I. J. Computer Network and Information Security, **2025, 4, 71-83**
Published Online on August 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2025.04.05

Real-time Sybil Attack Detection Based on Channel Characterization in VANET

Reham Almesaeed
University of Bahrain, College of Information Technology, Bahrain
E-mail: ralmesaeed@uob.edu.bh
ORCID iD: https://orcid.org/0000-0001-7267-3915

Received: 09 December 2024; Revised: 11 February 2025; Accepted: 13 April 2025; Published: 08 August 2025

Abstract: Vehicular Ad hoc Networks (VANETs) are vital for efficient and secure vehicle-to-infrastructure communication in intelligent transportation systems. sybil attacks, where malicious entities adopt multiple identities, are a major security concern in VANETs. Detecting and mitigating these attacks is crucial for ensuring communication reliability and trust. This article focuses on detecting sybil attacks in Vehicle-to-Vehicle (V2V) communication by using a novel mechanism that characterizes the wireless channel through Received Signal Strength Indicator (RSSI) and angular spread in both azimuth and elevation planes. By incorporating angular spread alongside RSSI, the proposed mechanism offers more accurate and robust detection, particularly in dense vehicle environments. Utilizing a precise wireless channel model based on ray tracing statistics, the approach outperforms traditional RSSI-based methods. Experimental results confirm the enhanced accuracy and reliability of the proposed mechanism for detecting sybil attacks in V2V communication scenarios.

Index Terms: VANET, Sybil Attack, RSSI, Channel Profile.

1. Introduction

Vehicular Ad hoc Networks (VANETs) have emerged as a critical component of intelligent transportation systems, enabling efficient and reliable communication among vehicles and infrastructure. However, the presence of sybil attacks poses a severe security threat to the integrity and trustworthiness of VANETs. sybil attacks involve malicious entities creating multiple false identities to disrupt the network's operations and compromise the safety of vehicular communication [1]. Detecting and mitigating sybil attacks in VANETs is of paramount importance to ensure the reliable and secure exchange of critical information among vehicles. Various approaches have been proposed in the literature to address this challenge, such as trust-based, reputation-based, cooperative-based detection approaches [2]. One promising approach being the utilization of channel profiling and Received Signal Strength Indicator (RSSI) analysis. In this approach the signal RSSI and other channel-related characteristics are being exploited to identify sybil nodes [3].

In the context of VANETs, sybil attacks represent a severe security threat stemming from the ability of malicious entities to fabricate multiple false identities within the network. These deceptive nodes can masquerade as legitimate vehicles or infrastructure components, artificially inflating their presence and influence. By creating a multitude of false personas, malicious actors can execute various nefarious activities such as spreading false traffic information, disrupting communication among genuine network participants, launching denial-of-service attacks, or even manipulating routing algorithms to divert traffic or compromise the entire network's functionality. The ramifications of sybil attacks in VANETs are profound. They can lead to traffic congestion, accidents, delays, and even jeopardize the safety of individuals on the road. Moreover, sybil attacks can compromise the trustworthiness and reliability of critical vehicular communication, essential for applications like collision avoidance systems, traffic management, and emergency services coordination. Detecting and mitigating sybil attacks in VANETs is a complex challenge that necessitates robust security mechanisms and protocols [1].

This article presents a novel approach for sybil attack detection in VANETs based on the analysis of the wireless channel profile and RSSI measurements [4]. The wireless channel profile captures the characteristics of the communication channel between vehicles, while RSSI provides valuable information about the signal strength received by each vehicle. By leveraging these two factors, the proposed detection mechanism aims to enhance the accuracy and robustness of sybil attack detection in VANETs. The key contribution of this article lies in the integration of channel profiling and RSSI analysis to detect sybil attacks effectively. By considering the characteristics of the wireless channel,

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

including signal strength variations and channel response patterns, along with the RSSI measurements, the proposed mechanism can differentiate between legitimate vehicles and sybil nodes. This comprehensive approach enables the detection of sybil attacks even in scenarios with dense vehicle populations, where traditional detection methods may encounter challenges. To ensure the accuracy and reliability of the proposed detection mechanism, an accurate wireless channel model based on ray tracing statistics is employed. This model allows for precise modelling of the RSSI and the characterization of the channel profile, facilitating more effective identification of sybil nodes.

The remainder of this article is organized as follows: Section 2 provides a comprehensive review of related research on sybil attack detection in VANETs. Section 3 presents a brief discussion on the 3D channel models deployed in this study, while section 4 describes the proposed detection mechanism in detail, highlighting the integration of channel profiling and RSSI analysis. Section 5 presents experimental results and performance evaluation, comparing the proposed approach with existing methods. Finally, Section 6 concludes the article, summarizing the findings and discussing future research directions.

2. Related Studies

A sybil attack is a type of security threat in computer networks and distributed systems where an attacker creates multiple fake identities or nodes to gain control or influence over the system. In a sybil attack, the attacker strategically creates and controls multiple identities, often referred to as sybil nodes or sybil identities, to deceive the system. These identities are usually indistinguishable from legitimate ones, making it difficult for the system to differentiate between real and fake entities [1]. This type of attack can also disturb the operation of V2V compromising the security of the communication of vital safety messages that are exchanges between vehicles [5]. Therefore, there are extensive studies that have proposed sybil attack detection protocols, following different approaches [6]. The main approaches in sybil attack detection are summarized as below:

2.1. Trust-based Mechanisims

Trust-based approaches rely on establishing trust among vehicles based on their past behaviour and interactions. Trust metrics are assigned to vehicles, and any significant deviation from the expected trust level can indicate the presence of sybil nodes. Research in this area includes the work proposed in [7] which considers high vehicle density and limited transmission power of the adversary. The proposed method in this study covers the mitigation procedure in creating the trust model and announcing to the neighbour vehicle the tempered identities in a secure way utilizing the Diffie-Hellman distribution. In addition, the study in [8] proposed a multi-level trust mechanism based on blockchain to detect the sybil attack. The author's approach is divided into three parts: (1) A Horizontal Trust Management mechanism, (2) A Vertical Trust Management mechanism (VTM) is used to launch a verification algorithm by the Roadside Unit (RSU) and (3) Distributed Trust Management mechanism. In addition, a hybrid trust-based defence mechanism against sybil attack is proposed in [9] where each node is assumed to have an obfuscated identity, and a trust centre is utilized in the form of RSU which assigns reputation values to each identity. The work also assumes a data-centric neighbour trust scheme where the neighbours will assess each other others based on the exchanged data. In [10], a hybrid scheme using trust-based method along with machine learning-based reputation systems is proposed to address accuracy, safety and real-world sybil attacks in VANET. In addition, the study [11] proposed a hybrid method which is a combination of position-based verification and trust certification to detect sybil attacks. In addition, the study in [12] has proposed a trust-based method for detecting sybil nodes based on network-related parameters such location of the node, timestamp of the message and trust value. The proposed method also considers the distance metric between the neighbour nodes together with the RSSI value.

