Vol.8 Issue 4 Oct 2025

Multimedia Research

Received 8 September, Revised 11 September, Accepted 10 October

Survey on Sybil Attack Detection in VANET

Balajee Maram
School of Computer Science and Artificial Intelligence,
SR University, Warangal, Telangana, 506371.
balajee.maram@sru.edu.in

Abstract: Vehicular Ad Hoc Networks (VANETs) are an essential component of intelligent transportation systems, enabling real-time communication between vehicles and infrastructure. They form the backbone of modern Intelligent Transportation Systems (ITS), where safety, efficiency, and user experience largely depend on secure and reliable communication. The VANETs help the road operators to monitor and control the vehicles from rash driving. However, their distributed and highly mobile nature makes them more vulnerable to sophisticated security breaches compared to traditional wireless networks. The very nature of these systems is open and dynamic, which creates a potential opportunity for security threats to arise. A Sybil attack refers to an adversarial node forging many different identities to change traffic information, delay services, or manipulate routing to compromise privacy. This research aims to analyze and review various techniques used for Sybil attack detection in VANET. By consolidating existing approaches, this survey provides deeper insights into their comparative strengths, weaknesses, and suitability for different VANET scenarios. Techniques like Machine Learning (ML), Deep Learning (DL), signal processing, and protocol-based techniques are the most utilized techniques for attack detection. This survey examines the various works on Sybil attack detection in VANET, emphasizing proposed methodologies, publication years, tools, and performance evaluations. In addition to this, the challenges faced by the various schemes is also included. The findings indicate that the use of DL techniques shows promising prospects for Sybil attack detection in VANET. Besides, NS2 is the tool utilized by most researchers for implementation.

Keywords: Sybil Attack, VANET, Deep Learning, Machine Learning, Security

Nomenclature

Abbreviation	Description
VANET	Vehicular Ad Hoc Network
ITS	Intelligent Transportation System
V2V	Vehicle to Vehicle Communication
V2I	Vehicle to Infrastructure Communication
V2X	Vehicle-to-Everything
RSU	Road Side Unit
DSRC	Dedicated Short Range Communication
ML	Machine Learning
DL	Deep Learning
ANN	Artificial Neural Network
DNN	Deep Neural Network
LSTM	Long Short-Term Memory Networks
TH-GAT	Temporal Heterogeneous Graph Attention Networks
GBEHO-DNN	Gradient Based Elephant Heading Optimization Deep Neural Network
ABESO	Adaptive Bald Eagle Search Optimization
MA-DQN	Multi Agent Deep Q Network
DRL	Deep Reinforcement Learning
MDFD	Multi Source Data Fusion Detection
KNN	K Nearest Neighbor
SVM	Support Vector Machines
FLC	Fuzzy Logic Controllers
RSSI	Received Signal Strength Indicator
LCSS	Longest Common Subsequence
CPD	Change Point Detection
CSI	Channel State Information
INTERLOC	Interference Aware RSSI Based Localization
PCISAD	Power Control Identification Sybil Attack Detection
EPORP	Emperor Penguin Optimization-Based Routing Protocols
SXOR	Secure XOR Based Encryption

https://doi.org/10.46253/j.mr.v8i4.a4

PASAD	Privacy Aware Sybil Attack Detection
DTW	Dynamic Time Warping
DST	Dempster Shafer Theory
LA-DETECTS	Local and Adaptive Data Centric Misbehavior Detection Framework
DT-LHBC	Digital Twin Lightweight Hashing Blockchain Cryptography
BSM	Basic Security Message
GPCR-ARE	Greedy Perimeter Coordinator Routing Attack Resilient and Efficient Protocol
TH-GAT	Temporal Heterogeneous Graph Attention Network
PoW	Proofs of Work
PoL	Proofs of Location
EC	Elliptical Curve

1. Introduction

VANET is an integral part of an Intelligent Transportation System. It acts as the communication backbone for connected vehicles, supporting traffic management, collision avoidance, and infotainment services in real time. VANET will lik ely create a sense of safety within roadways to support future aspirations. By enabling cooperative awareness among vehicles, VANET contributes to reducing accidents, enhancing fuel efficiency, and improving overall driving experiences. Connected vehicles are a reality today after the implementation of Google cars on the roadway. The primary attribute of VANET is its ability to self-organize vehicles, information sharing, and rapid communication. V2V and V2I communication in VANET is based upon the DSRC standard [1]. DSRC provides low-latency communication, which is crucial for safety-critical applications such as collision avoidance and lane-changing assistance. With the help of VANET, vehicles can communicate with each other, which helps passengers drive safely; primarily, communication between vehicles relies on exchanged information from other vehicles while traversing roadways. VANET is derived from an ad hoc wireless network; thus, it has all the issues related to the wireless medium and equally concerning substantial security threats [2]. These include high mobility, dynamic topology, intermittent connectivity, and susceptibility to jamming, all of which complicate the security design. Similar to conventional wired networks, VANETS are subject to attacks and vulnerabilities. VANETs can be affected by traditional attacks as well as specific attacks that focus on safety disruption and the dissemination of false information [3]. One of the major and troublesome attacks with respect to authenticity and identification issues is the Sybil attack. The Sybil attack is one of the most harmful vulnerabilities in VANETs as it presents not only a threat to the integrity, availability, and confidentiality of the network but also a potential danger to the lives of the drivers and passengers involved [4]. By fabricating multiple fake identities, a Sybil node can manipulate traffic flow data, disrupt routing decisions, and mislead drivers into unsafe road conditions.

A Sybil attack can be established in three ways: direct vs. indirect, fabricated identity attack vs. stolen identity, and simultaneous attack vs. non-simultaneous attack. Direct communication has the invader establishing direct communications with real nodes and directing traffic to those real nodes [4]. In indirect communications, the invader does not directly communicate with the real nodes; it communicates with the Sybil nodes. This flexibility in attack modes makes detection particularly challenging, as Sybil nodes can dynamically adapt their strategies. Research has been done to detect these types of attacks; however, a Sybil attack cannot communicate correct information about itself because it has to forge identity information [5]. The present methods of attack detection for Sybil attacks in mobile ad-hoc networks do not work well in vehicular networks. This is due to unique VANET constraints such as rapid topology changes and stringent latency requirements. Radio resource-based attack detection assumes simultaneous transmissions and reception on the same channel. This assumption does not apply to vehicular networks, as attackers can use multiple radios to attack [6]. A number of security mechanisms are proposed to detect and prevent Sybil attacks. An intruder can easily launch an attack in a highly mobile scenario. Hence, the detection of the existence of a sybil attack and identification of the sybil nodes is a problem in a transient neighborhood. This transient nature means that detection systems must operate in real time and with minimal computational overhead. There are primarily four broad classes of methods used to detect sybil attack, namely resource testing-based, cryptography-based, trust-based based and physical measurement-based methods [7]. Each category offers unique strengths: resource testing evaluates hardware constraints, cryptography secures identities, trust-based methods leverage behavioral history, and physical measurements exploit signal properties. DL methods are also employed for Sybil attack detection in VANET. DL has evolved as a tool for refining the Sybil attack detection in VANET [8].

