

Detection of Sybil attack in vehicular ad hoc networks by analyzing network performance

Nirbhay Kumar Chaubey¹, Dhananjay Yadav²

¹Department of Computer Science, GanpatUniversity, Mehsana, Gujarat, India

²Department of Computer Science, Gujarat Technological University, Ahmedabad, India

Article Info

Article history:

Received Apr 18, 2021

Revised Sep 18, 2021

Accepted Oct 11, 2021

Keywords:

Intrusion detection

Packet delivery ratio

Security

Sybil attack

Vehicular ad hoc networks

ABSTRACT

Vehicular ad hoc network (VANET) is an emerging technology which can be very helpful for providing safety and security as well as for intelligent transportation services. But due to wireless communication of vehicles and high mobility it has certain security issues which cost the safety and security of people on the road. One of the major security concerns is the Sybil attack in which the attacker creates dummy identities to gain high influence in the network that causes delay in some services and fake voting in the network to misguide others. The early detection of this attack can prevent people from being misguided by the attacker and save them from getting into any kind of trap. In this research paper, Sybil attack is detected by first applying the Poisson distribution algorithm to predict the traffic on the road and in the second approach, analysis of the network performance for packet delivery ratio (PDR) is performed in malign and benign environment. The simulation result shows that PDR decreases in presence of fake vehicles in the network. Our approach is simple and effective as it does not require high computational overhead and also does not violate the privacy issues of people in the network.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Dhananjay Yadav

Department of Computer Science, Gujarat Technological University

Nigam Nagar, Chandkheda, Ahmedabad, Gujarat 382424, India

Email: yadavdhananjay1@gmail.com

1. INTRODUCTION

Vehicular ad hoc networks (VANET) are an emerging wireless communication technology for vehicles on the road. It is mainly used for the communication between vehicles on the road as a part of intelligent transportation services. VANET plays a major role in providing early warning messages, intelligent transportation services, and safe driving. People can know about traffic scenario on road in advance, can pass warning messages in case of accidents and also enjoy other internet services. VANET is becoming the primary need for providing safety of people on the road as the number of vehicles on road is increasing day by day. The communication between vehicles is performed through wireless media. As shown in Figure 1, the VANET architecture includes road side unit (RSU), application unit (AU), and on-board unit (OBU). RSU is placed alongside the road which provides infrastructure communication for vehicles. AU is like PDA which helps in accessing the internet and is also used with OBU to provide vehicle-to-vehicle (V2V) communication. AU and OBU are equipped with vehicles, RSU connected with each other through wired and wireless media. The communication between vehicles is performed through wireless media using dedicated short-range communication (DSRC) protocol identified as IEEE802.11P [1].

Figure 1 shows the architecture of VANET. Each vehicle is equipped with AU and OBU. OBU provides vehicle to vehicle and vehicle to RSU communication. RSU's are equipped alongside the road

which has a communication range of approximately 1,000 meters. Each RSU connects with another RSU, and it helps in weather forecasting and informs other vehicles about traffic situations in the network. The communication in VANET is performed through wireless media so due to high speed and frequent topology change of vehicles security is always a major concern in VANET. The various security threats like black hole attack, bogus information attack and denial of service attack. In the paper, Mejri *et al.* [2] one of the major security attacks is Sybil attack in which a vehicle impersonates its identity to multiple vehicles and succeeds to convince roadside unit that there is high traffic on the road. The architecture of the Sybil attack is shown in Figure 2 where in the malicious vehicle creates illusion of presence of multiple vehicles in the network by changing its id or by changing its position [3].

