the threshold value $T_v$. Nodes with less $D_v$ will remain in the white list and the nodes with $D_v$ greater than the $T_v$ will move to the blacklist.

Length (Lt) – if the distance between monitor node and relay node is minimum, then the relay node will be monitored for more time. The decision parameter $D_p$ for all the nodes are computed based on the above three parameters.

$$D_p\text{=Wf1 * Wt + Wf2 * }D_v\text{+ Wf3 * Lt}$$

Wf1, Wf2, and Wf3 are the weight factors for the above parameters respectively.

$$\text{Wf1 + Wf2 + Wf3 = 1}$$

Limited nodes are selected for monitoring purposes to maintain network traffic and to detect the malicious node in a better way. To select some nodes as monitors for the node $N_r$, then their $D_v$ is compared with the threshold value $T_v$. nodes with lesser $D_v$ are selected as $N_m$ for node $N_r$. All nodes know the $D_v$ of all its neighbor nodes. When the monitor node $N_m$ finds some misbehavior in node $N_r$, it reports this to the RSU, then RSU verifies the $D_v$of $N_m$ to make sure that it is lower or equal to the $D_v$of $N_r$.

### 4.3 Proposed FDRO Algorithm

Step 1: Vehicle $N_r$ joins into the network
Step 2: Compute the parameters weight, length and distrust value for the node in the region of $N_r$
Step 3: Decision parameter $D_p$is calculated as
$D_p$=Wf1 * Wt + Wf2 * $D_v$+ Wf3 * Lt
Where Wf1 + Wf2 + Wf3 = 1
Step 4: Search for the nodes with less threshold value
($D_p$<$T_v$)
Step 5: Select the nodes from step 4 as monitor nodes for $N_r$
Step 6: Monitor nodes ($N_m$) monitors the behavior of $N_r$
Step 7: if $N_m$ founds abnormal behavior of $N_r$ then it reports the RSU.Goto Step 8 ;elsegoto Step 6
Step 8: RSU calculates the distrust value ($D_v$) of $N_r$
Step 9: if $D_v$is less than or equal to detection threshold $T_v$, then update the white list and goto Step 6; else goto Step 10
Step 10: Broadcast warning message to all nodes.
Step 11: Update the ID of $N_r$ in blacklist
Step 12: Malicious nodes are isolated from the network.

## 5. IMPLEMENTATION AND RESULTS

To implement the functionality of the proposed algorithm we have used NS-3.26 simulator setting on the operating system ubuntu version 16.04. The simulation parameters are given in Table 3. The vehicles are simulated here as dynamic nodes, for testing the number of the nodes (vehicles) range from 1-50, with speed as 15-25 m/s. The parameters associated with packet delivery ratio, delay and throughput are considered to calculate the performance of protocol. PDR is given as ratio of packets that are arrived at the destination with the packets initiated at the source.

**Table 3:** Simulation Parameters

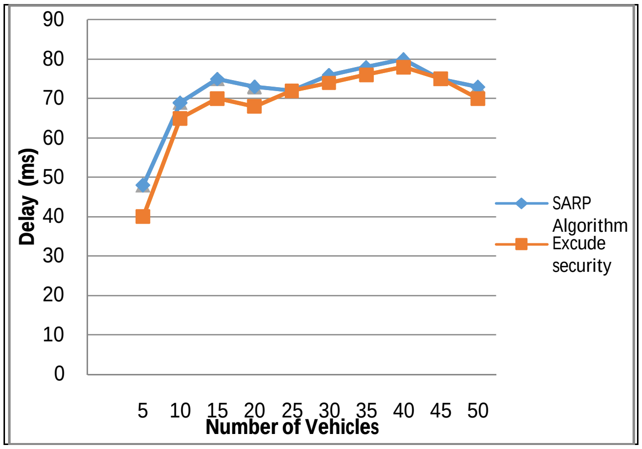
| Simulation Parameter | Value |
|---|---|
| Simulation time | 2000s |
| Number of nodes | 100 |
| Packet size | 100-200 bytes |
| MAC layer | IEEE 1609.4 |
| Frequency | 5.9 GHz |
| PHY layer | IEEE 802.11P |
| Data Rate | 18Mbps |
| Traffic Pattern | Constant bit rate |
| Number of malicious nodes | 5, 9, 15, 25, 40 |

Delay is the period of time between the origination of packets at source with the time of delivery of packets at the destination. Throughput is the amount of data transferred in one unit of time that is the successful transmission of packets is accountable. Figure below shows the performance evaluation of SARP protocol in which the protocol is considering with time taken for with and without additional security.