The major objective of this survey is to review the various methods utilized for detecting Sybil attacks in VANET. These techniques are grouped into four classes, namely DL, ML, signal processing, and protocol-based techniques. This classification helps in systematically analyzing the evolution of detection mechanisms from conventional approaches to advanced AI-driven methods. Moreover, this survey presents

the analysis of the various Sybil attack detection works in relation to implementation tools, techniques, publications, and performance metrics. The drawbacks of the present techniques are examined and highlighted for further development. This ensures that future research directions are aligned toward addressing unresolved gaps such as scalability, latency, and deployment feasibility.

This survey paper is structured as follows: Section 2 describes the general architecture for Sybil attack detection in VANET, and Section 3 elaborates on the several techniques employed for Sybil attack detection in VANET, grouped according to their techniques. Section 4 contains the literature survey of various sybil attack detection methods, and the research gaps and limitations of the present techniques are presented in Section 5. In Section 6, the analysis of the study concerning publishing years, simulation tools, evaluation metrics, and datasets is elucidated. Finally, the conclusion is outlined in Section 7.

2. General Architecture for Sybil Attack Detection in VANET

A Sybil attack in VANET occurs when an individual vehicle node generates multiple fraudulent identities to create an illusion of traffic jams. Such fabricated identities can mislead genuine drivers into making unsafe routing decisions and may also disrupt emergency vehicle prioritization. To avoid that, Sybil attack detection is performed on the vehicle nodes to eliminate the malicious nodes. Initially, the data is collected from the RSU, vehicles or other sources and is subjected to preprocessing, where the data is cleaned and normalized to enhance the detection accuracy. This stage also helps to reduce noise, eliminate redundant attributes, and prepare the raw vehicular communication data for analysis. After that, the preprocessed data is forwarded to the feature extraction phase, where the relevant features are extracted. Next, the extracted features are fed into the Sybil attack detection phase, where the features are classified as benign and malicious. Depending on the adopted detection framework, this classification may rely on statistical thresholds, learning models, or protocol-driven rules. The Sybil attack detection is performed using various techniques like various detection techniques, like ML-based techniques, DL-based techniques, signal processing techniques, and protocol-based techniques. Fig. 1 represents the general architecture of Sybil attack detection in VANET. The figure illustrates the sequential pipeline from data acquisition to final classification, emphasizing how each layer contributes to ensuring secure communication in VANETs.

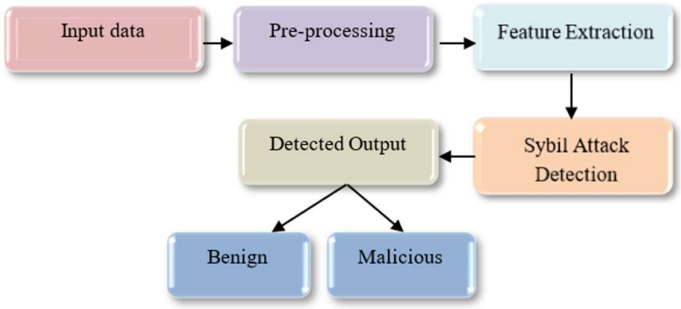

Fig. 1. *General Architecture of Sybil Attack Detection in VANET*

3. Categorization of Sybil Attack Detection in VANET

Sybil attack detection in VANET is accomplished based on various detection techniques, which can be categorized as ML-based techniques, DL-based techniques, signal processing techniques, and protocol-based techniques. The categorization of the various attack detection techniques in VANET is presented in Fig. 2. The figure highlights how these four categories complement each other, demonstrating that no single approach is sufficient in isolation, and hybrid solutions may offer more comprehensive detection capabilities.

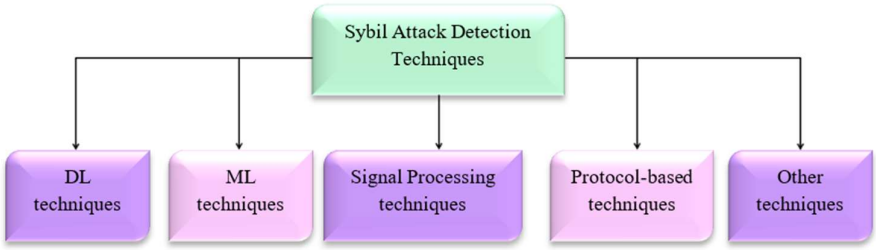

Fig. 2. *Classification of various Sybil attack detection techniques in VANET*

4. Literature Review

The literature review of various techniques utilized for Sybil attack detection in VANET is elaborated in this section. The techniques discussed in this study for detecting Sybil attacks in VANET are classified into four groups, namely ML-based techniques, DL-based techniques, signal processing techniques, and protocol-based techniques and are outlined as follows.

4.1 Deep Learning-Based Techniques

DL techniques are a part of ML techniques, which employ an ANN with many layers to train and understand the patterns in a large amount of data. These deep architectures can automatically extract hierarchical representations from raw data, eliminating the need for manual feature engineering. DL techniques are retrained with newly updated data to identify evolving or unseen attacks in the networks. This adaptability is particularly important in VANETs, where attacker behavior is dynamic and continuously changing. The various DL-based techniques used for Sybil attack detection in VANET are examined in this section.

Velayudhan, N.C., *et al.* [9] proposed a CMEHA-DNN approach to detect Sybil attacks in VANETs. The DNN classified vehicles based on behavioral features such as the vehicle's position and location, speed, time traveled, and message sending patterns. By capturing these behavioral indicators, the model sought to differentiate legitimate vehicles from those generating falsified identities. This method incorporated MD5 hashing to validate data transmission for integrity, and ECC for strong encryption in a VANET environment, thus balancing efficiency and security. The simulation results showed high detection rates with low communication overhead in CMEHA-DNN, resulting in improved performance compared to the conventional method. However, despite these gains, the reliance on MD5 presented a major drawback, as the hashing algorithm is considered cryptographically broken. Meanwhile, the use of MD5 created a security vulnerability since MD5 was a known cryptographic weakness that could potentially jeopardize the overall security approach.

