A Resilience Framework for Sybil Attacks on VANET with Machine Learning Based Classification

G.Athisha 1 Prof. (Dr.) S. K. Singh2
1Postdoctoral Researcher, Lincoln University College, Petaling Jaya, Selangor Darul Ehsan Malaysia
2Information Technology, Amity University Uttar Pradesh Lucknow Campus, Lucknow, Uttar Pradesh, India
Email ID: pdf.Athisha@lincoln.edu.my

Abstract

In Autonomous IoT networks, the IoT devices are equipped with artificial intelligence, edge computing, cloud computing and autonomous decision making. Applications of IoT networks include Autonomous Vehicles, Smart Cities, Industry 4.0, Precision Agriculture and Healthcare. Their distributed architecture and resource constrained devices make them vulnerable to identity – based threats and attacks. Vehicular Adhoc Networks (VANETs) are crucial for Intelligent Transportation System(ITS) and road safety. The VANETs are deployed in dynamic environments, with changing topologies, varying vehicle speeds and road conditions. The communication architecture used in VANETs are IEEE 802.11p in the PHY and MAC layers. IEEE 1609 standard is used in the upper layers to enable wireless access in Vehicular Adhoc Networks. A Sybil Attack is an attack in which a malicious device forges multiple identities to manipulate routing, trust and collaborative decision making. The effects of Sybil attack include reduced Packet Delivery Ratio, increased routing overhead, higher energy consumption, degraded network lifetime and false traffic congestion reports. Such Sybil attacks compromise safety and reliability of VANETs, since they rely on the exchange of trustworthy information. This paper focusses on the classification of Sybil attacks based on Machine Learning algorithms. The three machine learning algorithms Random Forest, K – Means clustering and Decision Tree are used for the classification of Sybil attacks and the results are compared. With effective Packet Delivery Ratio statistics, the resilience metrics such as PDR Degradation, Throughput Degradation, Packet Loss, Detection Time, Response Time and Recovery Time are calculated. Finally the Resilience Index(RI) is derived. The results show96.15% Accuracy, 98.84% Sybil detection rate, 97.89% F1-score, 50% reduction in Detection Time, 60% reduction in Response Time, Improved PDR and Throughput.

I. Introduction

Vehicular Ad Hoc Networks (VANETs) are an important component of Intelligent Transportation Systems (ITS), enabling vehicles to communicate with one another and with roadside infrastructure to exchange information such as traffic conditions, road hazards, accident warnings, and emergency messages. By supporting real-time communication, VANETs can improve road safety, traffic efficiency, and passenger convenience. However, the highly dynamic topology, wireless communication medium, decentralized architecture, and large number of mobile nodes make VANETs vulnerable to various security threats.

One of the most serious security threats in VANETs is the Sybil attack, in which a malicious vehicle creates and uses multiple false identities simultaneously or sequentially. For example, a malicious node may generate multiple false traffic congestion, accident, or road-condition messages, causing legitimate vehicles to make incorrect decisions.

Detecting Sybil attacks in VANETs is challenging because vehicles frequently change their network locations and communication partners, while attackers can generate multiple identities that appear legitimate. Traditional security mechanisms based only on cryptographic authentication may not always be sufficient, particularly when an attacker possesses valid credentials or compromises multiple identities. Therefore, intelligent detection techniques based on machine learning, behavioural analysis, mobility patterns, received signal characteristics, and communication features are increasingly being investigated.

Recent research has explored machine-learning and deep-learning approaches for identifying anomalous vehicle behaviour and distinguishing legitimate vehicles from Sybil identities. A robust

