Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

A NOVEL TWO STAGE APPROACH TO DETECT SYBIL AND DOS ATTACK IN VEHICULAR AD HOC NETWORKS

DHANANJAY YADAV
Pursuing Ph.D(Computer Science),Gujarat Technological University, Gujarat, India

NIRBHAY KUMAR CHAUBEY
Dean, Department of Computer Science, Ganpat University, Gujarat, India.
Corresponding Author

ABSTRACT
A vehicular ad hoc network is an emerging technology based on MANET which offers various services for safety and security of people on road. Vanet is helpful in providing secure and intelligent transportation services. But asvanet is dynamic in nature and topology of vehicles changes very rapidly it is also highly vulnerable to security attacks as compared to mobile ad hoc networks. One of the most threatening security attacks in vanet is Denial of Service (DoS) attack and Sybil attack. In DoS attack the attacker prohibit legitimate vehicle to use the network services by sending huge number of fake message so that network gets busy and it becomes unavailable for legitimate vehicles and in Sybil attack the attacker sends lots of fake messages in vanet to misguide other vehicles by changing its id. In this research paper we have used a two stage approach to detectthe DoS and Sybil attack in VANET. In first stage we have calculated the threshold value of number of vehicles and in second stage detected the attack by categorizing the vehicles based on number of hope count and determining and comparing the packet delivery ratio.

Index Terms – DoS, Packet Delivery ratio, Security, Vehicular Ad Hoc Networks, RSU, Sybil attack, traffic.

1.0 INTRODUCTION

A vehicular ad hoc network is one of the fastest growing areas in networking. It is derived from mobile ad hoc networks (MANET). The communication between vehicles in VANET is totally wireless that can be categorized into four types [1] as (a) vehicle to vehicle to communication, (b) Vehicle to roadside unit, (c) vehicle to broadband cloud communication and(d) in vehicle communication. Vanet architecture can be different for different regions. DSRC (Dedicated Short Range Communication) protocol is used in US. It is mainly used for vehicular communication with some set of standard protocols and standards. DSRC uses 75MHz spectrum which range from 5.850GHz to 5.925 GHz [i]. IEEE 802.11p is a standard for wireless access in vehicular communication (WAVE) which mainly focuses on PHY layer and MAC sub layer. IEEE 1609, which is based on IEEE802.11p, represents standards for middle layer protocol stack.

The vanet architecture includes Road Side Unit (RSU), On Board Unit (OBU) and Application Unit (AU)[1]. RSU are placed alongside road which are responsible for providing internet services in vanet. They also perform the task of informing other vehicles about traffic condition in the network. One board unit helps in providing ve-

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

hicle to vehicle communication in the network. Application Unit and On Board unit both are equipped with vehicles. AU is internal in vehicle and monitors drivers fatigue or drowsiness etc. The architecture of vanetis as shown in figure (1).

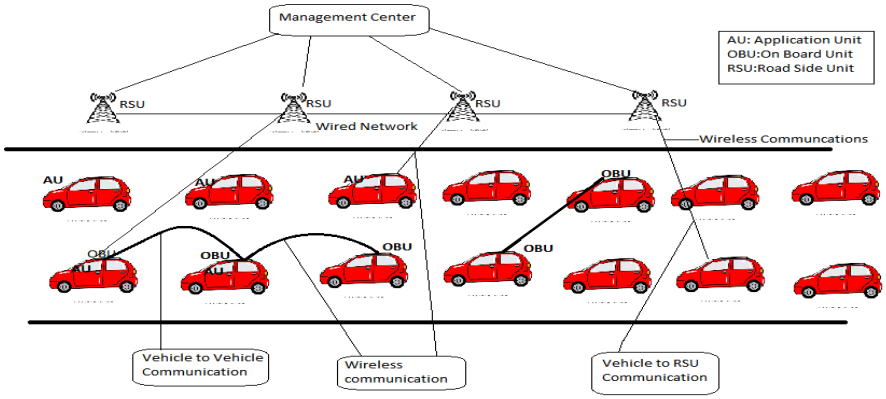

Fig.1 Architecture of VANET.