Zhang, Y.Y *et al.* [10] introduced a self-learning method to identify Sybil attacks in electric vehicles using LSTM networks. This technique modeled the sequential mobility and communication behaviors when determining identity impersonation. The LSTM's ability to capture temporal dependencies was leveraged to detect anomalies in node movement patterns and communication history. The proposed self-learning indicated that the model could detect identity impersonation without utilizing the labeled attack data. The LSTM model continuously learned by updating its weights based on historical and the user's previous behavioral datasets. This online learning ability allowed the system to adapt to changes without retraining from scratch, a key advantage in dynamic vehicular environments. Over time, detection accuracy improved via self-learning based on significant, robust datasets. One drawback of the proposed methodology was that if the mobility behavior changed dynamically, the ability of the model to learn was significantly undermined. In practice, highly dynamic road conditions may therefore reduce the effectiveness of this solution. Another issue with the study's approach was that users may not have sufficient historical data, which was insufficient for the user to identify whether the communication was done or not.

Chen, Y *et al.* [11] presented an approach to detect and trace Sybil attacks by using a TH-GAT in vehicular networks. The proposed model accurately modeled spatiotemporal vehicle behaviors and interactions using heterogeneous graphs and attention mechanisms to systematically localize and trace Sybil nodes even during times of silence or deception. This graph-based framework allowed the detection system to exploit relational dependencies between vehicles instead of relying only on individual behavioral features. The simulation studies showed that when the attack was active, there was a greater success rate for tracing Sybil nodes. The limitation of the TH-GAT model was that the reliance on synchronized broadcast patterns showed capacity for some tradeoffs or limitations that need to be addressed. In real-world VANETs, synchronization is often imperfect, which may reduce the applicability of such methods.

Nova, K *et al.* [3] described a GBEHO-DNN framework for secure communication in VANETs. The framework combined the Floyd-Warshall algorithm for optimized shortest path routing and a modified AES encryption algorithm. By integrating routing optimization and encryption within the detection framework, the method addressed both security and communication efficiency simultaneously.The Floyd-Warshall algorithm was used to discover shortest paths to improve communication reliability, and the modified AES algorithm was effective in using minimal processing speed while maintaining an appropriate level of strength in the encryption. The hybrid framework was secure and reliable, and the transmission latency was both low and the overhead was limited. The key challenge faced by the framework was the increased computational complexity of using graph-based routing in conjunction with non-threaded AES encryption, which also limited real-time performance in rapidly changing vehicular networks. This indicates that while the approach is theoretically strong, practical deployment may face scalability issues.

Ajin, M. and Shaji, R.S., [12] have developed a Sybil attack detection framework for VANETs, which is based on ABESO and MA-DQN. The ABESO algorithm helped to optimize the detection, and the MA-DQN framework facilitated cooperative learning to detect hidden patterns of attacks. This combination of metaheuristic optimization and reinforcement learning allowed the model to balance exploration and exploitation in decision-making. Simulations showed better detection and a lower false positive rate compared to existing methods, while also demonstrating evidence of adaptability in varied network conditions. The one noted disadvantage is that the high training and computational complexity of the deep Q-learning algorithm will impact the ability to create a model that can be applied in real-time to detect Sybil attacks in large-scale and low-resource VANET scenarios, particularly in situations where it is critical to provide a fast response time and use lightweight detection models.

Sultana, R., *et al.* [13] proposed an intelligent defense framework for VANETs, which utilized DRL to detect and respond to several evolving security attacks in VANET, including Sybil attacks. The DRL-based framework was able to auto-adapt to new attack variations without the costly retraining typically required, which increased the flexibility of the system and expandability to some extent. Such adaptability is vital in VANETs, where adversarial strategies can change rapidly, making static models ineffective. The simulation results indicated that the framework based on DRL successfully recognized and mitigated multiple threats, representing a potentially promising avenue for intelligent, adaptive security for VANETs. There was a heavy dependency on the framework's performance over training environments; if not sufficiently trained from either a lack of fidelity or bias in training scenarios, the system will struggle to generalize and not be as effective in real-world deployments. This limitation highlights the importance of realistic datasets and diverse training environments for DRL-based security solutions.

4.2 Machine Learning-Based Techniques

ML is one of the subfields of AI, which learn from examples and makes decisions based on the patterns of the data. ML does not need any external programming; it can learn the patterns by itself. This self-learning ability makes ML well-suited for dynamic environments such as VANETs, where attack strategies and mobility conditions evolve continuously. Several ML techniques utilized for Sybil attack detection in VANET are analyzed and reviewed below.

A MDFD was proposed by Chen Y *et al.* [14] to identify Sybil attacks in VANETs. The framework utilized traffic data from various sources and combined them into four classes. The vehicle sensors extracted features like spatiotemporal pattern extraction, the traffic flow, vehicle behavior, and sensor confirmation. By leveraging multiple sources of information, the model reduced reliance on any single dataset, thereby enhancing robustness. An ML classifier was utilized for identifying Sybil attacks and locating the road segments that were affected. The framework achieved high detection precision over multiple scenarios and types of attacks; however, the level of computational complexity and dependence on several sources of data limited the model's real-time application or use in resource-constrained environments. This tradeoff highlights a recurring challenge in ML-based VANET security: balancing accuracy with computational feasibility.

Azam, S., *et al.* [15] proposed a collaborative learning system for Sybil attack detection in VANETs by employing a majority vote from classifiers such as KNN, Naïve Bayes, Decision Tree, SVM, and Logistic Regression. The collaborative system utilized the strengths of the classifiers in a community-based approach to enhance the reliability and security of vehicle communications and reduce identity forgery attacks in VANETs. Ensemble learning in this context provided resilience by reducing the bias of individual classifiers and improving overall detection rates. However, the reliance on multiple classifiers increased the computational complexity and potentially degraded real-time capture performance during large-scale, high-mobility VANET-related applications.

Bhanja, U., *et al.* [24] introduced a novel detection model to tackle Sybil and DDoS attacks in VANETs using FLCs, which identified anomalies through assertions on Packet Loss Ratio, Signal to Noise Interference Ratio, and Total Busy Time. The adaptive nature of FLCs allowed the system to adjust its decision boundaries dynamically based on environmental changes. The proposed model was able to outperform existing techniques in accuracy, sensitivity, and recall, while maintaining a very low processing overhead, allowing for real-time applications. The FLCs permitted an adaptive decision-making process under various connectivity conditions, but models reliant on fuzzy logic struggled with accurate boundary mappings in some situations, which caused issues with false positive or negative results in highly volatile network circumstances.

4.3 Signal Processing Techniques

Signal processing techniques indicate that the analysis and interpretation of signals like sensor data, radio waves, etc., are employed for extracting useful information from the signals. Unlike ML or DL approaches, which require labeled datasets for training, signal processing leverages inherent physical properties of

wireless communication, making it more lightweight and infrastructure-independent. The various signal processing techniques utilized for Sybil attack detection in VANET are given as follows.