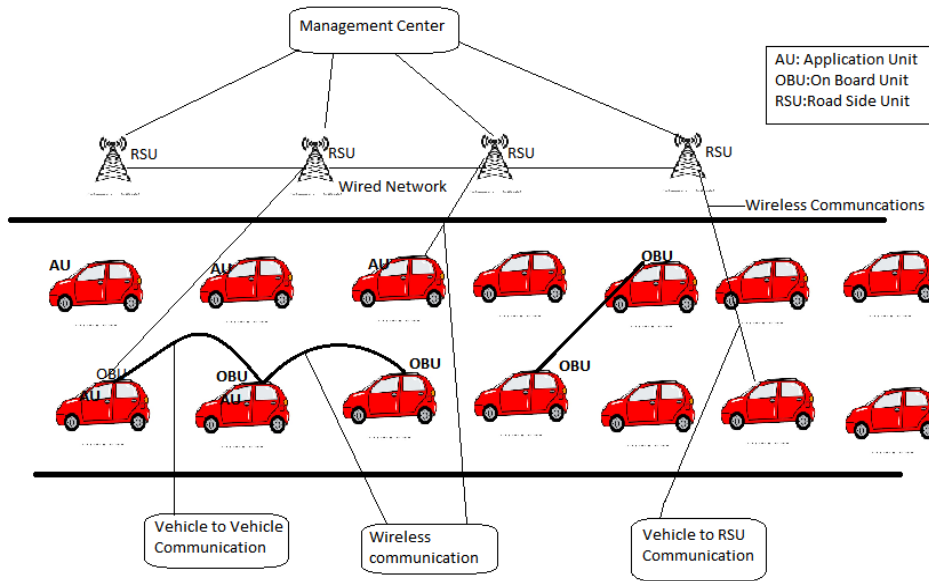


Figure 1. VANET architecture

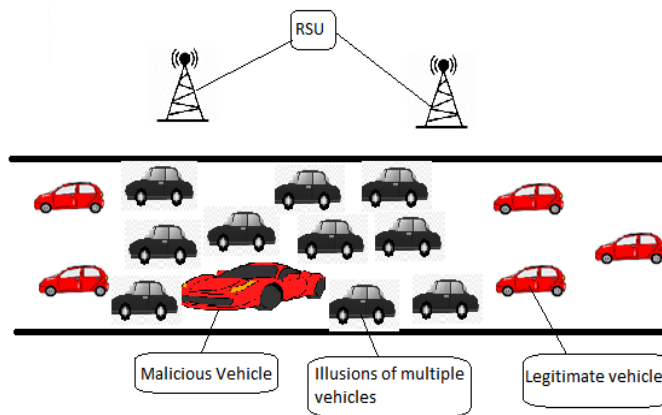


Figure 2. Sybil attack

In VANET, RSU periodically determines the traffic scenario on the road by receiving the polling responses from vehicles in the network and informs other vehicles about the current traffic situation [4]. The attacker by creating the illusion of heavy traffic forces RSU to send fallacious messages about traffic situations to the legitimate vehicles. Hence, the legitimate vehicles are bound to divert their route with the intention of malicious vehicles, making the route clear for the attacker. The attacker can now inject attacks like bogus information attack, masquerading attack and denial of service (DOS) attack [5]. This attack is the most dangerous attack in VANET as it costs safety and security of people on the road.

The Sybil attack can be performed at network layer or at the application layer. At network layer, the attack can be performed by frequent change of internet protocol (IP) addresses where, as at application layer, attack is performed by changing the identity [6]. The attacker can send multiple polling responses by changing its id or position and creates an illusion of the heavy traffic in the network. The RSU after getting large numbers of responses from different ids assumes that there is high traffic in the network and starts informing upcoming vehicles about heavy traffic on the road. Now the upcoming vehicle starts changing its route and is caught in a trap created by the attacker [7].

In this work, we have detected the Sybil attack by first predicting the number of vehicles on the road and then measuring the network performance by calculating the packet delivery ratio (PDR) in the network. PDR depends upon many factors such as transmission power, the actual physical phenomena, and topology change due to the high speed of vehicles. RSU is always fixed alongside the road making its transmission power and physical phenomena fixed so it gives less impact on the calculation of PDR. We have taken the constant vehicle speed for our simulation with the assumption that vehicles also follow some constant speed on highways and in rural areas.