2.2. Movement Pattern Analysis

This approach utilizes the movement patterns of vehicles to detect sybil attacks. By analysing the trajectories, speeds, and distances travelled by vehicles, suspicious patterns or inconsistencies can be identified. Example of studies conducted in this area is [13]; this study proposes a detection mechanism based on vehicle movement patterns and statistical analysis to identify sybil attacks in V2V networks. The authors in [14] focused on utilizing vehicle trajectories to detect sybil attacks in V2V networks, leveraging the movement patterns and behaviour of vehicles for accurate detection.

2.3. Machine Learning Techniques

Machine learning algorithms, such as Support Vector Machines (SVM), Random Forest, or Artificial Neural Networks (ANN), can be employed to learn patterns and characteristics of legitimate vehicles and detect anomalies or deviations associated with sybil nodes. This topic has been investigated extensively in recent years due to the advancements that have been experienced in the machine learning field. Relevant studies include the work achieved in [15], where authors used the raw-traffic data that has been collected to identify authorized and unauthorized APs in an integrated wired/wireless environment. This has been also incorporated into the IoT field through another study [10] which has exploited the naïve-bayes, random Forest and Logistic Regression machine learning methods to detect fake identities. The study shows that the naïve Bayes algorithm has achieved the highest detection accuracy. A combination of machine-learning and vehicle behaviour analysis is utilized in [16] for a complete accurate detection scheme which has been proven by author to accurately locate the specific road section where the attack occurred under different complex traffic scenarios and achieve therefore high detection accuracy.

The implementation of machine learning techniques has been investigated in [17] by proposing sybil detection protocol that implements different machine learning classifiers in centralized manner. This proposed mechanism is proven to work well under simple attack models and might deliver an accurate result in complex attacks scenarios. The use of machine learning techniques has also been utilized to reduce identification time, increase detection accuracy, and enhance scalability of sybil detection as proposed in [18]. The authors in this study implemented vehicle-specific learning machine features with the use of classifications which have been proven to reduce sybil assaults and sustain provider service in VANETs. In addition, the study in [19] has proposed a multi-source fusion detection based on the behaviour analysis of sybil attacks along with the use of machine learning classification model to complete the detection of the attack behaviour. The proposed method is proven to locate the specific road section where the attack occurs in a realistic traffic scenario considering different road types.

2.4. Reputation-based Techniques

Reputation-based approaches assign reputation scores to vehicles based on their past behaviour and interactions. Vehicles with low reputation scores or inconsistent behaviour may be flagged as potential sybil nodes. Many studies have focused on this approach such as the one in [20], where authors have proposed an event-based reputation system, in which dynamic reputation and trusted value for each event are employed to suppress the spread of false messages. The proposed technique can detect fabricated and stolen identities and defend against conspiring sybil attack. A combination of Blockchain-based Trust and Reputation Model (BTRM) is deployed in [21], which evaluates user reputation from many aspects and can resist multiple malicious attacks in the distributed network. Further investigation of reputation-based approach is conducted in [22] where authors proposed an enhanced Event based reputation system to defend sybil attacks which targets V2V and enhance Vehicle to Infrastructure (V2I) security.

2.5. Collaborative Detection

Collaborative detection mechanisms involve vehicles sharing information and cooperating to detect sybil attacks. By exchanging observations and verifying the consistency of information, the presence of sybil nodes can be identified. Examples of studies conducted in this area include [23], where the authors have proposed a soft and hard majority voting approach that has been proven to outperform other state-of-art techniques in sybil attack detection. Further research in this area is carried in [24] through proposing a computation less heuristic approach that focuses on detecting the sybil attacker using the signal strength and a collaborative strategy in detecting the suspicious nodes. Additionally, the authors in [25] have proposed a RSU cooperative detection mechanism involving triangulation and fake propagation by RSU to identify the sybil attacks in the VANET.

2.6. Physical Layer Analysis

This approach leverages physical layer information, including the RSSI, signal propagation patterns, and Angle of Arrival (AOA), to examine the characteristics of the wireless channel. These channel statistics can be utilized to estimate the locations of vehicles and detect sybil nodes. For instance, in [26], an enhanced RSSI-based detection scheme is proposed, which incorporates a screening phase, sybil node verification phase, and introduces a reputation module and adaptive threshold. Another study, [27], proposes a sybil attack detection method based on RSSI and voiceprint. Unlike previous studies that focused on absolute position or relative distance computation, this study adopts the voiceprint of RSSI time series as vehicular speech and compares the similarity among received samples. Additionally, [28] suggests an RSSI-based detection scheme that utilizes RSSI and the vehicle driving matrix, with the detection decision based on distance matching between the RSSI sequence and the driving matrix. Furthermore, the authors in [29] explore potential power control models for launching sybil attacks and propose a power control identification mechanism using RSSI and voiceprint. The combination of RSSI-based and encryption-based detection is also explored in [30]. The benefits of RSSI and voiceprint-based sybil detection are further studied and examined in [31], demonstrating that voiceprint is more effective in sybil detection as it is independent of any signal propagation modelling. In addition to the utilization of RSSI, other wireless channel metrics such as AOA have been investigated, as presented in [32]. AOA depends on the physical location of the vehicle, making it difficult to forge and suitable for sybil node detection. Another study, presented in [33], utilizes RSSI for localization and sybil attack detection. The wireless channel state information has been also exploited in sybil attack detection as presented in [34], by proposing a sybil detection scheme based on power gain and delay spread analysis and exploiting the spatial variability from their channel responses. Relevant study in this area is conducted in [35] where authors proposed sybil detection scheme that is based on the RSSI values along with the voiceprint to conduct widely pertinent, lightweight, and full distributed detection for VANETs. The proposed technique stimulates the spider monkey time synchronization technique for vast-scale VANETs to minimize energy consumption and raise packet delivery ratio.

The aforementioned studies highlight that the full potential of wireless signal characteristics has not been fully utilized in sybil detection. Therefore, this study explores other wireless channel metrics, such as angular spread in both azimuth and elevation domains, to accurately identify sybil nodes, especially in the dynamic environment of V2V communication.

3. 3D Wireless Channel Modelling

In this study, an enhanced three-dimensional (3D) 3GPP/ITU channel model is implemented based on the authors' previous research [36-37]. This channel model employs stochastic characteristics necessitating dual levels of randomness to simulate communication links among vehicles. Initially, large-scale (LS) attributes such as shadow fading, delay proportionality factor, and angular spreads are randomly selected from predefined distribution functions. Subsequently, small-scale (SS) parameters like cluster delays, cluster powers, and directions of arrival and departure are also randomly chosen based on tabulated distribution functions. Grounded in the clustered delay line (CDL) concept, the ITU channel model defines a cluster as the aggregate of multi-path components (MPC) sharing similar delay values. Furthermore, an additional layer of randomness is vital to generate distinct realizations for each link by varying phases across the scatterers.