Rakhi, S. and Shobha, K.R., [1] presented a lightweight, decentralized framework for Sybil attack detection in clustered VANETs based on a fusion of LCSS and CPD algorithms. Cluster heads employed RSSI sequence data from member vehicles to identify suspicious activity and attained enhanced detection accuracy, delay, and false positive ratios. The use of sequence-based analysis allowed the system to track long-term consistency in signal behavior, which is often difficult for attackers to mimic. Besides, this technique was independent of roadside equipment and did not rely on the preestablished trust among nodes. LCSS provided robustness against noise and sequence variance. Nonetheless, the most critical drawback was reliance on reliable clustering and consistent RSSI sampling, which could be unstable in high-mobility or sparse network scenarios, influencing detection consistency. Thus, the effectiveness of this approach is highly dependent on stable network density.

Tulay, H.B. and Koksal, C.E. [16] devised a Sybil attack detection scheme for vehicular networks based on CSI. The approach was based on spatiotemporal CSI fluctuations to distinguish spoofed and authentic vehicles. Because CSI reflects fine-grained channel variations, it provides attackers with fewer opportunities to replicate legitimate patterns. Real-world (V2X) communications obtained through DSRC were employed for improving the attack detection rate. The scheme was infrastructure agnostic and did not need any special hardware. But its biggest drawback was that it was prone to channel noise and multipath effects, which undermined the performance in highly dynamic or obstructed scenarios, even causing misclassification or decreased detection reliability.

Yao, Y., *et al.* [17] introduced an INTERLOC, a simple, purely decentralized Sybil attack detection mechanism in VANETs, based on RSSI time series analysis. Without any central infrastructure, INTERLOC used change-point detection to identify RSSI anomalies, which made it resilient to attack detection methods. This decentralized nature is particularly valuable for large-scale deployments where centralized servers may not be practical. This technique had high detection efficiency with minimal false positives and small computational overhead in simulations and actual experiments. This technique had the strength to leverage the signal properties of the physical layer, which was hard to mimic by the attackers. However, its main disadvantage was vulnerability to outside interference since RSSI values were dynamic based on noise or interference, which led to a reduced detection accuracy. Therefore, while INTERLOC is lightweight and scalable, it struggles in environments with fluctuating wireless conditions.

Yao, Y., *et al.* [18] proposed the PCISAD technique in VANETs that operates based on RSSI measurements to determine inconsistencies in power control. Their technique only anticipated observing RSSI values that fall within the expected range to detect possible Sybil nodes. By monitoring transmission power consistency, the system could distinguish between legitimate nodes and Sybil identities without requiring heavy computations. The technique was suitable for real-time applications, as the computational requirements were low, which made it suitable for resource-constrained applications. Reliability was a concern in the standard RSSI detection method, as other sources, like adversarial channel interference or natural fading reduction, had caused variations in RSSI measurements. This makes the technique more vulnerable in complex or highly dynamic environments where measurements may not be as effective. Hence, although PCISAD is computationally efficient, it may require integration with other detection layers for reliable performance in practice.

4.4 Protocol-based Techniques

Protocol-based techniques depend on the communication protocols and use default rules to receive and transmit data between the devices. These methods leverage the inherent structure of communication standards in VANETs, making them attractive for real-time detection without requiring heavy computational models. However, their effectiveness is closely tied to the scalability and adaptability of the underlying protocols. The various protocol-based techniques employed in Sybil attack detection in VANET are analyzed and elaborated below.

Velayudhan, N.C., *et al.* [19] introduced the Emperor Penguin Optimization-based Routing Protocol (EPORP) model, a Sybil attack detector and routing protocol for urban VANET, based on a technique called Emperor Penguin Optimization (EPO). EPORP used Rumor Riding for the attack detector and SXOR encryption for secure communications. Performance monitoring for routing indicated improved reliability, and improved location privacy was presented based on the features of SXOR encryption. By integrating bio-inspired optimization with routing, EPORP sought to achieve adaptive path selection while embedding Sybil resistance in the communication process. While the benefits of the EPORP were clear, its major drawback was the computational overhead for metaheuristic optimization and encryption. Therefore, this work is impractical in real-time and resource-constrained environments that are expected in VANETs, especially with densified vehicle flows and simulated topologies that could change rapidly. This highlights

a recurring issue in optimization-driven protocols: high accuracy but poor feasibility in real-world, fast-moving VANETs.

Funderburg, L.E. and Lee, I.Y., [20] proposed a hierarchical key management scheme for VANETs that guaranteed vehicle privacy and facilitated Sybil attack detection. The scheme used short group signatures at low-level hierarchies to ensure privacy and enabled Sybil attack detection by mid-level nodes. Top-level nodes with authorization could reveal the true identities of malicious nodes and could blacklist them from future entries. This hierarchical layering distributed responsibilities across different levels, creating a balance between privacy preservation and accountability. This approach promoted security and privacy with the alleviation of backward secrecy when no malicious traffic existed. However, the hierarchical structure introduced overhead and complexity, potentially impacting scalability and efficiency in highly dynamic VANET environments. Thus, while effective in structured settings, the approach may struggle in highly transient or decentralized vehicular networks.

Zhu, Y., *et al*. [21] proposed a Beacon-packet-based detection and traceability mechanism to detect and trace Sybil attacks in CAVs through specially customized key broadcasts compared to other sniff packets within the beacon packets. First, RSUs would send directions to use beacon packets by broadcasting a key with instructions for vehicles to listen and broadcast within communication range. When RSUs directed vehicles in the communication range to listen and broadcast, neighbor graphs were created to develop an edge success probability to determine the credibility of a vehicle. This mechanism cleverly exploited existing beacon signals, minimizing extra infrastructure requirements while enabling real-time Sybil tracking. Simulation results demonstrated that the scheme was able to achieve real-time detection with 98.53% precision and 95.93% recall, successfully tracing malicious vehicles, to improve the security and reliability of intelligent transportation systems. However, we need to consider that the proposed approach may run into scaling issues as the network expands and there are many interactions with the CAVs, which could impact real-time performance due to reliance on broadcasts, which decrease as the network size and density increase. Hence, scalability remains a critical barrier to deploying beacon-based approaches in future large-scale intelligent transportation systems.

Parham, M. and Pouyan, A.A., [22] proposed a PASAD scheme to enable secure communications in VANETs. Their solution combined cryptographic methods and reputation-based trust management to securely detect Sybil attacks and protect user privacy. Previous work has assumed a threat to privacy with Sybil attacks. The scheme was based on anonymous authentication and key management that enabled vehicles to communicate securely while concealing their identities. By fusing cryptography with trust management, PASAD introduced a dual-layer defense—ensuring both message authenticity and long-term reputation monitoring. The simulations of the scheme showed that it was capable of detecting Sybil attacks while maintaining secure communications. While this was a good detection scheme, the reputation-based trust management model employed could incur delays in detection since it required several measurements and hence might limit real-time detection in a time-critical, highly dynamic vehicular environment. This limitation underscores the tension between privacy protection and real-time responsiveness in protocol-based approaches.

