

Securing Vehicular Ad-Hoc Networks : A Sybil Detection Approach



By

Manahil Mehreen

00000320557

Supervisor

Dr. Safdar Abbas Khan

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters
of Science in Information Technology (MS IT)

In

School of Electrical Engineering & Computer Science (SEECS) ,


National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(July 2023)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Securing Vehicular Ad-Hoc Networks: A Sybil Detection Approach" written by MANAHAL MEHREEN, (Registration No 00000320557), of SEECs has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: _____  _____
SEECs

Name of Advisor: Dr. Safdar Abbas Khan _____

Date: 07-Jul-2023 _____

HoD/Associate Dean: _____

Date: _____


Signature (Dean/Principal): _____

Date: _____

Approval

It is certified that the contents and form of the thesis entitled "Securing Vehicular Ad-Hoc Networks: A Sybil Detection Approach" submitted by MANAHAL MEHREEN have been found satisfactory for the requirement of the degree

Advisor : Dr. Safdar Abbas Khan

Signature:  _____

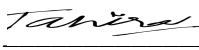
Date: 07-Jul-2023

Committee Member 1:Dr Farzana Jabeen

Signature:  _____

07-Jul-2023

Committee Member 2:Dr. Tahira Lashari

Signature:  _____

Date: 07-Jul-2023

Signature: _____

Date: _____

Dedication

This thesis is dedicated to my beloved parents who choose to provide me with the best education they could. Thank you for your love and support.

Certificate of Originality

I hereby declare that this submission titled "Securing Vehicular Ad-Hoc Networks: A Sybil Detection Approach" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: MANAHAL MEHREEN

Student Signature: 

Acknowledgments

In the name of Allah, the most beneficent and merciful, I want to start by expressing my gratitude to my supervisor Dr. Safdar Abbas for their excellent advice, knowledge, and support throughout the research process. The direction and caliber of this work have been greatly influenced by their continuous support.

I also owe a great deal of gratitude to the committee members on my thesis for their insightful comments and helpful recommendations. Their knowledge of the subject has been quite helpful in boosting the quality of this thesis overall and in streamlining the research technique.

I would like to extend my gratitude to my family and friends for their unwavering support, understanding, and encouragement throughout this journey. Their love, patience, and belief in my abilities have been a constant source of motivation and inspiration.

Manahil Mehreen

Contents

1	Introduction	1
1.0.1	Background Information	1
1.0.2	VANET Infrastructure	5
1.1	Problem Statement	6
1.2	Research Objective	8
1.3	Research Methods	9
1.4	Limitation	9
2	Background	11
2.1	Vehicle ad-hoc Networks	11
2.2	Vanet applications	12
2.3	Vanet Architecture	13
2.3.1	On-board Units	13
2.3.2	Roadside Units	14
2.3.3	Communication infrastructure	14
2.4	Communication Technology for Vanets	14
2.4.1	Dedicated Short Range Communication	15
2.4.2	Wireless Access in Vehicular Environment (WAVE)	15
2.4.3	VANET Characteristics	16
2.4.4	Sybil Attack in VANET	22

3	Literature Review	26
4	Design and Methodology	45
4.1	Research Objectives	45
4.2	System Architecture	46
4.2.1	Sybil Attacker Capabilities	47
4.3	Proposed Detection Methodology	49
4.3.1	Tool Used for Sybil attack detection	49
4.3.2	Neighborhood-based technique Algorithm	51
4.3.3	Technologies used for Sybil Attack Detection	53
4.3.4	Assumptions	54
4.3.5	Description of neighboring nodes	56
4.3.6	System Model	60
5	Implementation and Results	64
5.1	Detection Approach	64
5.1.1	Periodical Communication	65
5.1.2	Grouping of Neighboring Nodes	65
5.1.3	Sharing information with Nearby Nodes	65
5.1.4	Identification of Vehicles with Similar Neighboring Nodes	65
5.1.5	Simulation Scenario	67
5.1.6	Performance Analysis	75
5.1.7	Results	77
6	Conclusion and Future Work	81
6.1	Conclusion	81
6.2	Future Work	82

List of Figures

1.1	Vehicle to vehicle communication	4
1.2	Vehicle to infrastructure Communication	5
1.3	Sybil attack in VANET	7
2.1	VANET Architecture	12
3.1	Literature Review	32
4.1	Launching Veins	50
4.2	Physical Neighbors	57
4.3	Communication Neighbors	58
5.1	Record of neighboring vehicles	66
5.2	Urban envoinment	68
5.3	Road-side Units	69
5.4	Vehicles and Road-side units	70
5.5	Sybil Attacker	71
5.6	Sybil Nodes	72
5.7	Sending beacon packet to each node	73
5.8	Sending neighbors in formation to each node	74
5.9	Blockage due to Sybil Attacker	75
5.10	Receiving information about Attacker	76

LIST OF FIGURES

5.11 Resume Traffic	77
5.12 No. of neighboring nodes with and without attack	78
5.13 Detection in different time period	79

Abstract

Vehicular ad-hoc Networks (VANETs) and smart cities is an emerging area of research. Therefore, applications based on VANET are increasing day by day. There are a number of applications that can utilize the VANETs architecture to benefit the end-users. Vehicular Ad-Hoc Networks hold great promise in enhancing road safety by facilitating the exchange of sensor-derived information among vehicles. However, the successful deployment of VANETs necessitates addressing critical challenges, particularly those concerning security and privacy. The presence of malicious nodes within the network poses significant threats to its security and privacy. The focus of this thesis is to investigate the security and privacy concerns encountered by vehicles in VANETs, with specific emphasis on countering Sybil Attacks. These attacks involve a malicious vehicle illicitly acquiring multiple identities, intensifying the security vulnerabilities present in VANETs. Efforts are directed towards comprehending and mitigating these challenges to ensure the safe and reliable operation of VANETs.

The Sybil attacker sends numerous messages with apparent false identities (malicious nodes) to other vehicles in the network. This creates an optical illusion or confusion among the other vehicles on the same track. Sybil Nodes can cause serious damage by sharing/injecting erroneous data into the network. The proposed scheme makes the network secure and protects it from the harmful effects of Sybil's attack. The proposed scheme makes VANETs more secure by making them fault-tolerant and resisting the presence of detectable and re-portable Sybil nodes. Because VANETs are dynamic and fast-moving, a data-driven scheme is proposed that can determine whether a node is Sybil or normal by involving neighboring nodes.

CHAPTER 1

Introduction

1.0.1 Background Information

There have been a lot of variations in vehicles for the past three decades, such as navigation, fuel, and making driving more pleasant and comforting. Although there have been a lot of innovations in vehicles but traveling on roads is still quite risky as the mistake of one driver can lead to tragic incidents.

The integration of sensors, cameras, and radars in vehicles has paved the way for automation, enabling vehicles to communicate with each other and enhance overall efficiency. In response to this need, Vehicular ad-hoc networks (VANETs) have been deployed. VANETs serve as a network infrastructure where vehicles can communicate wirelessly, exchanging important information and improving the overall functionality of the transportation system. This technological advancement holds great promise for improving road safety, traffic management, and enabling new applications and services in the automotive industry. By facilitating seamless communication among vehicles, VANETs have the potential to revolutionize the way we travel and interact on the roads.[\[20\]](#)

The automotive industry has made impressive strides in its development over the past few decades. Modern cars are more fuel-efficient than ever before, thanks to advancements in automotive technology. However, while fuel efficiency has improved, road safety remains a persistent challenge. Despite various safety measures, vehicles are still susceptible to accidents caused by factors such as fog, ice, and other road hazards.[\[20\]](#) The primary contributing factor to these accidents, however, is human error. To address this issue, the automotive industry has been diligently working to integrate various sensors

into vehicles and connect them to onboard computers. These advancements aim to enhance vehicle safety by providing real-time data and enabling intelligent decision-making to mitigate the risks associated with human error.

Vehicular Ad-Hoc Network (VANET) is a specialized form of a mobile ad-hoc network [23] that focuses on improving traffic flow and enhancing road safety by providing real-time information to drivers and vehicles. The reliable and secure transmission of information is crucial in VANET to ensure the smooth functioning of the system and prevent any potential risks to people's safety on the road. As a result, security researchers have given significant attention to securing VANET communications.

VANET operates on a network infrastructure that includes Roadside Units (RSUs) and On-Board Units (OBUs). RSUs are strategically placed along the road edges to provide specific services and support communication with vehicles. OBUs are installed in individual vehicles and facilitate communication with other vehicles, RSUs, and relevant authorities.

The network infrastructure in VANET is designed to accommodate the movement of vehicles within predefined routes, typically road networks. To ensure proper registration, management, and coordination, specific authorities are responsible for overseeing VANET operations. RSUs play a crucial role in this regard, as they provide services such as traffic monitoring, information dissemination, and event reporting.[21]

VANETs enable vehicles to communicate with each other and infrastructure components, exchanging crucial information about road conditions, traffic congestion, accidents, and more. By sharing real-time data, these networks aim to enhance road safety and optimize traffic management. Vehicles equipped with communication devices can make [2]informed decisions and adapt their driving behavior based on shared information. This real-time information enables vehicles to make informed decisions and take appropriate actions to ensure safe and efficient driving.

However, due to the open and dynamic nature of VANET, securing the transmitted information becomes essential. Any alteration or manipulation of the data can potentially lead to system failure and compromise road safety.[21] Therefore, researchers and developers focus on implementing robust security measures to protect VANET communications from unauthorized access, tampering, and malicious attacks.

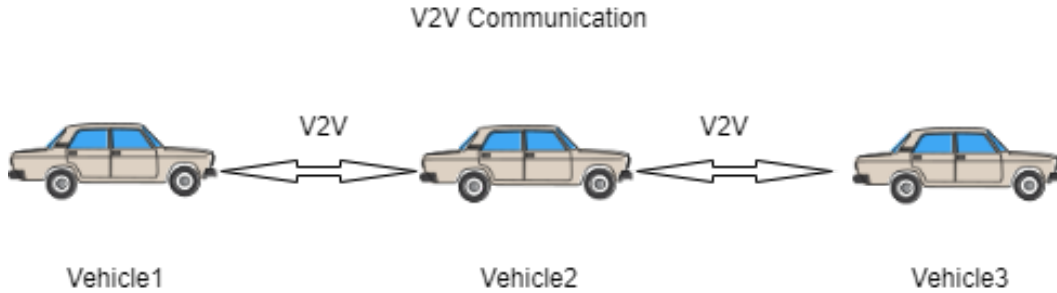
Efforts are made to employ various security mechanisms in VANET, including encryp-

tion and authentication techniques. Encryption ensures that the transmitted data is protected from unauthorized access by converting it into a secure form that can only be decrypted by authorized recipients. Authentication mechanisms verify the identity of the communicating entities, ensuring that messages are sent and received from trusted sources.

Furthermore, VANET security also addresses the detection and prevention of specific attacks, such as Sybil attacks, where an attacker creates multiple false identities to disrupt the network. Detection algorithms and protocols are developed to identify and mitigate such threats effectively. [21] [33]

Vehicular ad hoc networks (VANETs) are a specialized type of mobile ad hoc networks (MANETs) that utilize vehicles as mobile nodes to enable communication between vehicles as well as between vehicles and infrastructure. The primary objective of VANETs is to improve road safety by facilitating the exchange of critical information among drivers regarding unexpected incidents and road conditions. In a VANET, vehicles can store and process a wide range of data, including their own location, traffic emergency alerts, accident reports, road conditions, vehicle tracking information, weather updates, and message monitoring.[47][25] These features empower vehicles to actively participate in creating a comprehensive and up-to-date information network that enhances situational awareness and contributes to safer and more efficient driving experiences.

Vehicular ad hoc networks (VANETs) consist of two main types of nodes: On-Board Units (OBUs) and Road Side Units (RSUs). OBUs are devices installed in moving vehicles and are equipped with GPS for precise location tracking and radio communication capabilities to establish connections with other vehicles and RSUs. RSUs, on the other hand, are stationary units positioned along the roadside and serve as intermediaries or routers between vehicles. They facilitate communication between the vehicles and the infrastructure. OBUs and RSUs utilize Dedicated Short Range Communication (DSRC) radios, which enable the establishment of wireless links between the vehicles and RSUs.[3] Through this connectivity, vehicles can exchange information with other vehicles and access relevant data from the roadside infrastructure, contributing to enhanced safety, traffic management, and efficient transportation systems. There are mainly two modes of communication in VANET:[12]

Vehicle-to-vehicle communication (V2V)**Figure 2.****Figure 1.1:** Vehicle to vehicle communication

Vehicle-to-Vehicle (V2V) communication in Vehicular Ad-Hoc Networks (VANETs) refers to the exchange of information between vehicles on the road as shown in figure 1.1. It enables vehicles to communicate with each other directly, forming an ad-hoc network without the need for a centralized infrastructure. V2V communication plays a crucial role in enhancing road safety, improving traffic efficiency, and enabling a wide range of applications in VANETs. V2V communication relies on wireless communication technologies, such as Dedicated Short-Range Communication (DSRC) or Cellular Vehicle-to-Everything (C-V2X) communication, [29] to enable vehicles to exchange data. These technologies utilize specific frequency bands and protocols to establish wireless links between vehicles.

Through V2V communication, vehicles can share important information in real-time, such as position, speed, acceleration, heading, and vehicle status. This exchange of information allows vehicles to perceive their surrounding environment, including the presence and behavior of nearby vehicles. By receiving and processing data from neighboring vehicles, each vehicle can make informed decisions to optimize driving strategies, avoid collisions, and improve traffic flow.

Vehicle-to-infrastructure communication (V2I) via roadside units.

Vehicle-to-infrastructure (V2I) communication in VANETs refers to the exchange of information between vehicles and the roadside infrastructure as shown in figure 1.2. In this communication paradigm, vehicles interact with fixed infrastructure elements such

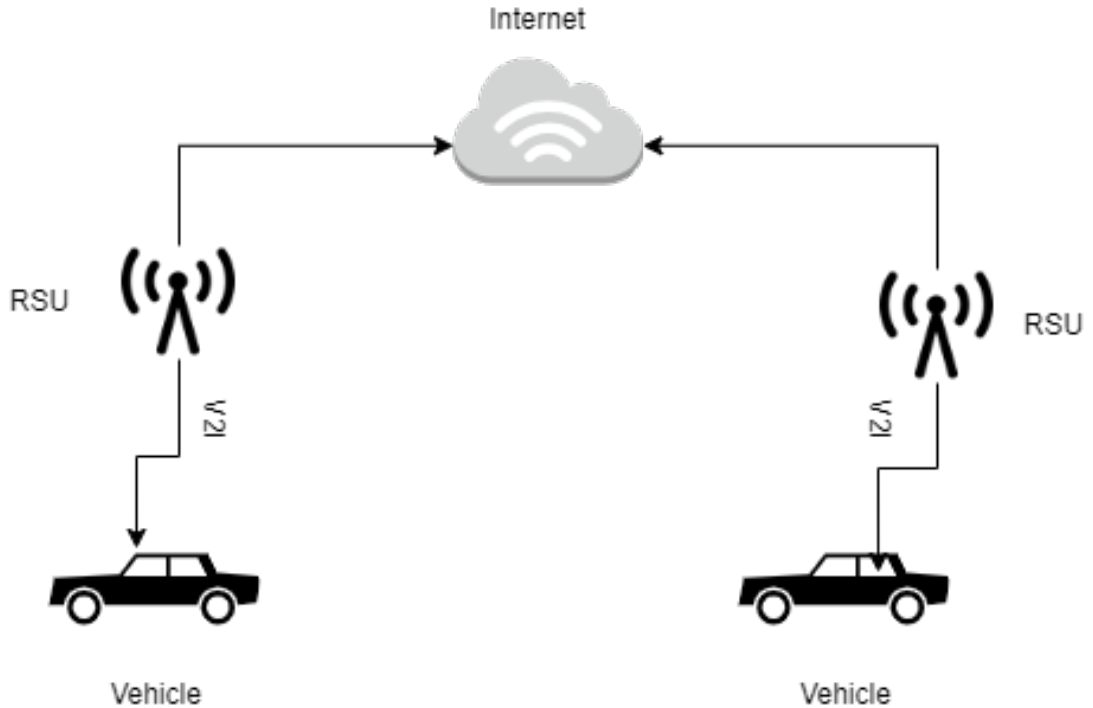


Figure 2.
Vehicle to Infrastructure Communication

Figure 1.2: Vehicle to infrastructure Communication

as roadside units (RSUs), traffic lights, and other infrastructure components. [21] V2I communication enables vehicles to access valuable real-time information, such as traffic conditions, road hazards, traffic signal timing, and road infrastructure updates. Vehicles can send requests for information or receive relevant data from the infrastructure, allowing them to make informed decisions and optimize their driving behavior. The infrastructure, equipped with sensors and communication devices, can relay important messages to vehicles, improving road safety, traffic efficiency, and overall transportation management. V2I communication plays a vital role in enabling advanced applications and services in VANETs, enhancing the overall driving experience and contributing to a smarter and more efficient transportation system.

1.0.2 VANET Infrastructure

Vehicular ad hoc networks (VANETs) infrastructure refers to the network of fixed elements and components that support communication and services in VANETs. This in-

Infrastructure includes roadside units (RSUs), traffic management systems, traffic lights, toll booths, and other fixed installations strategically placed along roadways. These infrastructure elements are equipped with sensors, communication devices, and processing capabilities to facilitate the exchange of information between vehicles and the infrastructure.

The VANET infrastructure serves as a backbone for communication, enabling seamless connectivity and data dissemination. It plays a crucial role in supporting various applications and services, such as traffic management, road safety, emergency assistance, navigation systems, and intelligent transportation systems. The infrastructure provides a platform for collecting and analyzing real-time data, allowing for better traffic control, congestion management, and efficient resource allocation. It serves as a reliable and robust foundation for enabling advanced functionalities in VANETs, contributing to safer and more efficient transportation systems.[14]

For VANET, IEEE specifies a communication stack for exchanging information known as Wireless Access for Vehicular Environment (WAVE) under IEEE 802.11p standards. The US federal communication commission (FCC) department defined 75 MHz of bandwidth at 5.9 GHz for dedicated short-range communication (DSRC).

1.1 Problem Statement

Vehicular Adhoc Networks (VANETs) encounter significant security and privacy challenges that must be addressed to ensure road safety. In VANETs, vehicles communicate with each other by exchanging messages containing crucial information about traffic and road conditions. These messages include data like the transmitting vehicle's position and speed, which are broadcasted to nearby vehicles. Given that drivers rely on this information to make informed decisions, security becomes a paramount concern. Simultaneously, privacy is also important to protect users from continuous tracking or identification. However, accountability is essential to promote responsible behavior among participants. Among the security and privacy issues faced by VANETs, Sybil attacks pose a significant threat that needs to be tackled effectively. [6]

Sybil attacks in VANETs can have serious consequences as they can compromise the integrity of the network and lead to dangerous situations such as collisions and accidents.

