Dicle University
Journal of Engineering

https://dergipark.org.tr/tr/pub/dumf
duje.dicle.edu.tr

Research Article

A better way to detect sybil attacks in vehiuclar ad hoc networks

Ziya Cihan TAYŞİ[1*]

[1] Yıldız Technical University, Department of Computer Engineering, cihan@yildiz.edu.tr, Orcid No: 0000-0003-3916-7492

ARTICLE INFO

Article history:

Received 3 November 2024
Received in revised form 9 January 2025
Accepted 9 January 2025
Available online 26 March 2025

Keywords:

Sybil Attack, Inter Vehicle Communication (IVC), Received Signal Strength Indicator (RSSI), Deep Learning

Doi: 10.24012/dumf.1578650

* Corresponding author

ABSTRACT

Sybil attacks, enabled by the anonymous nature of peer-to-peer broadcast communication in vehicular private networks (VANETs), pose a serious security threat. These attacks can significantly disrupt traffic flow, reduce efficiency, and potentially endanger traffic safety. Detecting Sybil attacks in VANETs is particularly challenging due to the dynamic network topology, real-time constraints of applications, and decentralized nature of these networks. This paper proposes a novel Sybil attack detection method for VANETs, leveraging deep learning analysis of received signal strength indicator (RSSI) time series. The proposed system is designed to deliver effective results, even in brief interactions. Experimental results demonstrate the efficacy of our LSTM-based and CNN-based approaches, achieving 93.45% and 94.28% sensitivity in detecting attack messages, respectively.

Introduction

A sybil attack [1] involves an attacker using multiple identities simultaneously to gain an advantage in a distributed computing system, which can be encountered in many fields of computer science. These attacks are particularly effective in peer-to-peer communication environments where real-time authentication processes are absent. Many Vehicle-to-Everything (V2X) applications rely on the cooperation between vehicles on broadcast messaging namely, Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs). An attacker performing a sybil attack on VANET can manipulate traffic flow as desired or potentially create risky situations that threaten traffic safety. For example, fabricating accident reports or slow traffic situations can prevent other vehicles from using a particular route. Moreover, generating messages containing false position, speed, and acceleration information may endanger nearby vehicles. A sybil attack example of traffic manipulation is given in Figure 1.

There are two main approaches for detecting sybil attacks in VANET, namely, proactive and reactive. Proactive methods mainly rely on the use of PKI-authorized certificates and preventing the use of multiple certificates simultaneously. The use of proactive methods is quite challenging due to the rapidly changing topology and real-time requirements of safety applications VANET. For example, a PKI-based solution requires periodic certificate updates, rendering them unsuitable for environments where network access to a central authority is unavailable. Furthermore, the latency caused by certificate validation and update procedures may cause the received information to become obsolete for time-critical applications.

On the other hand, reactive methods use the Misbehavior Detection System (MDS), similar to the Intrusion Detection Systems (IDS) used in traditional networks. MDS detects attackers by analyzing messages, vehicle status, and the properties obtained from the characteristics of the received packets. Depending on the capabilities of the used hardware, these properties include Time of Arrival (ToA), Angle of Arrival (AoA), Time Difference of Arrival (TDoA), and Received Signal Strength Indicator (RSSI). Properties such as ToA, AoA, and TDoA can only be obtained using special hardware, which results in higher costs in a large-scale deployment. Thus, the default hardware configuration for IVC systems only provides RSSI value for received packets.

RSSI readings can provide information about the sender's position and identity [2],[3]. However, environmental features, such as buildings, street width, and other vehicles, can affect the RSSI values obtained. Moreover, attackers can manipulate the RSSI readings of ghost vehicles by changing the output power. Furthermore, packet losses due to collusion are possible in areas with heavy vehicle traffic. Therefore, these situations should be considered in methods where RSSI readings are used to detect sybil attacks.