4.5 Other Techniques

The alternate techniques employed instead of DL and ML techniques in Sybil attack detection in VANET are discussed in this section. These approaches generally focus on hybrid methods, cryptographic enhancements, or consensus mechanisms that exploit vehicular behaviors, mobility models, and blockchain features to strengthen security beyond conventional data-driven strategies.

Sefati, S.S. and Tabrizi, S.G., [5] proposed a Sybil attack detection technique for VANETs, which operates based on a fitness function defined using signal strength and throughput metrics and evaluates node behavior (delay, packet drop, and throughput) to build an evaluation of node activity. Evaluations were undertaken by RSUs based on the data received from neighbor nodes. Research using NS3 simulations demonstrated that their method detected Sybil Attacks in VANETs more rapidly than with existing schemes. Sefati and Tabrizi's function also provided a comprehensive overview of the node behavior to allow for scalability and adaptability in dynamic travel forms. This made the approach appealing in heterogeneous environments, where attack behaviors may vary. However, there was a reliance on RSUs to make the evaluations, which could potentially create challenges for implementation in geographic areas with low RSU deployments or would create additional communication requirements.

Sultana, R., *et al*. [23] proposed a Cooperative two-tier misbehavior detection framework in VANETs that was capable of dealing with Sybil attacks at the vehicle layer and RSU layer. The framework utilized DTW on speed-time series for vehicle-level detection and used DST at the RSU level to analyze the attacks. This framework utilized the benefits of both methods, allowed for accurate identification and tracking of Sybil nodes, while allowing for Linkage Authorities to revoke malicious nodes. By combining time-series analysis with probabilistic reasoning, the system strengthened robustness against adaptive attackers. This

technique achieved a better detection rate than the existing systems. However, because the hybrid approach was basically two separate frameworks that required significant computation resources, DTW and DST also required considerable coordination of vehicles and RSUs; this implication of combining detection methods added latency and introduced complexity in data collection.

Sultana, R., *et al*. [25] developed a LA-DETECTS for misbehavior detection and mitigation in VANETs. The framework was essentially based on discovering false information using consistency and reliability checks, which did not depend on a centralized infrastructure. LA-DETECTS had a high level of accuracy in identifying misbehavior, which has enhanced the reliability and security of vehicular networks. Its distributed nature also made it appealing for lightweight deployments where infrastructure support is minimal. Nevertheless, the framework's focus on local data consistency led to limited efficiency while facing adversaries, which not only misbehaved but also inversely mimicking legitimate behavior over time. Moreover, assuming data is available from neighboring nodes, since the first two checks will likely lead to local nearby/neighbor coordinates, knowing that the data may also be considered compromised will limit the use of the local identification processes in more complex attacks.

Baza, M., *et al.* [26] developed a Sybil attack detection scheme for VANETs based on a combination of PoW and PoLs. RSUs provided tags that were time-stamped (PoLs), and vehicles were required to carry out computing tasks to obtain these tags. Doing so, they were able to eliminate the production of fake identities since legitimate vehicles could properly add on to paths via multiple RSUs. This integration of blockchain-inspired consensus mechanisms with mobility-based validation improved resistance against identity forgery. The simulation results indicated that the detection scheme was accurate while maintaining low false negatives. However, the main disadvantage was the communication and computational overhead, especially for those vehicles operating in dense urban environments, because this approach may be simply unreasonable for devices with limited resources, where latency is important in a fast-moving vehicular environment.

Man, Z., *et al.* [27] examined a more advanced privacy-preserved authentication scheme for VANETs to lessen the risks of Sybil attacks, which is based on group signatures with batch verification and immediate revocation. The V2V and V2I communication from a commitment scheme based on the Chinese Remainder Theorem and Schnorr's signature enabled the vehicles with limited computing power could able to verify the messages immediately. Security analysis showed the scheme to be secure against impersonation attacks as well as replay attacks. The batch verification process was particularly effective in reducing verification time, which is critical in real-time communication. The performance analysis demonstrated that the scheme produced less verification time and transmission time, which shows more practicality for the scheme in high-density environments. Nevertheless, the complexity of the cryptographic operations and the dependence on performance remaining with RSUs could lead to scalability problems in a highly dynamic or sparse environment.

Kishore, M.K., *et al.* [28] proposed a secure, DT-LHBC framework to increase the reliability of wireless communication in VANETs by allowing the creation of virtual models of real vehicles for both real-time monitoring and management purposes. Edge computing was included in the framework to eliminate any latency associated with monitoring and to improve the overall processing speed and efficiency of the data. The use of Digital Twin technology brought innovation by integrating virtual-physical synchronization with vehicular cybersecurity. Results from simulations showed an improvement in communication reliability and reduced delay times. However, the framework relied on the real-time and accurate synchronization of ECs and Vehicle Certificates (VCs), which may introduce challenges in highly dynamic networks and ultimately affect the overall performance.

Zhang, Z., *et al.* [29] proposed a method to detect and mitigate Sybil attacks while utilizing beacon signal messages. By analyzing the Basic Security Messages (BSMs), which are sent regularly at a defined rate, the proposed method estimated the physical transmission distance of BSMs using time and other related information important for vehicle movement. This approach leveraged already existing communication standards, making it practical for integration into current VANET frameworks. The simulations showed that the proposed system could accurately identify malicious Sybil nodes while being able to continue operation for regular vehicles, even in high-density urban environments. The limitation of the proposed method was strictly bound to time synchronization and accurate position data, which are crucial for improving the system's operability.

Hussain, N., *et al*. [30] introduced the GPCR-ARE protocol to improve the efficiency and security of GPCR in VANETs based on mobility awareness. The protocol was designed to limit the effects of Sybil attacks, which utilized mobility models and sequential numbers to control routing and reduce storage overhead. Simulations offered evidence that GPCR-MA outperformed traditional GPCRs in packet delivery ratio, end-to-end delay, and throughput. This mobility-aware routing demonstrated that combining location dynamics with routing rules could enhance both efficiency and security. The study concluded that mobility-aware routing protocols could provide benefits to the security and QoS in VANET. Although the protocol offered improvements, the authors acknowledged that reliance on correct mobility information, as

well as sequential numbers, could pose limits on the GPCR-MA protocol in cases where GPS inaccuracy is high, and/or mobility patterns are irregular, which greatly weakens the overall robustness in a large or urban environment.