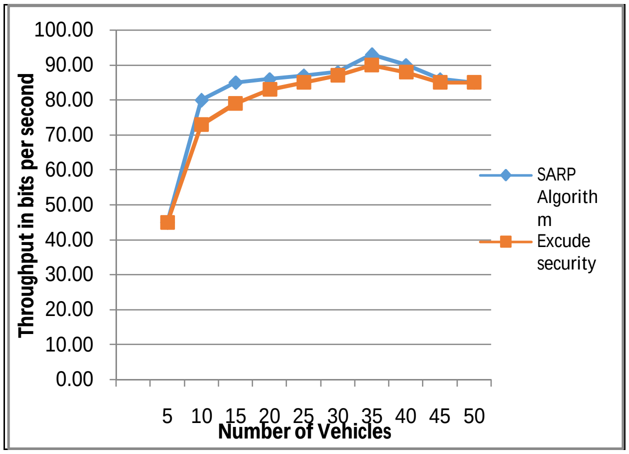
End-to-end delay between the OBUs and RSUs is the important factor as it depicts the additional overhead of security mechanisms increases the delay in the performance of RSU. The delay is depicted in the figure 3.a below. Here the computation time of RSU for decrypting the received message is only considered. It is noted that the delay is around 48ms for up to 5 nodes, and increases linearly with the nodes from 5 to 15.

Throughput between the RSUs and OBUs are shown with the security mechanisms and compared with without additional security. The below figure 3.b shows the measured throughput with and without additional security.The graph 3.c shows the comparison of successful delivery of packets before and after application of SARP protocol. The proposed protocol shows a linear rise between 90% and 95% with 40 vehicles, and starts to drop from 40 to 50 vehicles.

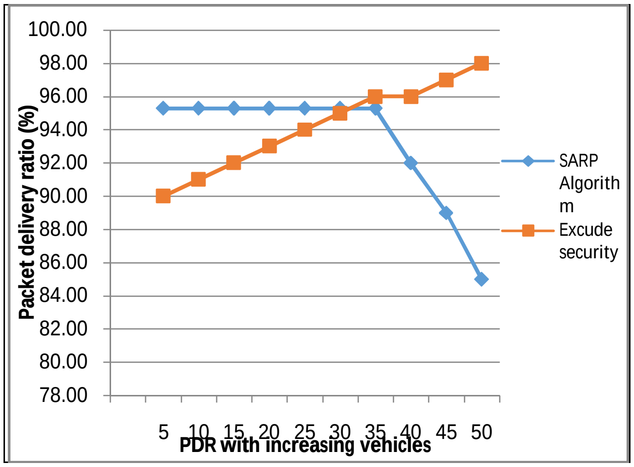
The performance of our FDRO algorithm is compared with the DMN algorithm with the performance metrics as E2E delay, throughput and packet delivery ratio. Figures 4 (a-c) given below shows the comparative analysis of our FDRO algorithm with DMV algorithm. From the resultant graphs it is observed that our proposed FDRO algorithm improves the performance of vehicular network in finding the malicious nodes by employing monitor nodes.



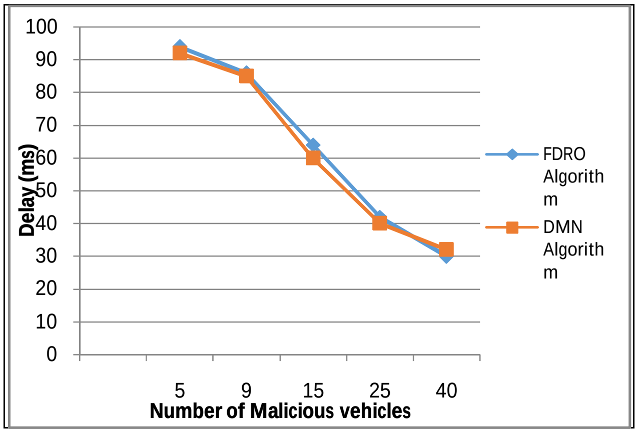
(a) End to end delay with SARP Algorithm