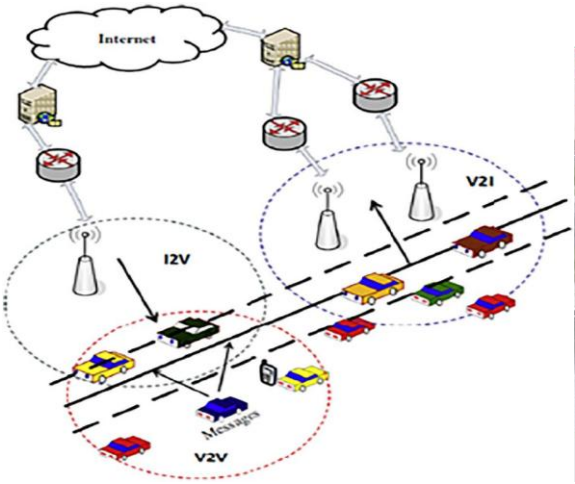
Sybil-attack detection framework should achieve high detection accuracy while minimizing false positives, communication overhead, processing delay. This study aims at such intelligent and adaptive security mechanism essential for improving the trustworthiness, safety, and resilience of next-generation VANETs.

II. Literature Survey

Adele et al. in [1] presented a comprehensive survey comparing existing Sybil attack detection and mitigation techniques in VANETs, highlighting the strengths and limitations of different approaches. Hadri et al. reviewed major Sybil attack detection techniques in VANETs, covering cryptographic, trust-based, machine-learning, and physical-layer approaches in [2]. Rakhi and Shobha in [3] proposed an LCSS-based Sybil detection and avoidance method for clustered vehicular networks using similarity in vehicle mobility and communication behaviour. Balaram et al. developed an Extreme Learning Machine-based Sybil detection approach that exploits vehicle-location information to improve detection accuracy in [4]. In [5], Zhang et al. proposed a Sybil attack detection and elimination mechanism for VANETs by identifying inconsistencies among multiple vehicle identities and communication behaviours. Zhong et al. introduced in [6] an LSTM-based BiGAN model for detecting Sybil attacks by learning temporal and behavioural characteristics of vehicular communication. Paranjothi and Khan in [7] investigated fog-computing-assisted Sybil attack detection, using distributed fog resources to improve detection efficiency and reduce latency in VANETs. Zhu et al. in [8] have proposed a beacon-packet-based detection and traceability mechanism that identifies Sybil vehicles through inconsistencies in beacon information and vehicle behaviour. Tulay and Koksal proposed signal-clustering-based Sybil detection, exploiting similarities and differences in physical-layer signal characteristics to identify malicious identities in [9]. Chen et al. in [10] proposed a multi-source data fusion detection framework (MDFD) that combines heterogeneous vehicular information to improve Sybil attack detection accuracy. Navinkumar and Somasundaram developed an optimized routing protocol using rumour-riding techniques to identify and isolate Sybil nodes in VANET environments in [11]. Krishnan and Koushik in [12] have proposed a decentralized distance-based Sybil detection strategy for identifying malicious nodes and reducing their impact on vehicular communication. Pareek et al. investigated ensemble machine-learning classifiers for Sybil attack detection, demonstrating the potential of combining multiple ML models for improved classification performance in [13]. Nayak et al. in [14] developed an AI-driven Sybil attack detection framework for software-defined vehicular networks, demonstrating the applicability of intelligent techniques to SDN-enabled VANET security. Morton et al. proposed a trust-aware Sybil detection mechanism that evaluates vehicular trustworthiness to identify malicious identities and enhance communication resilience in [15]. Khan et al. proposed a robust Sybil attack detection framework in [16] designed to improve detection reliability under varying vehicular network conditions. Hasan et al. investigated in-vehicle digital twins for collision warning and Sybil detection, integrating digital-twin technology with security mechanisms for connected vehicles in [17]. Hadri et al. in [18] provided a survey of Sybil detection mechanisms in VANETs, categorizing approaches according to authentication, trust, physical-layer, and intelligent detection techniques. Man et al. proposed a strong anonymous batch-authentication scheme that provides privacy preservation while preventing malicious vehicles from exploiting multiple identities in [19]. Abdelmaguid et al. proposed UAV-assisted Sybil detection (UAVSyDM) in [20] that uses aerial sensing to enhance the identification of malicious vehicles in VANETs.