5. Research Gaps and Limitations

The unexplored areas and the drawbacks of various Sybil attack detection techniques in VANET are depicted as follows. Overall, while multiple frameworks show promising results in simulation, their generalizability, scalability, and practicality in real-world deployments remain highly limited.

The problems encountered by DL techniques are discussed as follows: The CMEHA-DNN scheme in [9] relied on MD5 hashing, which was weak cryptographically and raised doubts about the reliability of data integrity and secure access in VANETs. Future research must explore stronger cryptographic primitives such as SHA-3 or lattice-based algorithms to address this vulnerability. The LSTM-based self-learning model in [10] lacked robustness in the presence of sparse data and further disregarded collaborative features or spatial features to improve generalizability. This highlights a key research gap in incorporating graph-based learning or hybrid sequential-spatial architectures that could better capture vehicular mobility dependencies. Even TH-GAT in [11] found it particularly challenging to detect Sybil nodes during Silent Attack phases and did not make use of multi-source information, thus limiting its adaptability. Finally, the GBEHO-DNN framework in [3] combined a routing algorithm, the Floyd–Warshall algorithm, and modified AES, but the hybrid framework posed exhaustive computational requirements for OBUs and would not be less than challenging to facilitate real-time applications in scenarios with limited computing resources. Lightweight model compression and edge-computing integration could be future directions for addressing this limitation. The ABESO framework proposed in [24] was not tested for scalability under real-world, large-scale VANET conditions. The DRL-based system in [30] had excessive training time and lacked explainability, which could lead to low adoption rates in safety-critical VANET-based applications.

The problems encountered by ML techniques are explained below. The MDFD method in [14] had behavior-based Sybil attack detection and only used identity-based detection, which limited its accuracy in dynamic environments. Incorporating ensemble learning with contextual behavioral features such as velocity fluctuations or trust scores could improve adaptability. The collaborative learning method in [15] did not use multi-mode features like voice or movement patterns, which could have increased detection accuracy. This points to the necessity of integrating multimodal fusion techniques to enhance robustness against adaptive Sybil behaviors.

The problems encountered by signal processing techniques are discussed as follows: The LSDCN approach in [1] was not evaluated in a highly dense urban context, which restricted the evaluation of performance in the presence of extreme network congestion. This gap highlights the importance of conducting stress tests in large-scale, real-time VANET scenarios to ensure detection reliability. The CSI in [16] was not tested against adaptive attackers based on potential signal obfuscation techniques, which reduced its robustness in an adversarial container. Future work should emphasize adversarial testing environments to ensure resilience against sophisticated attackers. The INTERLOC method in [17] lacked evaluation in real-world environments across hardware platforms and did not consider signal variation due to mobility. Hence, hardware-in-the-loop testing and mobility-aware calibration mechanisms are necessary to make such schemes practical. The PCISAD scheme in [18] provided no measures against environmental noise nor considered concurrent Sybil attackers using power control strategies. Also, all three methods did not include multi-modal data or cross-validation via a large-scale real-world study of VANETs. Therefore, integrating cross-layer data and validating on standardized vehicular datasets remain critical unexplored directions.

The problems encountered by protocol-based techniques are discussed as follows: The approach in [19], based on EPORP, was not validated using real-world VANET datasets, limiting its applicability beyond simulations. This demonstrates the pressing need to move beyond synthetic environments and test detection schemes on live vehicular testbeds. The key management scheme in [20] studied a hierarchical manner and did not evaluate scalability in large-scale VANETs where both the number of vehicles is bounded and the density is high. The Beacon-packet-based detection and traceability method in [21] used beacon packets and assumed full RSU coverage, which would not be realistic in sparse or rural environments. The privacy-aware detection scheme in [22] did not determine how well the trust model managed colluding Sybil nodes or dynamic vehicle behaviors. This omission suggests a gap in designing resilient reputation systems capable of handling collusion and rapidly evolving Sybil identities.

6. Results and Analysis

This section contains the overall assessment of various techniques of Sybil attack detection in VANET, concerning tools, publication dates, parameters, datasets, and performance metrics. Each technique is evaluated thoroughly, and the validation results are showcased beneath.

6.1 Analysis Based on Techniques

The techniques employed for Sybil attack detection in VANET comprise ML, DL, signal processing, protocol, and other detection techniques. The Analysis of various Sybil attack detection techniques is showcased in Fig. 3. In this survey paper, 6 DL techniques, 3 ML techniques, 4 signal processing techniques, 4 protocol-based techniques, and 8 other techniques are utilized for Sybil attack detection in VANET. DL techniques are the most employed technique for the Sybil attack detection in VANET. This observation highlights the growing shift in VANET security research toward data-driven and adaptive detection approaches, as DL frameworks are capable of handling large-scale, high-dimensional vehicular data streams more effectively than classical methods.

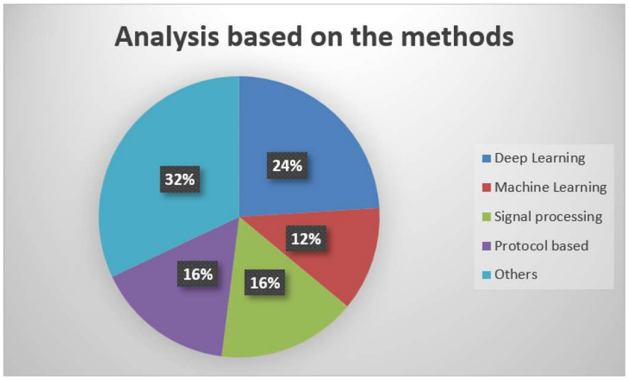

Fig. 3. *Evaluation of Sybil attack detection techniques*

6.2 Estimation Based on Tools

Fig. 4 represents the analysis of Sybil attack detection based on various tools. The tools employed for implementing the various methods for Sybil attack detection are C++, Python, MATLAB, Network Simulator (NS) -3, Simulation of Urban Mobility (SUMO) and NS2, Vein, and OMNeT++. Among these, NS2 and NS3 remain the most frequently adopted tools due to their flexibility in simulating vehicular mobility, communication protocols, and large-scale network environments. They provide a well-established platform for evaluating VANET-specific scenarios under controlled conditions.

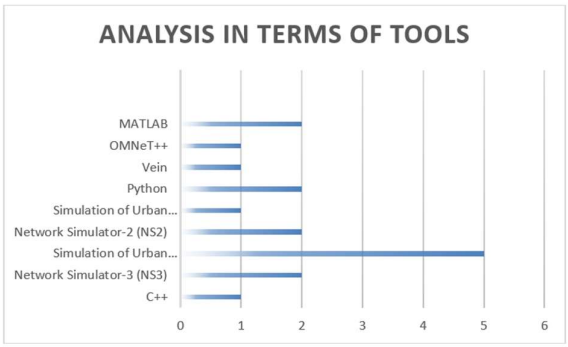

Fig. 4. *Analysis based on tools*

6.3 Evaluation Based on Publications

The analysis shows that most of the works are from 2024, which consists of seven papers, four papers from 2025, and five papers from 2023. Three papers each came from research papers published in 2022 and 2020, and one paper each came from 2021, 2019, and 2018. Fig. 5 demonstrates the evaluation of research papers based on the published years. This distribution highlights a clear upward research trend in recent years, with a peak in 2024, reflecting the growing urgency to address Sybil attack threats in VANETs as intelligent transportation systems mature.