Malicious nodes can impersonate multiple legitimate nodes in the network, allowing attackers to manipulate communication flow and disrupt the normal operations of the network. This can result in false traffic updates and misleading information, which can have serious implications for the safety of drivers on the road. [40]

The presence of sybil attacks in Vehicular Adhoc Networks (VANETs) poses a significant security challenge, jeopardizing the overall network integrity and introducing potential hazards such as accidents and collisions. Sybil attacks occur when a malicious node impersonates multiple legitimate nodes within the network, (Figure 1.3) granting the attacker the ability to manipulate communication and disrupt normal network operations. Conventional sybil attack detection techniques in VANETs have limitations, particularly in dynamic and rapidly changing network environments, where accurately identifying malicious nodes becomes challenging. [2] [3] To address this issue, there has been a growing interest in leveraging topic detection approaches to enhance the accuracy and effectiveness of Sybil attack detection in VANETs. By analyzing the content and context of network messages, topic detection enables the identification of patterns and anomalies associated with Sybil attacks, facilitating early detection and mitigation of malicious behavior.[9]

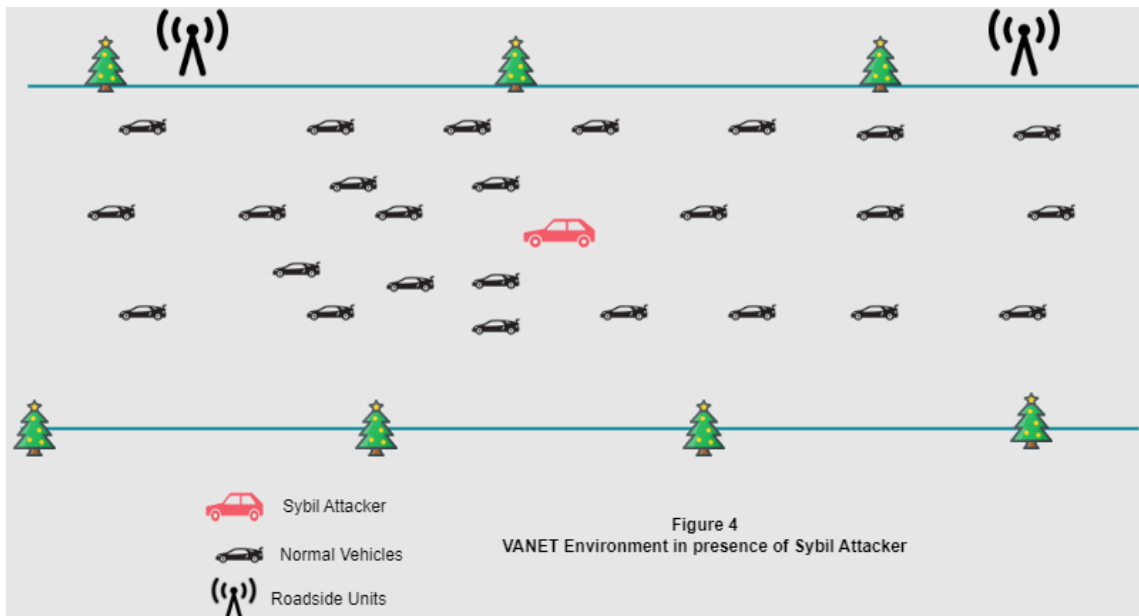


Figure 1.3: Sybil attack in VANET

1.2 Research Objective

Vehicular Ad-hoc Networks (VANETs) have unique requirements, including exchanging credible and accurate traffic information. In Vehicular Adhoc Networks (VANETs), cryptography plays a vital role in authenticating vehicles and maintaining the integrity of the shared information. However, the presence of Sybil attacks poses a significant challenge as malicious nodes can infiltrate the network and inject false data, compromising the reliability and trustworthiness of the information exchanged. To tackle this issue, extensive research is underway to develop effective techniques for detecting rogue nodes and enhancing the resilience of VANETs against false data injection.[27][22]

One key aspect of this research involves addressing sub-questions related to identity management. Establishing robust mechanisms for managing and assigning unique identities to vehicles is crucial for accurately identifying and differentiating legitimate nodes from malicious ones. By ensuring the integrity of identities, it becomes easier to detect and mitigate the impact of Sybil attacks.

Another focus area is the development of models that define normal and abnormal behavior in VANETs. By analyzing the behavior patterns of vehicles, deviations from expected norms can be identified, enabling the detection of suspicious activities that may indicate the presence of Sybil attacks. This helps in distinguishing genuine information from false data and maintaining the accuracy of the shared information.

Furthermore, efforts are being made to implement stringent access control mechanisms to prevent illegitimate nodes from infiltrating VANETs. By employing secure admission protocols and authentication procedures, the network can ensure that only authorized and trustworthy vehicles are allowed to participate in the information exchange, minimizing the risk of false data injection.

These research endeavors are crucial for establishing a secure and resilient VANET environment, where the safety and security of the network and its participants are prioritized. By effectively addressing the challenges posed by Sybil attacks and false data injection, VANETs can fulfill their potential in enhancing road safety and facilitating efficient communication among vehicles. The research question, therefore, is:

- how to detect sybil nodes in VANETs?
- how to prevent malicious nodes from entering the network?

- How to make and manage node identities?
- How to detect Sybil attacker in the network?
- And how to develop a VANET model to distinguish normal from abnormal behavior?

1.3 Research Methods

The research methodology employed to address the detection of sybil nodes in VANETs encompasses several sequential steps. The process begins with an extensive literature review to understand the security and privacy requirements specific to vehicular networks. This comprehensive understanding serves as a foundation for identifying various types of attacks that can target VANETs and formulating strategies for their detection and prevention.

Next, a VANET model is constructed, which enables the prediction of normal and exceptional behavior in different scenarios. This model acts as a reference for automated anomaly detection, incorporating a range of techniques and algorithms. The effectiveness of these techniques is evaluated through simulations conducted under diverse conditions to assess their performance in detecting malicious behavior within VANETs.

Throughout the research, the methodology adopts an iterative approach, continually refining and enhancing the detection techniques. This iterative process ensures that the selected methods are capable of accurately and efficiently identifying rogue nodes within VANETs. The goal is to achieve a robust and reliable sybil node detection system that can effectively safeguard the integrity and security of vehicular networks.[\[43\]](#)

1.4 Limitation

The research methodology employed to address the detection of rogue nodes in VANETs involves a systematic approach. Initially, a comprehensive literature review is conducted to gain insights into the specific security and privacy requirements of vehicular networks. This serves as a foundation for identifying the various types of attacks that can target VANETs and devising effective methods for their detection and prevention.

Subsequently, a VANET model is developed to simulate and predict the behavior of vehicles in both normal and special conditions. This model facilitates automated anomaly detection through the application of diverse techniques. To validate the model's accuracy and performance, simulations are carried out under different scenarios and conditions.

Throughout the research process, a range of techniques are explored and evaluated to select the most suitable approach for detecting malicious behavior in VANETs. This involves iterative testing, refinement, and improvement of the techniques to enhance their accuracy and effectiveness in identifying rogue nodes.

The research methodology emphasizes a systematic and iterative approach to ensure the development of robust and reliable techniques for detecting rogue nodes in VANETs. By combining literature review, VANET modeling, simulations, and technique evaluation, the research aims to contribute to the enhancement of security and privacy in vehicular networks.

Background

2.1 Vehicular ad-hoc Networks

Vehicular ad hoc networks (VANETs) are specialized networks formed by vehicles, including cars, buses, and trucks, along with their communication systems. These networks facilitate seamless communication and information exchange between vehicles and roadside infrastructure, such as traffic lights and toll booths as shown in figure 2.1. VANETs are envisioned to be a crucial component of intelligent transportation systems (ITS), which strive to enhance road safety, alleviate traffic congestion, and promote energy efficiency. By leveraging VANETs, vehicles can efficiently share important data and collaborate with their surroundings to enable smarter and more effective transportation solutions.

VANETs are characterized by their dynamic and fast-moving nature, which presents unique challenges for designing communication protocols and security mechanisms. Due to the high mobility of vehicles, nodes can frequently enter and leave the network, causing frequent topology changes. This makes it difficult to maintain stable network connections and ensure the delivery of messages. Moreover, the large number of nodes in VANETs and their varying speeds can lead to network congestion and high message delivery latency.

Another key challenge in VANETs is ensuring the security and privacy of communication. As vehicles exchange sensitive information about traffic conditions, road hazards, and other safety-related information, it is essential to ensure the authenticity, integrity, and confidentiality of the messages. Additionally, vehicles' privacy must be protected to

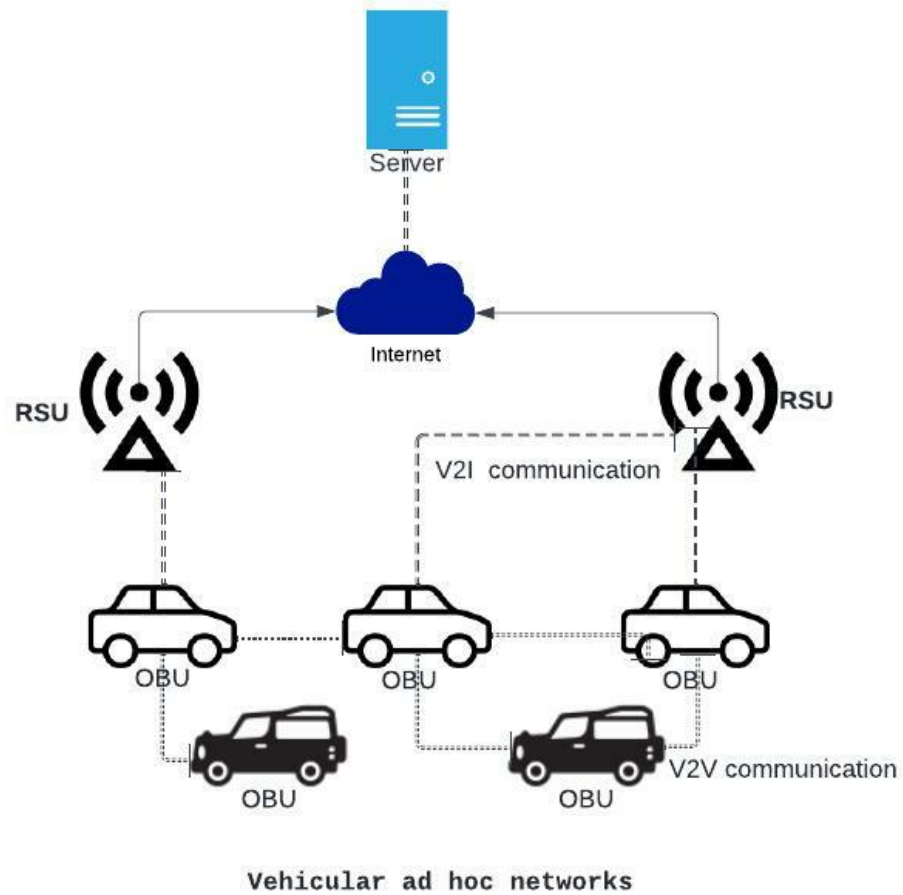


Figure 2.1: VANET Architecture

prevent unauthorized tracking and surveillance. Security and privacy in VANETs are crucial for maintaining trust among the network participants and ensuring the reliability of information exchanged.[31]

2.2 Vanet applications

Vehicular ad hoc networks (VANETs) have a wide range of potential applications in various fields.

- One of the primary applications of VANETs is in the area of intelligent transportation systems (ITS). In ITS, VANETs can be used to provide real-time traffic updates, identify and prevent accidents, and optimize traffic flow.

- With the help of VANETs, drivers can receive warnings about upcoming congestion, roadwork, and hazardous conditions, which can help them make informed decisions about their route and driving behavior.
- VANETs can also be used to enable emergency vehicles to communicate with other vehicles on the road and ensure a clear path for them to reach their destination as quickly as possible.

Another important application of VANETs is in the area of entertainment and infotainment.

- With the widespread use of smartphones and other handheld devices, VANETs can be used to provide passengers with a range of services such as internet access, video streaming, and music playback.
- VANETs can also be used to enable passengers to access real-time information about their surroundings, including nearby restaurants, shopping centers, and tourist attractions.
- By providing passengers with access to relevant information and services, VANETs can enhance the overall travel experience and make journeys more enjoyable and convenient.

2.3 Vanet Architecture

Vehicular Ad Hoc Networks (VANETs) are an emerging technology that provides wireless communication between vehicles on the road, and between vehicles and roadside infrastructure. The architecture of VANETs consists of three main components:

- On-Board Units (OBUs)
- Road-Side Units (RSUs)
- the communication infrastructure that connects them.

2.3.1 On-board Units

The On-Board Units (OBUs) are wireless devices installed in vehicles, incorporating sensors like GPS and accelerometers to gather important vehicle-related data such as

position, speed, and acceleration. These OBUs establish communication links with one another as well as with Road-Side Units (RSUs) using Dedicated Short Range Communication (DSRC) technology. DSRC operates within the 5.9 GHz frequency band and is specifically tailored for VANETs, offering features such as high-speed data transfer, low-latency communication, and secure transmission. This enables efficient and secure exchange of information among vehicles and between vehicles and the roadside infrastructure.[35]

2.3.2 Roadside Units

Road-Side Units are wireless access points that are installed along the roadside, and they are connected to the communication infrastructure via a wired or wireless network. RSUs provide an additional communication channel between vehicles and the infrastructure, and they can be used to deliver safety-related messages to vehicles, such as traffic congestion warnings, weather alerts, and road condition information. RSUs can also be used to provide Internet access to vehicles, enabling a wide range of new applications, such as infotainment, navigation, and e-commerce.

2.3.3 Communication infrastructure

The communication infrastructure that connects OBUs and RSUs is a crucial component of VANET architecture. It consists of a combination of wireless and wired networks, including cellular networks, Wi-Fi networks, and fiber-optic networks. The communication infrastructure enables OBUs and RSUs to exchange information in real time,[13] and it provides the necessary bandwidth and reliability to support a wide range of VANET applications. Additionally, the communication infrastructure can be used to collect and store data from vehicles and RSUs, which can be used for traffic management, urban planning, and other applications.[13]

2.4 Communication Technology for Vanets

Communication technology plays a critical role in enabling reliable and secure communication between vehicles and roadside infrastructure in VANETs.

2.4.1 Dedicated Short Range Communication

Dedicated Short Range Communication (DSRC) is the primary wireless communication technology specifically designed for Vehicular Adhoc Networks (VANETs). It operates in the 5.9 GHz frequency band and offers key features necessary for efficient vehicular communication. DSRC enables high-speed data transfer, ensuring quick and reliable transmission of information among vehicles and between vehicles and roadside infrastructure. It also ensures low-latency communication, allowing for near real-time exchange of critical data. To ensure secure communication, [37] DSRC utilizes advanced encryption techniques to protect the integrity and confidentiality of transmitted information. While other wireless technologies like Wi-Fi and cellular networks can also be used in VANETs, they are often employed for providing Internet access rather than optimized for vehicular communication. Hence, DSRC remains the primary choice for VANETs, and ongoing efforts are being made to further enhance its capabilities and promote interoperability with other wireless networks.

2.4.2 Wireless Access in Vehicular Environment (WAVE)

Wireless access in vehicular environments, also known as Vehicle-to-Everything (V2X) communication, is a key aspect of Vehicular Ad Hoc Networks (VANETs). It involves the establishment of wireless connections between vehicles and other entities, such as roadside infrastructure, pedestrians, and traffic management systems. This enables the exchange of information and data that can enhance road safety, improve traffic efficiency, and enable a wide range of applications.[19] [28]

In VANETs, vehicles are equipped with On-Board Units (OBUs) that use wireless communication technologies to exchange messages with each other and with Road-Side Units (RSUs) deployed along the road network. These units facilitate the transmission of safety-related information, such as traffic conditions, road hazards, and emergency alerts, to nearby vehicles.[1] Additionally, wireless access in VANETs enables vehicles to access the internet, providing opportunities for infotainment, navigation assistance, and real-time services.

The wireless access in VANETs relies on dedicated short-range communication (DSRC) or cellular-based technologies, such as LTE-V or 5G, to establish reliable and low-latency connections. These technologies allow for high-speed data transfer, support large-scale

deployments, and provide secure communication channels. Moreover, advanced antenna systems and communication protocols are employed to mitigate the challenges posed by the dynamic nature of the vehicular environment, including high mobility, varying signal strengths, and frequent topology changes.[32]

Overall, wireless access in vehicular environments is a fundamental component of VANETs, enabling vehicles to communicate with each other and with infrastructure elements. This communication plays a vital role in enhancing road safety, improving traffic management, and enabling a wide range of applications that enhance the overall driving experience.

2.4.3 VANET Characteristics

- High Mobility
- Low latency
- Trust
- Reliability

High Mobility

One of the key characteristics of VANETs is the high mobility of vehicles. As vehicles move rapidly in the network, their positions and connectivity constantly change. This dynamic mobility poses challenges for communication and coordination among vehicles and infrastructure components.

Low Latency

VANETs require low-latency communication due to the time-sensitive nature of many applications. Messages related to safety warnings, traffic information, and emergency situations need to be delivered quickly and efficiently to ensure timely responses and actions by vehicles and drivers.

Trust

Trust is a crucial aspect in VANETs as it ensures the reliability and authenticity of exchanged information. Establishing trust between vehicles and infrastructure components is essential to detect and mitigate potential security threats such as Sybil attacks. Trust mechanisms help in identifying trustworthy sources of information and filtering out malicious or false data.

Reliability

Reliability is of utmost importance in VANETs to ensure that critical information is accurately delivered and received by vehicles. Reliable communication is vital for safety-critical applications like collision avoidance, traffic management, and emergency response. Robust protocols and mechanisms are required to overcome the challenges posed by the dynamic nature of the network and ensure reliable data transmission.

Security Specifications in VANET

Security plays a vital role in the design and implementation of Vehicular Ad-Hoc Networks (VANETs) to ensure the protection and integrity of the network and its participants. Several security specifications are considered in VANETs to address various threats and vulnerabilities.

- **Authentication:** Authentication is a fundamental security requirement in VANETs to verify the identity of vehicles and ensure that messages are exchanged between trusted entities. Strong authentication mechanisms, such as digital signatures and certificates, are used to authenticate the source and integrity of messages.
- **Privacy Preservation:** Preserving privacy is crucial in VANETs to prevent unauthorized tracking or monitoring of vehicles' movements and activities. Techniques such as pseudonymity, mix-zones, and data aggregation are employed to anonymize vehicle identities and protect sensitive information.
- **Data Confidentiality:** VANETs involve the transmission of sensitive data, such as location information and emergency messages. Encryption techniques, such as

symmetric and asymmetric encryption algorithms, are used to protect the confidentiality of data during transmission and storage.

- **Message Integrity:** Ensuring message integrity is essential to prevent data tampering and manipulation by adversaries. Digital signatures and message authentication codes (MACs) are employed to verify the integrity of messages and detect any unauthorized modifications.
- **Access Control:** Access control mechanisms are implemented to regulate the participation of vehicles and restrict access to network resources. Only authorized vehicles are allowed to join the network and communicate with other trusted entities.
- **Intrusion Detection:** Intrusion detection systems monitor network activities and detect any malicious behavior or unauthorized access attempts. Anomaly-based and signature-based intrusion detection techniques are employed to identify potential attacks and take appropriate preventive measures.
- **Key Management:** Secure key management is crucial for maintaining the confidentiality and integrity of communication in VANETs. Key establishment, distribution, and revocation mechanisms are employed to ensure that keys are securely shared among trusted entities and revoked when compromised.
- **Resilience to Denial-of-Service (DoS) Attacks:** VANETs are vulnerable to various DoS attacks, which can disrupt communication, manipulate traffic information, or cause congestion. Resilient routing protocols, traffic monitoring mechanisms, and anomaly detection systems are implemented to detect and mitigate DoS attacks.
- **Trust Management:** Trust management systems evaluate the trustworthiness of vehicles based on their behavior, reputation, and endorsements from other trusted entities. Trust metrics and reputation scores are used to establish trust relationships and make informed decisions regarding message acceptance and collaboration.
- **Secure Firmware and Software Updates:** Ensuring the security of firmware and software in vehicles and RSUs is essential to prevent unauthorized modifications and code injection. Secure update mechanisms, digital signatures, and secure

bootstrapping techniques are employed to ensure the authenticity and integrity of updates.

These security specifications are crucial in VANETs to protect against various threats, including Sybil attacks, data tampering, privacy breaches, and DoS attacks. Implementing robust security measures and continuously monitoring the network for emerging threats are essential to maintain the safety and integrity of VANETs.

Security Challenges in VANET

Vehicular Ad-Hoc Networks (VANETs) are susceptible to various security attacks that can compromise the integrity, confidentiality, and availability of network resources and services. Here are some common types of security attacks in VANETs:

Sybil Attacks: In Sybil attacks, a malicious vehicle creates multiple fake identities or pseudonyms to gain unauthorized access to the network. These Sybil nodes can disrupt communication, manipulate traffic information, and launch various other attacks.