III. **A. VANET Architecture**

A typical VANET consists of,
Vehicles[On Board Units] – Exchange safety messages
Roadside Units[RSUs] – Fixed Infrastructure assisting communications
Trusted Authority [TA] – Manages vehicle registration and certificates
Cloud/Edge Servers – Process Traffic information
Types of Communication – Includes [a] Vehicle-to- Vehicle[V2V] [b] Vehicle -to- Infrastructure[V2I] [c] Vehicle-to- Network[V2N] and [d] Infrastructure-to-Vehicle[I2V]. Figure 1 shows the VANET architecture



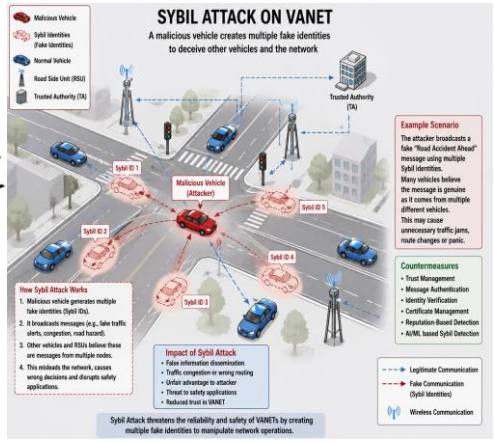


Figure.1 VANET Architecture **Figure.2 Sybil Attack in VANET**

III.B Sybil Attack on VANET

A malicious node joins the network. It creates and uses multiple fake identities[Sybil Nodes] to deceive other vehicles and roadside infrastructure. Each fake identity broadcasts false traffic information. Nearby vehicles believe multiple vehicles are reporting the same event. Drivers change routes unnecessarily and traffic control systems make incorrect decisions.

IV.A Simulation Scenario

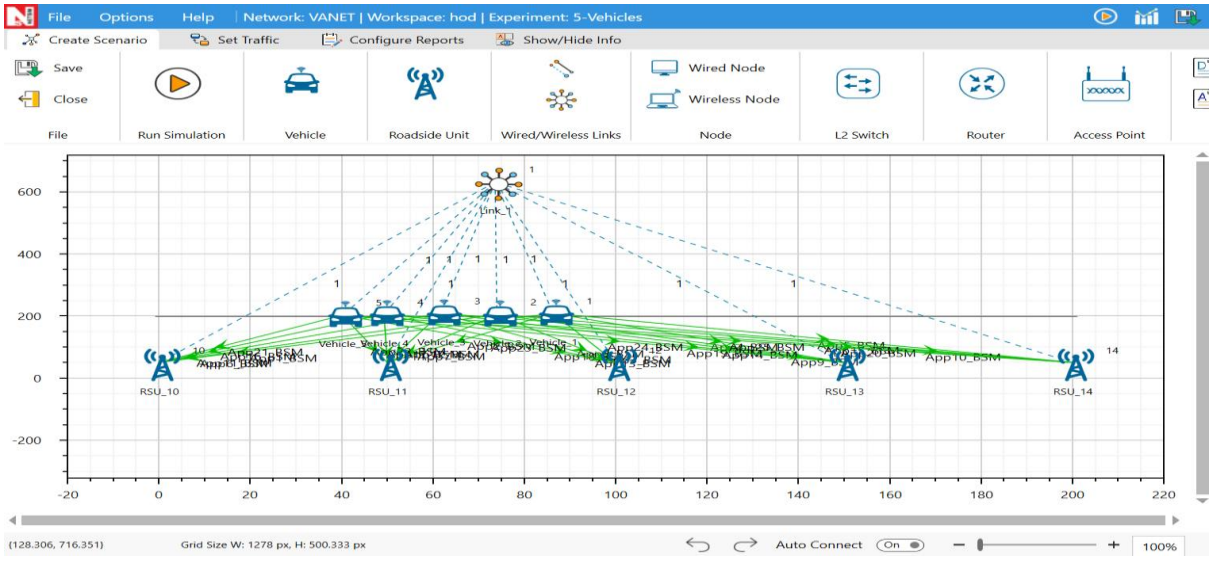


Figure.3 Sybil Attack Scenario in VANET

Attack Scenarios - Training Data Generation

5 scenarios are considered with varying total node counts [5,7,9,11,12]