In the context of this study and the characterization of the wireless channel between the vehicles, this deployed 3D model includes

- Multipath Propagation: The model accounts for the reflections, diffractions, and scattering of signals in three-dimensional space, considering the presence of obstacles and buildings that affect signal propagation.
- Shadowing Effects: It incorporates shadowing effects caused by obstacles, buildings, and other structures, which can attenuate the signal strength and introduce variations in the received signal power.
- Path Loss: The model accounts for path loss, which represents the reduction in signal power as it propagates through the environment due to factors like distance, obstacles, and absorption.
- Delay Spread: It considers the delay spread, which is the time delay between the arrival of the direct signal and its reflections, affecting signal quality and causing multipath interference.
- Doppler Shift: The model also includes Doppler shift effects caused by the movement of the transmitter, receiver, or scatterers in the environment, influencing the frequency of the received signal.

This channel model considers both azimuth and elevation planes to accurately represent propagation characteristics. The 3D ITU model incorporates large-scale fading effects by considering path loss and shadowing, as well as small-scale fading through detailed modelling of MPCs. The large-scale parameters (LSPs) utilized in this model are derived from 3D ray tracing predictions, providing comprehensive information on amplitude, phase, time delay, Angle of Arrival (AoA), and Angle of Departure (AoD) in both elevation and azimuth domains. For a more comprehensive understanding of the generation of the implemented 3D channel statistics and the modelling of related LSPs, the author recommends referring to previous published work in [38-39]. In this study, the Power Delay Profile (PDP) is analysed to assess the spatial correlation of the received angular spread in both the azimuth and elevation planes across multiple receivers. Specifically, focusing on examining the short-term power arrival angular profile by spatially averaging the instantaneous power arrival angular profiles over several tens of wavelengths. This averaging process helps to mitigate the effects of rapid fading and reduce variations in the measurements. The following discussion clarifies the modelling of the power angular profile at both the azimuth and elevation planes based on the ITU and 3D developed model by the author [40].

The modelling of the power azimuth arrival angular profile ($AOD_{NLOS,pow}(\Delta\theta, d)$) at the receiver involves normalizing it with respect to the maximum power of the path at a distance d, as shown in the following equations (1)-(3):

$$AOD_{Az,pow}(\Delta\theta,d)=\left(1+\frac{|\Delta\theta|}{\alpha(d)}\right)^{-\beta(d)} \tag{1}$$

where,

$$AOD_{Az,pow}(\Delta\theta,d)=\left(1+\frac{|\Delta\theta|}{\alpha(d)}\right)^{-\beta(d)} \tag{2}$$

$$\beta(d)=(-0.015H+0.63)d-0.16+0.76\log(h_b) \tag{3}$$

h_b is the receiver antenna height in m, and $|\Delta\theta|$ is the angular spread in degrees. On the other hand, the power elevation arrival angular profile at the receiver is modelled as,

$$AOD_{el,pow}(\Delta\vartheta,d)=EXP\,[-|\Delta\vartheta_v|/\sigma_v(d)] \tag{4}$$

where,

$$\sigma_v(d) = \frac{\left(h_b - \langle H \rangle\right).K_x}{\left(h_b - \langle H \rangle\right)^2 + \left(1000d\right)^2}.\left(\frac{180}{\pi}\right) \tag{5}$$

$$K_x \begin{cases} 320.\left(\dfrac{h_b}{\langle H \rangle}\right)^{-1.14} & \left(\Delta\vartheta < 0\right) \\ 59.\left(\dfrac{h_b}{\langle H \rangle}\right)^{-0.56}.\left\{1 + 5.5.EXP\left[-\left(\left(\dfrac{h_b}{\langle H \rangle}\right) - 1\right)^{1.4}\right]\right\} & \left(\Delta\vartheta \geq 0\right) \end{cases} \tag{6}$$

It is important to note that the values of azimuth and elevation angular spread are randomly generated for different physical locations, following the simulation setup described in [36], these values are based on the statistical angular spread model previously proposed by the author and summarized in table 1. Using the provided angular spread values, the angular power profiles in both the azimuth and elevation planes are generated according to the equations (1)-(6). The variation in angular profile is used in the proposed work explained below to identify sybil nodes.

The channel statistics utilized in this study, obtained through ray tracing analysis of an urban environment at 5.9 GHz, as presented in table 1. These statistics are derived from an ideal isotropic antenna to eliminate the impact of antenna characteristics. This ensures that any antenna pattern can be applied later when generating the 3D channel matrix. Table 1 includes the following parameters: SF (Shadow Fading), RMS DS (Root Mean Square Error for the delay spread), ASD (Arrival Azimuth Angular Spread), ASA (Arrival Azimuth Angular Spread), ESD (Departure Elevation Angular Spread), and ESA (Arrival Elevation Angular Spread).

Table 1. 3D Channel statistics parameters

Parameter		5.9 GHz	
		LOS	NLOS
SF (dB)		8.6	11.3
K factor (dB)	μ	12	1.7
	σ	6.3	6.14
RMS DS $\log_{10}$(ns)	μ	-7.95	-6.96
	σ	0.78	0.51
ASD $\log_{10}$(Degree)	μ	-0.16	0.83
	σ	0.75	0.65
ASA $\log_{10}$(Degree)	μ	1.24	1.66
	σ	0.57	0.43
ESD $\log_{10}$(Degree)	μ	-0.7	-0.11
	σ	1.14	0.68
ESA $\log_{10}$(Degree)	μ	0.29	0.77
	σ	1.25	0.47

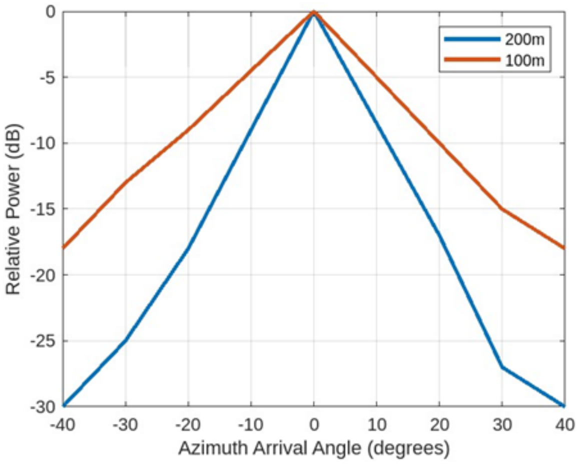


Fig.1. Arrival azimuth angular profile for two physical locations

Conversely, the path loss model is defined as a function of the distance from the Base Station (BS), exhibiting a linear increase in logarithmic scale with distance (d). Hence, the equation representing the path loss at 5.9 GHz carrier frequency is as follows:

$$PL = \mathrm{A}_{\mathrm{PL}} .log_{10}\left(d\right) + \mathrm{B}_{\mathrm{PL}} \tag{7}$$

The value of A_{PL} is determined as 27 for Line-of-Sight (LOS) conditions and 35 for Non-Line-of-Sight (NLOS) conditions. Additionally, B_{PL} is evaluated as 26 for LOS scenarios and 39 for NLOS scenarios. Fig.1 illustrates the impact of the distance between the transmitter and the receiver on the azimuth angular spread, accompanied by the corresponding received relative power. The PL here affect the RSSI which is an important metric in the detection of the sybil nodes.