In vehicle-to-vehicle communication PDR calculation is affected more because both are in motion but in RSU to vehicle communication speed has very less impact as RSU is stationary and it can send packets to all vehicles in its range. To determine the probability of the number of vehicles passing through the road within certain duration of time, we have used the Poisson distribution algorithm. When RSU finds a number of vehicles greater than the probable number of vehicles then it sends confirmation messages in the network and calculates the packet delivery ratio. Tarapiah *et al.* [8] suggested that ad hoc on-demand distance vector routing (AODV) routing protocol gave better performance results and also proved that with an increasing number of vehicles the PDR increases. In our simulation setup, we have used the AODV routing protocol and results show that with increase of number of vehicle PDR increases but in case of attack PDR decreases. The cause of decrease in PDR is the presence of large number of fake vehicles as they can't receive packets at same time. The rest of the paper is organized as follows: in section 2 related work is presented. Section 3 includes the algorithm, method and simulation parameters used for detection of Sybil attack. The experimental evaluation has been discussed in section 4 followed by conclusion in section 5.

2. RELATED WORK

The related research work to detect Sybil attack can be classified as encryption and cryptography, received signal strength-based indication (RSSI), resource testing, data mining and speed and position verification-based approaches. Table 1 gives a brief description of these approaches. In cryptography approach, only the authorized vehicle can send the encrypted messages in networks and the receiver first verifies the authenticity of the vehicle by some signature verification. Only after verification, the vehicles are able to send or receive messages [5]. Panchal *et al.* [9] propose the RSU based identification. Kamal *et al.* [10] proposed a session key-based certification method to detect the Sybil attack.

RSSI is a measurement of power present in received radio signals. Singh *et al.* [11] use the signal strength to detect the Sybil attack in VANET. Yao *et al.* [12] proposes an algorithm to detect Sybil attack without the use of RSU and base station. Dutta *et al.* [13] use data clustering of vehicles to detect the Sybil attack in VANET. Their idea is based on the fact that two vehicles can't be in the same cluster for a longer duration. But this approach is not good enough for highways. In Gu *et al.* [14] consider that two or more vehicles can't have the same driving pattern for some longer time and use K nearest neighbor algorithm for detection while in [15] uses K-means algorithm.

Some Intrusion detection algorithms have been developed to detect attacks in vehicular ad hoc networks using machine learning. These detection algorithms are classified as signature based and anomaly based [16]. Liang *et al.* [17] used a feature extraction and classifier method to detect the attack. A hybrid data driven model is proposed in [18]. Bovenzi *et al.* [19] intrusion detection algorithm is developed to detect attacks in IoT systems. Speed and position verification of vehicles are also used to detect Sybil attack. In Ayaida *et al.* [20] use a macroscopic traffic model to detect the attack. They found the difference between the probable speed of vehicles and measured speed and if there is a deviation in both then they considered it as an attack. Saggi *et al.* [21] is also based on certification and speed of vehicles in the network. Hamdan *et al.* [22] use a combination of two algorithms for detection. Privacy-preserving detection of abuses of pseudonyms (P2DAP) algorithm is used when speed is low, otherwise they use footprint algorithms. Baza *et al.* [23] verified the position of vehicles to detect the attack.

Resource testing is the first approach applied by J. Douceur to detect the Sybil attack in the point to point (P2P) network. In this approach, they tested resources by sending requests and accepting replies from each node. But it is difficult in VANET as malicious nodes can reply with multiple fake IDs. Newsome *et al.* [24] claimed that the above method is not suitable in wireless sensor networks as all replies converging to verifier will result in network congestion in that part, also there is time boundation for accepting replies. Newsome

proposes radio resource testing, registration, and position verification for detecting attacks in sensor networks. Yan *et al.* [25] claimed that radio resource testing proposed by [25] is not valid in VANET as nodes can attain multiple channels, registration is also not valid as nodes can attain multiple identities and position verification relies on outside infrastructure as well as maintaining the record of each vehicle which increases congestion and cost. In Piro *et al.* [26] uses vehicles medium access control (MAC) and IP addresses to detect the attack. The attacker can use multiple devices to beat this method. Moreover, privacy is a major issue with this method as MAC and IP addresses are tracked and recorded. In Zaidi *et al.* [27] uses a timestamp to detect the attack. RSU assigns each vehicle a timestamp after verifying its certificate. The certificate is provided by registering authority. These increases cost due to the requirement of registering authority. Also, the network remains always busy in generating and verifying timestamp value for each vehicle.