RSU are connected through wired and wireless media which are approximate 1000 meters apart. The communication in vanet is performed through wireless media and due to very high speed, topology changes very frequently. So security is always a major concern in vanet. The various security attacks in vanet are explained in [2]. One of the most perilous attacks in vanet is a Denial of service attack. This attack cost to life of people, so it is considered as one of the most dangerous attack in vanet. In denial of service attack, the attacker sends lots of fake messages in such a way that RSU becomes too busy to manage those messages and it becomes unavailable for other vehicles in the network for communication. The attacker uses a large number of compromised nodes to generate the attack [3]. As the network becomes unavailable for vehicle this can cause the serious hazardous situations in the network.There are two main ways from which attackers can make attacks [4].

Case-1: The attacker targets a vehicle and repeatedly and continuously sends lots of messages so that the victim becomes busy and not able to communicate with other vehicles in the network.

Case-2: the attacker targets the infrastructure (RSU) of the VANET. When node tries to communicate with RSU, it is found to be overloaded. The architecture of DoS attack is as given below.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

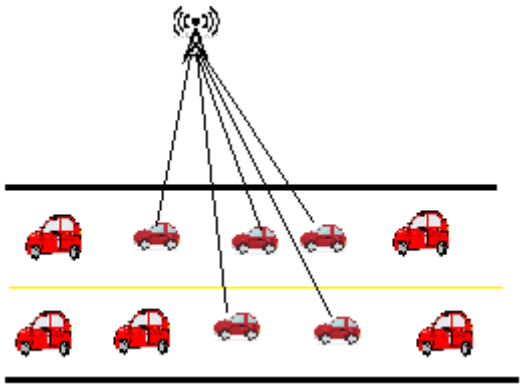

Fig.2 Architecture of DoS attack

The above figure (2) shows the architecture of Dos attack in vanet. Multiple vehicles with different id send lots of fake messages to RSU to make it unavailable for other legitimate vehicles in the network.

Sybil attack is an attack in which the attacker sends multiple messages in the vanet by frequently changing its id and makes an illusion of the presence of multiple vehicles in the network. Due to this, RSU announces wrong information of heavy traffic on the road and other legitimate vehicles divert their route due to this wrong information and illusion created by the attacker. Figure (3) shows the architecture of the Sybil attack in VANET.

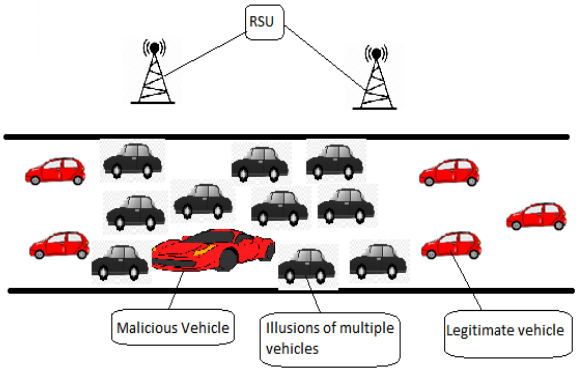

Fig.3 Architecture of Sybil attack

The early detection of these attacks can minimize the hazardous event and save the lives of people in the network. In this research paper, we have detected and predicted these attacks. Our algorithm is based on two approaches. In the first approach we have predicted the traffic flow in the network at a given instance of time and in the next approach compared the received packets and PDR with threshold value.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

2.0 LITERATURE BACKGROUND

In paper [5] the authors use the reCAPTCHA controller mechanism to detect the DDos attack. They have first calculated the frequency of packets in the detection window and then find the covariance and entropy to detect the attack. If entropy is greater than the threshold they applied the reCAPTCHA algorithm and detected the attack.