4. Proposed RTSCD Technique

This section introduces the proposed Real-Time sybil Detection and Classification (RTSDC) technique scheme for detecting sybil attacks in V2V communication, where vehicles exchange safety and other pertinent information while in motion. It is assumed that a physical vehicle utilizing multiple forged identities, while the claimed virtual identities are referred to as sybil nodes. The proposed scheme comprises three primary phases: Acquisition, signal analysis, and verification. A comprehensive discussion is provided of each phase. The proposed detection method employs three wireless channel metrics, namely the RSSI, AOA in the azimuth plane, and AOA in the elevation plane. These metrics are utilized to effectively identify and distinguish sybil nodes with high accuracy.

4.1. Acquisition Phase

During this phase, it is assumed that each vehicle's On-Board Unit (OBU) operates in the Control/Service channels (CCH/SCH) alternating switch mode as defined in the IEEE 1609.4 protocol [41]. In this mode, every vehicle broadcast safety messages at a frequency of 10Hz (equivalent to 10 packets per second) on the common control channel. The vehicles utilize the synchronization interval to collect test packets and examine the characteristics of the received signals. These test packets contain relevant vehicle information, such as identity and current speed. The triggering rate of the acquisition phase can be dynamically controlled by the proposed protocol, based on the speed of neighbouring vehicles. To determine the coherence time of the received signal from each neighbour, the vehicles calculate the time interval during which the signal maintains a correlation above a certain threshold, referred to as τ_{thr} , which can be dynamically adjusted. Assuming the correlation time is τ_c, the vehicle is required to perform channel scanning every τ_c, as wireless signals undergo dynamic changes that result in signal correlation falling below τ_c. This allows the vehicle to have accurate estimation and comparison of the signal characteristics among neighbours. The correlation coefficient $r_{x,y}$for the received signal samples $x \,\&\, y$ is calculated using the sample standard deviations (S_x and S_y) and sample covariance ($S_{x,y}$)), as given by equation (8):

$$r_{x,y} = {}^{S_{x,y}}\!\big/_{S_y S_x} \tag{8}$$

The highly correlated signal samples are identified by satisfying equation (9):

$$\tau_c \geq \tau_{thr} \tag{9}$$

During this phase, data based on wireless signals received from neighbouring vehicles is generated and saved in the local cache of every vehicle i in time sample t.

$$Entry_{i,t} = ID_i, RSSI_{i,t}, AOA\_az_{i,t}, AOA\_el_{i,t} \tag{10}$$

Where, $RSSI_{i,t}$ is the received signal power calculated based on equation (7), $AOA\_az_{i,t}$ $\&AOA\_el_{i,t}$ are the angle-of-arrival profiles in the azimuth and elevation planes consequently. This phase is further clarified in Algorithm 1. It's worth mentioning that the correlation threshold τ_{thr} is set to 0.5 in this study.

Algorithm 1 takes into account several inputs, including the vehicle ID ($nodeID_x$), the radio transmission range (R_x) based on the communication system in use, and the received channel profile described by the received signal power ($RSSI_x$) and the angular spreads denoted as ($CH_{(d,pt_x),}$). Additionally, the algorithm incorporates the vehicle speed (S_x) and the previously defined correlation threshold (τ_{thr}). The algorithm iterates through each vehicle, assessing their received signals from neighboring vehicles within their radio range, determining the time interval where signal correlation exceeds the correlation threshold. It then calculates the received signal strength ($RSSI_{i,t}$) and the angular spread in both azimuth and elevation planes, referred to as ($AOA\_az_{i,t}, AOA\_el_{i,t}$).

Algorithm 1: Pseudocode of Acquisition phase

```
Input: $nodeID_x, node\ range\ transmission\ R_x, Channel\ Profile\ (CH_{(d,pt_x)}, RSSI_x)$, vehicle speed $S_x$, $\tau_{thr}$
Output: List of $Entry_{i,t} = \langle ID_i, RSSI_{i,t}, AOA\_az_{i,t}, AOA\_el_{i,t} \rangle$
For $\forall t \in T$ do   //for each time sample collected
    For $\forall i \in V^i$ do   //for each neighbour vehicle in range $R_x$,
        Calculate $\tau_c$ //calculate the time interval where signal correlation > $\tau_{thr}$
        If $t > \tau_{thr}$ Retrieve $nodeID_x, S_x$ // the broadcast is on the CCH channel.
            Calculate $RSSI_{i,t}, AOA\_az_{i,t}, AOA\_el_{i,t}$
        End if
    End For
End For
```

4.2. Signal Analysis

Following the collection of the wireless signal samples in the acquisition phase, the second phase which is referred to as "Signal analysis" is concerned with the analysis of the RSSI, angular spread in both azimuth and elevation domains to compare these metrics for signals received from multiple vehicles. It is worth mentioning here that malicious nodes don't perform any power regulations. Therefore, the sybil attack can be detected by measuring the similarity of three signal-based metrics $(RSSI, AOA\ (az), AOA(el))$ measured in different time series. The similarity in this study is computed using the Dynamic Time Warping (DTW) [42] which adopts dynamic programming to determine the best matching between two time series by warping the series with different length N and M. Considering the characteristics of the data series utilized in this research, DTW emerges as a proficient algorithm due to its precision, adaptability, and relatively lower computational complexity when contrasted with alternative techniques.