Table 1. Different approaches used to detect Sybil attack

Approach	Methods used	Problem associated with approach.
Encryption/Decryption	Signature verification for each vehicle. Certification of vehicles. Need of central authority.	Increased network congestion due to certification of each vehicle. Costly due to need of central authority.
RSSI	Determine and identify signal strength.	Variation in signal strength at peak hours or passing through tunnels.
Data mining	Clustering. K nearest neighbour. K means.	Storage requirement for each vehicle and its neighbours increases computation cost.
IDS design	Machine learning	Security concern in data analytics process. Augmentation of vehicular data do not address well
Speed and position based	Measure the speed of vehicles. Verify position of each vehicle and its neighbour.	Measuring speed of each vehicle and its neighbours increases computation cost and congestion in network. Sharing position in network creates privacy issues.
Resource testing	Verification of node based on reply message. Sharing mac and IP addresses.	Increased network congestion problem.

In [8], [28] shows that with increase of number of vehicles the PDR increases. Arora *et al.* [29] claimed that with increase of number of vehicles PDR increases but in case of attack with increase of number of vehicles PDR decreases. Their approach to detect attack is based on resource testing in which they rely on vehicles' reply to responses. Yan *et al.* [25] claimed that resource testing is inadequate in vehicular ad hoc networks, also in this approach each node is required to be certified by RSU using a public private key pair. Vehicles send its ID with key to RSU to get its location timestamp but there is a chance that an attacker can get multiple location certificates by using multiple IDs for having multiple keys or some stolen keys. Also sending messages to every node and counting and verifying each reply message increases the network congestion problem.

Our research is based on some extent to resource testing as in this approach RSU sends a verification message to all nodes within range but is not dependent on taking replies from other vehicles. RSU sends the confirmation message to each vehicle and then calculates the PDR based on which it detects the attack. We first predict the total number of vehicles at a particular time and then calculate the PDR by sending messages to each vehicle through RSU and after comparing the PDR value the attack can be easily detected. We have used a very simple approach with the objective to reduce the congestion due to computational overhead in the network, detect attacks without the use of vehicle certification and registration and also without violating the privacy issues of vehicles in the network. This approach is better in the sense that it does not require certification and registration of vehicles, less congestion as it is not based on requests and replying to messages, no privacy issues as vehicles are not required to share their information like position, speed, IP, and detection algorithm needs to be executed only when the number of vehicles exceeds the threshold value. Our approach is useful to detect Sybil attack performed by both impersonating the ID and location of vehicles in the network.

3. PROPOSED WORK

In this research, the attack detection is done in two phases. In the first phase prediction of total number of vehicles passing through road at a particular time is performed by applying the Poisson distribution algorithm followed by the calculation of the packet delivery ratio in the second phase.

- Poisson distribution algorithm: Poisson distribution algorithm is used to forecast the number of vehicles passing the road at particular time. The Poisson distribution is a useful algorithm to model the count of

vehicle arrival i.e., how many vehicles can arrive at particular time duration [30]. The probability of vehicle count using Poisson distribution can be given as:

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

where μ is the flow of traffic, x is the actual number of successes at particular time and $P(x)$ is the probability that x success occurs.

- Packet delivery ratio (PDR): PDR is defined as the number of data packets successfully received by the estimations divided by the total number of data packets sent by source [31].

$$\text{Packet Delivery Ratio} = \frac{\text{Number of data packets received}}{\text{Total number of data packets sent by source}}$$

Proposed algorithm

1. Determine the threshold value of number of vehicles on road
2. Check whether the number of vehicles is greater than threshold or not
3. Check if ((veh_count>Threshold) && (Received_alert_msg)) Then
4. Sends confirmation message to vehicles in the network and determine PDR
5. If (High_PDR_Value) Then
6. Print "No Sybil Attak"
7. Else
8. Print "Sybil Attack"
9. End If
10. Check if ((veh_count>Threshold) && (No_alert_msg)) Then
11. Print "Sybil Attack"
12. Check if ((veh_count<Threshold) && (No_alert_msg)) Then
13. Print "Smooth Traffic"