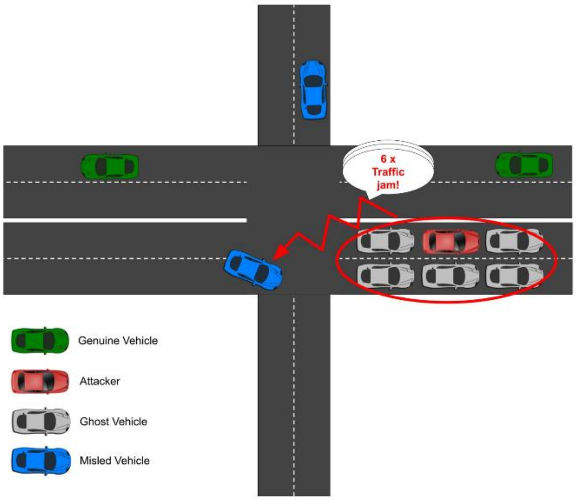

Figure 1. A sybil attack scenario in a VANET, where an attacker forges multiple identities to create a false traffic congestion.

Our literature review and experiments have revealed that existing studies on sybil attack detection methods that use reactive approaches are quite limited for realistic vehicular traffic environments. The studies [4], [5] are mostly based on datasets generated via simulations with minimal traffic density or specific scenarios such as highways. A dataset or sybil attack detection method targeted for highway traffic scenarios may not reflect situations that occur in daily life. For example, vehicles stuck in traffic jams lead to packet collisions or losses. Also, differences in the road patterns in urban areas compared to highways cause vehicles to move in different directions, speeds, and angles, which creates extreme differences in mobility patterns compared to highway scenarios.

In this work, we propose a fast sybil attack detection method that achieves high success in comprehensive sybil attack scenarios. Our sybil attack detection method works locally using a precomputed deep learning model on vehicles without requiring a consistent connection to the central authority. The model classifies messages by examining RSSI measurements. The main contributions of this paper are as follows:

- We developed a deep learning model that detects sybil attacks using RSSI as a sequence.

- We experimented with two deep learning models, namely Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN).

- We compared our method with the methods in the literature over various mobility and distance situations in vehicle traffic.

The rest of the paper is organized as follows. In the following section, previous work on sybil attack detection methods is summarized. Materials and methods section describes the dataset, and explains the implementation details of existing methods along with our proposed deep learning models. In result section, details of the experiment set and parameters are given, and the results are examined. Finally, conclusions and future work are outlined in the final section.

Related work

Sybil attacks present a significant challenge in VANETs. In sybil attack, a malicious node creates numerous false identities, aiming to disrupt communication or gain influence in the network. To counter this threat, diverse sybil attack detection approaches have been explored in literature, including techniques based on packet inspection [6],[7], location proofs with Road Side Units (RSUs) [8] or 5G [9], and the analysis of physical signal attributes of DSRC [10]. This section specifically focuses on methods that leverage Received Signal Strength Indicator (RSSI).

Yu et al. proposed a method [11] for detecting sybil attacks that relies on cooperative location verification among vehicles traveling in opposite directions. In this method, vehicles gather position certifications from roadside base stations and signal strength measurements from nearby vehicles to validate the positions of other vehicles. However, this method is primarily designed for highway traffic flow, where vehicles have consistent movement patterns in both directions. This requirement might significantly limit its effectiveness in urban traffic, where traffic flow is multidirectional.

Garip et al. proposed INTERLOC[2], an RSSI-based method for both localization and sybil attack detection that dynamically adapts to interference levels. In this method, vehicles use RSSI values to estimate their distances, cooperatively share estimated distances for position validation, and exchange parameters for distance calculation to learn interference levels. However, the method's performance relies on the predefined radio propagation model accurately matching the environment. It has been shown that the method's performance decreases when there is a change in the propagation model [10].

Yao et al. proposed Voiceprint [3], a sybil attack detection method that analyzes the similarity of RSSI time series data obtained from V2V messages. It aims to match the sybil vehicles of the same attacker by comparing the similarity of the characteristic fluctuations in their RSSI time series, treating these patterns like unique fingerprints. However, this method is susceptible to manipulation by attackers who intentionally change their transmit power, leading to altered RSSI patterns and potentially compromising detection accuracy. In [4], the authors extended Voiceprint with a time-series change-point detection method and examined five potential power control patterns that could be used in sybil attacks. They proposed a power control identification method [10] for sybil attack detection, which uses support vector machines (SVM) classification to distinguish sybil nodes from normal nodes. However, these methods were tested on a very sparse simulation area, and the method requires each vehicle to send 200 packets during the SCH period. Successful transmission of 200 messages in 50 ms in dense deployment will not be possible due to interference and collisions.