Total Node Count = Normal Node Count + Sybil Attacker Count + Sybil Node Count

5	=	3	+1	+1
7	=	5	+1	+1
9	=	7	+1	+1
11	=	9	+1	+1
12	=	9	+1	+2

Sybil Node Count [1,1,1,1,2]

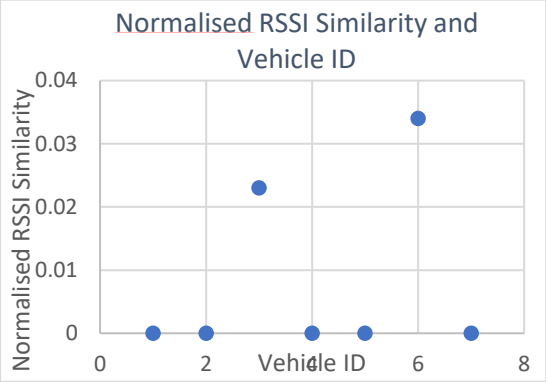
Total Dataset : 44 vehicles, 3 features each

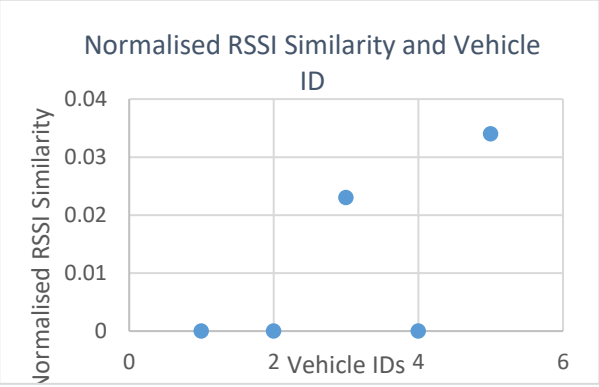
Data Processing

- Data are extracted from IEEE Radio Measurement Log.
- Calculate the pairwise RSSI differences between vehicle to each RSU.
- Compute the Mean RSSI difference for each vehicle pair.
- Assign a threshold to classify vehicle pairs
- Identify similar vehicle pairs based on threshold[0.02,0.03,0.9]
- Calculate the Average RSSI similarity for each unique pair.

Feature Visualisation

Vehicle Pair	RSSI Similarity	Similarity Score
3-1	0.000	0
3-2	0.023	1
4-5	0.000	0
1-4	0.000	0
3-5	0.034	1
5-1	0.000	0
4-2	0.981	1



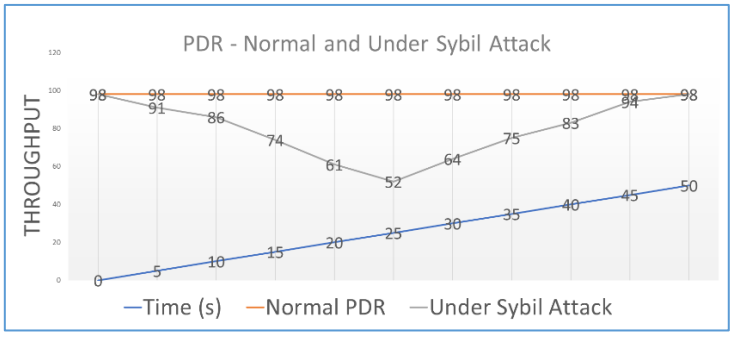


IV. A. Sybil Attack Classification using Machine Learning Algorithms.

The Sybil attacks are classified using 3 algorithms. The results of the 3 algorithms are tabulated.

Classifier	Accuracy in %	Precision in %	Recall in %	F1-Score in %
Random Forest	96.49	97.33	98.84	98.08
K – Nearest Neighbour	95.42	97.70	97.33	97.52
Decision Tree	96.15	96.96	98.84	97.89

B. Packet - to – Delivery Ratio [PDR] Analysis



From the Packet trace, the PDR is observed under 2 conditions, the normal PDR and the PDR under the Sybil attack. It is found that there is a degradation in the PDR when the VANET experiences a Sybil attack.