In paper[3], the authors suggest that the attack can be done by synchronizing the RSU frame with the attacker frame to collide so that RSU can not make announcements. The attack was mitigated by randomizing the RSU frame and increasing the contention window.

In the paper [7] authors developed a p secure algorithm. Vehicles information like position and speed is stored. They have assigned the maximum limit to RSU as 20. If any number of packets reached to threshold the packets drop. If speed is less or more then it is also considered as malicious.

Authors[8] classify the packets in safety and non-safety message. Preprocessed the packets based on features like time, source, TTL, payload, etc to detect the attack. The rules are generated based on average payload, an average number of packets, and average hop count.

There [9] approach is useful for V2V communication.OBU stores packet information for 10 seconds and forwards the packet count to the comparator. The comparator compares the packet count in that time duration if it exceeds the threshold value, considered malicious.

The detection algorithm[10] is based on bandwidth consumption. The bandwidth consumption in a normal situation is considered as threshold and compared to detect the attack. Every vehicle sends the reports of packets processed to the controller. The controller keeps records of the number of packets and flow rule generated and if it exceeds the threshold the vehicle is considered a victim.

Authors in [11] use the K means algorithm to detect the attack. They collect information like P, S, and K for each IP where P stands for power spectral density, S stands for skewness, and k stands for kurtosis. Send this information to Master RSU. K Means algorithm is applied to make clusters of normal and abnormal vehicles.

The authors have detected the Sybil attack in vanet based on the Received Signal Strength Indication [12]. This algorithm is totally based on signal strength hence results vary at peak time and non-peak time of traffic.

Authors in [13]consider that two or more vehicles can’t have same driving pattern for some longer time and use K nearest neighbour algorithm for detection while[14] uses the K means algorithm. These algorithms also create unnecessary network overhead because they have to maintain a driving pattern of each and every vehicle and also

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

there are some scenarios like highways where some vehicles maintain their pattern for some longer duration.

The authors in[15] use timestamps to detect the attack. RSU verifies the certificate of vehicles and assigns a timestamp value to each vehicle. The certificate is provided by registering authority. This technique is costly due to the requirement of registering authority and also the network is always in a busy state for generating and verifying timestamp value for each vehicle.

In research papers [16] and [17] the authors rely on resource testing and their result shows that with attack the PDR decreases, But as mobility is very high in vanet hence resource testing becomes inadequate.

These research algorithms are based on determining the number of packets sent by the attacker node. The authors apply their algorithm to calculate the threshold value of the number of packets sent by a legitimate vehicle in a normal situation and based on that they predicted the attack as if the number of packets exceeds the threshold value they have considered this as an attack.

Attack Model:

In DDoS attack, an attacker can send multiple packets by frequently changing its id and with different positions. The attacker vehicles synchronize themselves in such a way that they will not cross the threshold value and still they are able to make an attack. Hence attacker can easily create an attack without crossing the threshold value and in this case, it becomes impossible for algorithms for early detection of this attack. The below figure (4) shows the attack created by attacker vehicles without crossing the threshold limit.

We consider that RSU has a maximum capacity of 500 packets to manage. So an alarm is set that if any vehicle sends packets more than 400 then that vehicle is removed from the network and in this way attack cannot be performed. But if the attacker uses compromised nodes and sends packets synchronously with the maximum limit of 100 packets, still they are able to create an attack as more than five compromised vehicles are able to make the network unavailable for other legitimate vehicles in the network. As the attack is performed by multiple vehicles with different ids, hence it becomes very difficult to detect the attack.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