Assuming two series $X_N\{x_1, x_2, x_3, \ldots, x_N\}$, and $Y_M\{y_1, y_2, y, \ldots, y_N\}$. DTW establishes first an N-by-M cost matrix C containing the distance $d_{i,j}$ between each pair of points in series X and Y. The cost is defined according to the Euclidean distance:

$$d_{i,j} = \left(x_i - y_i\right)^2 \tag{11}$$

Then the DTW computes the minimum matching accumulated cost $C_{i,j}$ as follows:

$$C_{i,j} = d_{i,j} + min\left\{C_{i-1,j}, C_{i,j-1}, C_{i-1,j-1}\right\} \tag{12}$$

In equation (12), the value $C_{0,0}$ is initialized by zero, while other values in the cost matrix set to ∞. Then the DTW will generate an optimal warp path $Z = z_1, z_2, z_3, \ldots, z_k(z_k = (i,j))$ which means the i_{th} element of X is aligned with j_{th} element of Y with minimum total accumulated cost. Finally, the DTW distance is measured as the total accumulated cost as follows:

$$C_{DTW}\left(X,Y\right) = C_{N,M} \tag{13}$$

Based on the above discussion, let us assume the statistics collected at time t for vehicle v is referred to as $RSSI_{t,v}$ for the received signal power computed according to Section 3, and the azimuth & elevation angular profiles are referred to as $AOAz_{t,v}$, $AOAe_{t,v}$ modelled in Section 3. Therefore, after sufficient samples collection in the acquisition phase, each vehicle will calculate the DTW distance for each of the above-mentioned parameters, which are referred to as $RSSI_{DTW}$, $AOAz_{DTW}$ and $AOAe_{DTW}$.

Finally, the calculated DTW distances are normalized using the min-max normalization, as presented in equation(14):

$$C_{nDTW_{i,j}} = \frac{C_{DTW_{i,j}} - C_{DTW_{min}}}{C_{DTW_{max}} - C_{DTW_{min}}} \tag{14}$$

where $C_{DTW_{min}}$ and $C_{DTW_{max}}$ are the minimum and maximum values of all DTW distances respectively.

4.3. Verification Phase

During this phase, every vehicle possesses a set of signal statistics obtained from nearby vehicles within its radio range. These statistics are stored locally and updated regularly as the vehicle initiates the acquisition phase. Hence, the gathered statistics are utilized in this phase to determine a trust metric, denoted as $\varepsilon_{i,j}$, for each pair of neighboring vehicles i, j. The trust metric is computed as a weighted average of the DTW distances calculated in the signal analysis phase, using the following formula:

$$\varepsilon_{i,j} = \alpha.RSSI_{nDTW} + \beta.AOAz_{nDTW} + \gamma.AOAe_{nDTW} \tag{15}$$

Where $RSSI_{nDTW}$, $AOAz_{nDTW}$ and $AOAe_{nDTW}$ are the normalized DTW distances for the RSSI, AOAaz and AOAel respectively, while the symbols α, β and γ represent the weight factors. The weighting factors can be dynamically adjusted to allocate varying weights to the RSSI and the AOA during the calculation of the trust metric $\varepsilon_{i,j}$. Therefore, the trust metrics for the sybil nodes are expected to be very small and approaches 0, since the DTW distances for sybil nodes is also small. The trust metrics are generated for each pair of received signals as follows:

$$\varepsilon = \varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_k \left(\varepsilon_k = (i, j) \right) \tag{16}$$

The signal analysis and verification phases are clarified in Algorithm 2. As per Algorithm 2, every vehicle will utilize metrics derived from Algorithm 1, such as the received power ($RSSI_{i,t}$) and the angular spread denoted as $(AOA\_az_{i,t}, AOA\_el_{i,t})$. Subsequently, the vehicle will iterate through each neighboring vehicle in the list, analyzing each time sample collected to compute the DTW distance for the mentioned parameters. This process generates variables $(RSSI_{DTW(i)}, AOAz_{DTW(i)}, AOAe_{DTW(i)})$. Following the calculation of DTW distances, the algorithm proceeds to evaluate trust metrics for all received signals from neighboring vehicles ($\varepsilon_k = (i, j)$), Subsequently, suspect vehicles are identified based on the computed metrics and stored in the variable (suspect (n)).

Algorithm 2: Pseudocode of signal analysis and verification phases

```
Input: $nodeID_x, node\ range\ transmission\ R_x, Channel\ Profile\ (CH_{(d,pt_x)}, RSSI_x),\ \alpha, \beta\ and\ \gamma,$
Output: List of  $Entry_{i,j} = \langle \varepsilon = (i,j) \rangle$   //generate list of trust metrics
For $\forall t \in T$ do      //for each time sample collected
        n=0; // List of suspect's index
For $\forall i \in V^i$ do     //for each neighbour vehicle in range $R_x$,
        Calculate   $RSSI_{DTW(i)}$, $AOAz_{DTW(i)}$, $AOAe_{DTW(i)}$   //calculate the DTW for $RSSI, AOA\_az$ & $AOA\_el$
        End if
      End For
For $\forall i \in K^i$do      //$K^i = \{RSSI_{DTW(i)}, AOAz_{DTW(i)}, AOAe_{DTW(i)}\}$
        Calculate  $(\varepsilon_k = (i,j))$ // The trust metrics for all received signals.
            End For
For $\forall i \in \varepsilon^i$do     //$list\ of\ trust\ metrics$
        If   $\varepsilon_{i,j} \approx 0$ then
            suspect (n)= {i}
            n=n+1
        End if
        End For
End For
```

5. Performance Analysis

5.1. Simulation Setup

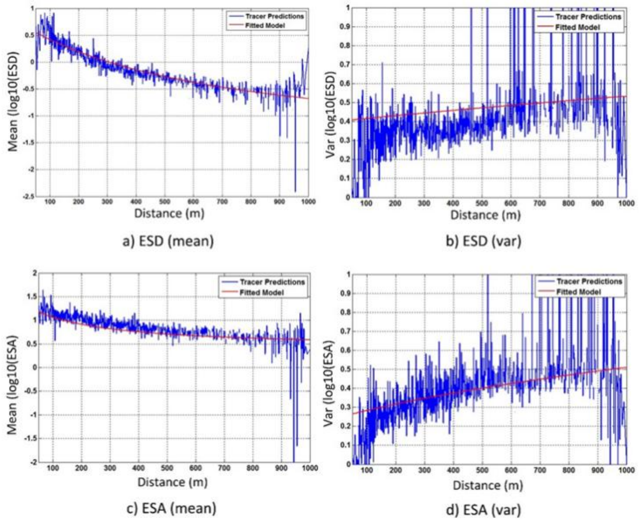
The proposed RTSDC sybil detection technique is simulated in MATLAB using Mento-Carlo-based simulation. The vehicles are aligned in two lanes road. The vehicles may have random mobility speed in the range of 60-100 km/h, and the number of vehicles is set randomly between 50 to 200. It is assumed that all vehicles have fixed transmission power of 23 dBm and a packet size of 500 Bytes. All nodes broadcast 10 packets per second. A complete set of simulation parameters is presented in table 2. The propagation model presented in Section 3, and the channel related parameters provided in table 1 are considered in this simulation. Please note the weight factors used in equation (15) are assigned to 0.5, 0.25 and 0.35 for α, β, γ respectively. This implies that 50% of the trust decision factor is based on the correlation in the RSSI power, while the angular spread in both azimuth and elevation have a combined weight of 50%. As discussed in previous sections, the variation in the wireless channel profile is considered based on the model provided in section 3, where the vehicles' received signal power and characteristics are varying dynamically based on vehicles mobility and physical location.