Denial-of-Service (DoS) Attacks: DoS attacks aim to disrupt the normal functioning of the network by overwhelming it with excessive traffic, consuming network resources, or exploiting vulnerabilities in the network protocols. This can lead to a loss of service availability and affect the overall performance of the VANET.

Masquerade Attacks: In masquerade attacks, an attacker impersonates a legitimate vehicle or authority to gain unauthorized access or manipulate the network. By masquerading as a trusted entity, the attacker can deceive other vehicles, RSUs, or infrastructure components.

Replay Attacks: Replay attacks involve the interception and re-transmission of previously captured network messages. Attackers may capture genuine messages exchanged between vehicles and replay them at a later time, causing confusion, false information propagation, or unauthorized access.

Eavesdropping and Information Disclosure: Eavesdropping attacks involve unauthorized interception and monitoring of communication between vehicles or between a vehicle and an RSU. Attackers can exploit this to gather sensitive information, such as location data, personal details, or communication patterns, leading to privacy breaches and potential misuse of the information.

GPS Spoofing and Tampering: GPS spoofing attacks involve the manipulation of Global Positioning System (GPS) signals to deceive vehicles and misguide their navigation systems. Attackers can provide false GPS information or alter legitimate GPS signals, leading to inaccurate positioning, incorrect routing, and potential accidents.

Traffic Information Manipulation: In these attacks, adversaries manipulate traffic-related information, such as congestion warnings, traffic flow data, or road conditions, to cause traffic jams, divert traffic to specific areas, or create chaos on the roads. This can disrupt the efficient flow of traffic and compromise road safety.

Message Falsification and Modification: Attackers may tamper with messages exchanged between vehicles or between vehicles and RSUs to modify their content, alter routing information, or inject false data. This can lead to misinformation, wrong decisions by vehicles, and compromised trust within the network.

Insider Attacks: Insider attacks involve malicious activities performed by trusted entities within the VANET, such as compromised RSUs, corrupt authorities, or rogue vehicles. These insider threats can exploit their privileged access to compromise network security, integrity, or privacy.

Physical Attacks: Physical attacks target the physical components of the VANET infrastructure, such as RSUs or onboard units. These attacks may involve physical tampering, vandalism, or theft, which can disrupt network operations and compromise the overall security and functionality of the VANET.

It is important to develop robust security mechanisms, protocols, and intrusion detection systems to detect and mitigate these security attacks in VANETs. Regular security assessments, updates, and collaboration among network participants are crucial to maintain the trust, confidentiality, and reliability of VANET environments.

Types of Attacks in Vanets

Vehicular Ad-Hoc Networks (VANETs) are susceptible to various security attacks that can compromise the integrity, confidentiality, and availability of network resources and services. Here are some common types of security attacks in VANETs [46]:

- **Sybil Attacks:** In Sybil attacks, a malicious vehicle creates multiple fake identities or pseudonyms to gain unauthorized access to the network. These Sybil nodes can

disrupt communication, manipulate traffic information, and launch various other attacks.

- **Denial-of-Service (DoS) Attacks:** DoS attacks aim to disrupt the normal functioning of the network by overwhelming it with excessive traffic, consuming network resources, or exploiting vulnerabilities in the network protocols. This can lead to a loss of service availability and affect the overall performance of the VANET.
- **Masquerade Attacks:** In masquerade attacks, an attacker impersonates a legitimate vehicle or authority to gain unauthorized access or manipulate the network. By masquerading as a trusted entity, the attacker can deceive other vehicles, RSUs, or infrastructure components.
- **Replay Attacks:** Replay attacks involve the interception and retransmission of previously captured network messages. Attackers may capture genuine messages exchanged between vehicles and replay them at a later time, causing confusion, false information propagation, or unauthorized access.
- **Eavesdropping and Information Disclosure:** Eavesdropping attacks involve unauthorized interception and monitoring of communication between vehicles or between a vehicle and an RSU. Attackers can exploit this to gather sensitive information, such as location data, personal details, or communication patterns, leading to privacy breaches and potential misuse of the information.
- **GPS Spoofing and Tampering:** GPS spoofing attacks involve the manipulation of Global Positioning System (GPS) signals to deceive vehicles and misguide their navigation systems. Attackers can provide false GPS information or alter legitimate GPS signals, leading to inaccurate positioning, incorrect routing, and potential accidents.
- **Traffic Information Manipulation:** In these attacks, adversaries manipulate traffic-related information, such as congestion warnings, traffic flow data, or road conditions, to cause traffic jams, divert traffic to specific areas, or create chaos on the roads. This can disrupt the efficient flow of traffic and compromise road safety.
- **Message Falsification and Modification:** Attackers may tamper with messages exchanged between vehicles or between vehicles and RSUs to modify their content,

alter routing information, or inject false data. This can lead to misinformation, wrong decisions by vehicles, and compromised trust within the network.

- **Insider Attacks:** Insider attacks involve malicious activities performed by trusted entities within the VANET, such as compromised RSUs, corrupt authorities, or rogue vehicles. These insider threats can exploit their privileged access to compromise network security, integrity, or privacy.
- **Physical Attacks:** Physical attacks target the physical components of the VANET infrastructure, such as RSUs or onboard units. These attacks may involve physical tampering, vandalism, or theft, which can disrupt network operations and compromise the overall security and functionality of the VANET.

It is important to develop robust security mechanisms, protocols, and intrusion detection systems to detect and mitigate these security attacks in VANETs. Regular security assessments, updates, and collaboration among network participants are crucial to maintain the trust, confidentiality, and reliability of VANET environments.

2.4.4 Sybil Attack in VANET

In a Vehicular Ad-Hoc Network (VANET), a Sybil attack refers to a malicious activity where a single node illegitimately creates multiple fake identities, known as Sybil nodes, to deceive other nodes in the network. These Sybil nodes can then engage in various malicious activities, such as spreading false information, disrupting communication, or launching coordinated attacks.

The impact of Sybil attacks in VANETs can be severe, as the trust and reliability of the network are compromised. These attacks can lead to misinformation, traffic congestion, accidents, and overall degradation of the system's performance and safety.

Sybil attacks exploit the decentralized nature of VANETs, where vehicles communicate directly with each other or with Roadside Units (RSUs). Since VANETs are based on wireless communication, it becomes challenging to authenticate the identity of each vehicle and ensure that it is not controlled by a Sybil attacker.

One common characteristic of Sybil attacks is the ability of malicious nodes to create multiple fake identities, which can be used to manipulate the network's behavior and compromise the integrity of data transmission. Sybil nodes can forge their identities,

generate false messages, and even create virtual platoons or groups to gain trust and influence the network's operations.

Detecting Sybil attacks in VANETs is a crucial research area to maintain the security and reliability of the network. Various detection approaches have been proposed, leveraging techniques such as cryptographic protocols, trust management systems, and anomaly detection mechanisms.

Cryptographic protocols involve the use of encryption, digital signatures, and secure key exchange to ensure the authenticity and integrity of messages exchanged between vehicles and RSUs. By validating the identity and integrity of the communication entities, these protocols can detect and prevent Sybil attacks.

Trust management systems aim to establish trust relationships among vehicles and RSUs based on reputation scores, endorsements from trusted entities, or historical behavior analysis. By monitoring and evaluating the trustworthiness of nodes, these systems can detect inconsistencies and deviations that may indicate Sybil attacks.[16]

Anomaly detection mechanisms analyze the behavior and communication patterns of nodes to identify deviations from normal operations. These approaches rely on statistical analysis, machine learning algorithms, or network traffic analysis to detect suspicious activities associated with Sybil nodes.

It is important to note that no single detection approach can completely eliminate Sybil attacks in VANETs. Therefore, a combination of multiple techniques and strategies is often employed to enhance the security and resilience of the network.

Sybil's attacks pose significant threats to the security and reliability of VANETs. Detecting and mitigating these attacks require the development of robust and efficient mechanisms that can verify the identities of nodes, detect anomalous behavior, and ensure the trustworthiness of communication within the network. Continuous research and advancements in this field are crucial to address the evolving challenges posed by Sybil attacks in VANETs.[15]

Types of Sybil Attack in VANET

In Vehicular Ad-Hoc Networks (VANETs), Sybil attacks are a type of security threat where malicious entities create multiple fake identities to deceive other vehicles and the

network. These attacks can have severe consequences, compromising the integrity and reliability of the communication and leading to various malicious activities. Here are the types of Sybil attacks commonly observed in VANETs[46]:

Identity Replication: In this type of Sybil attack, a malicious vehicle creates multiple fake identities, each with its own unique identifier. These fake identities pretend to be distinct vehicles, leading to an inflated number of vehicles in the network. By replicating identities, the attacker gains an unfair advantage in influencing network behavior, misdirecting traffic, or disrupting communication.

Identity Theft: In an identity theft Sybil attack, the malicious vehicle steals the identity of a legitimate vehicle. By impersonating a trusted entity, the attacker gains unauthorized access to the network and can perform various malicious activities, such as disseminating false information, injecting malicious code, or launching further attacks.

Sybil Collusion: Sybil collusion occurs when multiple malicious vehicles work together to coordinate their fake identities and deceive other vehicles or the network. By collaborating, these Sybil nodes can amplify their influence, manipulate network protocols, and disrupt the normal functioning of the VANET.

Sybil Wormhole: In a Sybil wormhole attack, malicious nodes create a virtual tunnel or shortcut between different parts of the network, allowing them to bypass normal communication routes. This enables the attackers to gain an advantage in terms of message propagation, causing delays, congestion, or even selectively blocking communication between legitimate vehicles.

Sybil Jamming: Sybil jamming attacks involve a malicious vehicle generating multiple fake identities and occupying a significant portion of the wireless spectrum, overwhelming the communication channels and causing interference. By flooding the network with excessive traffic, these Sybil nodes disrupt the communication between legitimate vehicles and degrade overall network performance.[31]

Sybil Misinformation: In this type of Sybil attack, the malicious vehicle disseminates false or misleading information to deceive other vehicles or manipulate traffic management systems. By injecting deceptive data, the attacker can create chaos, cause accidents, or manipulate traffic flow, leading to safety risks and disruption in the VANET. These types of Sybil attacks in VANETs undermine the trust and reliability of the network, compromising critical functionalities like traffic management, collision avoidance,

and emergency services. To counter these attacks, robust security mechanisms, including authentication, trust management, intrusion detection, and anomaly detection, are crucial to identify and mitigate the presence of Sybil nodes in the network, ensuring the integrity and safety of the VANET environment.

Literature Review

Vehicular Ad Hoc Networks (VANETs) are innovative technological systems designed to enhance road safety, optimize traffic flow, and enhance passenger convenience in contemporary transportation systems. These networks enable vehicles to establish communication links with one another as well as with roadside infrastructure, enabling the exchange of vital real-time information such as traffic updates, road hazards, and collision alerts. Nonetheless, VANETs encounter various security challenges, one of which is known as the Sybil attack..[17] [44]

The Sybil attack is a well-known security threat in VANETs. It involves attackers creating multiple fake identities [11] to gain unfair advantages or disrupt the network. By impersonating multiple vehicles, attackers can spread false information, manipulate routing protocols, create traffic congestion, or cause other harmful disruptions.

The Sybil attack is a serious problem in VANETs because accurate and reliable information is essential for safe and efficient transportation. False messages about road conditions can lead to incorrect routing decisions, traffic congestion, and even accidents. Trust and reputation mechanisms used in VANETs can also be exploited by attackers, undermining the overall reliability of these systems.[39][16]

Researchers have been working on developing security mechanisms and protocols to tackle the Sybil attack in VANETs. This literature review provides an overview of the latest approaches, methods, and advancements in detecting, mitigating, and preventing the Sybil attack in VANETs[46].

In this review, we will first explain the basics of VANETs, focusing on their unique security challenges. We will then discuss the different types and techniques of Sybil

attacks in VANETs, explaining their potential consequences. Next, we will explore existing methods proposed by researchers to detect and prevent Sybil attacks, analyzing their strengths and weaknesses.

We will also look at how researchers evaluate the effectiveness of Sybil attack detection and prevention schemes in VANETs, discussing the metrics and methodologies used. Additionally, we will identify gaps in the current research and highlight areas for future investigation [17]. Finally, we will summarize the key findings, discuss their implications for VANET security, and suggest future research directions.

This literature review aims to provide a comprehensive understanding of the Sybil attack in VANETs, examining existing research efforts, challenges, and advancements in mitigating this security threat. By analyzing state-of-the-art approaches, this review aims to contribute to the development of strong and reliable security mechanisms that ensure the safe and efficient operation of VANETs in real-world scenarios.

In a paper [2] based on localization of sybil nodes, author proposes a technique for detecting and localizing Sybil nodes in Vehicular Ad Hoc Networks (VANETs). The technique presented in the paper offers several advantages in addressing the Sybil attack in VANETs.

One advantage of the proposed technique is its ability to detect Sybil nodes by analyzing the unique physical properties of wireless communications in VANETs. By leveraging the signal strength and signal propagation characteristics, the technique can differentiate between legitimate and Sybil nodes, thus providing an effective means of detection. Furthermore, the technique offers the advantage of localization, enabling the identification of the physical location of Sybil nodes within the network. This information is valuable for taking appropriate action against the attackers and ensuring the security of the VANET. [2] [10]

However, the technique also has certain limitations. One limitation is its reliance on signal strength measurements, which can be affected by various environmental factors such as interference and obstacles. These factors can lead to inaccuracies in the detection and localization process. Additionally, the technique may face challenges in scenarios with high mobility, as the rapid movement of vehicles can impact the consistency and reliability of signal strength measurements.

So the paper presents a technique for detecting and localizing Sybil nodes in VANETs,

offering advantages such as leveraging physical properties for detection and providing localization capabilities. However, the technique also has limitations related to signal strength measurements and challenges in high mobility scenarios. Future research could focus on improving the robustness and accuracy of the technique, considering the dynamic nature of VANETs and addressing the limitations for more reliable detection and localization of Sybil nodes.

Platoon dispersion is an approach used to detect Sybil attacks in vehicular networks. In a platoon, vehicles travel closely together, which helps optimize communication signals, reduce congestion, and improve road safety [12]. However, various factors such as human behavior, lane changes, and road conditions can cause the platoon to disperse, losing its optimal formation.

In [8], two protocols are proposed to address this issue. The first protocol is executed by each vehicle within the platoon. It involves storing the identities of all the vehicles with which it has communicated while traveling between two Roadside Units (RSUs). These stored identities are then forwarded to the next RSU encountered along the route. The second protocol is executed by the RSU itself. Upon receiving the identities of vehicles in the platoon, the RSU waits for the minimum travel time. It then collects the forwarded identities from each vehicle.

Using the collected data, the RSU calculates the Cumulative Distribution Function (CDF) for the vehicles in the platoon. The CDF represents the probability distribution of the identities within the platoon. By analyzing this distribution, the RSU can identify any anomalies and determine if a Sybil attack is occurring.

The goal of this approach is to detect Sybil attacks by analyzing the dispersion pattern of vehicles within a platoon. If there are inconsistencies or abnormal distributions in the received identities, it suggests the presence of Sybil nodes. This method helps ensure the integrity and security of the platoon by identifying potential malicious activities.

By combining the vehicle-level protocol and the RSU-level protocol, this approach provides a comprehensive detection mechanism for Sybil attacks in platooning scenarios. It leverages the communication patterns and identity information to identify anomalies, making it a valuable contribution to the security of vehicular networks.

In another paper [3] author presents a defense mechanism against Sybil attacks in Vehicular Ad Hoc Networks (VANETs) by leveraging the support of roadside units (RSUs).

The paper proposes a novel approach that offers several advantages in mitigating the Sybil attack threat in VANETs.

One advantage of the proposed defense mechanism is its utilization of RSUs as trusted entities to validate the authenticity of vehicles in the network. The RSUs act as reliable points of reference, verifying the identity and integrity of vehicles and detecting any Sybil nodes present. By having the RSUs actively involved in the authentication process, the mechanism enhances the overall security of the VANET by minimizing the risk of false information propagation.

Furthermore, the use of RSUs enables efficient Sybil attack detection and isolation. The paper suggests a collaborative scheme between RSUs, where they exchange information about detected Sybil nodes and collectively take actions to isolate and neutralize the attackers. This collaborative approach leverages the communication infrastructure of RSUs to effectively identify and respond to Sybil attacks, thereby safeguarding the integrity of the VANET communication.

However, the defense mechanism does have some limitations. One limitation is the dependency on a well-established RSU infrastructure. For the proposed mechanism to be effective, a sufficient number of RSUs must be deployed, covering a substantial portion of the VANET area. This infrastructure requirement might pose challenges in regions with limited resources or in scenarios where the RSU deployment is not extensive.

Additionally, the scalability of the proposed defense mechanism may be a concern. As the number of vehicles and the complexity of the VANET increase, the communication overhead between RSUs may become significant, impacting the system's efficiency and response time. [3] Hence, further research is necessary to evaluate the scalability and performance of the defense mechanism in large-scale VANET deployments.

[3] the paper presents a defense mechanism against Sybil attacks in VANETs by leveraging the support of RSUs. The mechanism offers advantages such as utilizing trusted RSUs for authentication, efficient detection, and collaborative isolation of Sybil nodes. However, limitations related to infrastructure requirements and scalability should be considered for real-world deployment. Future research could focus on addressing these limitations and optimizing the performance of the defense mechanism in various VANET scenarios.

In the context of detecting Sybil attacks, the use of Received Signal Strength (RSS) is

proposed in [5]. The RSS is calculated by subtracting the signal attenuation from the transmission power. This approach relies on the analysis of RSS values by Roadside Units (RSUs), which are trusted nodes in the network.

In this scheme, vehicles periodically send beacons containing their identity and the time of transmission to the nodes within their communication range. Only RSUs have the capability to analyze these packets. The RSUs group similar RSS signals together, forming distinct groups. When a vehicle starts moving, its RSS value is observed by different RSUs at specific time intervals [5].

Legitimate nodes, also known as honest nodes, tend to exhibit varying RSS values depending on the group they belong to. On the other hand, Sybil attacks involve malicious nodes that consistently send the same RSS value. This repetitive behavior enables the RSUs to detect and identify Sybil attacks.

By leveraging the analysis of RSS values and comparing them across different RSUs, this approach provides a means to distinguish between legitimate nodes and Sybil nodes. The consistency in RSS values exhibited by Sybil nodes acts as a key indicator for their detection. This detection mechanism enhances the security and reliability of the network by identifying and mitigating the impact of Sybil attacks.

In summary, the proposed approach in [5] utilizes RSS analysis by RSUs to identify Sybil attacks. The variation in RSS values among legitimate nodes compared to the repetitive behavior of Sybil nodes allows for effective detection within the vehicular network.

In another paper [4] author presents a novel defense mechanism to combat Sybil attacks in Vehicular Ad Hoc Networks (VANETs). The paper introduces an innovative approach that offers several advantages in effectively detecting and mitigating the Sybil attack threat in VANETs.

One advantage of the proposed defense mechanism is its utilization of vehicle movement patterns to identify and isolate Sybil nodes. The mechanism leverages the unique movement characteristics of vehicles, such as speed, direction, and trajectory, to distinguish between legitimate vehicles and Sybil nodes. By analyzing and comparing the movement patterns of neighboring vehicles, the mechanism can detect any inconsistencies or anomalies that indicate the presence of Sybil attacks. [4] This approach enhances the accuracy of detection and reduces false positives, thereby improving the overall security of the VANET.

Furthermore, the proposed defense mechanism incorporates a reputation-based system to enhance the detection and isolation process. Each vehicle maintains a reputation score based on its past behavior and interactions within the network. Vehicles with high reputation scores are considered trustworthy, while those with suspicious or malicious behavior receive lower reputation scores. By using reputation as a criterion, the mechanism can further validate the authenticity of vehicles and effectively isolate Sybil nodes from the network.

However, the defense mechanism does have certain limitations. One limitation is the reliance on accurate and up-to-date location information. Since the mechanism heavily depends on analyzing vehicle movement patterns, accurate positioning data is crucial for detecting Sybil attacks. However, in real-world scenarios, factors such as GPS inaccuracies, signal loss, or deliberate spoofing can introduce errors in location information, which may affect the effectiveness of the defense mechanism.