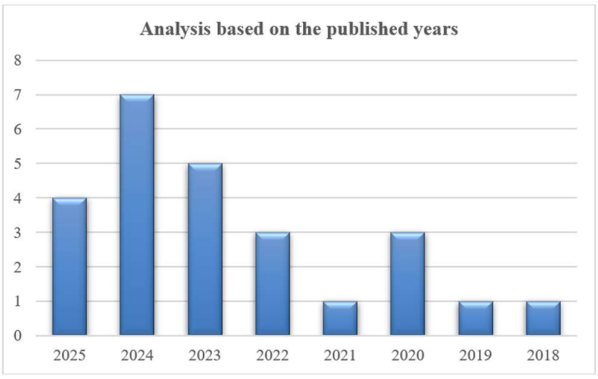

Fig. 5. *Evaluation based on published years*

6.4 Validation Based on Datasets

The datasets utilized by various Sybil attack detection techniques in VANET include the VeReMi Extension Dataset, VeReMi Dataset, and the Sybil attack detection dataset. The VeReMi Extension Dataset is the most commonly used dataset for Sybil attack detection in VANET and was used in 3 papers, while the Sybil attack detection dataset was used in 2 works and the VeReMi Dataset was used in 1 paper. Most of the works considered the simulation of the VANET framework. Fig. 6 represents the estimation of Sybil attack detection techniques based on various datasets. The frequent use of the VeReMi Extension Dataset highlights its adaptability and comprehensiveness, as it includes diverse attack scenarios and realistic mobility traces that are highly relevant to Sybil attack evaluation.

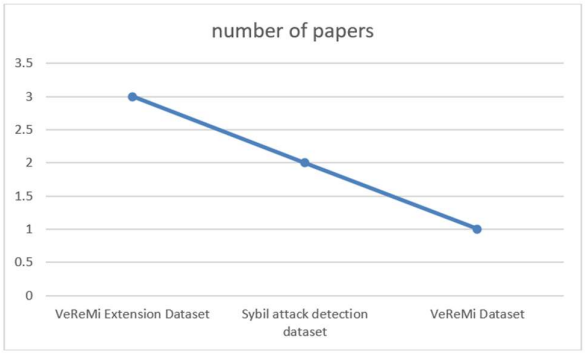

Fig. 6. *Validation based on datasets*

6.5 Exploration Based on Evaluation Metrics

The section presents an analysis of various measures from 25 studies aimed at Sybil attack detection in VANET. Table 1 classifies these studies depending on the order of performance metrics, such as Accuracy, Recall, Precision, Detection rate (DR), False Positive Rate (FPR), F1-Score, False Negative Rate (FNR), Security analysis, Sensitivity, Specificity, Delay, Threshold, Encryption time, Computation cost, Receiver operating characteristic curve (ROC-curve), Packet loss, False Detection Rate (FDR), Delivery ratio, Detection delay, Decryption, Throughput, Mathew Correlation Coefficient (MCC), Positive Predictive Value (PPV), Negative Predictive Value (NPV), Communication cost, Communication overhead, storage cost, Detection time, Average end-to-end delay, Average Energy Consumption, Average network throughput, Miss Detection Rate (MDR), Classification accuracy, Message delay, and True Positive Rate (TPR) are analyzed. From the analysis, it is found that accuracy and recall are the two metrics mostly employed for Sybil attack detection systems in VANET. This preference for accuracy and recall underscores the priority of correctly identifying malicious Sybil nodes while minimizing false alarms, as both are critical to maintaining vehicular safety and trustworthiness in real-time applications.

Table 1. *Exploration based on evaluation metrics*

Evaluation metrics	Published Paper
Accuracy	[5], [3], [9], [14], [15], [24], [25], [12], [28], [13]
Recall	[3], [9], [14], [15], [24], [25], [21], [28], [29], [13]
Precision	[3], [9], [14], [15], [25], [21], [28], [29], [13]
Detection rate (DR)	[1], [10], [11], [16], [23], [17], [12], [26]
False Positive Rate (FPR)	[1], [16], [17], [18], [12], [26], [13]
F1-score	[3], [9], [25], [28], [13]
False Negative Rate (FNR)	[15], [12], [26], [13]
Security analysis	[3], [20], [27]
Sensitivity	[24], [12]
Specificity	[9], [12]
Delay	[5], [19]
Threshold	[16], [17]
Encryption time	[3] [19]
Computation cost	[20], [27]
Receiver operating characteristic curve (ROC-curve)	[15], [18]
Packet loss	[5], [19]
False Detection Rate (FDR)	[10], [11]
Delivery ratio	[19]
Detection delay	[1]
Decryption	[19]
Throughput	[19]
Mathew Correlation Coefficient (MCC), Positive Predictive Value (PPV), Negative Predictive Value (NPV),	[12]
Communication cost	[27]
Communication overhead, storage cost	[20]
Detection time	[21]
Average end-to-end delay, Average Energy Consumption, Average network throughput	[30]
Miss Detection Rate (MDR)	[13]
Classification accuracy	[18]
Message delay	[27]
True Positive Rate (TPR)	[18]

7. Conclusion

This survey consists of several Sybil attack detection techniques in VANETs that include ML, DL, signal processing, protocol-based, and other techniques to detect a Sybil attack. These papers are analyzed from prominent academic publishers like Elsevier, Springer, MDPI, Wiley Online Library, Taylor and Francis, and IEEE. The study points out the research gaps and limitations encountered in Sybil attack detection in VANET and analyzes these techniques by utilizing various factors like tools, publication year, datasets, and evaluation metrics. The comparative review highlights that while DL-based techniques show promising improvements in adaptability and accuracy, they often require heavy computational resources, making them less practical in real-time vehicular environments without optimization. Most of the papers reviewed are from 2024, with NS-2 being the predominant tool employed for Sybil attack detection. Accuracy is the most commonly utilized evaluation metric for evaluating the effectiveness of the Sybil attack detection systems. Moreover, these techniques lacked adaptability to dynamic environments and failed to take responsibility for the attacks that occur in the evolving environment. Future research should also consider cross-layer detection mechanisms, hybrid approaches combining cryptography with ML/DL, and privacy-preserving models to strengthen trust in VANET communications. The future enhancements should focus on creating more lightweight, scalable, easy-to-interpret models for the detection or prevention of a Sybil attack that consider real data with real mobility patterns, guaranteed privacy, and detection in real time, to begin an effective method for enhancing security in VANETS.