Table 2. Simulation parameters

Parameter	Value
Road length	2 km
Lanes	2
Number of simulation iterations	100
Number of vehicles	50 - 200
Frequency	5.9 GHz
Bandwidth	10 MHz
Transmit power	23 dBm
Packet size	500 Bytes
Packet rate	10 Hz
Observation time (CCH)	20s
Simulation time	120s
Mobility	60-100 km/h
Data rate	3 Mbps
α, β, γ	0.5, 0.25.0.25
Standard compliance	IEEE 1609.4

5.2. Results Analysis

This study focuses on two performance metrics: the True Positive Ratio (TPR) and the False Positive Rate (FPR). The TPR metric represents the proportion of correctly identified sybil nodes out of the total illegitimate nodes, while the FPR ratio indicates the rate at which normal nodes are incorrectly classified as malicious nodes. The presented results are an average of numerous simulation iterations. In each iteration, random channel profiles are generated for each vehicle based on the parameters described in Section 3. The duration of each iteration is 120 seconds, as specified in table 2. Before delving into the evaluation of the RTSDC technique's performance, an analysis of the angular spread, with a focus on the elevation angular spread, is presented. This analysis is based on the channel model employed in this study. As depicted in fig.2, it can be observed that as the distance between the transmitter and receiver increases, the elevation angle spread decreases at the receiver side. Similar trends were observed in the ray tracing data. Fig. 2 illustrates the mean and variance of the logarithm of the predicted angular spreads for different vehicle locations, considering both arrival and departure elevation spreads. The mean elevation. spread demonstrates a decreasing trend in relation to the reciprocal of the distance. This suggests that as vehicles approach each other, the receiver tends to experience higher average elevation spreads. Additionally, the predictions indicate an increasing variance in the logarithm of the elevation spread with distance, while the standard deviation of the elevation spread decreases.



a) ESD (mean)

b) ESD (var)

c) ESA (mean)

d) ESA (var)

Fig.2. Mean and variance of the logarithm angular spreads

To assess the effectiveness of the proposed RTSDC mechanism, the simulation is conducted under the assumption of a single sybil node injected into the network during each simulation iteration. The simulation results are then compared to the performance of the Power Control Identification sybil attack Detection (PCISAD) technique proposed in [29]. The authors of the PCISAD technique employed RSSI-based channel statistics and field measurements to accurately model wireless channels. While the PCISAD serves as the benchmark for evaluating the proposed algorithm, it is important to note that the RTSDC is also on par with other techniques that depend on RSSI for sybil attack detection. The selection of PCISAD is specifically to exemplify RSSI-based detection mechanisms. For additional information on physical-layer related detection mechanisms, readers are directed to section 2, sub-section (F).

By comparing the TPR between the two techniques, it becomes evident, as depicted in fig.3, that the RTSDC technique offers a higher TPR ratio compared to the PCISAD technique. The TPR is evaluated across a range of vehicle densities, and it is observed that as the number of vehicles increases, the TPR ratio decreases for both mechanisms. Nonetheless, the RTSDC technique demonstrates greater robustness as the decline in the detection ratio is less pronounced compared to the PCISAD technique. The reason behind this behaviour can be attributed to the fact that, despite the increase in vehicle densities, an RSSI-based model may struggle to accurately differentiate between vehicles based solely on RSSI, especially when vehicles are in close spatial proximity. On the other hand, the RTSDC technique considers the angular spreads of the incoming signals, which provides an additional dimension for distinguishing between vehicle signals, even when they maintain a similar spatial distance from the observer. Further analysis of fig.3 reveals that as the number of vehicles increases from 10 to 100, the TPR of the PCISAD technique drops by 24%, while the TPR of the RTSDC technique only decreases by 18%. For instance, when the number of vehicles approaches 100, the proposed RTSDC technique is capable of detecting 80% of sybil nodes, whereas the PCISAD technique can detect a maximum of 70% of sybil nodes.

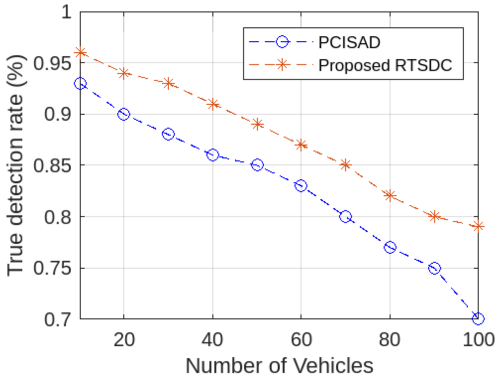


Fig.3. True positive ratio

In addition to analysing the TPR it is also crucial to consider the FPR. Fig.4 illustrates the performance of the proposed RTSDC algorithm in comparison to the PCISAD technique. The presented results unequivocally demonstrate the improvement offered by the proposed technique over the state-of-the-art PCISAD algorithm. For instance, when the total number of vehicles is 70, the proposed sybil detection mechanism yields a FPR of 5%, whereas the PCISAD algorithm results in a 10% FPR. Furthermore, as the number of vehicles increases, the FPR also increases. However, the proposed technique exhibits consistent performance, with the increase in false detections not exceeding 7% compared to 10% in the PCISAD technique when the number of vehicles is increased from 10 to 100. It is notable that the functionality of the suggested algorithm remains unaffected by the overall quantity of vehicles, with each node handling signals received from vehicles within its radio coverage independently. Nonetheless, the computational time and complexity escalate with an increasing number of these vehicles, a challenge that can be mitigated by bolstering the computational speed and storage capacity of the hardware utilized in the vehicles.

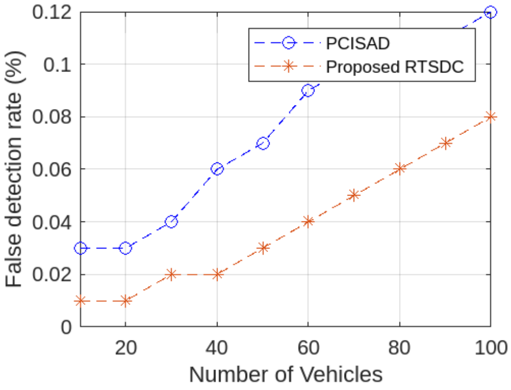


Fig.4. False positive ratio

The improved effectiveness of the RTSDC algorithm over the PCISAD algorithm stems from a crucial difference in their operational mechanisms. While the PCISAD primarily relies on RSSI for pinpointing suspicious nodes, this approach encounters challenges when nodes are in close proximity, as the received signal powers tend to be similar, leading to ambiguity in distinguishing signals from the same physical source. In contrast, the RTSDC algorithm incorporates RSSI as just one component in the decision-making process. Additionally, it takes into account angular spread alongside RSSI. This dual consideration enables the algorithm to leverage angular spread as an additional parameter, enhancing its ability to differentiate between devices even when they are spatially close. The integration of angular spread as a supplementary factor contributes to the refinement of the detection process, as highlighted in the aforementioned enhancements.