Additionally, the scalability of the proposed mechanism may be a concern, especially in highly dynamic and congested VANET environments. As the number of vehicles increases, the computation and communication overhead required for analyzing and comparing movement patterns may become a challenge. Thus, further research is needed to assess the scalability of the defense mechanism and optimize its performance in large-scale VANET deployments.[4]

In conclusion, the paper presents a novel defense mechanism against Sybil attacks in VANETs, utilizing vehicle movement patterns and a reputation-based system for detection and isolation. The mechanism offers advantages such as improved accuracy in detecting Sybil nodes and leveraging reputation scores for validation. However, limitations related to accurate location information and scalability should be taken into account when considering real-world deployment. Future research could focus on addressing these limitations and evaluating the mechanism's performance in various VANET scenarios.[36]

In another paper, [12] author presents a defense mechanism against Sybil attacks in Vehicular Ad Hoc Networks (VANETs) by leveraging the support of roadside units (RSUs). The paper proposes a novel approach that offers several advantages in mitigating the Sybil attack threat in VANETs.

One advantage of the proposed defense mechanism is its utilization of RSUs as trusted

CHAPTER 3: LITERATURE REVIEW

Article name	Year	Tool Used	Methodology	Limitations
Detection and Localization of Sybil Nodes in VANETs.	2006	SUMO, MOVE	Neighbors authentication	Vulnerable to false signal strength measurement, not suitable for the dense traffic and
Defense Against Sybil attack in vehicular AD hoc network Based on roadside unit	2009	SUMO	Aggregated timestamp	Not suitable for complex roads
A Novel Defense Mechanism against Sybil Attacks in VANET	2010	NCTUns-5.0 simulator	Position based verification	More false positives in a small scale network.
A Sybil Attack Detection Approach using Neighboring Vehicles in VANET	2011	multi-agent microscopic traffic simulator (MMTS)	Neighboring information	Fails in high-density traffic scenarios
Isolation of sybil attack in vanet using neighboring information	2015	NS2	Neighboring information	the larger number of Sybil nodes will degrade the detection rate.
Distributed Consensus based sybil nodes detection in VANETs	2017	NS3	Neighboring information	potential impact of colluding attackers
On detection of Sybil attack in large scale VANETs using spider-monkey technique	2018	Not mentioned	Time based	Performance not evaluated on realistic traffic data.
A Macroscopic Traffic Model Based Approach for sybil attack detection in Vanets	2019	NS3, SUMO	Neighboring information	scalability of the proposed mechanism may be a concern
A collaborative strategy for detection and eviction of sybil nodes and sybil attackers in VANET	2020	NS2, SUMO	Physical location, ESS, RSS	Privacy issues are not considered.
Sybil Attack with RSU Detection and Location Privacy in Urban VANETs: An efficient ERSS Technique	2021	NS2	Encryption Decryption	Authentication and privacy not considered.

Figure 3.1: Literature Review

entities to validate the authenticity of vehicles in the network. The RSUs act as reliable points of reference, verifying the identity and integrity of vehicles and detecting any Sybil nodes present.[7] By having the RSUs actively involved in the authentication process, the mechanism enhances the overall security of the VANET by minimizing the risk of false information propagation.

Furthermore, the use of RSUs enables efficient Sybil attack detection and isolation. The paper suggests a collaborative scheme between RSUs, where they exchange information about detected Sybil nodes and collectively take actions to isolate and neutralize the attackers. This collaborative approach leverages the communication infrastructure of RSUs to effectively identify and respond to Sybil attacks, thereby safeguarding the integrity of the VANET communication. [12]

However, the defense mechanism does have some limitations. One limitation is the dependency on a well-established RSU infrastructure. For the proposed mechanism to be effective, a sufficient number of RSUs must be deployed, covering a substantial portion

of the VANET area. This infrastructure requirement might pose challenges in regions with limited resources or in scenarios where the RSU deployment is not extensive.

Additionally, the scalability of the proposed defense mechanism may be a concern. As the number of vehicles and the complexity of the VANET increase, the communication overhead between RSUs may become significant, impacting the system's efficiency and response time. Hence, further research is necessary to evaluate the scalability and performance of the defense mechanism in large-scale VANET deployments.

In conclusion, the paper presents a defense mechanism against Sybil attacks in VANETs by leveraging the support of RSUs. The mechanism offers advantages such as utilizing trusted RSUs for authentication, efficient detection, and collaborative isolation of Sybil nodes. However, limitations related to infrastructure requirements and scalability should be considered for real-world deployment. Future research could focus on addressing these limitations and optimizing the performance of the defense mechanism in various VANET scenarios. [12]

In the paper [6] presents a novel defense mechanism to combat Sybil attacks in Vehicular Ad Hoc Networks (VANETs). The paper introduces an innovative approach that offers several advantages in effectively detecting and mitigating the Sybil attack threat in VANETs.

One advantage of the proposed defense mechanism is its utilization of vehicle movement patterns to identify and isolate Sybil nodes. The mechanism leverages the unique movement characteristics of vehicles, such as speed, direction, and trajectory, to distinguish between legitimate vehicles and Sybil nodes. By analyzing and comparing the movement patterns of neighboring vehicles, the mechanism can detect any inconsistencies or anomalies that indicate the presence of Sybil attacks. This approach enhances the accuracy of detection and reduces false positives, thereby improving the overall security of the VANET.

Furthermore, the proposed defense mechanism incorporates a reputation-based system to enhance the detection and isolation process. Each vehicle maintains a reputation score based on its past behavior and interactions within the network. Vehicles with high reputation scores are considered trustworthy, while those with suspicious or malicious behavior receive lower reputation scores. By using reputation as a criterion, the mechanism can further validate the authenticity of vehicles and effectively isolate Sybil nodes

from the network. [6]

However, the defense mechanism does have certain limitations. One limitation is the reliance on accurate and up-to-date location information. Since the mechanism heavily depends on analyzing vehicle movement patterns, accurate positioning data is crucial for detecting Sybil attacks. However, in real-world scenarios, factors such as GPS inaccuracies, signal loss, or deliberate spoofing can introduce errors in location information, which may affect the effectiveness of the defense mechanism. [6]

Additionally, the scalability of the proposed mechanism may be a concern, especially in highly dynamic and congested VANET environments. As the number of vehicles increases, the computation and communication overhead required for analyzing and comparing movement patterns may become a challenge. Thus, further research is needed to assess the scalability of the defense mechanism and optimize its performance in large-scale VANET deployments.

The paper presents a novel defense mechanism against Sybil attacks in VANETs, utilizing vehicle movement patterns and a reputation-based system for detection and isolation. The mechanism offers advantages such as improved accuracy in detecting Sybil nodes and leveraging reputation scores for validation. [38] However, limitations related to accurate location information and scalability should be taken into account when considering real-world deployment. Future research could focus on addressing these limitations and evaluating the mechanism's performance in various VANET scenarios.

Another paper [24] where author presents a novel approach for detecting Sybil attacks in Vehicular Ad Hoc Networks (VANETs) by utilizing a macroscopic traffic model. The paper introduces a technique that offers a unique perspective in detecting and mitigating the Sybil attack threat in VANETs.

The approach presented in the paper leverages the macroscopic traffic model to analyze the overall traffic patterns and characteristics in the VANET. By considering the collective behavior of vehicles, the technique aims to identify abnormal patterns that may indicate the presence of Sybil nodes. The macroscopic traffic model provides insights into the global behavior of the network, enabling the detection of discrepancies and inconsistencies caused by Sybil attacks.

The technique also utilizes statistical analysis techniques to extract relevant features and parameters from the macroscopic traffic model. These features are then used to

train a machine learning model, such as a support vector machine (SVM), to classify normal and Sybil traffic patterns. By learning from the extracted features, the machine learning model can accurately identify the presence of Sybil attacks in real-time. [24]

The experimental evaluation conducted in the paper demonstrates the effectiveness of the proposed approach. The results show that the approach achieves high detection accuracy and low false-positive rates when tested on real-world VANET datasets. The technique's ability to leverage macroscopic traffic information and machine learning models provides a promising solution for detecting and combating Sybil attacks in VANETs.

The limitations of the paper include potential challenges in implementing the technique in real-world VANET environments, scalability concerns as the number of vehicles increases, susceptibility to advanced evasion techniques employed by attackers, and the overhead and resource requirements associated with deploying and maintaining machine learning models. Further research is needed to address these limitations and ensure the effectiveness and practicality of the proposed approach.

The paper titled [42] "A Collaborative Strategy for Detection and Eviction of Sybil Nodes and Sybil Attackers in VANETs" presents a collaborative strategy for effectively detecting and evicting Sybil nodes and Sybil attackers in Vehicular Ad Hoc Networks (VANETs). The proposed technique combines a reputation-based system and a cooperative verification process among vehicles to enhance the security of the VANET.

The technique leverages a reputation-based system where each vehicle maintains a reputation score based on its behavior and interactions within the network. The reputation score serves as an indicator of trustworthiness, allowing vehicles to assess the authenticity of their neighbors. [42] Vehicles with high reputation scores are considered reliable, while those with suspicious or malicious behavior receive lower scores. This reputation-based system helps identify potential Sybil nodes and Sybil attackers.

Additionally, the technique employs a cooperative verification process among vehicles. When a vehicle encounters a suspicious neighbor, it collaborates with other nearby vehicles to verify the authenticity of the suspected node. The vehicles exchange information and collectively analyze the behavior and communication patterns of the suspected node. Through this cooperative verification process, the technique aims to detect and evict Sybil nodes and Sybil attackers from the VANET effectively.

One limitation of the proposed technique is the potential impact of colluding attackers.

In scenarios where multiple Sybil nodes or Sybil attackers collaborate and coordinate their activities, it becomes challenging to distinguish them from legitimate vehicles solely based on reputation scores and cooperative verification. Collusion among attackers can lead to more sophisticated and deceptive behavior, posing a challenge for accurate detection and eviction.

Furthermore, the scalability of the technique may be a concern, particularly in large-scale VANET deployments. As the number of vehicles increases, the communication and computational overhead required for cooperative verification may become significant. The effectiveness and efficiency of the technique in detecting and evicting Sybil nodes and Sybil attackers should be evaluated in scenarios with a higher number of vehicles and network congestion. [42]

In a paper [45] regarding security concerns author presents an efficient technique called EPORP (Efficient Pseudonym Change with Online Reputation Protocol) for detecting Sybil attacks with Roadside Unit (RSU) assistance and preserving location privacy in Urban Vehicular Ad Hoc Networks (VANETs).

The technique utilizes a combination of pseudonym change and online reputation mechanisms to detect Sybil attacks. Each vehicle periodically changes its pseudonym to prevent Sybil nodes from persistently impersonating multiple identities. The RSUs play a crucial role in assisting with the pseudonym change process and maintaining a trusted authority for verifying the integrity of vehicles in the network.

The online reputation protocol is employed to assess the trustworthiness of vehicles based on their behavior and interactions within the network. Reputation scores are assigned to each vehicle, considering factors such as message forwarding, cooperation, and adherence to network protocols. The reputation scores are updated dynamically, allowing the detection of suspicious and malicious vehicles that may be engaged in Sybil attacks.[30]

Additionally, the technique focuses on preserving location privacy in urban VANETs. Vehicles employ k-anonymity techniques, where multiple vehicles in close proximity share the same pseudonym and position, making it difficult for adversaries to accurately track the movements of individual vehicles. [45] One limitation of the EPORP technique is the dependency on RSUs for pseudonym change assistance. In areas with limited RSU coverage, the effectiveness of the technique may be compromised. The availability and

deployment of RSUs play a crucial role in ensuring the efficiency and reliability of the pseudonym change process and the overall detection of Sybil attacks.

Furthermore, the technique may face challenges in highly dynamic urban environments with frequent vehicle mobility and varying network topologies. Rapid changes in the network structure and intermittent connectivity can impact the efficiency and accuracy of the online reputation protocol and the preservation of location privacy. The robustness and adaptability of the technique under such dynamic conditions should be further evaluated. [47]

In conclusion, the paper presents the EPORP technique for detecting Sybil attacks with RSU assistance and preserving location privacy in urban VANETs. The technique combines pseudonym change, online reputation mechanisms, and k-anonymity techniques. However, limitations related to RSU dependency and highly dynamic urban environments should be considered for real-world implementation. Further research can focus on addressing these limitations and optimizing the performance of the EPORP technique in diverse urban VANET scenarios.

In a paper based on consensus approach [23], author proposes a distributed consensus-based technique for detecting Sybil nodes in Vehicular Ad Hoc Networks (VANETs). The paper presents a literature review and analysis of this technique, highlighting its advantages and limitations.

The technique leverages the principles of distributed consensus to detect Sybil nodes effectively. It utilizes a voting-based approach where vehicles in the network collaborate to reach a consensus regarding the authenticity of neighboring vehicles. Each vehicle collects and exchanges information with its neighbors, including position, speed, and communication patterns. By analyzing this information and comparing it with the consensus reached by the neighboring vehicles, Sybil nodes can be identified. [23]

One advantage of the proposed technique is its decentralized nature, allowing detection without relying on a centralized authority or infrastructure. This decentralized approach enhances the scalability and resilience of the detection mechanism, as it can operate effectively even in large-scale VANETs with dynamic network conditions. Additionally, the technique does not require extensive communication overhead, as only local information exchange is necessary for consensus formation.

However, the technique has certain limitations. First, the accuracy of Sybil node detec-

tion heavily relies on the assumption that the majority of vehicles in the network are honest and behave correctly. In scenarios with a high concentration of Sybil nodes or a large-scale collusion among attackers, the detection accuracy may decrease, and false negatives or false positives could occur.

Another limitation is the vulnerability of the technique to attacks aimed at manipulating the consensus formation process. Malicious nodes may attempt to bias the consensus by strategically influencing the information exchanged or by launching Sybil attacks specifically designed to deceive the consensus-based detection. The paper does not extensively discuss countermeasures or mitigation strategies for such attacks.

So the distributed consensus-based technique for Sybil node detection in VANETs presents a decentralized approach with advantages in scalability and resilience. However, limitations related to the assumption of majority honesty and vulnerability to attacks on the consensus formation process should be taken into account. Future research can focus on addressing these limitations, improving the accuracy of detection under adversarial conditions, and exploring additional security measures to enhance the effectiveness of the technique in real-world VANET deployments.

Security and Privacy Preserving Schemes in VANETs

In order to safeguard the security of VANETs, preserving the confidentiality of location information, commonly referred to as Location Privacy, is of utmost importance. Unauthorized disclosure of this sensitive data can potentially enable adversaries to track vehicles or monitor their routes (Author's Last Name, Year). To tackle this issue and ensure anonymity and privacy protection, several security schemes have been developed, each employing distinct underlying security mechanisms. These schemes can be broadly categorized as follows:

Pseudonyms coupled with Public Key Infrastructure (PKI): This approach involves the use of pseudonyms, or temporary identities, for vehicles to communicate within the network. These pseudonyms are managed using a Public Key Infrastructure, which provides a framework for secure key management and authentication.

- Trust-based schemes: Trust-based schemes establish trust relationships among vehicles to ensure secure communication. They utilize trust metrics or reputation systems to assess the reliability and integrity of participating vehicles, enabling

the detection of malicious entities.

- **Group signatures:** Group signature schemes provide a means for vehicles to collectively sign messages while maintaining the anonymity of individual signers. This ensures that the origin of a message can be verified without revealing the identity of the sender.
- **Identity-based signature schemes:** Identity-based signature schemes use unique identifiers, such as vehicle identifiers or attributes, to generate signatures. These schemes offer a flexible and efficient approach to authenticate messages and ensure the privacy of vehicle identities.
- **K-anonymity schemes:** K-anonymity schemes aim to achieve anonymity by ensuring that a vehicle's location information remains indistinguishable among a group of at least K similar vehicles. By blending in with a larger set of vehicles, individual vehicles can protect their privacy and prevent identification.

Each of these schemes employs different techniques and approaches to safeguard location privacy and mitigate the risks associated with unauthorized tracking or monitoring. [26] There's some issues faced regarding these techniques which are already proposed and will be discussed further :

In Vehicular Ad Hoc Networks (VANETs), preserving privacy is crucial when vehicles transmit location information for accident warnings. Two research papers, referenced as [24] and [26], propose using pseudonyms to protect users' real identities and maintain unlinkability. However, it's important to note that if a user engages in illegal activities, the Trusted Authority (TA) responsible for issuing pseudonyms can reveal the real identity, enabling traceability. [40]

In the context of VANETs, the On Board Unit (OBU) installed in vehicles is typically considered as a secure device that cannot be tampered with. Each OBU is assigned a unique Vehicle Identification Number (VIN) which serves as its identifier. During the registration process, a trusted entity such as a transport authority (TA) associates an identity certificate with the VIN of the vehicle. These identity certificates are then used to establish secure communication between the vehicles and Road Side Units (RSUs).

To protect the privacy of vehicles, the TA assigns blocks of pseudonyms or certificates to the vehicles. These pseudonyms are used by the vehicles for communication with

the RSUs, ensuring that their actual identities are not revealed. The pseudonyms have a limited validity period, and to enhance privacy, vehicles periodically switch to new pseudonyms within the allocated blocks. The frequency of pseudonym changes can vary depending on the specific scheme or policy implemented.[24] However, it is important to strike a balance, as frequent pseudonym changes can impose additional computational overhead on the RSUs, potentially impacting the delivery of packets in the network.

It is crucial to note that while the use of pseudonyms and identity certificates helps preserve the privacy of vehicles in VANETs, the frequency of pseudonym changes should be carefully considered to optimize the trade-off between privacy protection and computational efficiency. Finding the right balance ensures that vehicles can maintain their anonymity while minimizing any potential impact on the performance of the network. [15]

While pseudonym schemes ensure identity privacy, they do not guarantee location privacy. Attackers can potentially monitor changes in certificates as vehicles move between observation points with the same speed in the same lane. Moreover, the TA/CA has the capability to identify a vehicle's real identity based on its anonymous certificate. To enhance security, methods have been proposed that involve multiple authorities for de-anonymizing a user. Some studies suggest changing pseudonyms only at predetermined locations known as mix zones, where vehicle density and speed frequently change. However, this technique may provide limited privacy due to the lack of randomness in vehicle mobility.

A significant challenge with pseudonym schemes is maintaining the Certificate Revocation List (CRL) to track revoked certificates of misbehaving vehicles. Checking the CRL for each vehicle can be time-consuming and resource-intensive. To address this, researchers propose reducing the CRL size by limiting it to specific regions, with each Regional Transportation Authority (RTA) maintaining its own CRL. [12]

In summary, using pseudonyms coupled with PKI-based schemes in VANETs ensures unlinkability and privacy preservation. However, challenges exist, including the need for pseudonym refreshing, the computational overhead of PKI, the trade-off between privacy and location information, and the management of CRLs. Further research is necessary to address these limitations and enhance the security and privacy mechanisms in VANETs.

Trust-based security schemes have been proposed for Vehicular Ad Hoc Networks (VANETs) by researchers. These schemes involve assigning a trust score to each vehicle, which can be managed either centrally or through self-organization. In the case of centralized trust management, a centralized system is responsible for recording and maintaining trust scores. However, efficiently managing a large list of users can be challenging. On the other hand, self-organizing trust schemes assign trust scores based on direct or indirect interactions, taking into account current or past behavior. However, such schemes face challenges such as determining default trust scores for new users and protecting against insider attacks within the network. [40]

To address these challenges, researchers have proposed data-centric trust schemes, as mentioned in [58]. These schemes focus on identifying malicious nodes by analyzing the exchanged data. For instance, in [8], a data-centric mechanism is suggested where users can aggregate data and detect rogue nodes that transmit false information. This detection allows for reporting such nodes and subsequently disregarding their data. It is important to note that a detailed discussion on data-centric schemes will be provided in the subsequent chapter.