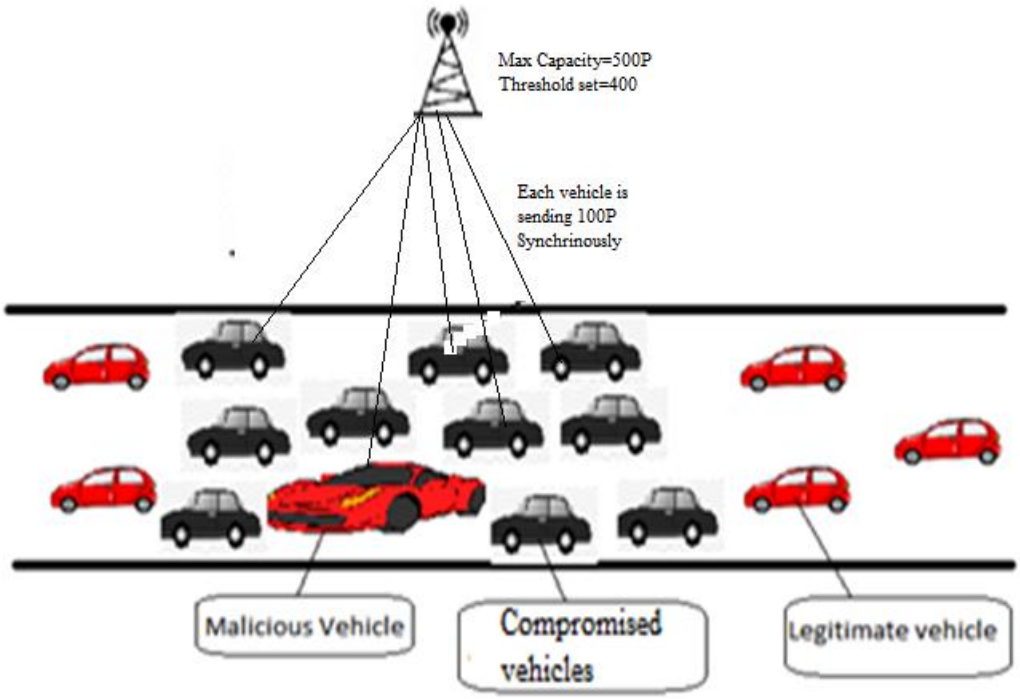

Fig.4 Attack model(DDoS).

The Sybil attack model is given in figure (3). In both attacks, the attacker uses fake ids and sends lots of fake messages in the network to create an attack. Our algorithm is suitable for the detection of both types of attack as we first predict the traffic on road at a particular time based on the previous history and determine the threshold value of a number of vehicles on road at a particular time. And if the total number of vehicles on road crosses this threshold value then we apply the next approach to determine whether it is an attack or its real traffic.

3. PROPOSED APPROACH

The proposed approach follows two-step procedures. In the first step, we apply the poison distribution algorithm to detect the attack and in the second approach we have identified the attacker vehicle by calculating the number of hope counts for vehicles who are sending the frequent messages, and after that RSU sends the confirmation message to all vehicles and calculated the packet delivery ratio. If PDR is low then it is an attack and the node is removed from the network else it is concluded that there is no such attack.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

The algorithm is given below.

Step-1: If (max_nodes)>=Threshold_V

Send nodes in suspect mode check frequency of packets

Step-2 if(received_packets<= Threshold_P)

Print("No DDoS attack" }

Step-3: Else

Categorize nodes with same hope count and position.

Step-4: Send broadcast message to these nodes to check the PDR

Step-5: if (low_Pdr)

Then it is an attack

else Randomly suspend nodes for few milli seconds

End if

4.0 SIMULATION AND RESULT

The Poisson distribution algorithm is a useful technique for determining number of vehicles on road at a particular time [18]. The probability of vehicle count using Poisson distribution can be given as

$$P(x) = (e^{-\mu}) (\mu^{x}) / x!$$

We first generate the traffic scenario on road by using SUMO (Simulation of Urban Mobility). The parameters used to generate the traffic scenario using SUMO are shown in Table-1.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

Table-1 (Simulation parameter)

Parameters	Values
Simulator	SUMO
Vehicle Type	Car, bus, truck
Max_Speed	35 km/h
Number of attempts	05
Duration	15 minutes

After simulation of road traffic with SUMO, we found that the probability of passing the 45 vehicles on road is maximum and 60 vehicles are the minimum at a particular moment of time. Hence we have taken 45 as the threshold value of the number of vehicles.