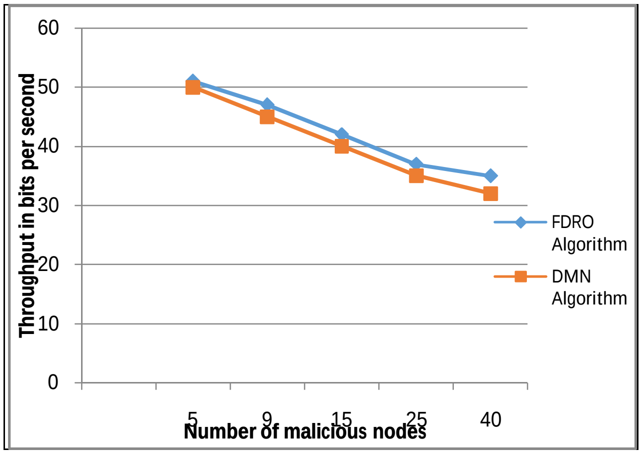
(b) Throughput with SARP Algorithm



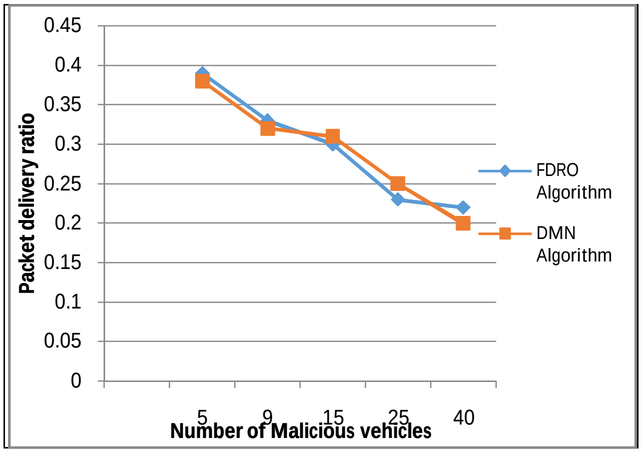
(c) Packet delivery ratio with SARP Algorithm,
**Figure 3 (a-c):** Performance metrics – SARP



(a) End to end delay using FDRO Algorithm



(b) Throughput using FDRO algorithm



(b) Packet delivery ratio using FDRO algorithm (c)

**Figure 4. (a-c):** Performance metrics – FDRO

## 6. CONCLUSION

The authentication of vehicles in VANET is effectively stated in this paper. The SARP algorithm not only authenticates the vehicles but also secures the identity of the vehicles. The need for centralized authority is reduced by the use of the SDN controller. SDN controller provides security and also it eliminates the malicious nodes in the network. The blockchain technology keeps the transactions between the nodes in the secure ledger. The FDRO algorithm is a novel approach that effectively eliminates the malicious nodes by monitoring the behavior of the nodes by employing monitor nodes also the performance of the VANET is improved herewith. The performance metrics of SARP are compared with the parameters without security measures and the performance of FDRO is compared with the DMN algorithm. Both the SARP and FDRO algorithms are effectively applied VANET in improving security.

## REFERENCES

1. Al-kahtani, MS (2012, December). **Survey on security attacks in Vehicular Ad hoc Networks (VANETs).***In 2012 International Conference on Signal Processing and Communication Systems* (pp. 1-9). IEEE. Gold Coast, QLD, Australia.

2. Isaac JT, Zeadally S, Camara JS, (2010). **Security attacks and solution for Vehicular ad hoc Networks**, *IET communication*; 4(7), 894-903.

3.Martinez.F.J, Fogue.M, Toh.C.K, Cano.J.C, Calafate.C.T, Manzoni.P, (2013). **Computer simulations of VANETs using realistic city topologies**, *Wireless Personal Communications*, 69(2), 639–663.

4. Mishra B, Nayak P, Behera S, Jena D, (2011, February). **Security in vehicular adhoc networks: a survey**. *In 2011 International Conference on Communication, Computing and Security* (pp. 590-595). ACM. Odisha, India.

5. Bißmeyer N, Njeukam J, Petit J, Bayarou KM, (2012, June). **Central Misbehavior Evaluation for VANETs based on Mobility Data Plausibility**. *In 2012 Proceedings of the International Workshop on Central Misbehavior Evaluation for VANETs based on Mobility Data Plausibility Vehicular inter-networking, Systems, and Applicatio*ns (pp.73-82). ACM, Bay Lake District, UK. https://doi.org/10.1145/2307888.2307902

6. Puthal.D, Malik.N, Mohanty.S.P, Kougianos.E and Yang.C. (2018). **The blockchain as a decentralized security framework**. *IEEE Consumer Electronics Magazine*, 7(2), 18-21.