Although VANETs share similarities with Mobile Ad-Hoc Networks (MANETs), such as their decentralized nature, mobility, and openness, they differ significantly due to the larger number of nodes and the faster-changing topology caused by high-speed vehicles. Trust-based routing schemes developed for MANETs have also been applied to VANETs. However, establishing a trustworthy network in VANETs presents unique challenges because the focus is not solely on reliable packet delivery but also on making rapid decisions to ensure safety within the limited time available. [4]

Trust establishment in VANETs can be achieved through infrastructure-based or self-organizing approaches. Infrastructure-based trust establishment relies on a central authority or security infrastructure. However, implementing such a system quickly in VANETs is challenging due to the constraints of scale and time.

In summary, trust-based security schemes in VANETs involve assigning trust scores to vehicles. These schemes can be managed centrally or through self-organization. Researchers have also proposed data-centric trust schemes that focus on analyzing exchanged data to detect malicious nodes. VANETs have unique characteristics compared to MANETs, emphasizing the need for trustworthy networks to ensure safety.

Trust establishment in VANETs can be approached through infrastructure-based or self-organizing methods, with the former facing challenges in implementation due to the scale and time constraints involved. [18]

Research based on authentication

In the field of VANET security, several schemes have been developed to ensure secure communication between vehicles. These schemes involve encrypting and decrypting messages using various cryptographic techniques such as symmetric encryption, asymmetric encryption, hash functions, and digital certificates. They aim to establish a link between a vehicle's position and its identity. Below, I will describe three schemes that fall under this category:

Footprint Scheme:

In [12], the authors propose a scheme called "Footprint" that relies on the trajectory or path of a vehicle to identify it uniquely. When a vehicle passes by a Road Side Unit (RSU), the RSU issues an authorization message to the vehicle, serving as evidence that the vehicle has passed by that specific RSU. This scheme leverages the concept of RSUs as trusted entities in the network.

Timestamp Series Certificate Approach and Temporary Certificate Approach:

In [24], the authors present two schemes that focus on the type of certificate used. These schemes aim to reduce system architecture requirements and computational costs associated with certificate management, making them suitable for early-stage VANET deployment. The components of these schemes include a Certificate Authority (CA) and RSUs.

The first approach is the "Timestamp Series Certificate Approach." Each RSU generates a certificate containing the current timestamp. When a vehicle passes by an RSU, it receives a certificate with the current timestamp. This allows vehicles to obtain a series of timestamp certificates. However, this approach faces challenges in urban environments due to complex road structures and intersections, which may lead to similar timestamps among vehicles. Deploying RSUs at the edges can help mitigate these challenges.

The second approach is the "Temporary Certificate Approach." In this approach, RSUs generate temporary key pairs and certificates that are valid for a short period. A vehicle

undergoes authentication by an RSU to obtain the initial certificate. Subsequently, the vehicle regenerates its key pair and certificate with each subsequent RSU, creating a chain of certificates. This approach increases the likelihood of detecting Sybil nodes compared to the previous approach that relies on one certificate at a time.

Privacy-Preserving Detection of Abuses of Pseudonyms (P2DAP) Scheme: In another scheme introduced in [42], named "Privacy-Preserving Detection of Abuses of Pseudonyms" (P2DAP), the system components include the Department of Motor Vehicle (DMV) and Road Side Boxes (RSBs), which are similar to RSUs in previous schemes. RSBs are securely connected to the DMV via a backhaul wired network. The P2DAP scheme assumes that the DMV generates a sufficient number of pseudonyms for all vehicles. These pseudonyms undergo a two-step hashing process. First, a one-way global key K_c is used to hash the pseudonyms, and this key is distributed to all RSBs in the network. The resulting hashed pseudonyms are then organized into coarse-grained groups based on selected bits. Next, these groups are further hashed using another one-way key K_f , known only by the DMV, creating fine-grained groups.

Sybil attack detection in the P2DAP scheme operates in two levels. Initially, RSBs overhear message exchanges and create a list of used pseudonyms. They then calculate the coarse-grained hash value for each event. If two or more vehicles are found in the same coarse-grained group, it suggests a potential Sybil attack, and the RSB sends a report to the DMV. Subsequently, the DMV hashes the suspicious pseudonyms using K_c and K_f . If the hashed pseudonyms are found in the same fine-grained group, they are identified as Sybil nodes; otherwise, it is considered a false alarm.

Performance Comparison

To conduct a comprehensive performance comparison of the discussed schemes in this thesis, it is essential to obtain detailed information about the algorithms proposed for each scheme. Parameters such as communication overhead and bandwidth utilization are commonly used to evaluate network performance. However, accurately calculating these values requires specific knowledge about the data types and sizes that will be handled by the On-Board Unit (OBU). Given that the exact applications to be deployed in VANETs have not been finalized, estimating these parameters becomes challenging.[34] [11]

To facilitate scheme comparison, we have defined or adjusted certain parameters aiming

to capture significant performance characteristics. Additionally, we have highlighted the primary features and limitations of each scheme. In order to simplify the comparison process, we have assigned a rating system of HIGH, MED, and LOW to indicate the relative performance of the schemes.[\[41\]](#) Figure 3.1 shows methodology used in previous scheme and their limitations.

While group signatures offer a heightened level of privacy, scalability becomes a challenge as the group size increases, leading to potential issues. Additionally, implementing group signatures can incur higher computational costs.

Design and Methodology

4.1 Research Objectives

The research objectives of studying Sybil attacks in VANETs are:

- To investigate the vulnerabilities and potential risks posed by Sybil attacks in Vehicular Ad Hoc Networks.
- To develop effective and efficient detection methods to identify and mitigate Sybil attacks in real-time scenarios.
- To evaluate the performance and effectiveness of the proposed detection techniques in terms of accuracy, false positive/negative rates, and computational overhead.
- To enhance the security and reliability of VANETs by developing countermeasures against Sybil attacks, thereby ensuring the integrity and trustworthiness of the network.
- To contribute to the body of knowledge in the field of VANET security by exploring novel approaches and methodologies for Sybil attack detection and prevention.
- To assess the impact of Sybil attacks on various VANET applications, such as traffic management, collision avoidance, and emergency services, and propose solutions to ensure the uninterrupted operation of these applications in the presence of such attacks.
- To raise awareness among network administrators, policymakers, and stakeholders

about the significance of Sybil attacks in VANETs and the need for robust security measures to safeguard the integrity and privacy of vehicular communications.

- By addressing these research objectives, the study aims to advance the understanding of Sybil attacks in VANETs and contribute to the development of effective countermeasures to protect the network from malicious activities and ensure secure and reliable vehicular communications.

4.2 System Architecture

The system architecture of a Sybil attack in VANET involves various components and entities within the network. At a high level, the architecture includes the following elements:

Vehicles (VANET Nodes): These are the individual vehicles equipped with On-Board Units (OBUs) that communicate with each other and with infrastructure elements. Each vehicle acts as a node in the VANET and participates in information exchange.

Road Side Units (RSUs): These are stationary units deployed along the road infrastructure that provide communication and support services to the vehicles. RSUs serve as the access points for vehicles to connect to the infrastructure network.

Certificate Authorities (CAs): CAs are responsible for issuing and managing digital certificates that validate the authenticity of vehicles in the network. They play a crucial role in establishing trust and secure communication between vehicles and infrastructure.

Trust Authorities (TAs): TAs are entities that assess the trustworthiness of vehicles based on their behavior and interactions within the network. They assign trust scores or ratings to vehicles to identify potential malicious activities.

Communication Channels: VANETs utilize various communication channels, including Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) channels, for exchanging messages and sharing information. These channels facilitate the dissemination of safety-related warnings, traffic data, and other relevant information.

Sybil Attackers: Sybil attackers are malicious entities that aim to compromise the integrity and trust within the VANET. They create multiple fake identities (Sybil nodes) to deceive other nodes and gain undue advantage, such as disrupting traffic flow or

spreading false information.

Sybil Attack Detection Mechanisms: These mechanisms are designed to identify and detect the presence of Sybil attackers in the VANET. They employ various techniques, such as analyzing communication patterns, monitoring node behavior, or utilizing trust-based algorithms, to differentiate between legitimate nodes and Sybil nodes.

The system architecture of a Sybil attack in VANETs involves the interaction and communication among these components. Understanding this architecture is crucial for developing effective detection and prevention mechanisms to safeguard the VANET from Sybil attacks and ensure the reliability and security of vehicular communications.

4.2.1 Sybil Attacker Capabilities

Sybil attackers pose a significant threat to the security of Vehicular Ad Hoc Networks (VANETs). These attackers maliciously create multiple fake identities or nodes, deceiving other vehicles and the network itself. By impersonating multiple vehicles, Sybil attackers can exploit vulnerabilities, launch various types of attacks, and disrupt the normal functioning of the network. Understanding the capabilities of Sybil attackers is crucial in devising effective countermeasures to detect and mitigate their malicious activities. Here, we will discuss the capabilities of Sybil attackers in VANETs in detail.

Identity Multiplicity: Sybil attackers have the ability to generate multiple fake identities or nodes, making it difficult to distinguish them from genuine vehicles. By creating numerous virtual vehicles, the attacker can amplify their influence, increase their presence in the network, and potentially control a significant portion of the communication.

False Information Dissemination: Sybil attackers can exploit their multiple identities to disseminate false information throughout the network. They can inject misleading or incorrect data into the communication, leading to inaccurate decisions and compromising the reliability and integrity of the information exchanged among vehicles.

Denial of Service (DoS) Attacks: Sybil attackers can launch DoS attacks by overwhelming the network with a large number of fake identities. By flooding the network with malicious packets or excessive traffic, they can consume the available resources, degrade the network performance, and disrupt communication among legitimate vehicles.

Collusion and Coordination: Sybil attackers can collaborate and coordinate their ac-

tivities among their fake identities. They can exchange information, collectively plan attacks, and execute synchronized malicious actions. Such collusion allows them to amplify their impact and make it even more challenging to detect their malicious behavior.

Resource Exhaustion: Sybil attackers can exploit their multiple identities to deplete network resources. By continuously requesting services, occupying bandwidth, or consuming computational resources, they can cause congestion, deteriorate system performance, and impede the normal functioning of the network.

Reputation Manipulation: Sybil attackers can manipulate reputation systems implemented in VANETs. By having multiple fake identities vouch for each other, they can artificially inflate their reputation scores, gain trust from legitimate vehicles, and potentially bypass security mechanisms based on trust or reputation.

Location Spoofing: Sybil attackers can forge their location information to deceive other vehicles and location-based services. By broadcasting false location coordinates, they can mislead the routing protocols, disrupt traffic flow, or even manipulate the decision-making processes of neighboring vehicles.

Sybil Wormholes: Sybil attackers can create virtual tunnels or shortcuts in the network by strategically placing their fake identities. These Sybil wormholes can be exploited to facilitate the rapid propagation of malicious messages, redirect traffic, or bypass security mechanisms deployed in the network.

To counter the capabilities of Sybil attackers, various detection and prevention techniques have been proposed, such as cryptographic-based solutions, trust-based systems, and anomaly detection algorithms. These mechanisms aim to identify and isolate Sybil attackers, verify the authenticity of vehicles and messages, and ensure the overall security and integrity of VANETs.

In conclusion, Sybil attackers in VANETs have the ability to create multiple fake identities, disseminate false information, launch DoS attacks, collaborate with other Sybil nodes, exhaust network resources, manipulate reputation systems, spoof their location, and create Sybil wormholes. Understanding these capabilities is essential in developing robust security mechanisms that can detect, prevent, and mitigate the threats posed by Sybil attackers in VANETs.

4.3 Proposed Detection Methodology

Sybil's attack is considered a serious security threat in ad-hoc networks and sensor networks. The major issue of Sybil's attack in VANETS is traffic congestion caused by Sybil nodes. These fake traffic congestions can cause serious damage not only to infrastructure but to the drivers as well. A lightweight scheme is needed to promptly identify and eliminate existing and potential Sybil nodes and suppress any incoming Sybil attacks. [6] RSUs authenticate and assign unique keys to any node coming into the network.

RSUs will provide the node with the list of neighborhood information already assigned to existing nodes in the network. RSU will also have timestamps for all its activities. Attack:

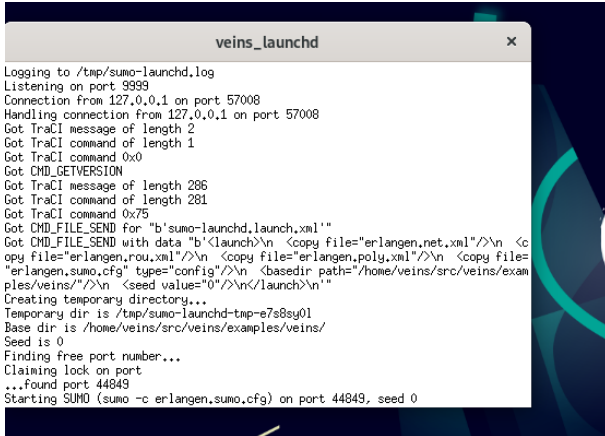
Sybil attacker enters the network. Generate malicious nodes known as sybil nodes. Detection: Neighbor nodes will detect if there is any duplicate key. Speed and position of duplicate nodes are observed by neighbors. With the help of velocity, location, direction, and timestamp. Actual and predicted nodes's locations can be determined. With the help of this information, sybil node will be singled out and removed from the network.

4.3.1 Tool Used for Sybil attack detection

For implementation we are using VEINS for simulations of network. Veins is an open-source framework developed for simulating and evaluating vehicular communication systems, specifically focusing on V2X (Vehicle-to-Everything) communication in VANETS. It is built on top of the OMNeT++ discrete event simulation framework and incorporates the SUMO traffic simulator to provide realistic mobility patterns for vehicles.

Veins provides a comprehensive simulation environment for studying various aspects of VANETS, including vehicle mobility, wireless communication, and application layer protocols. It allows researchers and developers to analyze the performance, efficiency, and security of VANET applications and protocols under different scenarios and conditions (Figure 4.1).

The framework offers a range of features and functionalities that are beneficial for studying Sybil attacks in VANETS. Some key aspects of Veins relevant to Sybil attack detection include:



```

veins_launchd
Logging to /tmp/sumo-launchd.log
Listening on port 9999
Connection from 127.0.0.1 on port 57008
Handling connection from 127.0.0.1 on port 57008
Got TraCI message of length 2
Got TraCI command of length 1
Got TraCI command 0x0
Got CMD_GETVERSION
Got TraCI message of length 286
Got TraCI command of length 281
Got TraCI command 0x75
Got CMD_FILE_SEND for "b'sumo-launchd.launch.xml'"
Got CMD_FILE_SEND with data "b'<launch>\n <copy file="erlangen.net.xml"/>\n <copy file="erlangen.rcu.xml"/>\n <copy file="erlangen.poly.xml"/>\n <copy file="erlangen.sumo.cfg" type="config"/>\n <basedir path="/home/veins/src/veins/examples/veins"/>\n <seed value="0"/>\n</launch>\n"'
Creating temporary directory...
Temporary dir is /tmp/sumo-launchd-tmp-e7s8sy01
Base dir is /home/veins/src/veins/examples/veins/
Seed is 0
Finding free port number...
Claiming lock on port
...found port 44849
Starting SUMO (sumo -c erlangen.sumo.cfg) on port 44849. seed 0

```

Figure 4.1: Launching Veins

Realistic Mobility Modeling: Veins utilizes the SUMO traffic simulator to generate realistic mobility traces for vehicles, considering factors such as road networks, traffic flow, and vehicle movement patterns. This enables researchers to evaluate Sybil attack detection mechanisms in dynamic and realistic vehicular scenarios.

Communication Modeling: Veins models the wireless communication between vehicles using the IEEE 802.11p standard, which is specifically designed for VANETs. It stimulates the propagation of messages, signal interference, and channel access mechanisms, allowing researchers to assess the effectiveness of Sybil attack detection techniques in the context of VANET communication.

Application Layer Support: Veins provides an application layer framework that facilitates the development and evaluation of VANET applications. Researchers can implement and test their Sybil attack detection algorithms within this framework, leveraging the functionality provided by Veins for message exchange, event handling, and integration with the lower layers of the protocol stack.

Customization and Extensibility: Veins offers a flexible architecture that allows researchers to customize and extend its functionalities according to their specific requirements. This enables the implementation and evaluation of novel Sybil attack detection approaches, algorithms, and metrics in VANETs.

In summary, Veins is a powerful simulation framework designed for VANET research, offering realistic mobility modeling, wireless communication simulation, and application layer support. Its capabilities make it well-suited for studying Sybil attacks and evaluating Sybil attack detection mechanisms in the context of VANETs. By utilizing

Veins, researchers can gain insights into the performance and effectiveness of their detection strategies and contribute to the advancement of secure and trustworthy vehicular communication systems.

4.3.2 Neighborhood-based technique Algorithm

The neighboring node-based algorithm is a distributed approach used for detecting Sybil attacks in VANETs without relying on trusted nodes or centralized authorities. This algorithm utilizes the neighborhood information of each node to identify potential Sybil attackers within the network.

In this algorithm, each vehicle actively participates in the detection process by forming groups of neighboring nodes at fixed intervals of time. The goal is to analyze these groups collectively instead of investigating each node independently. By considering the communication range of a node, a group of neighboring nodes is formed based on the reception of beacon packets.

The beacon packets serve the purpose of announcing the presence of a node and are periodically broadcasted by all vehicles in the network. When a beacon packet is received, all the nodes within the communication range of the sender form a group of neighboring nodes. These groups provide valuable information about the connectivity and proximity of vehicles in the network.

To detect potential Sybil attacks, the algorithm analyzes the composition of these neighboring node groups. It checks for any inconsistencies or abnormalities that may indicate the presence of Sybil attackers. For example, if a group contains multiple nodes claiming to be the same vehicle or if a node forges its neighboring list by including non-existent vehicles, it raises suspicion of a Sybil attack.

By continuously monitoring and analyzing these neighboring node groups, the algorithm aims to identify and distinguish between legitimate nodes and potential Sybil attackers. The distributed nature of the algorithm allows for real-time detection and reduces the reliance on centralized entities, enhancing the security and reliability of the VANET system.

Overall, the neighboring node-based algorithm leverages the information exchanged between neighboring vehicles to collectively identify Sybil attacks, promoting the safety

and integrity of vehicular communication in VANETs.

- Start the MyVeinsApp application, which is a subclass of BaseWaveAppLayer from the Veins framework.
- Implement the calculateDistance function to calculate the Euclidean distance between two vehicles given their coordinates (x1, y1) and (x2, y2). The function uses the distance formula.
- Implement the detectSybilAttack function that takes the current vehicle's position (currentX, currentY), its identity (currentIdentity), a vector of neighboring vehicles (neighboringVehicles), and a threshold distance (thresholdDistance) as input.
- Iterate over each neighboring vehicle in the neighboringVehicles vector.
- Calculate the distance between the current vehicle and the neighboring vehicle using the calculateDistance function.
- Check if the calculated distance is less than the thresholdDistance.
- If the distance is within the threshold, compare the identity (currentIdentity) of the current vehicle with the identity of the neighboring vehicle (neighbor.identity).
- If the identities match, it indicates a Sybil attack, and the function returns true.
- If no Sybil attack is detected after iterating through all neighboring vehicles, the function returns false.
- Override the necessary methods from the Veins framework, such as onWSM, to handle incoming WaveShortMessages (WSMs) in the VANET.
- Inside the onWSM method, obtain the current vehicle's position (currentX, currentY) and identity (currentIdentity).
- Get the neighboring vehicles' information by calling mobility->getNeighbors() and store it in the neighboringVehicles vector.
- Set a threshold distance (threshold distance) to define the maximum distance for considering neighboring vehicles.

- Call the `detectSybilAttack` function, passing the current vehicle's information and the neighboring vehicles, to check for Sybil attacks.
- Based on the detection result, print a message indicating whether a Sybil attack is detected or not.
- Continue with other processing in the Veins framework by calling `BaseWaveApplLayer::onWSM(wsm)`

4.3.3 Technologies used for Sybil Attack Detection

Sybil attacks pose a significant threat to the security and reliability of communication in Vehicular Ad-Hoc Networks (VANETs). Detecting and mitigating these attacks is crucial for ensuring the integrity of vehicular communication. Various techniques have been developed to address the challenge of Sybil attack detection in VANETs. Two commonly employed approaches include neighboring-based detection and trust-based detection.