V. Calculation of Resilience Index

The Resilience parameters are calculated from the network and are tabulated as follows,

Metric	Normal	Sybil Attack	Proposed Method	Interpretation
PDR (%)	98	61	89	Higher is good
Throughput (Mbps)	9.6	7.4	8.2	Higher is good
Delay (ms)	45	79	63	Lower is good
Packet Loss (%)	12	56	34	Lower is good
Detection Time (s)	—	8	4	Lower is good
Response Time (s)	—	5	2	Lower is good
Recovery Time (s)	—	10	8	Lower is good

Resilience Index can be calculated as:

$RI=w_1$ PDRN$+w_2$ TN$+w_3$ DN$+w_4$ PLN where:

PDRN $=PDR_{normal}/PDR$

TN $=Throughput_{normal}/Throughput$

DN $=Delay/Delay_{normal}$

PLN $=Packet\ Loss/Packet\ Loss_{normal}$

Weights are taken as $w_1=w_2=w_3=w_4=0.25$

Therefore, $RI=41[9889+9.68.2+6345+3412]$

Resilience Index [RI] ≈0.7074

VI. Conclusion

The simulations show results with 96.15% Accuracy, 98.84% Sybil detection rate, 97.89% F1-score,50% reduction in Detection Time, 60% reduction in Response Time, Improved PDR and Throughput. The proposed machine-learning-based framework effectively detects Sybil attacks in VANETs, achieving 96.15% accuracy, 98.84% detection rate, and 97.89% F1-score.
The resilience evaluation demonstrates reduced detection and response times, along with improved Packet Delivery Ratio and Throughput. Future research can investigate deep learning, federated learning, and reinforcement learning for adaptive and privacy-preserving Sybil detection in highly dynamicVANETenvironments.

References

[1] G. Adele, A. Borah, A. Paranjothi, and M. S. Khan, “A survey and comparative analysis of methods for countering Sybil attacks in VANETs,” in Proc. IEEE 14th Annu. Comput. Commun. Workshop Conf. (CCWC), Las Vegas, NV, USA, 2024, pp. 1–7, doi: 10.1109/CCWC60891.2024.10427979.
[2] H. Hadri, M. Ouadou, L. Chakour, and K. Minaoui, “Sybil attack detection in vehicular ad hoc networks (VANETs): A comprehensive survey,” Innovations Syst. Softw. Eng., vol. 21, no. 2, pp. 453–474, 2025, doi: 10.1007/s11334-025-00603-7.
[3] S. Rakhi and K. R. Shobha, “LCSS based Sybil attack detection and avoidance in clustered vehicular networks,” IEEE Access, vol. 11, pp. 75179–75190, 2023, doi: 10.1109/ACCESS.2023.3294469.
[4] A. Balaram, S. A. Nabi, K. S. Rao, and N. Koppula, “Highly accurate Sybil attack detection in VANET using extreme learning machine with preserved location,” Wireless Netw., vol. 29, no. 8, pp. 3435–3443, 2023, doi: 10.1007/s11276-023-03399-1.