7. Yuan.Y, and Wang.F.Y, (2016, November). **Towards Blockchain-based Intelligent Transportation Systems**. *In 2016 International Conference on Intelligent Transportation Systems* (pp.2663-2668). IEEE. Rio De Janeiro, Brazil.

8. Wang.F.Y, (2010). **Parallel control and management for intelligent transportation systems: concepts, architectures, and applications**, *IEEE Transactions on Intelligent Transportation Systems*, 11(3), 630 – 638.

9. Daeinabi A, Rahbar AG, (2013). **Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks**. *Multimedia Tools and Applications An International Journal*,66(1), 325-338.

10. Zhu.L, Chen.C, Wang.X, and Lim.A.O, (2011, March). **SMSS: Symmetric masquerade security scheme for VANETs.** In 2011 *International Symposium onAutonomous Decentralized Systems.* (pp. 617-622). IEEE. Tokyo, Japan.

11. Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and MuhmmadKhurram Khan (2017). **Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET**. *IEEE Transactions of Vehicular Technology*, 66 (4), 3235- 3248.

12. Li.C.T, Hwang.M.S and Chu.Y.P, (2008). **A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks.***Computer Communications*, 31(12), 2803-2814.

13. Lim.K, and Manivannan.D, (2016). **An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks**. *Vehicular Communications*, 4(1), 30-37. https://doi.org/10.1016/j.vehcom.2016.03.001

14. Kerrache.C.A, Lakas.A, Lagraa.N, and Bakra.E, (2017). **UAV-assisted technique for the detection of malicious**

**and selfish nodes in VANETs**. *Vehicular Communications*, 11(1), 1-11.

15. Coussement.R, Saber BAB, Biskri.I, (2013). **Decision support protocol for intrusion detection in VANETs**. *In 2013 International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications* (pp.31 – 38).ACM. Barcelona, Spain.

16. Grover J, Laxmi V, Gaur MS, (2011, December). **Misbehavior Detection Based on Ensemble Learning in VANET**. *In 2011 International Conference on Advanced Computing, Networking and Security (*pp. 602-611). Springer. Surathkal, India.

17. Harit SK, Singh G, Tyagi N, (2012, November). **Fox-Hole Model for Data-centric Misbehaviour Detection in VANETs**. *In 2012 International Conference on Computer and Communication Technology* (pp. 271-277). IEEE. Allahabad, India.

18. Huang D, Williams SA, Shere S, (2012, June) **Cheater Detection in Vehicular Networks.***In2012 International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 193-200). IEEE. Liverpool, UK.

19. Kim CH, Bae IH. A, (2012) **Misbehavior based reputation management system for VANETs**. In James J Park, Young Sikjeong et.al (ed) Embedded and Multimedia Computing and Service, Springer. pp. 441-450.

20. Deepti Rani, Nasib Singh Gill (2019, June). **Lightweight Protocols for Internet of Things: A Review.** *In International Journal of Advanced Trends in Computer Science and Engineering.*8(3), (pp. 707 – 719). https://doi.org/10.30534/ijatcse/2019/58832019

21. Rawat DB, Bista BB, Gongjun Y, Weigle MC, (2011, June). **Securing Vehicular Ad-hoc Networks Against Malicious Drivers: A Probabilistic Approach.***In 2011International Conference on Complex, Intelligent and Software Intensive Systems* (pp.146-151). IEEE. Seoul, South Korea.

22. Vulimiri A, Gupta A, Roy P, Muthaiah SN, Kherani AA, (2010, May). **Application of Secondary Information for Misbehavior Detection in VANETs**. *In 2010 International Conference on Research in Networking* (pp. 385-396). Springer. Chennai, India.

23. Prabavathi.H, Kavitha.K, Pradeep.G, (2019). **The delay and energy efficient multicasting routing protocol for vehicular networks using IWO and MOLO algorithm.** *International Journal of Innovative Technology and Exploring Engineering,* 8(12), 3048-3055. https://doi.org/10.35940/ijitee.K2469.1081219