Rakhi et al. proposed a sybil attack detection method [5] that leverages the Longest Common Subsequence (LCSS) algorithm to analyze the similarity of RSSI time series. This approach shares conceptual similarities with the work in [10], which also employs time series similarity analysis and change-point detection techniques. However, a key distinction is the use of LCSS instead of Dynamic Time Warping (DTW), aiming to lower computational cost. Additionally, the method utilizes a clustering technique where the Cluster Head (CH) executes the LCSS algorithm and calculates the similarity index. Furthermore, it leverages standard 10Hz CCH messages, rather than relying on custom 200 Hz test packages. However, an important consideration is that the LCSS algorithm requires categorical values. Therefore, a method is needed to quantize the floating-point RSSI to use as categorical values without lowering the method's accuracy. Additionally, time series similarity-based detection could produce false positives in multidirectional urban traffic since multiple legitimate vehicles exhibiting similar mobility patterns relative to the observer could be misclassified as sybil nodes.

Ercan et al. [12] proposed a machine learning approach to detect position falsification attacks, leveraging two novel features: Angle of Arrival (AoA) and estimated RSSI distance extracted from the VeReMi dataset. However, a critical limitation is that the AoA calculations rely on exact position values from the dataset rather than simulating the inherent uncertainties and potential errors of real-world signal reception.

The availability of publicly accessible datasets and frameworks for sybil attack detection is limited in the literature. The Vehicular Reference Misbehavior Dataset (VeReMi) [13] is the first public dataset for evaluating misbehavior detection mechanisms in VANET. VeReMi is created with the Veins simulation environment [14]. It contains message logs, RSSI values of captured messages and receiving vehicles' mobility information. In addition to the genuine messages, the dataset contains malicious messages that misbehavior detection methods aim to detect. Kamel et al. proposed the VeReMi Extension dataset [15] and extended VeReMi by adding realistic sensor error models [16] and a new set of attacks, including Sybil attacks. However, the VeReMi Extension dataset is quite limited in terms of both map area and traffic density, covering a 1.6 km^2 area with 67.4 Veh/km^2 peak traffic density. Additionally, it utilizes 1 Hz broadcast frequency, which may not suitable for existing methods that rely on time-series analysis techniques like those proposed by Yao et al.[3],[4].

While numerous approaches leverage RSSI measurements to address sybil attacks in VANETs, existing methods often lack applicability across diverse traffic scenarios, such as urban and highway environments. The scarcity of comprehensive, realistic datasets further hinders the development and evaluation of robust detection mechanisms. This underscores the need for an adaptable sybil attack detection method effective in real-world VANET deployments. A comparison of these existing RSSI-based approaches is provided in Table 1.

Table 1. Summary of existing RSSI-based methods

Paper	Accuracy	Limitations
[2]	%87	- Vulnerable to intelligent Sybil attacks
[3]	<%90	- Accuracy decreases dramatically when the vehicle density increases - Vulnerable to intelligent Sybil attacks
[4]	%96.5 - %97.4	- not suitable for dense networks - creates network overhead, since it requires transmission of 200 messages
[5]	%92 - %98	- not suitable for dense networks - creates overhead in network
[12]	%93.02 - %95.04	- requires extra hardware - uses synthetic AoA values which increases accuracy

Material and methdos

In VANET environments, vehicles rapidly exchange critical mobility data (position, speed, acceleration, lane information) under strict time constraints. Due to the maximum broadcast frequency of 10 Hz specified by both the European Telecommunications Standards Institute (ETSI) [17] and The Society of Automotive Engineers (SAE) [18], sybil attack detection algorithms must operate efficiently to analyze messages within this limited window. In order to address this challenge, our work explores leveraging RSSI for rapid sybil attack detection. We propose a sequential deep learning-based sybil attack detection method that utilizes RSSI time series analysis to identify suspicious message patterns indicative of attackers.

The remainder of this chapter provides details of the key components of our sybil attack detection methodology, including the attacker model, dataset characteristics, feature engineering techniques, and implementation specifics.