3.1. Phase1 vehicle prediction

To generate real-time road traffic scenario a portable, open source and continuous traffic simulation model, simulation of urban mobility (SUMO) is used. The parameters used to generate the traffic scenario are shown in Tables 2 and 3. After obtaining the simulated result, the Poisson distribution algorithm is implemented using Python to forecast the number of vehicles. It is observed from the results that the maximum probability is found in the range 40 to 45 vehicles, and it is almost equal to zero for 60 or more vehicles. The probability distribution for vehicles in different range is as given in Table 4.

Table 2. Simulation parameter

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

Table 3. Simulated vehicles for particular time

Attempt	Duration(minutes)	Vehicle count
1	15	40
2	15	48
3	15	44
4	15	46
5	15	49

*Number of vehicles are counted for particular duration at certain time passing through road

Table 4. Probability of vehicles

Vehicle (in range)	P(x)
35-40	0.17
40-45	0.27
45-50	0.26
50-55	0.15
55-60	0.06
60-65	0.01
65-70	0.00

*P(x) shows the probability

Figures 3 and 4 displays the probability of 45 and 60 vehicles respectively passing through the road. As stated above we observed minimum probability for 60 vehicles or above. As a result, 60 is considered threshold value for detecting Sybil attack. In case when RSU encounters responses from more than 60 vehicles then it starts verifying the actual scenario of vehicles on road.

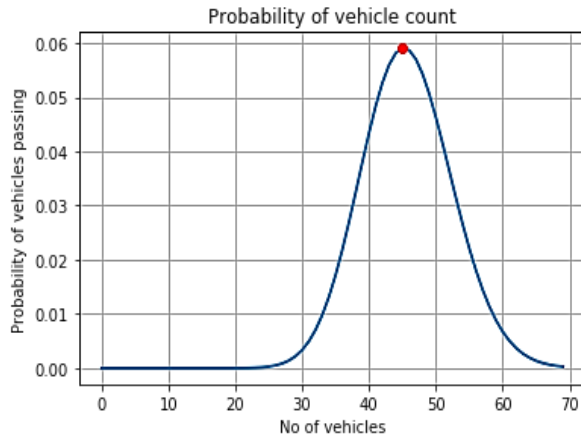


Figure 3. Shows probability of 45 vehicles

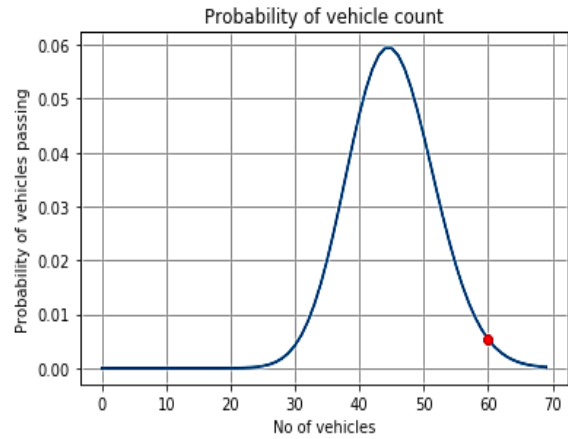


Figure 4. Shows probability of 60 vehicles

3.2. Phase 2 simulation setup

Here, in this section the simulation setup used to carry out experiment is being shown in the Table 5. The simulation is done using network simulator NS3.30. To implement this proposed work AODV routing protocol has been modified, the range of RSU is taken as 500 m and time taken for simulation is 10 seconds. Total number of vehicles is in the range 40 to 75 and PDR is calculated consequently by adding 5 more vehicles up to 75.