To evaluate the performance of the proposed RTSDC technique in scenarios with a varying number of sybil nodes, the simulation is conducted with different numbers of sybil nodes ranging from 1 to 6. The obtained results are compared to a scenario where detection is solely based on RSSI. Table 3 presents a comparison of the TPR for both mechanisms. The results clearly indicate that the proposed RTSDC technique maintains a consistent performance in terms of the detection ratio, even as the number of forged identities increases. In contrast, the RSSI-based approach experiences a significant decline in its detection capability, resulting in a lower detection ratio. This can be attributed to the fact that as the number of forged identities increases, the probability of normal nodes exhibiting similar RSSI levels to the sybil nodes also increases. As a result, the true detection ratio decreases for the RSSI-based method.

Table 3. Comparison of TPR: RSSI vs RTSDC

# sybil nodes	1	2	3	4	5	6
RSSI	91%	89%	86%	83%	79%	75%
RTSDC	96%	94%	93%	92%	91%	90%

Impact on VANET Performance:

Improving the TPR and FPR ratios in the context of detecting sybil attacks in VANETs has significant implications for VANET performance and security.

- Impact on Security: Enhancing TPR and reducing FPR in sybil attack detection mechanisms directly influences the security posture of the VANET. A high TPR indicates the effectiveness of identifying genuine sybil attacks, ensuring that malicious nodes are accurately detected and isolated from the network. On the other hand, a low FPR signifies the minimization of falsely identifying legitimate nodes as malicious, thereby reducing the risk of disrupting or blocking genuine network participants.
- Network Reliability: Improving TPR and reducing FPR enhances the reliability of VANET communication by strengthening the network's resilience against malicious activities. Accurate detection of sybil attacks through high TPR ensures that the network can quickly identify and respond to security threats, maintaining the integrity of data transmission and trust among connected vehicles.
- Resource Utilization: Efficient detection of sybil attacks with improved TPR and reduced FPR optimizes resource allocation within the VANET. By accurately identifying malicious nodes while minimizing false alarms, the network can allocate resources effectively towards defending against security breaches, enhancing overall network performance and efficiency.
- Traffic Management: Better TPR and FPR in sybil attack detection mechanisms contribute to improved traffic management within the VANET. Accurate identification of malicious entities allows for more reliable data transmission, reduced congestion, and enhanced traffic flow control. This, in turn, leads to smoother communication among vehicles, better routing decisions, and ultimately improved overall VANET performance.

6. Conclusions & Future Works

In this article, a novel approach for detecting sybil attacks in V2V communication is proposed based on the analysis of the wireless channel profile presented by the angular spread and the RSSI measurements. By integrating the characteristics of the wireless channel and the signal strength information, the proposed RTSDC detection mechanism aims to enhance the accuracy and robustness of sybil attack detection in VANETs. Through the conducted comprehensive review of related research and analysis of the existing challenges, the article identified the need for a more effective and reliable sybil attack detection mechanism in VANETs. Leveraging the unique characteristics of the wireless channel profile, including signal strength variations and angular spread of the arriving rays, the proposed approach offers a promising solution to this ongoing problem. The experimental results and performance evaluation show the effectiveness of the proposed mechanism particularly in scenarios involving dense vehicle populations where RSSI-based detection methods may struggle. The proposed mechanism satisfied higher detection rate for sybil node for range of vehicles densities and have achieved robust performance in terms of false detection ratio as compared to state-of-the-art techniques. This research has the potential for expansion by exploring diverse vehicle mobility scenarios and patterns beyond the confines of a two-lane road. It could also encompass the consideration of different detection abilities linked to specific vehicle types. Furthermore, the study may delve into investigating how adjusting the transmit power levels among vehicles influences the overall efficacy of the detection system. Interference between the vehicles can also another interesting problem to consider in future studies.

References

[1] J. R. Douceur, “The Sybil Attack,” IPTPS, p. 251–260, 2002.

[2] M. raya, P. Papadimitratos and J. Habaux, “Securing Vehicular Communications,” IEEE Wireless Communications, vol. 13, no. 5, p. 8–15, 2006.

[3] Y. Zhang, B. DAS and F. Qiao, “Sybil Attack Detection and Prevention in VANETs: A Survey,” in Proceedings of the Future Technologies Conference (FTC), 2020.

[4] C. Wang, L. Zhu, L. Gong, Z. Zhao and L. Yang, “Channel State Information-Based Detection of Sybil attacks in Wireless Networks,” Journal of Internet Services and Information Security, vol. 8, no. 1, 2018.

[5] A. A. Mane, “Sybil attack in VANET,” International Journal of Computational Engineering Research, vol. 6, no. 12, p. 2250 – 3005, 2016.

[6] M. Bhise and S. D. Kamble, “Review on Detection and Mitigation of Sybil Attack in the Network,” Procedia Computer Science, vol. 78, pp. 395-401, 2016.

[7] G. D. Putra and S. Sulistyo, “Trust Based Approach in Adjacent Vehicles to Mitigate Sybil Attacks in VANET,” in 2017 International Conference on Software and e-Business, 2017.

[8] A. Haddaji, S. Ayed and L. C. Fourati, “Blockchain-based Multi-Levels Trust Mechanism Against Sybil Attacks for Vehicular Networks,” in 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), 2020.

[9] Rhamdhan and F. Hidayat, “Hybrid Trust-based Defense Mechanisms Against Sybil Attack in Vehicular Ad-hoc Networks,” in Mathematics, Science, and Computer Science Education for Addressing Challenges and Implementations of Revolution-Industry 4.0(MSCEIS), 2019.

[10] Mehbodniya, J. L. Webber, H. Mohafez and K. Yadav, “Machine Learning Technique to Detect Sybil Attack on IoT Based Sensor Network,” IETE Journal of Research, 2021.

[11] S. M. Faisal, B. K. Gupta and T. Zaidi, “A hybrid framework to prevent VANET from Sybil Attack,” in 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), 2022.

[12] S. Venugopal and E. A. M. Anita, “An efficient trust based method for Sybil node detection in mobile wireless sensor network,” in Proceedings of the 3rd International Conference on Applied Science and Technology (ICAST’18), 2018.