Attacker model

There are various ways to carry out a sybil attack described in the literature [1], [4], [19]. In a sybil attack, an attacker can manipulate two properties: the content of the message and its transmission power. The forged message content can be generated with random values, as a grid pattern in a selected region, or replayed values of the captured messages of the genuine vehicles. Power control schemes used in sybil attacks can be classified into three categories: no manipulation, where the attacker maintains a constant power level; random variations, where the attacker's power level changes unpredictably; and predefined patterns [4], where the attacker follows specific power patterns, such as rectangular, stairs, or sawtooth waves. To address these attack types, in this work, we used a dataset that contains 20 distinct attack types, including four sybil attack methods and five power control methods.

Dataset and input preparation

To develop and evaluate our sybil attack detection method, we created a comprehensive VANET dataset using the SUMO [20] and Veins [21] simulators. We followed the dataset generation approach outlined in the VeReMi dataset [13], combined with the F2MD simulation model [6] to ensure consistency with established benchmarks. Our dataset presents significantly heavier traffic conditions than existing public datasets [6], [15], offering a more challenging and realistic environment for rigorously evaluating detection methods. Unlike VeReMi-Extension dataset [15], we have implemented RSSI recording in our simulation, which provides valuable data for sybil attack detection techniques. The source code of the simulation environment and the dataset is available on the GitHub repository [22]. Detailed statistics for the subsection of the dataset used in this study are given in Table 2.

Table 2. Summary of dataset properties.

Property	Value
Dataset size	820 GB
Simulation area	11.2 km^2
Simulation time	25 minutes
Beaconing rate	10 Hz
Peak density	164.73 Veh/km^2
Genuine vehicle	7,876
Ghost vehicles	652
Received genuine messages	849,231,132
Received attack messages	84,997,919
Transmitted genuine messages	21,112,206
Transmitted attack messages	2,003,527

In VANETs, inspection of raw features like location, speed, and acceleartion within a single message is inadequate for robust sybil attack detection due to their susceptibility to manipulation. To overcome this limitation, examining vehicle behavior over time offers a more reliable approach. One method, proposed by Yao et al. [3], involves comparing message sequences between vehicles to identify abnormal similarities in patterns, suggesting potential sybil attacks where attackers forge multiple identities with identical behavior. Alternatively, a behavioral profile can be established for each vehicle based on its individual message sequence, with deviations from this profile indicating potential attacks as a vehicle's behavior may change significantly due to malicious intent.

The sequence learner we use in our study aims to detect RSSI patterns in consecutive message sequences. The formula of the extracted features is given in (1).

$$RSSISequence = \{r_1, r_2, r_3, \dots, r_N\} \qquad (1)$$

The N parameter represents the processed message count. In our work, we used N as 20, which are captured within 2 seconds of vehicle interaction at a 10 Hz messaging rate. Earlier works [3], [4] requires 200 RSSI samples, which corresponds to 20 seconds of vehicle interaction.

Implementation of the methods

This section describes the implementation details and changes on existing methods, namely, Voiceprint and Power Control Identification along with the propsed LSTM and CNN based methods.

Voiceprint [3] and Power Control Identification [4] methods use the last N packets from vehicles to check whether messages belong to the same vehicle or use power control. However, it is not possible to compare these methods directly with our study because they require the use of the Service Channel (SCH) at 200 Hz frequency. For this reason, these methods were slightly modified to detect the individual attack packages to compare with our study.

Voiceprint uses the similarity between two vehicles by comparing RSSI time series to detect sybil attacks. As in the original method [3], the implementation calculates distances of every 200 samples long RSSI series received from nearby vehicles in the 20s detection period with dynamic time warping (DTW). RSSI series whose similarity level is more than the threshold determined using Linear Discriminant Analysis (LDA) are marked as belonging to the sybil vehicle. Unlike the original study, we do not filter detected sybil nodes for the next detection period to detect messages belonging to the attackers instead of ghost vehicles.

The primary purpose of the Power Control Identification method is to detect power level changes in attack messages, which are caused by output power changes made by the attacker to mislead Voiceprint. As in the original method [4], our implementation uses two features of the RSSI series, namely, the average number of change points and the cumulative average variation of segment means. The SVM classifier determines the decision boundary between the RSSI series belonging to the attackers and the genuine vehicles. While the original method proposes four schemes, our implementation only includes two schemes that use the Control Channel (CCH). The other two schemas require the SCH usage at 200 Hz frequency, which is not implemented in our dataset.