Compliance With Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] 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.

[2] Z. A. Abdulkader, A. Abdullah, . M. T. Abdullah and Z. A. Zukarnain, "A survey on sybil attack detection in vehicular ad hoc networks (VANET)," *Journal of Computers,* vol. 29, no. 2, pp. 1-6, 2018.

[3] K. N. U. A. S. S. Jacob, G. . B. S. S and M. S. P. Balaji, "Floyd–Warshalls algorithm and modified advanced encryption standard for secured communication in VANET," *Measurement: Sensors,* vol. 27, p. 100796, 2023.

[4] K. Liu, J. Deng, P. . K. Varshney and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE transactions on mobile computing,* vol. 6, no. 5, pp. 536-550, 2007.

[5] S. S. Sefati and S. G. Tabrizi, "Detecting sybil attack in vehicular ad-hoc networks (vanets) by using fitness function, signal strength index and throughput," *Wireless Personal Communications,* vol. 123, no. 3, pp. 2699-2719, 2020.

[6] M. Kabbur and D. V. . A. Kumar, "MAR_Sybil: Cooperative RSU based detection and prevention of Sybil attacks in routing process of VANET," in *In Journal of Physics: Conference Series*, 2020.

[7] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang and X. Zhou, "On secure and privacy-aware sybil attack detection in vehicular communications," *Wireless personal communications,* vol. 77, no. 4, pp. 2649-2673, 2014.

[8] J. J.Q. and Y. , "Sybil attack identification for crowdsourced navigation: A self-supervised deep learning approach," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 7, pp. 4622-4634, 2020.

[9] N. C. Velayudhan, A. . A. and M. Madanan, "Sybil attack detection and secure data transmission in VANET using CMEHA-DNN and MD5-ECC," *Journal of Ambient Intelligence and Humanized Computing,* vol. 14, no. 2, pp. 1297-1309, 2023.

[10] Y.-Y. Zhang, J. Shang, X. Chen and K. Liang, "A self-learning detection method of Sybil attack based on LSTM for electric vehicles," *Energies,* vol. 13, no. 6, p. 1382, 2020.

[11] Y. Chen , Y. Lai and C. Zeng, "Sybil attack detection and traceability scheme based on temporal heterogeneous graph attention networks," *Journal of Network and Computer Applications,* p. 104261, 2025.

[12] M. Ajin and R. Shaji, "Enhancing Security in Vanets: Adaptive Bald Eagle Search Optimization Based Multi-Agent Deep Q Neural Network for Sybil Attack Detection," *Vehicular Communications,* p. 100928, 2025.

[13] R. Sultana, M. Tripathi, J. Grover and P. Sharma, "Intelligent defense strategies: Comprehensive attack detection in VANET with deep reinforcement learning," *Pervasive and Mobile Computing,* vol. 103, p. 101962, 2024.

[14] . 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," *Computer Networks,* vol. 224, p. 109608, 2023.

[15] S. Azam, M. Bibi, R. Riaz, S. S. Rizvi and S. J. Kwon, "Collaborative learning based sybil attack detection in vehicular ad-hoc networks (vanets)," *Sensors,* vol. 22, no. 18, p. 6934, 2022.

[16] H. T. Bugra and C. E. Koksal, "Sybil attack detection based on signal clustering in vehicular networks," *IEEE Transactions on Machine Learning in Communications and Networking,* vol. 2, pp. 753-765, 2024.

[17] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang and X. Zhou, "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, 2018.

[18] Y. Yao, B. Xiao, G. Yang, Y. Hu, L. Wang and X. Zhou, "Power control identification: A novel Sybil attack detection scheme in VANETs using RSSI," *IEEE Journal on Selected Areas in Communications,* vol. 37, no. 11, pp. 2588-2602, 2019.

[19] N. C. Velayudhan, D. A. Anitha and M. Madanan, "Sybil attack with RSU detection and location privacy in urban VANETs: An efficient EPORP technique," *Wireless Personal Communications,* vol. 122, no. 4, pp. 3573-3601, 2022.

[20] E. Funderburg and I.-Y. Lee, "A privacy-preserving key management scheme with support for sybil attack detection in VANETs," *Sensors,* vol. 21, no. 4, p. 1063, 2021.

[21] 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, p. 2153, 2024.

[22] M. Parham, A. A and P. , "An effective privacy-aware Sybil attack detection scheme for secure communication in vehicular ad hoc network," *Wireless Personal Communications,* vol. 113, no. 2, pp. 1149-1182, 2020.

[23] R. Sultana, J. Grover and M. Tripathi, "Cooperative approach for data-centric and node-centric misbehavior detection in VANET," *Vehicular Communications,* vol. 50, p. 100855, 2024.

[24] U. Bhanja, A. Majhi, S. Sahoo and D. Parida, "Detection of Sybil & DDoS attacks in VANET using intelligent technique," *International Journal of Computers and Applications,* vol. 46, no. 10, pp. 811-829, 2024.

[25] R. Sultana, J. Grover and M. Tripathi, "LA-DETECTS: Local and Adaptive Data-Centric Misbehavior Detection Framework for Vehicular Technology Security," *IEEE Open Journal of Vehicular Technology,* 2024.

[26] M. Baza, M. Nabil, N. Bewermeier, K. Fidan , M. Mahmoud and M. Abdallah, "Detecting sybil attacks using proofs of work and location in vanets," *IEEE Transactions on Dependable and Secure Computing,* vol. 19, no. 1, pp. 39-53, 2020.

[27] Z. Man, S. Pan, Z. Xu and M. Ye, "Strong anonymous batch authentication scheme against sybil attack in VANET," *Wireless Networks,* pp. 1-22, 2025.

[28] M. Kishore, V. G. Kumar and B. Nancharaiah, "Secure lightweight digital twin (DT) technology for seamless wireless communication in vehicular ad hoc network," *Computers and Electrical Engineering,* vol. 123, p. 110291, 2025.

[29] Z. Zhang, Y. Chen, Y. Lai, J. Wei and Y. Wang, "Detection method to eliminate Sybil attacks in Vehicular Ad-hoc Networks," *Ad Hoc Networks,* vol. 141, p. 103092, 2023.

[30] N. Hussain, P. Maheshwari, P. S. Kumar and A. Singh, " Attack resilient and efficient protocol based on greedy perimeter coordinator routing—mobility awareness for preventing the attack in the VANET," *Wireless Personal Communications,* vol. 126, no. 4, pp. 2841-2868, 2022.