Table 5. Simulation parameter

Parameters	Values
Network Simulator	NS3.30
Routing Protocol	AODV
Simulation Area	300m*1500m
Transmission Power	20dbm
Vehicle Speed	20m/s
Transmission range	500
Transmission Delay	10ms
Total no of vehicles	First scenario=40 and adding by 5 up to 75 in each scenario
Mobility Model	Random Way point
IEEE 802.11p data rate	2 mbps
Packet size	200 bytes

4. RESULTS AND DISCUSSION

As discussed in previous section, when RSU predicts higher traffic responses compared to the threshold value in VANET, it is considered as an attack. It is clear from Table 3 that the possibility of number of vehicles greater than the threshold value is zero. However, in certain unwanted situations on road causes high traffic due to any mishappening, thus vehicles send alert messages in the network. RSU send broadcast messages within the range to verify actual scenario. If some incident has happened on road, then the number of vehicles increases due to obstruction and most of the vehicles should receive the confirmation message followed by high PDR value. However, PDR value decreases as in case of attack most of the vehicles have fake ids. Figure 5 shows the PDR value in benign (without attack) and malign (with attack) network scenario. The upper line shows the PDR value in a normal situation when there is no attack, and the lower line shows the PDR value with the attack. For same number of vehicles, PDR decreases in case of attack or due to presence of fake vehicles. So, by comparing the PDR value the attack detected.

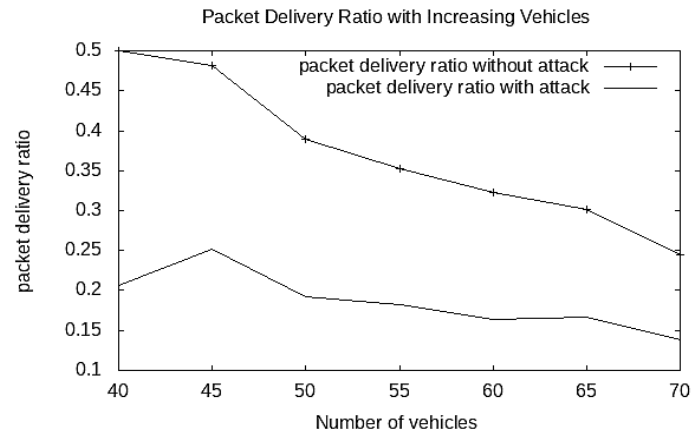


Figure 5. PDR and number of vehicles before and after attack

5. CONCLUSION

In this paper, we proposed a new approach that does not require continuous monitoring and certifications of vehicles to detect Sybil attack. The vehicles are also not required to share their position or id, so the privacy of vehicles is preserved. Our simulation result shows that the packet delivery ratio (PDR) decreases for same number of vehicles in case of attack. The PDR decreases due to the higher packet drop of non-existent vehicles as all fake ids cannot accept the confirmation message at the same time. Also, in our approach attack detection algorithm is required to execute only when there is a need i.e., when traffic crosses the threshold value. But other research that we have gone through requires continuous execution of their algorithm for storing and extracting vehicle information like id, position, and neighbours' information. which makes the network always busy for computation. Detecting attacker vehicle will be the focus of our future work.