LSTM networks are a special type of Recurrent Neural Network (RNN) designed to handle long-term dependencies in sequential data. Unlike traditional feedforward networks, LSTMs have the ability to use information from past inputs when processing current input. This makes LSTMs well-suited for analyzing temporal dependencies such as time series. In our study, we leveraged this capability of LSTMs to analyze RSSI information obtained from individual vehicle messages, treating each vehicle's sequence of messages as a one-dimensional time series. Figure 2 shows the LSTM model used in our study.

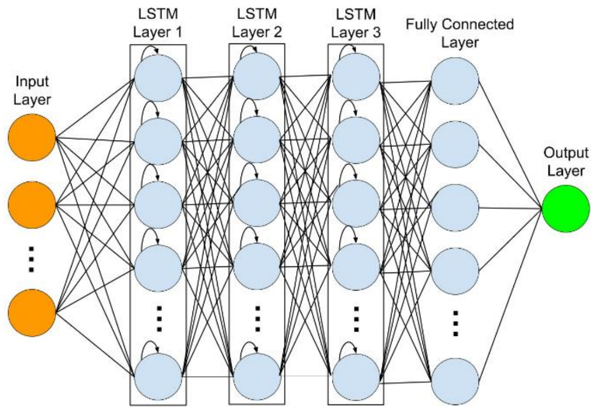

Figure 2. The 3-layer LSTM model.

Our LSTM model consists of three LSTM layers, each with 32 units, followed by dropout layers with a probability of 0.2 to prevent overfitting. The final layer is a fully connected dense layer with 256 units, which serves as the classifier for sybil attack detection.

CNN is a special type of deep neural network that is talented at processing data with a grid-like structure, such as images. CNNs can adapt to process time series by using 1D convolutions instead of the typical 2D convolutions used in image processing. Using 1D filters slide along the temporal dimension allows the network to learn local patterns within the time series. CNNs can also learn broader patterns by reducing dimensions using multiple layers and downsample methods such as pooling.

Like the LSTM model, our CNN based approach uses a one-dimensional time series of RSSI values as input. The architecture of our CNN model shown in Figure 3 incorporates three 1D convolutional layers with increasing filter counts: 128, 256, and 512. Each convolutional layer uses a kernel size of 3. To reduce dimensionality and prevent overfitting, max pooling layers with a pool size of 2 and dropout layers with a dropout probability of 0.2 are applied between each convolutional layer. A fully connected layer with ReLU activation precedes a sigmoid-activated output layer, which performs binary classification for sybil attack detection.

Results

This section provides a comprehensive evaluation of our proposed RSSI sequence-based sybil attack detection method.

Experimental setup

The proposed method was evaluated using a continuous 1000 second long segment extracted from the high-density partition of our custom dataset, as described in the previous section. To rigorously assess performance across the entire 1000-second segment and mitigate potential biases introduced by a single dataset split, 5-fold cross-validation was employed. Due to the dataset's extensive size, model training was conducted on a randomly selected 2.5\% sample from each training fold within the cross-validation process.

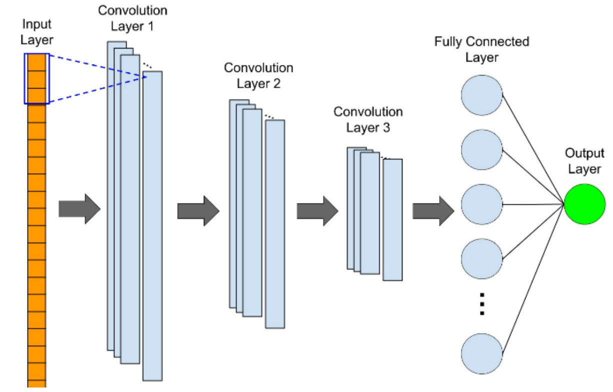

Figure 3. The 3-layer CNN model

Given the broadcast nature of VANETs, where multiple vehicles capture the same message, we employed temporal partitioning within the cross-validation process, as shown in Figure 4. This approach ensured that identical messages did not appear in both training and test sets within each fold, thus reducing the risk of memoization. Specifically, the dataset was divided into 10-second partitions. Training and test segments were selected from these partitions to be as contiguous as possible, with 10-second buffers inserted between them to ensure strict separation.