Phase-2

We have taken 45 as the threshold value [19]. If the number of vehicles crosses this threshold value then RSU first sends a confirmation message in the network and categorizes the vehicles based on the number of hop counts and position and after that checks PDR. As in research papers [16] and [17] author's results show that PDR decreases after the result. Our result also shows that at the time of attack PDR decreases due to fake IDs and non-receiving of messages. The below figure (5) shows that in a normal situation with ideal infrastructure there is no packet drop. But as the congestion increases the network has a high packet drop. PDR can be calculated as packet Delivery ratio (PDR) = Received packets/Total packets sent

As in normal and ideal conditions, the packet delivery ratio is very high. Our algorithm shows that in a normal and ideal situation all packets get delivered as shown in the below figure.

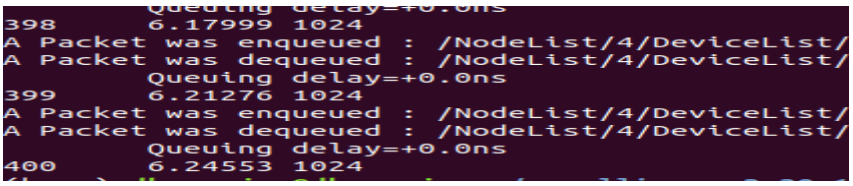

Fig.5 All packets delivered in idealsituation

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

However, as congestion increases PDR decreases very rapidly. If RSU finds very low PDR comparison to normal situation then it detected as attack.

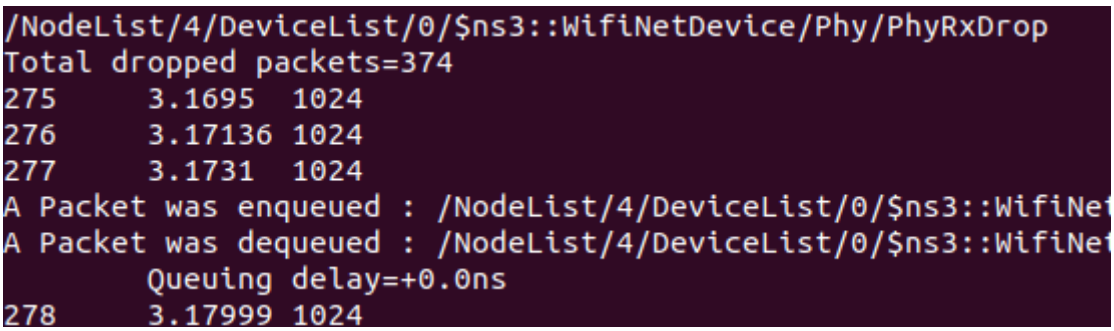

Fig.6 Most packets dropped after attack

The above figure (6) shows that 374 packets dropped out of 400 which decrease packet delivery ratio.

5. CONCLUSION

In this research, we proposed a new algorithm that is able to detect Sybil and Dos attacks both. The attack is detected without violating the privacy issues of vehicles in the network. Central authority and vehicle certification are also not required to detect attacks. This approach does not make the network busy in storing, updating, and sharing the vehicle's information. Hence this approach is simple and also does not create extra congestion in network for processes like storage, sharing, and identification of vehicle information. Our algorithm is novel compared to other research as it is able to detect DoS and Sybil attacks both.

References

[1] Chaubey, N., & Yadav, D. (2020). A Taxonomy of Sybil Attacks in Vehicular Ad-Hoc Network (VANET).

[2] M. N. Mejri, J. Ben-Othman, and M. Hamdi, 2014, “Survey on VANET security challenges and possible cryptographic solutions,” *Veh. Commun*.