REFERENCES

- [1] M. H. Alwan, K. N. Ramli, Y. A. Al-Jawher, A. Z. Sameen, and H. F. Mahdi, "Performance comparison between 802.11 and 802.11p for high speed vehicle in VANET," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3687–3694, Oct. 2019, doi: 10.11591/ijece.v9i5.pp3687-3694.
- [2] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, Apr. 2014, doi: 10.1016/j.vehcom.2014.05.001.
- [3] N. K. Chaubey and D. Yadav, "A taxonomy of sybil attacks in vehicular ad-hoc network (VANET)," in *IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks*, 2020, pp. 174–190.
- [4] F. Perry, K. Raboy, E. Leslie, Z. Huang, and D. Van Duren, "dedicated short range communications roadside unit specifications," National operations center of excellence. 2017, FHWA-JPO-17-589, Accessed: Dec, 2020. [Online]. Available: <https://transportationops.org/publications/dedicated-short-range-communications-roadside-unit-specifications>
- [5] M. Rahbari and M. A. Jabreil Jamali, "Efficient detection of sybil attack based on cryptography in VANET," *International Journal of Network Security & Its Applications*, vol. 3, no. 6, pp. 185–195, Nov. 2011, doi: 10.5121/ijnsa.2011.3614.
- [6] S. Pal, A. Mukhopadhyay, and P. Bhattacharya, "Defending mechanisms against Sybil attack in next generation mobile ad hoc networks," *IETE Technical Review*, vol. 25, no. 4, pp. 209–215, 2008, doi: 10.4103/0256-4602.42813.
- [7] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): A comprehensive study," *International Journal of Security and Its Applications*, vol. 10, no. 5, pp. 261–274, May 2016, doi: 10.14257/ijnsa.2016.10.5.25.
- [8] S. Tarapiah, K. Aziz, and S. Atalla, "Analysis the performance of vehicles ad hoc network," *Procedia Computer Science*, vol. 124, pp. 682–690, 2017, doi: 10.1016/j.procs.2017.12.205.
- [9] A. Panchal and D. D. Singh, "Segregation of sybil attack using neighbouring information in VANET," *International Advanced Research Journal in Science, Engineering and Technology (IARJSET)*, vol. 4, no. 6, pp. 172–180, Jun. 2017, doi: 10.17148/IARJSET.2017.4631.
- [10] R. Prakash and K. Soni, "Improved session key based certificate to detect sybil attack," *International Journal of Engineering Research and Technology (IJERT)*, vol. 3, no. 4, pp. 116–119, 2014.
- [11] K. Singh and H. Kaur, "Evaluation of proposed technique for detection of Sybil attack in VANET," *International Journal of Scientific Research in Computer Science and Engineering*, vol. 6, no. 5, pp. 10–15, Oct. 2018, doi: 10.26438/ijsrcse/v6i5.1015.
- [12] Y. Yao *et al.*, "Multi-channel based sybil attack detection in vehicular ad hoc networks using RSSI," *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 362–375, Feb. 2019, doi: 10.1109/TMC.2018.2833849.
- [13] N. Dutta and S. Chellappan, "A time-series clustering approach for sybil attack detection in vehicular ad hoc networks," *The Second International Conference on Advances in Vehicular Systems, Technologies and Applications*, 2013.
- [14] P. Gu, R. Khatoun, Y. Begriche, and A. Serhrouchni, "k-Nearest Neighbours classification based Sybil attack detection in Vehicular networks," in *2017 Third International Conference on Mobile and Secure Services (MobiSecServ)*, Feb. 2017, pp. 1–6, doi: 10.1109/MOBISECSERV.2017.7886565.
- [15] S. Diwakar and D. R. Kashyup, "Detecting sybil attack using hybrid fuzzy K-Means algorithm in WSN," *International Journal of Engineering Development and Research*, vol. 5, no. 2, pp. 1560–1565, 2017.