[5] Z. Zhang, Y. Lai, C. Ye, J. Wang, and Y. Wang, “Detection method to eliminate Sybil attacks in vehicular ad hoc networks,” Ad Hoc Netw., vol. 141, Art. no. 103092, 2023, doi: 10.1016/j.adhoc.2023.103092.
[6] Y. Zhong, H. Yang, Y. Li, B. Yang, X. Li, Q. Yue, J. Hu, and Y. Zhang, “Sybil attack detection in VANETs: An LSTM-based BiGAN approach,” in Proc. IEEE Int. Conf. Data Security Privacy Protection (DSPP), 2023, pp. 113–120, doi: 10.1109/DSPP58763.2023.10404993.
[7] A. Paranjothi and M. S. Khan, “Enhancing security in VANETs with Sybil attack detection using fog computing,” in Proc. IEEE 98th Veh. Technol. Conf. (VTC-Fall), Hong Kong, 2023, doi: 10.1109/VTC2023-Fall60731.2023.10333491.
[8] Y. Zhu, J. Zeng, F. Weng, D. Han, Y. Yang, X. Li, and Y. Zhang, “Sybil attacks detection and traceability mechanism based on beacon packets in connected automobile vehicles,” Sensors, vol. 24, no. 7, Art. no. 2153, 2024, doi: 10.3390/s24072153.
[9] H. B. Tulay and C. E. Koksal, “Sybil attack detection based on signal clustering in vehicular networks,” IEEE Trans. Mach. Learn. Commun. Netw., vol. 2, pp. 753–765, 2024, doi: 10.1109/TMLCN.2024.3410208.
[10] Y. Chen, Y. Lai, Z. Zhang, H. Li, and Y. Wang, “MDFD: A multi-source data fusion detection framework for Sybil attack detection in VANETs,” Comput. Netw., vol. 224, Art. no. 109608, 2023, doi: 10.1016/j.comnet.2023.109608.
[11] V. R. Navinkumar and D. Somasundaram, “Developing an optimized routing protocol with rumor riding technique for detection of Sybil attack in VANET environment,” Int. J. Commun. Syst., vol. 37, no. 6, Art. no. e5715, 2024, doi: 10.1002/dac.5715.
[12] P. Remya Krishnan and R. Koushik, “Decentralized distance-based strategy for detection of Sybil attackers and Sybil nodes in VANET,” J. Netw. Syst. Manage., vol. 32, Art. no. 91, 2024, doi: 10.1007/s10922-024-09869-x.
[13] P. K. Pareek, P. Siddhanti, S. Anupkant, S. O. Husain, and I. Bhuvaneshwarri, “Ensemble based machine learning classifier for Sybil attack detection in vehicular ad-hoc networks (VANETS),” in Proc. 2nd Int. Conf. Data Sci. Inf. Syst. (ICDSIS), 2024, pp. 1–4, doi: 10.1109/ICDSIS61070.2024.10594488.
[14] R. P. Nayak, S. K. Bhoi, K. S. Sahoo, S. Sethi, S. Mohapatra, and M. Bhuyan, “Unveiling Sybil attacks using AI-driven techniques in software-defined vehicular networks,” Security Privacy, vol. 8, no. 1, Art. no. e487, 2025, doi: 10.1002/spy2.487.
[15] T. L. Morton, A. Borah, A. Paranjothi, and M. S. Khan, “Trust-aware Sybil attack detection for resilient vehicular communication,” Internet Technol. Lett., vol. 8, no. 5, Art. no. e617, 2025, doi: 10.1002/itl2.617.
[16] J. Qi, N. Zheng, M. Xu, P. Chen, and W. Li, “A hybrid-trust-based emergency message dissemination model for vehicular ad hoc networks,” J. Inf. Secur. Appl., vol. 81, Art. no. 103699, 2024, doi: 10.1016/j.jisa.2024.103699.
[17] G. Rathee, A. Kumar, C. A. Kerrache, and C. T. Calafate, “A trust management solution for 5G-based future generation Internet of Vehicles,” Comput. Netw., vol. 248, Art. no. 110501, 2024, doi: 10.1016/j.comnet.2024.110501.
[18] Z. Man, S. Pan, Z. Xu, and M. Ye, “Strong anonymous batch authentication scheme against Sybil attack in VANET,” Wireless Netw., vol. 31, no. 7, pp. 4519–4540, 2025, doi: 10.1007/s11276-025-04002-5.
[19] C. Zhang, X. Chang, X. Jia, S. Zhang, and X. Wang, “Sybil-resistant and privacy-preserving authentication based on short-term pseudonym for Internet of Vehicles,” Sci. Rep., vol. 15, Art. no. 44966, 2025, doi: 10.1038/s41598-025-28854-1.
[20] N. Khatri, S. Lee, and S. Y. Nam, “Sybil attack-resistant blockchain-based proof-of-location mechanism with privacy protection in VANET,” Sensors, vol. 24, no. 24, Art. no. 8140, 2024, doi: 10.3390/s24248140.