Neighboring-based detection relies on analyzing the behavior of neighboring vehicles to identify potential Sybil attackers. By measuring proximity, velocity difference, and communication patterns, this technique assesses the likelihood of a Sybil attack. It considers metrics such as distance, speed, and communication frequency to identify anomalies and suspicious activities among neighboring vehicles.

Trust-based detection, on the other hand, leverages trust scores assigned to vehicles to identify potential Sybil attackers. Vehicles are evaluated based on their past interactions, recommendations from other vehicles, or centralized trust management systems. Trust metrics such as reputation, reliability, and behavior history are taken into account to determine the trustworthiness of vehicles.

These detection techniques are implemented within simulation frameworks such as Veins, which provide realistic representations of vehicular movement and communication. Through extensive simulations, the performance of neighboring-based and trust-based detection techniques is evaluated. Key performance metrics, including detection accuracy, false positive rate, and computational overhead, are measured and analyzed. The robustness and efficiency of the detection techniques are assessed under various attack scenarios and network conditions to determine their suitability for different VANET deployment

scenarios.

To validate the proposed detection techniques, they are compared with existing analytical models or research findings. Sensitivity analysis is performed to understand the impact of different parameters, such as network size, density, and attacker behavior, on the detection accuracy and efficiency of the techniques.

Throughout the research, ethical considerations are prioritized to ensure data privacy and confidentiality. Personal or sensitive information collected during the data collection phase is anonymized and securely handled.

By employing neighboring-based and trust-based detection techniques, researchers aim to enhance the security and reliability of VANETs by effectively identifying and mitigating Sybil attacks. The findings from this research can contribute to the development of robust and efficient Sybil attack detection mechanisms in VANETs, ensuring the integrity of vehicular communication systems.

4.3.4 Assumptions

In the context of Sybil attack detection in VANETs, several assumptions are made to frame the proposed detection approach. These assumptions are crucial for understanding the system dynamics and designing effective countermeasures. Here are the assumptions described in detail:

- **Identity Authentication Infrastructure:** The VANET implementation incorporates an electronic license plate (ELP) system. This infrastructure involves a hierarchical structure of central authorities (CAs) responsible for managing vehicle identities registered within their respective geographic regions. The ELP system ensures the authenticity and integrity of vehicle identities, forming the foundation for secure communication and trust establishment.
- **Security of Road-Side Units (RSUs):** RSUs, which are roadside infrastructure units in VANETs, are considered to have higher security compared to individual vehicles. Due to their tamper-proof capabilities, RSUs are more difficult to compromise. However, it is acknowledged that RSUs may be present in isolated locations, making them potentially vulnerable to physical attacks or manipulation attempts. Nonetheless, their inherent security features make compromising RSUs

significantly challenging.

- **Persistence of Sybil Attacks:** The proposed detection approach assumes that Sybil attacks persist for a substantial duration of time. This assumption acknowledges the fact that Sybil attacks can have detrimental effects on VANET applications when they are sustained over extended periods. By considering the longer persistence of Sybil attacks, the detection approach can be tailored to identify and mitigate these attacks effectively.
- **Sybil Attack Broadcasting:** The assumption is made that an attacker carrying out a Sybil attack broadcasts packets containing the same information using all the fake identities associated with it. This behavior allows the attacker to amplify the impact of the attack by flooding the network with multiple instances of the same malicious information. By assuming this broadcasting strategy, the proposed detection approach can focus on identifying patterns and anomalies in the broadcasted packets to differentiate between legitimate and malicious activities.

Detection of Sybil Attack involving neighboring nodes

Neighboring node-based techniques have emerged as a promising approach for detecting Sybil attacks in Vehicular Ad-Hoc Networks (VANETs). These attacks involve malicious entities impersonating multiple identities to disrupt the network's integrity and reliability. By leveraging the behavior and interactions of neighboring nodes, these techniques aim to identify and mitigate Sybil attacks effectively.

In neighboring node-based detection, each vehicle in the network collects information about its surrounding vehicles, such as their positions, velocities, and communication patterns. By analyzing these characteristics, the technique seeks to detect abnormalities or inconsistencies that may indicate the presence of Sybil attackers. Key metrics considered in this approach include distance, speed, communication frequency, and the timing of messages exchanged between neighboring nodes.

Through careful analysis and comparison of the observed data, the neighboring node-based technique identifies discrepancies or deviations from normal behavior patterns. For instance, it may detect situations where multiple vehicles claim to be in the same physical location or exhibit uncharacteristic movement patterns. Such anomalies can

raise suspicions of Sybil attacks and trigger further investigation.

To improve the accuracy of Sybil attack detection, neighboring node-based techniques often incorporate statistical analysis, machine learning algorithms, or rule-based systems. These methods can effectively classify normal and abnormal behavior patterns, enabling the identification of potential Sybil attackers with a higher degree of confidence.

To evaluate the performance of neighboring node-based detection techniques, extensive simulations using VANET simulation frameworks, such as Veins, are conducted. Various scenarios are considered, including different network sizes, vehicle densities, and attacker behaviors. Performance metrics such as detection accuracy, false positive rate, computational overhead, and response time are measured and analyzed to assess the effectiveness and efficiency of the proposed technique.

Furthermore, ethical considerations are taken into account throughout the research process. Data privacy and confidentiality are safeguarded by anonymizing sensitive information collected during simulations or real-world experiments.

By utilizing neighboring node-based techniques for Sybil attack detection, researchers aim to enhance the security and resilience of VANETs. The findings of this research can contribute to the development of robust and efficient mechanisms that enable early detection and mitigation of Sybil attacks, thereby ensuring the trustworthiness and reliability of vehicular communication systems.

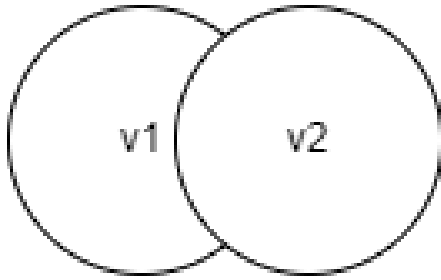
4.3.5 Description of neighboring nodes

In Vehicular Ad Hoc Networks (VANETs), vehicles communicate with each other wirelessly. The success of communication depends on various factors such as the state of the wireless medium and the efficiency of the transceivers used. The ability to receive packets is influenced by parameters used in propagation models, including packet transmission power, the ratio of received power to noise and interference, the distance between the transmitting and receiving vehicles, and losses in the wireless medium like fading and scattering.

Neighboring nodes in VANETs can be classified into two categories: physical neighbors and communication neighbors.

Physical Neighbors

Vehicle V1 is considered a physical neighbor (PV1) of another vehicle V2 if V1 is within a certain physical distance (denoted as 'r') from V2. Moreover, if V1 is able to receive packets from V2, then V2 is also able to receive packets from V1. This classification is based on the physical proximity between vehicles and their bidirectional communication capability as shown in figure 4.2.



Physical Neighbors

Figure 4.2: Physical Neighbors

Communication Neighbors

Vehicle V1 is considered a communication neighbor (CV1) of another vehicle V2 if V1 is within the communication range of V2, enabling V1 to receive packets transmitted by V2. However, it is not necessary for V2 to be able to receive packets from V1. This classification focuses solely on the ability to receive packets from a specific vehicle, irrespective of bidirectional communication as shown in figure 4.3.

It is important to note the differences between physical and communication neighbors. For instance, if a vehicle Ve2 adjusts its transmission power by improving its transceivers, it may fall within the communication range of another vehicle Ve1 (CVe1), but not within its physical proximity (PVe1).

In VANETs, the concept of neighboring nodes encompasses both physical proximity and communication capabilities. However, it is important to note that physical proximity alone does not guarantee communication between vehicles. For example, two vehicles, Ve1 and Ve2, may be physically close to each other (PVe1 and PVe2), but if there are obstacles blocking the line of sight, Ve2 may not be able to send or receive packets from

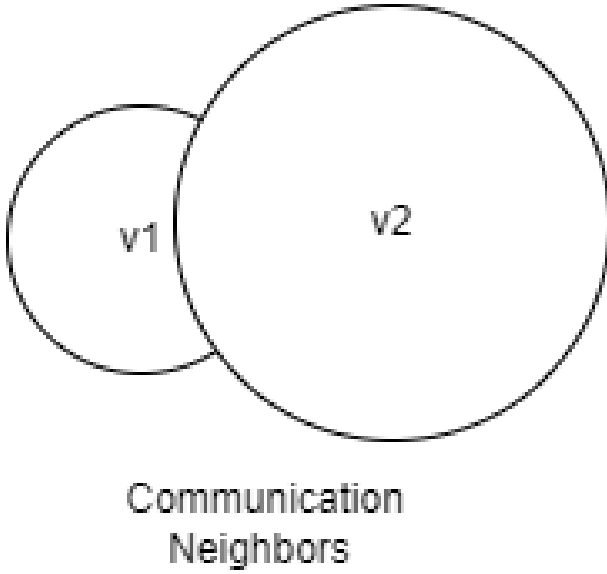


Figure 4.3: Communication Neighbors

V1. In such cases, V2 would not be considered a communication neighbor ($V2 \notin CV1$). To establish communication, the distance between V1 and Ve2, denoted as $D(Ve1, Ve2)$, needs to be within a predefined physical distance threshold 'r'.

While physical neighbors are symmetric in terms of communication, meaning if Ve1 can receive messages from Ve2, Ve2 can also receive messages from Ve1, the same does not hold true for communication neighbors. Asymmetric transmission of packets among communication neighbors can occur due to various factors, including adjustments in transmission power by attackers or other environmental conditions. Therefore, if Ve3 can receive messages from Ve4, it does not necessarily mean that V4 can also receive messages from Ve3.

To summarize, the classification of neighboring nodes in VANETs serves to define the relationships between vehicles based on both physical proximity and communication range. Understanding these classifications is crucial for designing efficient communication protocols and addressing the unique challenges posed by VANETs. It allows for the development of robust mechanisms that consider the limitations and dynamics of vehicle-to-vehicle communication, enabling effective and reliable data exchange in VANET environments.

Advantages of using neighboring nodes

One of the key advantages of utilizing neighboring node techniques for Sybil attack detection in VANETs is their ability to leverage the immediate proximity and interactions between vehicles. Unlike other techniques that rely on centralized trust management or data-centric analysis, neighboring node techniques operate in a decentralized manner, making them more suitable for dynamic and highly mobile VANET environments. By considering the behavior and communication patterns of neighboring vehicles, these techniques can capture real-time information and detect Sybil attacks in a timely manner. Additionally, the use of neighboring nodes provides a localized perspective, enabling the detection of attacks that may occur within a specific geographical area or cluster of vehicles.

This localized approach improves the accuracy of detection and reduces false positives, as it focuses on the immediate vicinity rather than relying solely on global network-wide information. Furthermore, neighboring node techniques can be easily integrated into existing VANET protocols and do not require significant changes to the underlying infrastructure, making them practical and cost-effective solutions for enhancing the security of VANETs.

Limitations

When utilizing neighboring node techniques for Sybil attack detection in VANETs, there are certain limitations that need to be considered:

Limited Coverage: Neighboring node techniques rely on the availability of nearby vehicles for detection. In sparse or low-density areas, where the number of neighboring vehicles is limited, the effectiveness of these techniques may be compromised. This can result in a reduced detection accuracy and an increased risk of false negatives.

Dynamic Network Topology: VANETs exhibit rapid changes in network topology due to the high mobility of vehicles. As vehicles enter or leave the communication range, the set of neighboring nodes constantly changes. This dynamic nature poses a challenge for neighboring node techniques as they need to maintain an up-to-date and accurate view of neighboring vehicles. Failure to do so may lead to delays in detecting Sybil attacks or even result in missed detections.

Collaborative Attacks: Neighboring node techniques assume that neighboring vehicles are trustworthy and do not collude to launch Sybil attacks. However, in scenarios where multiple vehicles collude to deceive the detection mechanism, neighboring node techniques may become less effective. Colluding vehicles can manipulate their behavior and communication patterns in a coordinated manner, making it difficult to differentiate between legitimate and malicious entities solely based on proximity.

Resource Consumption: Neighboring node techniques require vehicles to exchange information about their identities, positions, and other relevant attributes. This communication overhead can lead to increased resource consumption, including bandwidth, computational power, and energy. In resource-constrained VANET environments, this additional overhead may impact the overall network performance and scalability.

Privacy Concerns: Sharing information with neighboring nodes raises privacy concerns for vehicles in VANETs. By revealing their identities and location information to neighboring vehicles, vehicles may become more susceptible to privacy breaches or targeted attacks. [6] Ensuring the privacy of vehicles while still maintaining effective Sybil attack detection becomes a critical challenge in neighboring node techniques.

4.3.6 System Model

We propose a distributed scheme to defend against Sybil attacks in VANETs using the neighborhood information of each node. Our approach eliminates the need for trusted nodes, such as RSUs, to perform the detection operation. Instead, every vehicle actively participates in the detection process by forming groups of neighboring nodes at regular intervals. Rather than investigating each node independently, we analyze the composition of these groups to identify potential Sybil attackers.

In our scheme, vehicles in the network regularly broadcast beacon packets to announce their presence on the road. Additionally, alert packets are used to ensure the safety of vehicles and support various VANET applications. These alert packets are broadcasted when specific application-related conditions are met. When a sender transmits these packets, all the nodes within its communication range receive them and form a group of neighboring nodes.

By leveraging the group formation and analyzing the received packets, we can detect potential Sybil attacks. The analysis involves examining the consistency and behavior of

neighboring nodes within the formed groups. Any discrepancies or suspicious patterns in the received packets can indicate the presence of Sybil attackers.

Our proposed technique enables distributed detection without relying on a centralized authority or trusted nodes. It leverages the collective behavior of neighboring nodes and the information contained in the broadcasted packets to identify and mitigate the threat of Sybil attacks in VANETs.

pdfscape

Algorithm 2: Sybil Group Detection Algorithm

Input : $V = \{V_1, V_2, \dots, V_n\}$: Set of n vehicles on the road;
 A : Set of Sybil attackers;
 T : Duration of simulation time;
 $N_j^{(t)}$: Neighbors of node V_j at time t interval;
 $Timer_j = 0$: Time instance for measuring the duration of similarity in neighboring nodes;
 σ : Threshold (time duration during which normal nodes may have the same set of neighbors);
 $C_{tj,k}$: Set of common neighbors of node V_j and V_k at time t interval;
 $M_j^{(t)}$: Set of nodes V_j present in the minimum transmission range of the fake node list;

Output: Sybil-group and Legitimate-nodes classification

```

for  $t = 1$  to  $T$  do
    |
    |   for  $j = 1$  to  $n$  do
    |   |   createNeighborList( $N_j^{(t)}$ );
    |   |   // Communication neighbors
    |   |   end
    |   end
end

```

This algorithm aims to detect Sybil attackers in VANETs by analyzing the similarity of neighboring nodes. Here's a step-by-step explanation:

We start by defining the set of vehicles (V) and the duration of the simulation (T).

In each time interval (t), we create the neighbor list (N_{jt}) for each vehicle (V_j) by

Algorithm 3: Algorithm name(Part 2)

```

for  $t = 1$  to  $T$  do
  for  $j = 1$  to  $n$  do
    for  $k = j + 1$  to  $N_j^{(t)}$  do
       $C_{tj,k} = N_j^{(t)} \cap N_k^{(t)}$ ;
      if  $C_{tj,k} = \emptyset$  then
        // Malicious node forges neighboring list
        break;
      end
       $M_j^{(t)} = M_j^{(t)} \cap C_{tj,k}$ ;
    end
  end
   $Timer_j = Timer_j + 1$ ;
  for  $j = 1$  to  $n$  do
    if  $(Timer_j > \sigma)$  and  $(M_j^{(t)} \neq \emptyset)$  then
       $M_j^{(t)} \in \text{Sybil-group}$ ;
      break;
    end
    else
       $M_j^{(t)} \in \text{Legitimate-nodes}$ ;
      continue;
    end
  end
end
  
```

considering its communication neighbors.

Next, we iterate through each vehicle (V_j) and compare its neighbor list (N_{jt}) with other vehicles' neighbor lists (N_{kt}). We check for the common neighbors ($C_{tj,k}$) between V_j and V_k .

If there are common neighbors ($C_{tj,k}$), we update the set of nodes (M_{jt}) that are within the minimum transmission range of the fake node list.

The timer ($Timer_j$) is incremented for each vehicle (V_j) in each time interval (t).

If the conditions in step 7 are not met, it implies that the nodes in M_{jt} are legitimate and belong to the Legitimate-nodes group.

The algorithm helps identify Sybil attackers based on the similarity of neighboring nodes and distinguishes them from legitimate nodes in the VANET.

Implementation and Results

5.1 Detection Approach

We propose a distributed scheme to counter Sybil attacks in VANETs, utilizing the neighborhood information of each node. Unlike existing approaches that rely on trusted entities such as RSUs, our scheme operates in a decentralized manner, involving the active participation of every vehicle for detection. Instead of examining individual nodes independently, we analyze groups of neighboring nodes at regular intervals, which improves efficiency and eliminates the need for centralized authorities.

In our scheme, vehicles in the VANET communicate through various types of messages. Beacon packets, which are periodically broadcasted by all nodes, serve the purpose of announcing their presence in the network. Alert packets, designed for specific applications and ensuring road safety, are broadcasted when required. When a vehicle sends out a beacon packet, all neighboring nodes within its communication range receive the packet, forming a group of neighboring nodes. It is important to note that Sybil identities originating from an attacker node share the same physical device, representing a malicious node. Consequently, they also share the same set of physical neighbors. However, the communication neighbors of Sybil nodes may differ since they can adjust their transmission power while sending beacon packets. Our proposed detection approach is capable of identifying all potential Sybil identities launched from the same malicious node.

The overall Sybil node detection approach consists of four phases:

5.1.1 Periodical Communication

In this phase, each vehicle V_j on the road periodically sends beacon packets and receive beacon packets from neighboring nodes. Beacon packets are essential for all vehicles in the VANET to announce their presence. Neighboring vehicle information can be obtained through an overhearing process. However, we leverage the periodic communication characteristic of VANET nodes. Each time a node sends a message, it includes its neighbor list in the packet. The beacon packet contains the sender's identity, geographical position, and transmission time.

5.1.2 Grouping of Neighboring Nodes

Once a vehicle collects a sufficient number of beacon messages from neighboring vehicles, it constructs a record of neighboring nodes N_{it} in the form of groups at regular intervals. The neighboring nodes N_{it} can be described as follows: $N_{it} = ID_j$, where $ID_j \in CID_i$. The construction of neighboring node groups occurs at a regular time interval g , which is longer than the beacon interval b . This extended interval allows for the identification of nodes present within the transmission range of neighboring nodes.

5.1.3 Sharing information with Nearby Nodes

After a significant duration of time, depending on factors such as vehicle density and speed, nodes exchange their records of neighboring nodes with other nodes in their vicinity.

5.1.4 Identification of Vehicles with Similar Neighboring Nodes

Upon receiving neighboring node groups, each node V_j compares its neighbor table with the neighbor table N_{jt} of the neighboring node V_k . If certain nodes are observed simultaneously by neighboring nodes for a duration exceeding a threshold, these nodes are categorized as Sybil-group nodes. By employing this approach, our scheme is capable of detecting all fake identities (Sybil nodes) originating from a Sybil attacker.

By leveraging neighborhood information and utilizing the distributed nature of VANETs, our scheme provides an effective means to detect Sybil attacks without the need for trusted nodes. It enhances the security and trustworthiness of VANETs, contributing

to safer and more reliable communication among vehicles.

The proposed detection approach is elaborated by considering a VANET scenario illustrated in Figure 2. In this scenario, Vehicle VE2 is identified as a Sybil attacker and participates in the network by employing three Sybil identities: VE1, VE5, and VE8.