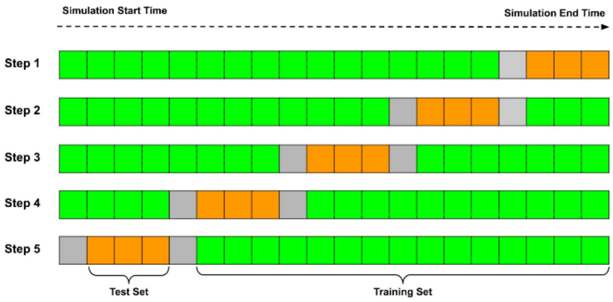

Figure 4. The dataset partitioning and 5-fold cross-validation scheme which used for prevent overfitting.

Metrics

In the context of evaluating sybil attack detection at the individual message level, a true positive (TP) represents an attacker-generated message correctly classified as an attack. A false positive (FP) refers to a legitimate message from a genuine vehicle that is incorrectly classified as an attack. A false negative (FN) represents an attacker-generated message that the detection method fails to identify.

To thoroughly evaluate our sybil attack detection method, we employed the widely accepted metrics of precision, recall, and F1 score, grounded in these TP, FP, and FN classifications. Precision quantifies the accuracy of the model in identifying attacker-generated messages, measuring the proportion of correctly classified attacker messages out of all messages flagged as such. Recall (sensitivity) assesses the model's ability to detect all attacker-generated messages, representing the proportion of true attacker messages correctly identified. The F1 score, a harmonic mean of precision and recall, provides a balanced assessment of the model's overall performance in both accurately identifying attacker messages and minimizing false alarms.

Performance evalutation

Table 3 provides a comparative analysis of precision, recall, and F1 scores for our proposed LSTM and CNN models alongside the existing Voiceprint and modified PCI techniques.

The results in Table 3 clearly shows our proposed LSTM and CNN models outperform Voiceprint and PCI methods. This is likely due to designs of the existing works originally targeting highway scenarios with sparser traffic conditions and less complex traffic pattern variations compared to our high-density urban dataset.

Additionally, both the original Voiceprint [3] and PCI methods [4] uses 200 samples, which can only be collected through a 20 seconds interaction. However, this is not always possible to due the dynamic nature of the network and packet lossses in dense deployments. In contrast, our work uses only 20 samples which is more likely in such environments. These factors, including the potential impact of sample size on performance, highlight the strengths of our models in adapting to complex urban environments.

Table 3. Sybil attack detection performance comparison of proposed LSTM and CNN models with modified Voiceprint [3] and PCI [4] methods, using a sequence length (N) of 20 for all models.

Model	Precision	Recall	F1-Score
Voiceprint	0.00	0.00	0.00
PCI	82.43	30.57	44.60
LSTM	93.45	64.52	76.33
CNN	94.28	64.66	76.71

Conclusion

Sybil attacks pose a significant threat to the integrity and functionality of VANET. Their ability to disrupt communication, manipulate traffic flow, and even create risky situations to threaten safety necessitates robust detection mechanisms. In this paper, we presented a sybil attack detection method based on sequential deep learning with RSSI readings, evaluated on a heavy traffic urban scenario and compared to existing RSSI sequence-based methods.

Our findings demonstrate that existing RSSI sequence-based methods offer limited accuracy in urban traffic, achieving only 82.43% precision when using message sequences with a length of 20. In contrast, our proposed LSTM and CNN-based deep learning models achieve a superior precision of 93.45% and 94.28%, respectively. This demonstrates that our models significantly outperform existing RSSI sequence-based methods even when utilizing a substantially smaller sequence length.

For future work, we plan to expand our approach by exploring the usage of other features found in CAMs alongside RSSI. This may include information such as signal strength variations, packet timing patterns, or location data. Additionally, we will investigate the extraction of new, more discriminative features to further enhance the accuracy and robustness of our sybil attack detection mechanism.

Ethics committee approval and conflict of interest statement

"There is no need to obtain permission from the ethics committee for the article prepared"

"There is no conflict of interest with any person / institution in the article prepared"

References

[1] B. Hammi, Y. M. Idir, S. Zeadally, R. Khatoun and J. Nebhen, "Is it Really Easy to Detect Sybil Attacks in C-ITS Environments: A Position Paper," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 18273-18287, Oct. 2022, doi: 10.1109/TITS.2022.3165513.