[3] S. Biswas, J. Mišić and V. Mišić, "DDoS attack on WAVE-enabled VANET through synchronization," *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 1079-1084, doi: 10.1109/GLOCOM.2012.6503256.

[4] D. Rampaul, R. K. Patial, and D. Kumar, “Detection of DoS Attack in VANETs,” *Indian J. Sci. Technol.*, vol. 9(47), no. December 2016, pp. 1–6.

[5] M. Poongodi, V. Vijayakumar, and F. Al-turjman, “Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics,” *IEEE Access*, vol. 7, pp. 158481–158491, 2019.

[6] M. Shabbir, M. A. Khan, U. S. Khan and N. A. Saqib, "Detection and Prevention of Distributed Denial of Service Attacks in VANETs," *2016 International Conference on Computational Sci-*

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/3VJB7

ence and Computational Intelligence (CSCI), 2016, pp. 970-974, doi: 10.1109/CSCI.2016.0186.

[7] Reza Fatohi,YaserEbazadeh,MohammadSayyarGeshlag, A New Approach for Improvement Security against DoS Attacks in Vehicular Ad-hoc Network, 2016, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 7, pp-10-16.

[8] Barath Kumar, Shiva Kumar, An efficient way to prevent DoS attack in vanet, 2021, Journal of Emerging Technologies and Innovative Research (JETIR), volume-8, Issue-5, pp-g632-g650.

[9] S. RoselinMary, M. Maheshwari and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)",*2013 International Conference on Information Communication and Embedded Systems (ICICES)*, 2013, pp. 237-240, doi: 10.1109/ICICES.2013.6508250.

[10] Arunmozhi, S. &Venkataramani, Y. (2011). DDoS Attack and Defense Scheme in Wireless Ad hoc Networks. International Journal of Network Security & Its Applications. 3. 10.5121/ijnsa.2011.3312.

[11] MahabaleshwarKabbur, V. Arul Kumar, Detection and Prevention of DoS Attacks in VANET with RSU's Cooperative Message Temporal Signature, 2019, International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-2,pp-6371-6377.

[12] Y. Yao *et al.*, "Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI," *IEEE Trans. Mob. Comput.*, vol. 18, no. 2, pp. 362–375, 2019.

[13] P. Gu, R. Khatoun, Y. Begriche, and A. Serhrouchni, "K-Nearest Neighbours classification based Sybil attack detection in Vehicular networks," in *Proceedings of the 2017 3rd Conference on Mobile and Secure Services, MOBISECSERV 2017*, 2017.

[14] D. Shipra and R. Kashyap, "DETECTING SYBIL ATTACK USING HYBRID FUZZY K-MEANS ALGORITHM IN WSN," vol. 5, no. 2, pp. 1560–1565, 2017.

[15] T. Zaidi, "Timestamp Based Detection of Sybil Attack in VANET," *Int. J. Netw. Secur.*, vol. 22, no. February, pp. 397–408, 2020.

[16] E. P. Arora, E. P. Singh, N. Dhillon, M. T. S. R. I. E. T, and C. Science, "An Efficient Detection and Prevention of Sybil Attack by using Different Parameters in VANET," *Int. Res. J. Eng. Technol.*, vol. 7, no. 10, pp. 683–688, 2020.

[17] S. K. V and R. B. D. R, "Sybil Attack Detection in Vehicular Ad-hoc Networks using Direct Trust Calculation," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 10, pp. 67–73, 2020.

[18] T. Mathew, "Vehicle Arrival Models: Count," in NPTEL Transportation System Engineering, IIT Bombay, 2014 Accessed on :Nov 2020.[Online] Available:https://nptel.ac.in/content/storage2/courses/105101008/downloads/cete_13.pdf.

[19] Nirbhay Kumar haubey, Dhananjay Yadav, Detection of Sybil attack in vehicular ad hoc networks by analyzing network performance, *Int. J. Electr. Comput. Eng.*, vol. 12, no. 2, pp-1703-1710, DOI: 10.11591/ijece.v12i2