Table in figure 5.1 presents the groups of neighboring nodes for all vehicles at different time intervals. To maintain clarity, the neighboring nodes of the Sybil attacker VE2 and its Sybil identities (VE1, VE5, VE8) are not shown in the table since these nodes can modify the group of neighboring nodes while propagating them to their neighbors. By examining the table, it can be observed that the group of neighboring nodes consisting of VE3, VE4, VE6, and VE10 includes the Sybil nodes (VE1, VE2, VE5, VE8) for a significant duration of time. This indicates that the set of Sybil nodes remains together for an extended period compared to legitimate nodes due to the mobility of vehicles and the periodic exchange of beacon packets. Utilizing these fundamental VANET features, it becomes feasible to detect Sybil attackers. During the implementation phase, the Sybil node's group is observed by a greater number of neighboring nodes for a duration longer than a predetermined threshold.

	t_0	t_1	t_2	t_3
V_3	$V_1, V_2, V_8, V_5, V_{10}$	$V_1, V_2, V_3, V_8, V_5, V_{10}$	V_5, V_8	V_8
V_{10}	$V_1, V_2, V_8, V_5, V_{12}, V_3$	$V_1, V_2, V_8, V_5, V_3, V_{12}$	V_3, V_5, V_8	V_8, V_{12}
V_4	$V_1, V_2, V_5, V_8, V_7, V_6$	V_1, V_2, V_5, V_8, V_7	V_1, V_2, V_5, V_8	V_1, V_2, V_5, V_8, V_6
V_6	$V_1, V_2, V_5, V_8, V_4, V_{11}$	$V_1, V_2, V_5, V_8, V_{11}$	$V_1, V_2, V_5, V_8, V_{11}$	V_1, V_2, V_4, V_5, V_8
V_7	$V_1, V_4, V_5, V_8, V_{12}, V_{15}$	V_1, V_4, V_5, V_8	V_5, V_8	V_1, V_5, V_8
V_{12}	$V_1, V_5, V_7, V_8, V_{10}$	V_1, V_5, V_8, V_{15}	V_5, V_8, V_{15}	V_8, V_{15}
V_{11}	$V_1, V_5, V_8, V_6, V_{13}$	V_1, V_5, V_8, V_{13}	V_8, V_{13}	V_5, V_8
V_{13}	V_5, V_8, V_{11}	V_5, V_8, V_{11}	V_8, V_{11}	V_8
V_{14}	V_8	V_8	V_8	--
V_{15}	V_5, V_8	V_1, V_5, V_8	--	--

Table 1: Each vehicle makes a record of neighboring vehicles at discrete interval of time

Figure 5.1: Record of neighboring vehicles

The proposed approach can equally detect attacks wherein the attacker transmits messages simultaneously on multiple radio channels using fake identities. The underlying principle is that two nodes cannot have the same set of neighbors for a time period exceeding the threshold. In cases of low density, the impact of Sybil attacks on VANET performance is negligible. The implementation of the proposed approach at the vehicle level, based on the similarity in neighboring nodes, enables swift detection of attacks without requiring infrastructure support. As a result, the communication overhead is

reduced, as there is no need for periodic message exchanges between infrastructure units (RSUs) to detect Sybil attacks. Other detection approaches for Sybil attacks in VANET (discussed in Section 2) rely on the support of RSUs. However, the major contribution of this paper lies in detecting attacks without infrastructure support, solely using the records of neighboring nodes.

To summarize, the proposed detection approach analyzes the grouping of neighboring nodes in a VANET scenario to identify potential Sybil attacks. By leveraging the mobility and periodic communication of vehicles, the approach can detect Sybil nodes originating from a single attacker without relying on infrastructure support. The method demonstrates effectiveness even in cases where attackers employ multiple radio channels. It offers a low communication overhead and swift detection capabilities, making it a valuable contribution to VANET security.

5.1.5 Simulation Scenario

The evaluation of the VANET system is conducted within a simulated urban area, where vehicles have the flexibility to navigate in any direction. To emulate a realistic urban environment, the vehicles are randomly positioned on the road network, ensuring a diverse distribution throughout the simulation. The vehicle density varies across scenarios, ranging from 20 to 125 vehicles per kilometer.

Within this simulated urban environment (Figure 5.2), mentioned in below figure the road infrastructure allows for two-way traffic, accommodating vehicles moving in both directions. This design choice reflects the typical characteristics of urban road networks and enables the evaluation to capture the intricacies and challenges associated with real-world urban driving scenarios.

To ensure the reliability and validity of the evaluation, each simulation run maintains an average uptime of approximately 500 seconds. This duration allows for an adequate period to observe vehicle interactions, information exchange, and other relevant activities within the VANET system.

To obtain statistically significant results and account for variations, the simulation is executed multiple times. Approximately 50 simulation runs are conducted, providing a robust assessment of the VANET system's performance under diverse conditions and scenarios.

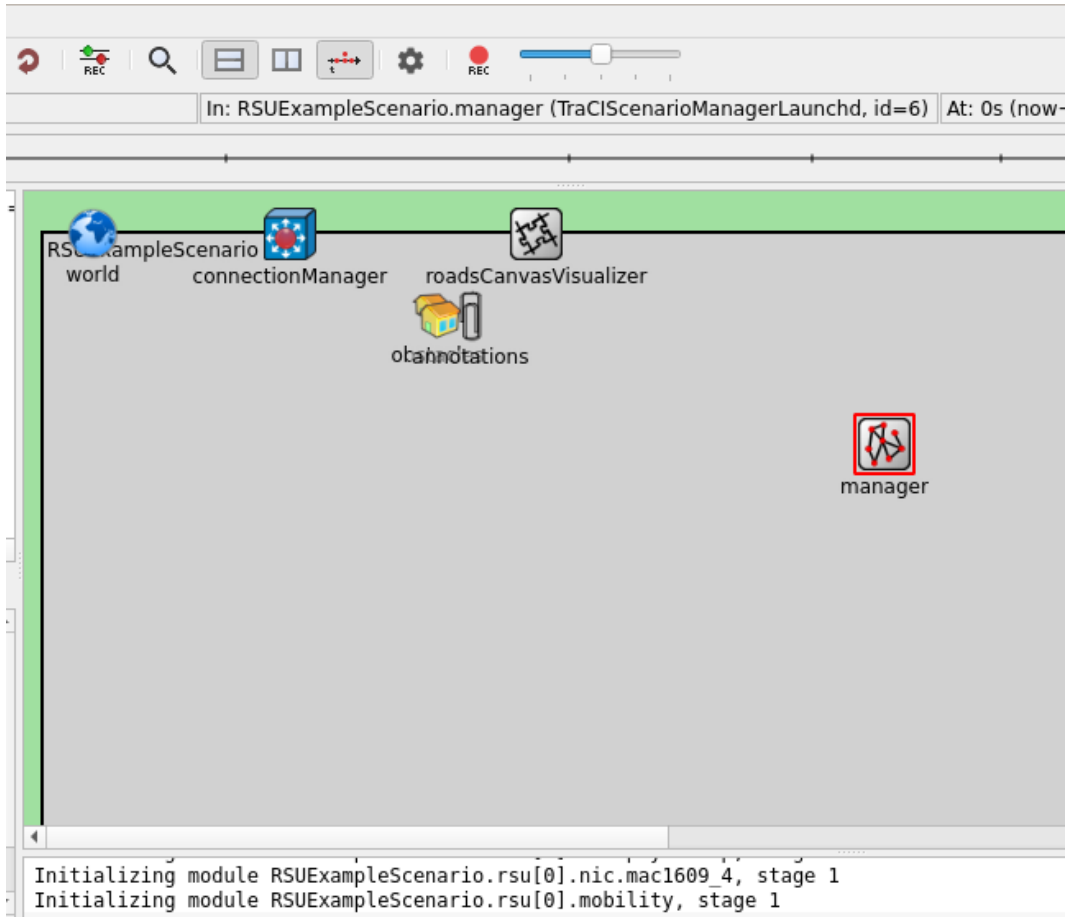


Figure 5.2: Urban environment

It is important to note that the simulations are performed utilizing the VEINS framework, a widely adopted tool specifically designed for simulating vehicular communication and networking scenarios. VEINS offers a realistic simulation environment that encompasses various aspects of vehicular communication protocols, mobility models, and road traffic dynamics.

By simulating the VANET system within an urban area, considering varying vehicle densities, and accounting for the two-way traffic nature of roads, the evaluation aims to provide valuable insights into the system's behavior, performance, and effectiveness in real-world urban settings. The outcomes derived from these simulations contribute to the advancement and enhancement of VANET technologies, protocols, and security mechanisms.

In evaluating the scenario for the algorithms, several metrics are employed to assess their performance and effectiveness. These metrics provide valuable insights into different

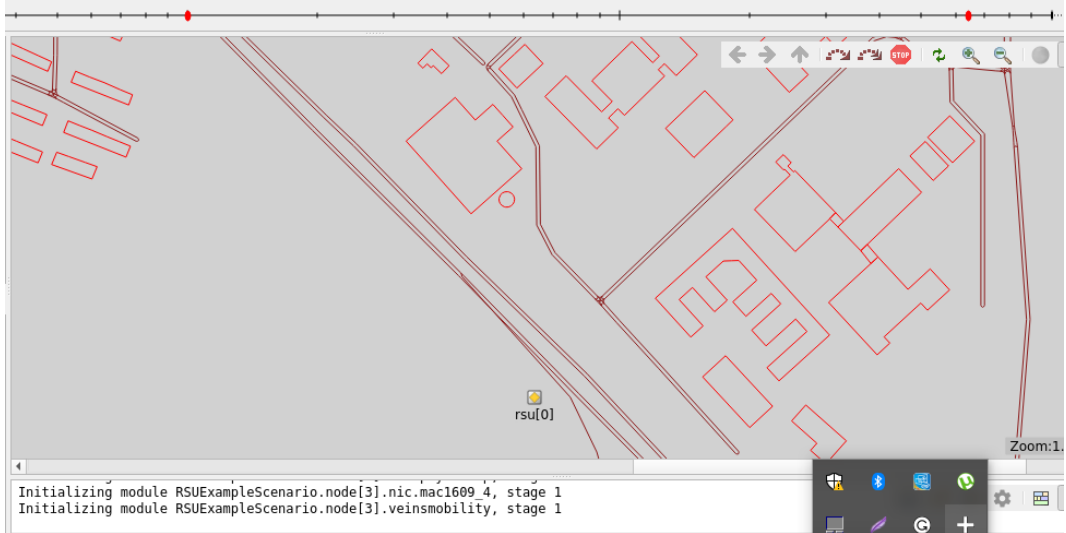


Figure 5.3: Road-side Units

aspects of the algorithms' behavior within the simulated environment.

One crucial metric is Information Coverage, which measures the percentage of the area covered by successfully received packets. It indicates the extent to which transmitted packets effectively reach their intended destinations and provide information within the VANET system. Higher information coverage implies a more comprehensive dissemination of data throughout the network.

Average Transmission Delay is another significant metric used to evaluate the algorithms. It quantifies the time taken for a packet to travel from the transmitting node to the receiving node. A lower transmission delay is generally desirable as it indicates faster and more efficient communication within the VANET system.

Packet Delivery Ratio is a metric that measures the ratio of received packets to the overall transmitted packets. It provides insights into the reliability and effectiveness of the algorithms in delivering information successfully. A higher packet delivery ratio signifies a more efficient data delivery process, ensuring that a significant proportion of transmitted packets reach their intended destinations.

Node Density is an essential metric that reflects the number of vehicles present per kilometer in the simulated scenario. It quantifies the level of congestion or traffic density within the VANET system. By varying the node density, the evaluation can capture the algorithms' performance under different traffic conditions, enabling a comprehensive understanding of their effectiveness in various scenarios.

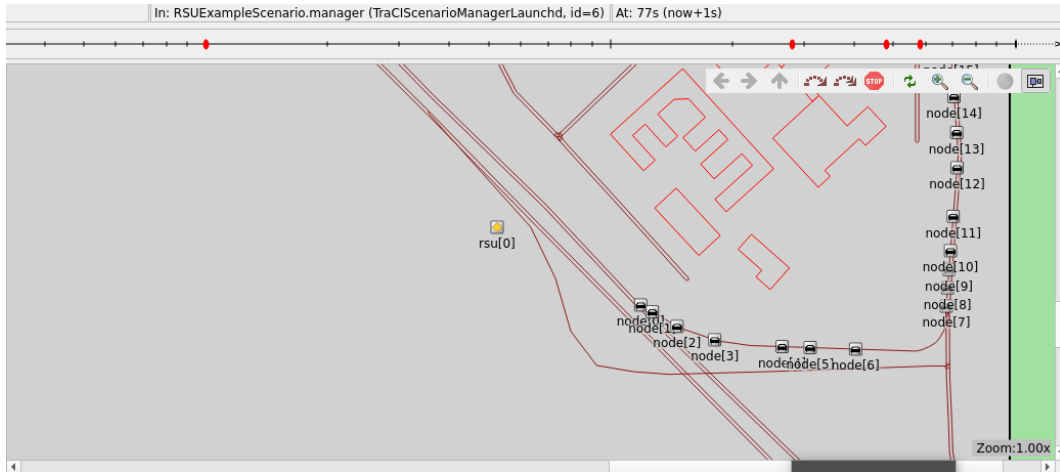


Figure 5.4: Vehicles and Road-side units

By analyzing these metrics, the evaluation can provide valuable information about the algorithms' performance, including their ability to achieve high information coverage, minimize transmission delays, ensure a high packet delivery ratio, and adapt to different node densities. These metrics contribute to assessing the algorithms' overall efficiency, reliability, and suitability for real-world VANET deployments.

In the VEINS simulation scenario, vehicles are moving towards RSU 0 for communication and data exchange. However, an unfortunate event occurs where the smooth flow of communication is disrupted due to the presence of a Sybil attacker. This malicious entity, indicated in red, blocks or interferes with the communication process, causing disruptions and potentially compromising the integrity and security of the VANET system.

As the vehicles approach RSU 0, their intention is to establish a connection and exchange information with the roadside unit. This interaction is crucial for various purposes such as traffic updates, safety notifications, and coordination between vehicles and infrastructure.

However, the Sybil attacker, operating within the network, intentionally disrupts this communication by employing deceptive tactics. This attacker creates multiple fake identities or nodes, appearing as legitimate vehicles within the network. These Sybil nodes may flood the communication channels, inject false information, or perform malicious actions that hinder the normal operation of the system.

The presence of this Sybil attacker poses significant challenges and risks to the VANET

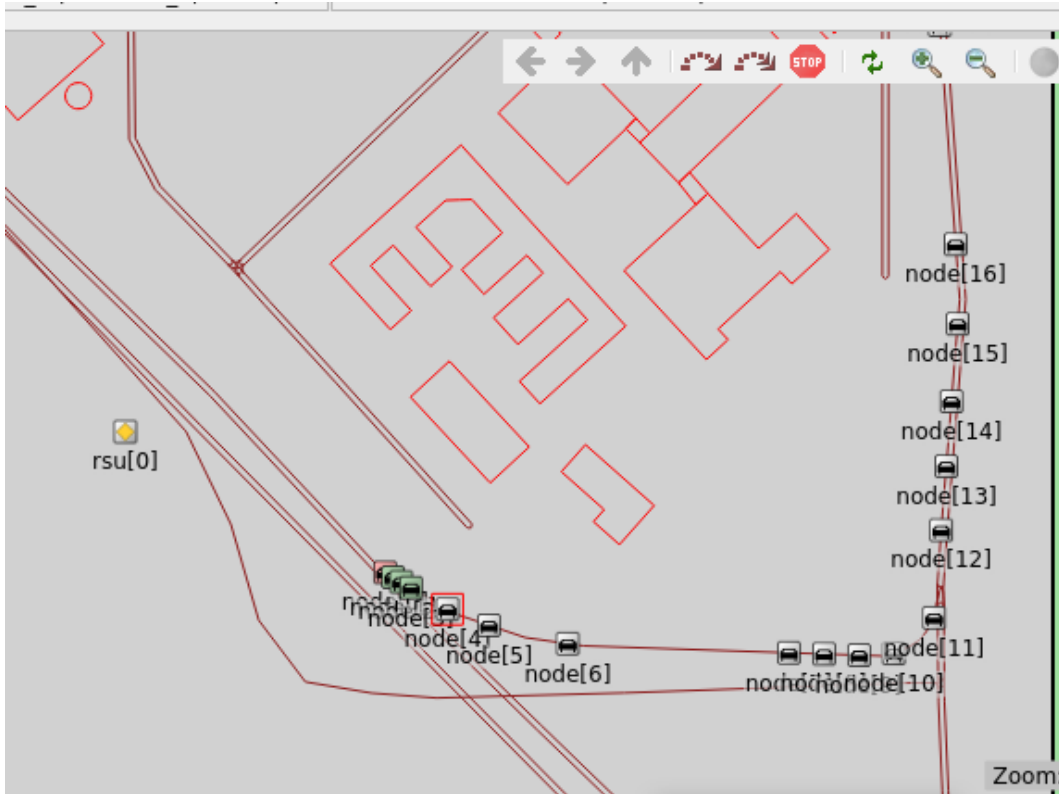


Figure 5.5: Sybil Attacker

system. It can cause congestion, delays, and even lead to misinformation being propagated among the vehicles and the RSU. The disruption caused by the attacker's actions can compromise the overall efficiency, reliability, and safety of the VANET system.

It becomes crucial for researchers and developers to devise effective countermeasures and security mechanisms to detect and mitigate Sybil attacks in VEINS simulations. These countermeasures should aim to identify and isolate the Sybil nodes, allowing the legitimate vehicles to continue their communication with the RSU unhindered.

By addressing the challenges posed by the Sybil attacker and implementing robust security measures, the VEINS simulation scenario can provide valuable insights into the detection and prevention of such attacks in real-world VANET deployments. These findings contribute to the development of more secure and resilient vehicular communication systems, enhancing overall road safety and efficiency. In the given VEINS scenario, after the initial communication disruption caused by the Sybil attacker, the nodes (vehicles) in the network adapt a mechanism to share information with each other. Specifically, they exchange messages, known as "AS AIRFRAME," containing details about their group neighbors. These messages serve the purpose of disseminating information and updat-

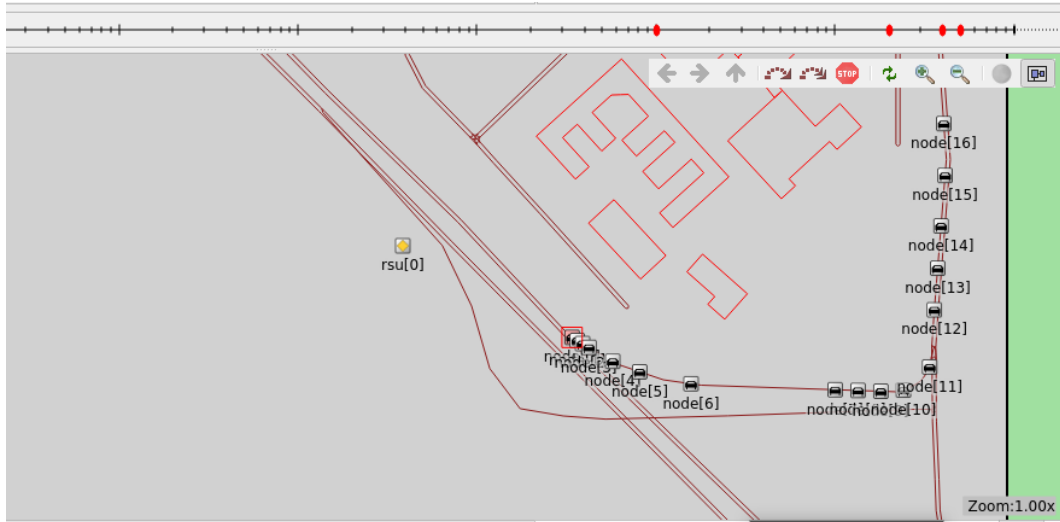


Figure 5.6: Sybil Nodes

ing each vehicle’s knowledge about the surrounding vehicles within their communication range.