[13] M. S. Naveed and M. H. Islma , “Detection of Sybil Attacks in Vehicular Ad Hoc Networks,” Universal Journal of Communications and Network, vol. 3, no. 1, pp. 15-25, 2015.

[14] J. Li, Z. Song, Y. Li, C. Cao and Y. He, “Trajectory as an Identity: Privacy-Preserving and Sybil-Resistant Authentication for Internet of Vehicles,” Security and Communication Networks, 2021.

[15] M. Mounica, R. Vijayasaraswathi and R. Vasavi, “Detecting Sybil Attack In Wireless Sensor Networks Using Machine Learning Algorithms,” in 2nd International Conference on Machine Learning, Security and Cloud Computing (ICMLSC 2020), 2021.

[16] Y. Chen, Y. Lai, Z. Zhang, H. Li and Y. W. Yang, “MDFD: A multi-source data fusion detection framework for Sybil attack detection in VANETs,” Computer Networks, vol. 224, 2023.

[17] Hammi, M. Y. Idir and R. Khatoun, “A machine learning based approach for the detection of sybil attacks in C-ITS,” in 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), 2022.

[18] S. Kakulla and S. Malladi, “Sybil Attack Detection in VANET Using Machine Learning Approach,” Ingénierie des Systèmes d’Information, vol. 27, no. 4, pp. 605-611, 2022.

[19] T. Alladi, . V. Kohli, . V. Chamola and F. R. Yu, “A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems,” Digital Communications and Networks, vol. 9, no. 5, pp. 1113-1122, 2023.

[20] X. Feng, C.-y. Li, D.-x. Chen and J. Tang, “A method for defensing against multi-source Sybil attacks in VANET,” Peer-to-Peer Networking and Applications, vol. 10, p. 305–314, 2017.

[21] Z. Tu, H. Zhou, K. Li, H. Song and Y. Yang, “A Blockchain-based Trust and Reputation Model with Dynamic Evaluation Mechanism for IoT,” Computer Networks, vol. 218, 2022.

[22] K. J. Dutt and S. B. J. oshi, “Defending Against Sybil Attacks by Enhanced Event Based Reputation System in VANET,” International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 2, pp. 2249-8958, 2019.

[23] S. Azam, M. Bibi, R. Riaz, S. S. Rizvi and S. J. Kwon, “Collaborative Learning Based Sybil Attack Detection in,” Sensors (Basel), vol. 22, no. 18, 2022.

[24] R. Krishnan and A. R. Kumar, “A collaborative strategy for detection and eviction of Sybil attacker and Sybil nodes in VANET,” International Journal of Communication Systems, vol. 34, no. 3, 2020.

[25] M. Kabbur and. V. A. Kumar, “MAR_Sybil: Cooperative RSU Based Detection and Prevention of Sybil Attacks in Routing Process of VANET,” Journal of Physics: Conference Series, vol. 1427, 2019.

[26] Y. Liu and Y. Wu, “An Enhanced RSSI-Based Detection Scheme for Sybil Attack in Wireless Sensor Networks,” in Future of Information and Communication, 2020.

[27] Y. Yao and B. Xiao, “Multi-channel based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI,” IEEE Transactions on Mobile Computing, vol. 18, pp. 362-375, 2018.

[28] W. Li and D. Zhang, “RSSI Sequence and Vehicle Driving Matrix Based Sybil Nodes Detection in VANET,” in IEEE 11th International Conference on Communication Software and Networks (ICCSN), 2019.

[29] Y. Yao, B. Xiao, G. Yang, Y. Hu and L. Wang, “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.

[30] M. Bharti, S. Rani and. P. Singh, “RTBSAD: RSSI and Trust-Based Sybil Attack Detection in MANET,” Indian Journal of Computer Science and Engineering (IJCSE), vol. 13, no. 3, 2022.

[31] Y. Yao and B. Xiao, “Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs,” in 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017.

[32] T. Ma, Y. Hu, A. Aseeri, M. Nejad and R. Zhang, “Sybil Detection in Connected Vehicle Systems via,” in 3 IEEE International Conference on Mobility, Operations, Services and Technologies (MOST), 2023.

[33] 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,” in 14th IEEE Annual Consumer Communications & Networking

Conference (CCNC)., 2017.

[34] Q. Li, K. Zhang, M. Cheffena and X. Shen, “Channel-Based Sybil Detection in Industrial Wireless Sensor Networks: A Multi-Kernel Approach,” in 2017 IEEE Global Communications Conference (GLOBECOM), 2017.

[35] V. Indhuja, M. Kowshika, K. Naveena and V. Purni , “Extensive Detection of Sybil Attack using Spider Monkey Time Synchronization Technique in VANETs,” in First International Conference on Innovations and Challenges in Computing, Analytics and Security (ICICCAS-2020), 2020.

[36] R. Almesaeed, A. S. Ameen, E. Mellios, A. Doufexi, and A. R. Nix, “A proposed 3D extension to the 3GPP/ITU channel model for 800 MHz and 2.6 GHz bands,” in the 8th European Conference on Antennas and Propagation (EuCAP 2014), 2014.

[37] R. Almesaeed, A. Doufexi,, N. Dahnoun and A. R. Nix, “TVWS extension of the 3GPP/ITU channel model,” in 2013 IEEE 24th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), 2-13.

[38] R. Almesaeed, A. S. Ameen, E. Mellios and A. Doufexi, “3D channel models: Principles, characteristics, and system implications,” IEEE Communications Magazine, vol. 55, no. 4, pp. 152-159, 2017.

[39] R. Almesaeed, “Comparison of 2D and 3D Propagation in Wi-Fi Networks,” in 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2018.

[40] I.-R. P.1816-4, “The prediction of the time and the spatial profile for broadband land mobile services using UHF and SHF bands,” ITU, 2019.

[41] IEEE, “1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation,” IEEE, 2016.

[42] S. Salvador and P. K. Chan, “Toward Accurate Dynamic Time Warping in Linear Time and Space,” in Intelligent Data Analysis, 2004.

Authors’ Profiles

Assistant professor Reham Almesaeed, Department of Computer Engineering, College of Information Technology, University of Bahrain, Bahrain
(ORCID ID https://orcid.org/0000-0001-7267-3915)

Major interests: wireless channel modeling, wireless local area networks, WSN, Long Term Evolution, fifth-generation communications systems, mmWave communications, and massive MIMO.

How to cite this paper: Reham Almesaeed, "Real-time Sybil Attack Detection Based on Channel Characterization in VANET", International Journal of Computer Network and Information Security(IJCNIS), Vol.17, No.4, pp.71-83, 2025. DOI:10.5815/ijcnis.2025.04.05