[2] M. T. Garip, P. H. Kim, P. Reiher and M. Gerla, "INTERLOC: An interference-aware RSSI-based localization and sybil attack detection mechanism for vehicular ad hoc networks," 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2017, pp. 1-6, doi: 10.1109/CCNC.2017.8013424.

[3] Y. Yao et al., "Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs," 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, USA, 2017, pp. 591-602, doi: 10.1109/DSN.2017.10.

[4] 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," in IEEE Journal on Selected Areas in Communications, vol. 37, no. 11, pp. 2588-2602, Nov. 2019, doi: 10.1109/JSAC.2019.2933888.

[5] S. Rakhi and K. R. Shobha, "LCSS Based Sybil Attack Detection and Avoidance in Clustered Vehicular Networks," in IEEE Access, vol. 11, pp. 75179-75190, 2023, doi: 10.1109/ACCESS.2023.3294469.

[6] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa and P. Urien, "Simulation Framework for Misbehavior Detection in Vehicular Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6631-6643, June 2020, doi: 10.1109/TVT.2020.2984878.

[7] E. Kristianto, P. Lin, R. Hwang, “Misbehavior detection system with semi-supervised federated learning,” in Vehicular Communications, vol. 41, 2023, doi: 10.1016/j.vehcom.2023.100597.

[8] M. Baza et al., "Detecting Sybil Attacks Using Proofs of Work and Location in VANETs," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 39-53, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2993769.

[9] F. Boeira, M. Asplund, and M. P. Barcellos, “Vouch: A Secure Proof-of-Location Scheme for VANETs,” in Proc. MSWIM '18, Montreal, Canada, 2018, pp. 241-248.

[10] Y. Yao et al., "Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI," in IEEE Transactions on Mobile Computing, vol. 18, no. 2, pp. 362-375, 1 Feb. 2019, doi: 10.1109/TMC.2018.2833849.

[11] B. Yu, C. Xu, B. Xiao, “Detecting Sybil attacks in VANETs,” in Journal of Parallel and Distributed Computing, vol. 73, no. 6, 2013, doi : 10.1016/j.jpdc.2013.02.001.

[12] S. Ercan, M. Ayaida and N. Messai, "New Features for Position Falsification Detection in VANETs using Machine Learning," ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500411.

[13] R. W. Heijden, T. Lukaseder, and F. Kargl, “Veremi : A dataset for comparable evaluation of misbehavior detection in VANETs,” in Proc. SecureComm, Singapore, Singapore, 2018, pp. 318-337.

[14] C. Sommer, R. German and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," in IEEE Transactions on Mobile Computing, vol. 10, no. 1, pp. 3-15, Jan. 2011, doi: 10.1109/TMC.2010.133.

[15] J. Kamel, M. Wolf, R. W. van der Hei, A. Kaiser, P. Urien and F. Kargl, "VeReMi Extension: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9149132.

[16] J. Kamel, A. Kaiser, I. ben Jemaa, P. Cincilla and P. Urien, "CaTch: A Confidence Range Tolerant Misbehavior Detection Approach," 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1-8, doi: 10.1109/WCNC.2019.8885740.

[17] Intelligent Transport Systems; Vehicular Communications; Basic Set of Applications; Part2 : Specification of Cooperative Awareness Basic Service, ETSI EN 302 637-2, 2014

[18] SAE Surface Vehicle Standard, J2735, 2020

[19] J. Kamel, I. B. Jemaa, A. Kaiser, L. Cantat and P. Urien, "Misbehavior Detection in C-ITS: A comparative approach of local detection mechanisms," 2019 IEEE Vehicular Networking Conference (VNC), Los Angeles, CA, USA, 2019, pp. 1-8, doi: 10.1109/VNC48660.2019.9062831.

[20] German Aerospace Center (DLR) and others. Sumo user documentation. https://sumo.dlr.de/docs/, 2023. [Online; accessed 20-October-2024]

[21] Christoph Sommer. The open source vehicular network simulation framework. https://veins.car2x.org/, 2021. [Online; accessed 20-October-2024]

[22] Istanbul vanet sybil attack dataset. https://github.com/VANET-IstanbulSybil-Attack-Dataset/dataset-src, 2024. [Online; accessed 11-October2023]