- [16] H. Bangui, M. Ge, and B. Buhnova, "A hybrid data-driven model for intrusion detection in VANET," *Procedia Computer Science*, vol. 184, pp. 516–523, 2021, doi: 10.1016/j.procs.2021.03.065.
- [17] J. Liang, J. Chen, Y. Zhu, and R. Yu, "A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position," *Applied Soft Computing*, vol. 75, pp. 712–727, Feb. 2019, doi: 10.1016/j.asoc.2018.12.001.
- [18] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: survey," *Procedia Computer Science*, vol. 184, pp. 877–886, 2021, doi: 10.1016/j.procs.2021.04.014.
- [19] G. Bovenzi, G. Aceto, D. Ciunzo, V. Persico, and A. Pescape, "A hierarchical hybrid intrusion detection approach in IoT scenarios," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, Dec. 2020, pp. 1–7, doi: 10.1109/GLOBECOM42002.2020.9348167.
- [20] M. Ayaida, N. Messai, S. Najeh, and K. Boris Ndjore, "A macroscopic traffic model-based approach for sybil attack detection in VANETs," *Ad Hoc Networks*, vol. 90, Jul. 2019, doi: 10.1016/j.adhoc.2019.01.010.
- [21] M. K. Saggi and R. Kaur, "Isolation of Sybil attack in VANET using neighboring information," in *2015 IEEE International Advance Computing Conference (IACC)*, Jun. 2015, pp. 46–51, doi: 10.1109/IADCC.2015.7154666.
- [22] S. Hamdan, A. Hudaib, and A. Awajan, "Detecting Sybil attacks in vehicular ad hoc networks," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 36, no. 2, pp. 69–79, Mar. 2021, doi: 10.1080/17445760.2019.1617865.
- [23] M. Baza *et al.*, "Detecting sybil attacks using proofs of work and location in VANETs," *IEEE Transactions on Dependable and Secure Computing*, 2020, Art. no. 1, doi: 10.1109/TDSC.2020.2993769.
- [24] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & Defenses," in *Proceedings of the third international symposium on Information processing in sensor networks - IPSN'04*, 2004, pp. 168–259, doi: 10.1145/984622.984660.
- [25] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, vol. 31, no. 12, pp. 2883–2897, Jul. 2008, doi: 10.1016/j.comcom.2008.01.009.
- [26] C. Piro, C. Shields, and B. N. Levine, "Detecting the sybil attack in mobile ad hoc networks," in *2006 Securecomm and Workshops*, Aug. 2006, pp. 1–11, doi: 10.1109/SECCOMW.2006.359558.
- [27] S. M. Faisal and T. Zaidi, "Timestamp based detection of sybil attack in VANET," *International Journal of Network Security*, vol. 22, no. 3, pp. 1–12, 2020, doi: 10.6633/IJNS.
- [28] D. Garg, R. S. Bali, and A. Kaur, "Performance evaluation of data delivery mechanism for cognitive radio vehicular and vehicular ad-hoc networks," *Procedia Computer Science*, vol. 57, pp. 596–605, 2015, doi: 10.1016/j.procs.2015.07.410.
- [29] E. P. Arora, E. P. Singh, and D. N. Dhillon, "An Efficient Detection and Prevention of Sybil Attack by using Different Parameters in VANET," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 10, pp. 683–688, 2020.
- [30] T. Mathew, "Vehicle arrival models: count," *NPTel Transportation System Engineering, IIT Bombay*, 2014.
- [31] H. Alani, M. Abdelhaq, and R. Alsaqour, "Dynamic routing discovery scheme for high mobility in mobile ad hoc wireless networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 3702–3714, Aug. 2020, doi: 10.11591/ijece.v10i4.pp3702-3714.

BIOGRAPHIES OF AUTHORS



Nirbhay Kumar Chaubey     working as a Dean of Computer Science, Ganpat University, Gujarat India. He received Ph.D. degree (Computer Science) from the Gujarat University, Ahmedabad, India. His research interests lie in the areas of Wireless Networks (Architecture, Protocol Design, QoS, Routing, Mobility and Security), Ad Hoc Network, Sensor Network, IoT, Cloud Computing and Cyber Physical System. He has authored four (4) books published by the Springer and IGI Global, published fifty (50) research papers in peer reviewed Scopus and web of science indexed international journals and conference proceedings, published five (5) book chapters, and contributed two (2) patents. Prof. Chaubey is a Senior Member of the IEEE, ACM, and a Life Member of Computer Society of India. He has received several awards including IEEE Outstanding Volunteer Award- Year 2015 (IEEE Region 10 Asia Pacific), Gujarat Technological University (GTU) Pedagogical Innovation Awards (PIA) -2015, IEEE Outstanding Branch Counselor Award - Year 2010 (IEEE Region 10 Asia Pacific). He can be contacted at email: nirbhay.chaubey@ganpatuniversity.ac.in.



Dhananjay Yadav pursuing     in Computer Science from Gujarat Technological University, Ahmedabad, India. He Completed MCA from FIT Faridabad in 2007 and M. Tech (C S) from Jamia Hamdard University New Delhi in 2013, qualified the UGCNET exam in 2018. He has 10+ years of academic experience. He has authored a book chapter and published three research papers. He can be contacted at email: yadavdhananjay1@gmail.com.