Upon receiving these AS AIRFRAME messages, each vehicle maintains a table to store the information received from other vehicles. This table contains entries specifying the group neighbors of each vehicle, allowing them to keep track of the vehicles present in their vicinity.

To detect potential Sybil nodes within the network, a threshold period of time is set. If a vehicle remains in a particular group of neighbors for a duration longer than the defined threshold, it becomes a subject of suspicion. The rationale behind this approach is that Sybil nodes, being malicious entities, may not exhibit the same mobility patterns as legitimate vehicles. Therefore, their presence in a specific group of neighbors for an extended period can raise doubts about their authenticity.

By monitoring the duration of each vehicle’s presence within a group of neighbors and comparing it to the threshold, the system can identify suspicious vehicles that may be potential Sybil nodes. These vehicles can be subjected to further investigation or appropriate countermeasures to ensure the integrity and security of the VANET system.

Implementing such mechanisms and algorithms enables the detection and identification of Sybil nodes based on their abnormal behavior and prolonged presence within a specific group of neighbors. This approach enhances the resilience of the network and helps to maintain the trustworthiness of the communication among vehicles in VEINS simu-

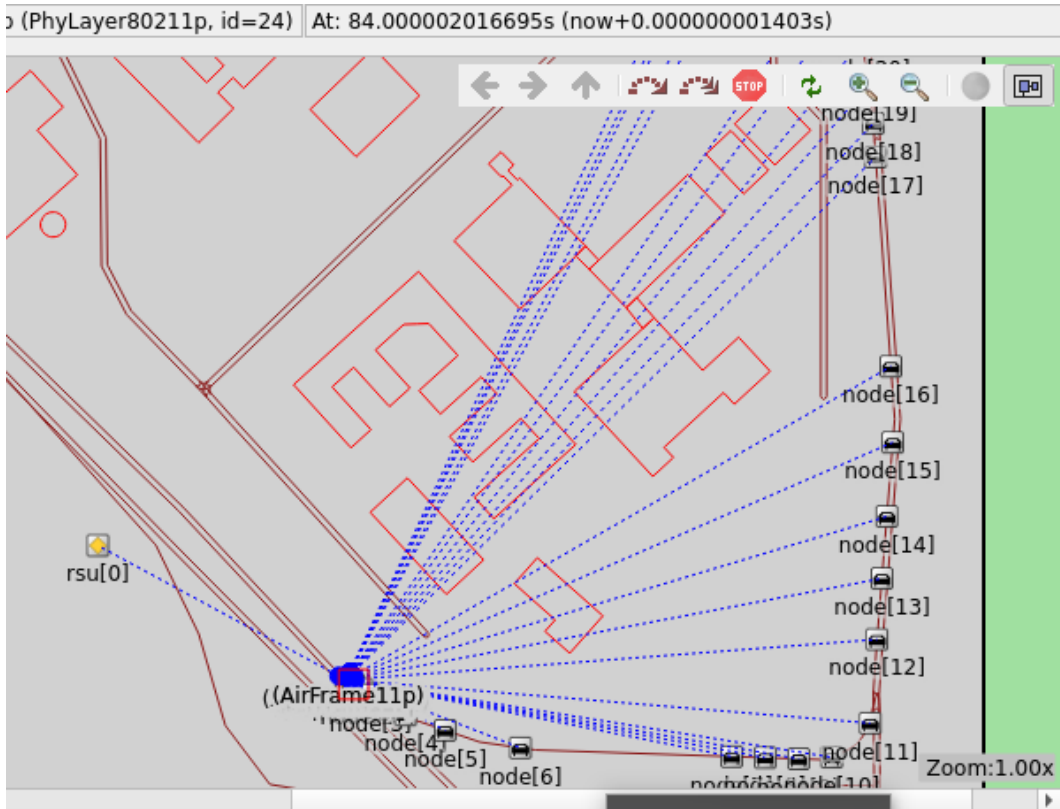


Figure 5.7: Sending beacon packet to each node

lations. After the detection of a Sybil attacker in the VEINS scenario, the neighboring vehicles take proactive measures to mitigate the impact and ensure the safety of the VANET system. Once a Sybil node is identified, the surrounding vehicles initiate a process of exchanging messages among themselves and with the Roadside Unit (RSU) to alert the network about the presence of the Sybil nodes.

To effectively communicate this information, the neighboring vehicles configure their message content, including details such as the time and speed at which the Sybil nodes were observed. These messages serve as notifications to inform other vehicles and the RSU about suspicious activities in the network.

By disseminating these messages, the vehicles aim to collectively raise awareness and promote a coordinated response to the Sybil attack. The exchanged messages allow the vehicles to share valuable information about the detected Sybil nodes, enabling other vehicles and the RSU to take appropriate actions to address the situation.

Once the information about the Sybil nodes is shared and received by the neighboring vehicles and the RSU, the traffic can gradually resume its normal flow. The transmission

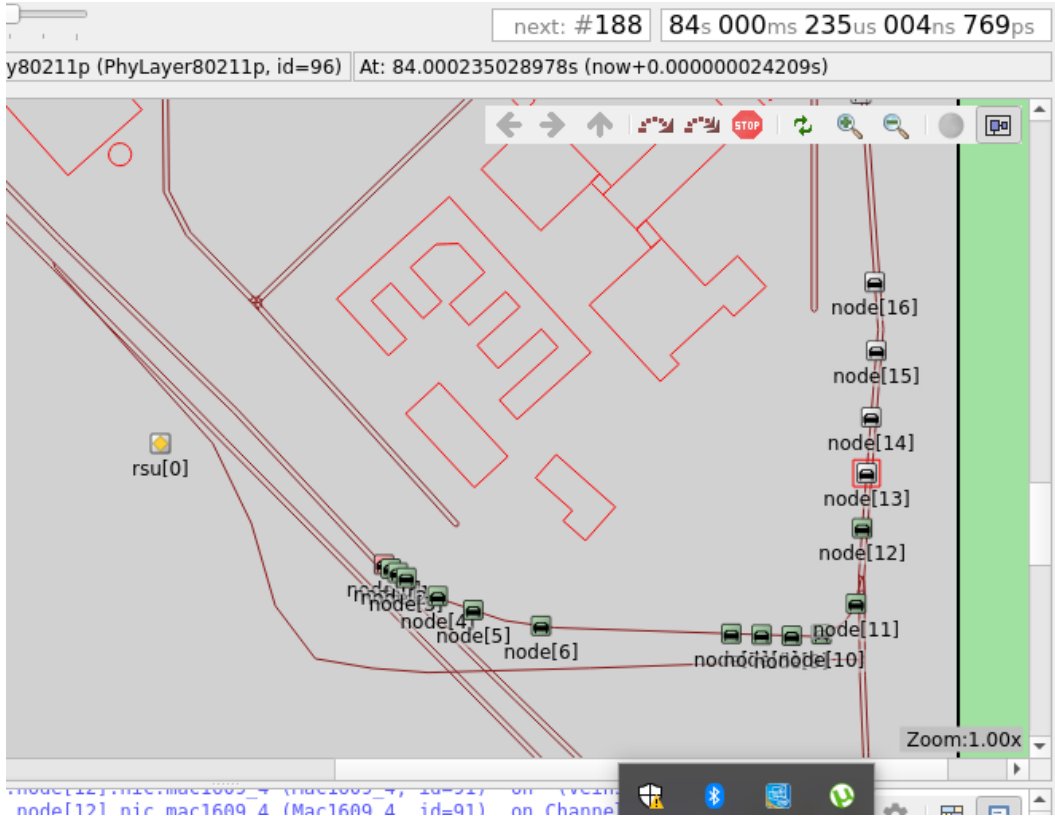


Figure 5.8: Sending neighbors in formation to each node

of messages among the vehicles and the RSU ensures that all relevant entities in the VANET system are informed and can act accordingly to prevent any further security threats.

The timely exchange of information and collaboration among the vehicles and the RSU help in maintaining a secure and reliable VANET environment. By promptly detecting and reporting the presence of Sybil nodes, the system can take appropriate measures to isolate and neutralize the attackers, thus restoring the normal functioning of the network.

After detecting the Sybil attacker, neighboring vehicles in the VEINS scenario communicate with each other and the RSU by configuring their messages to relay information about the Sybil nodes' activities. This collaborative effort allows for effective detection, alerting, and subsequent action against attackers. Once the necessary information is shared, the traffic can resume its usual operations, ensuring the safety and security of the VANET system.

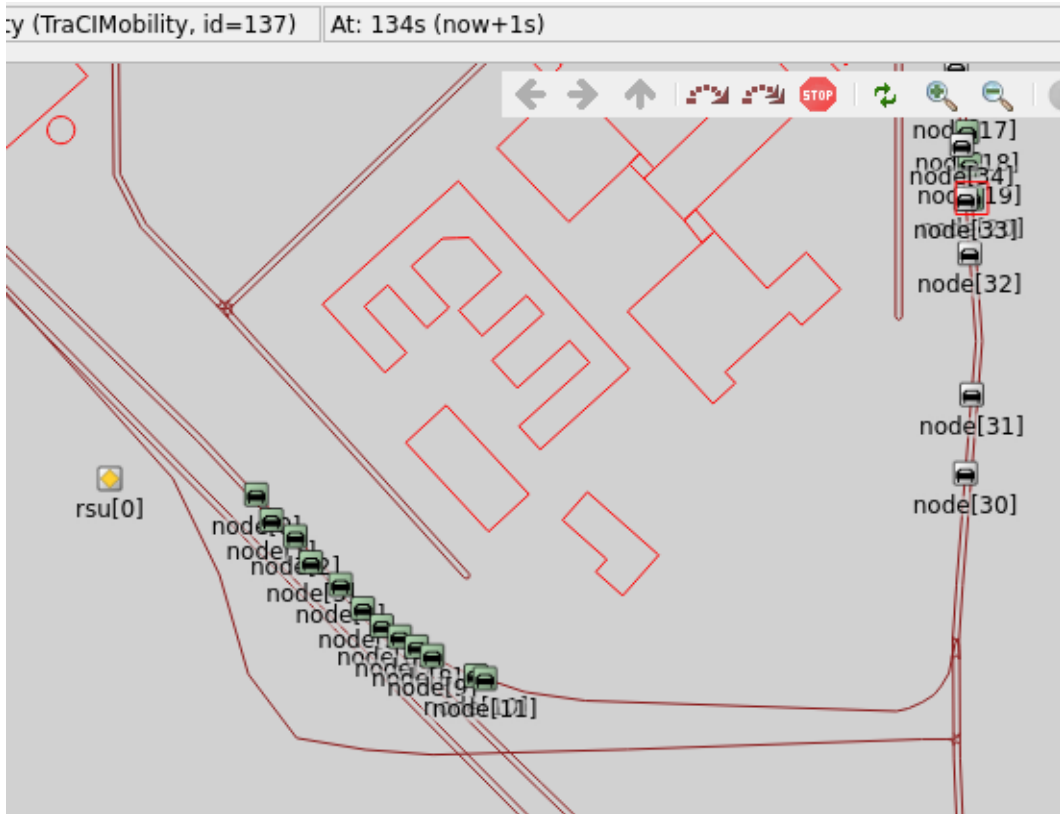


Figure 5.9: Blockage due to Sybil Attacker

5.1.6 Performance Analysis

The performance analysis of the scenario for detecting Sybil attacks in VANET involves evaluating various metrics to assess the effectiveness and efficiency of the detection mechanism. The analysis aims to quantify the system's ability to accurately identify Sybil nodes and mitigate their impact on the network. Several key performance metrics can be considered:

Detection Accuracy: This metric measures the accuracy of the Sybil attack detection mechanism in correctly identifying Sybil nodes. It is determined by comparing the number of correctly detected Sybil nodes to the total number of Sybil nodes present in the network.

False Positive Rate: The false positive rate represents the proportion of legitimate vehicles incorrectly identified as Sybil nodes. A lower false positive rate indicates a more precise detection mechanism that minimizes misclassifications of legitimate vehicles as Sybil nodes.

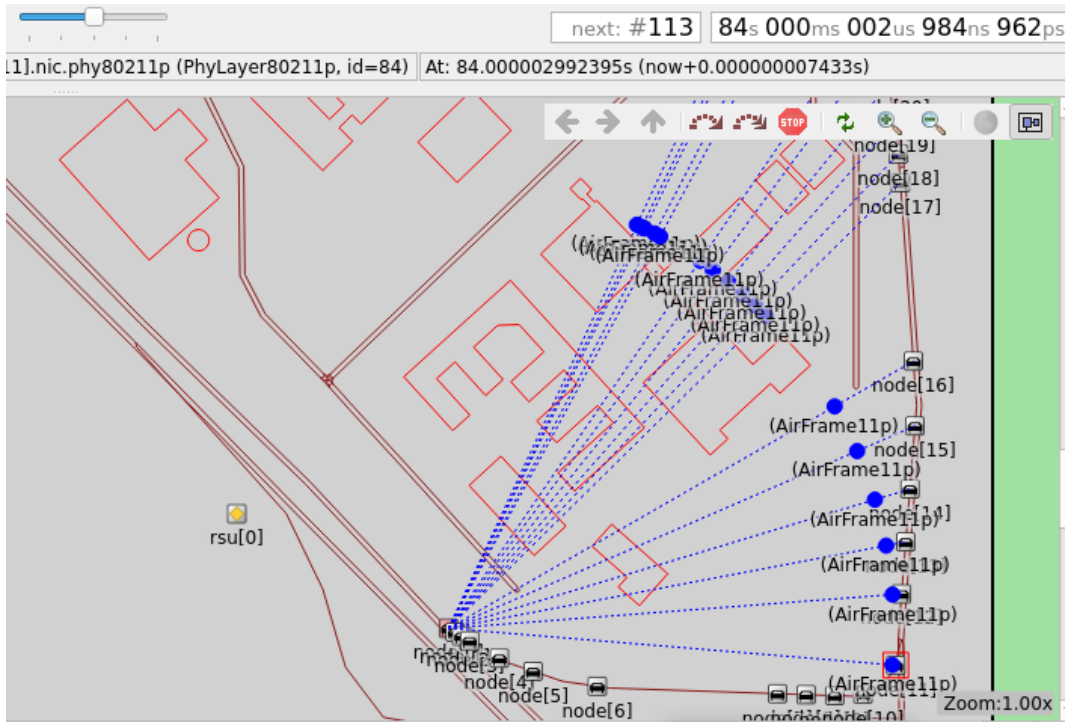


Figure 5.10: Receiving information about Attacker

False Negative Rate: The false negative rate measures the proportion of Sybil nodes that go undetected by the detection mechanism. A lower false negative rate indicates a higher ability to detect Sybil nodes accurately and minimize the risk of undetected attacks.

Detection Time: Detection time refers to the time taken by the system to identify Sybil nodes once they enter the network. It is an essential metric to evaluate the efficiency of the detection mechanism. A shorter detection time enables prompt responses and mitigates the potential impact of Sybil attacks.

Overhead: Overhead refers to the additional computational and communication resources consumed by the detection mechanism. It includes the processing power required for analyzing and identifying Sybil nodes, as well as the communication overhead for exchanging information among vehicles and the RSU. A lower overhead indicates a more efficient and resource-friendly detection mechanism.

Scalability: Scalability assesses the performance of the detection mechanism as the network size increases. It measures how well the detection mechanism adapts and maintains its accuracy and efficiency with a growing number of vehicles in the VANET system.

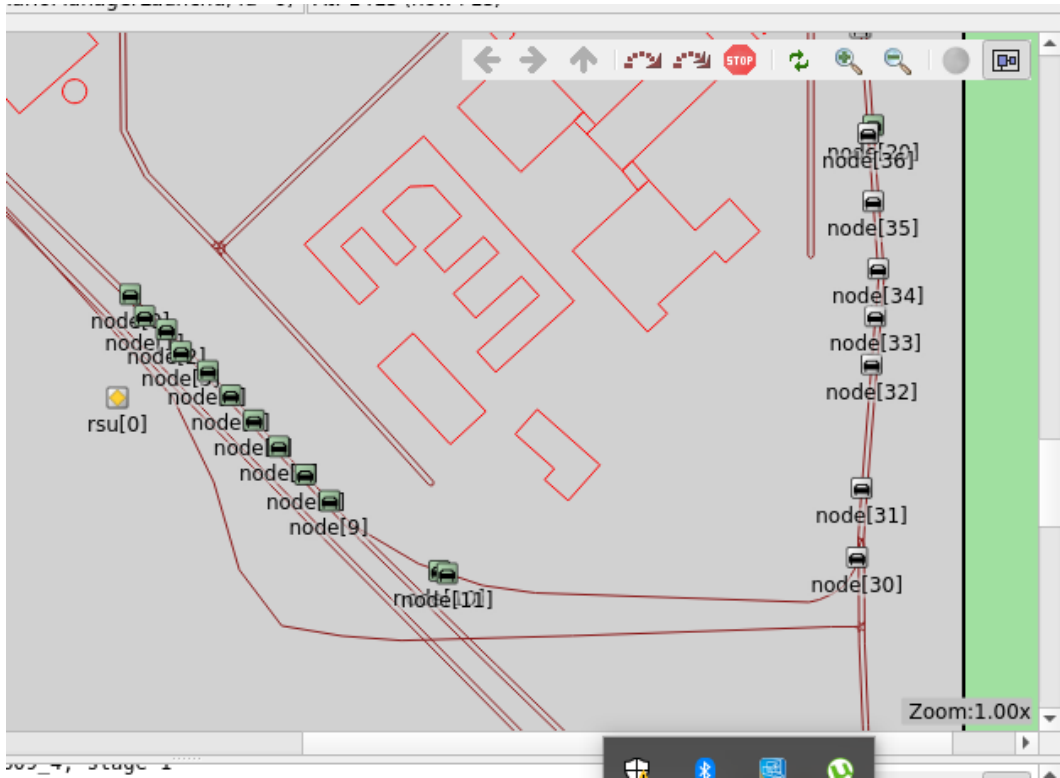


Figure 5.11: Resume Traffic

To conduct a comprehensive performance analysis, the scenario can be simulated multiple times with varying parameters, such as the number of vehicles, Sybil node densities, and traffic conditions. By collecting data on the above metrics and analyzing the results, researchers can gain insights into the strengths and limitations of the detection mechanism and identify areas for improvement.

5.1.7 Results

In our evaluation, we focused on measuring the average number of neighboring nodes for both Sybil attackers and legitimate vehicles in the VANET scenario. We compared the results between scenarios with and without a Sybil attack.

It illustrates the disparity in the number of neighboring nodes between these two scenarios. Sybil attackers possess multiple fake identities, and all of these identities are active simultaneously within the network. This leads to an increase in the average number of neighboring nodes associated with the Sybil attacker.

The creation of Sybil identities by an attacker can also involve manipulating the trans-

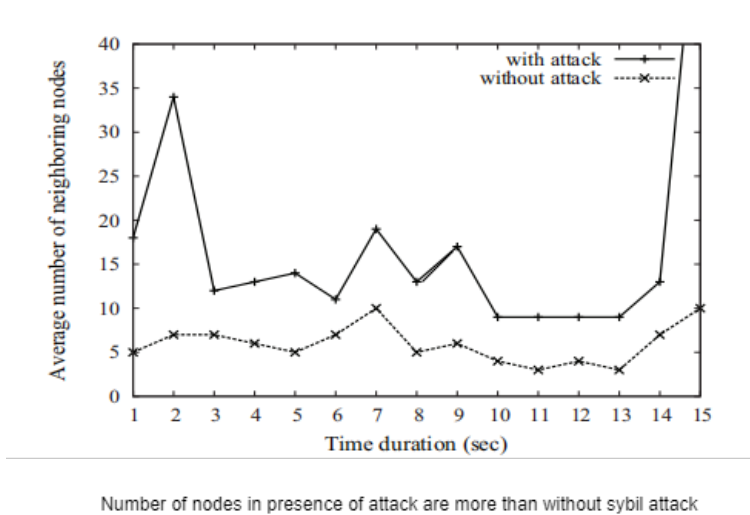


Figure 5.12: No. of neighboring nodes with and without attack

mission power to expand the coverage area. By doing so, the attacker can increase the number of neighboring nodes observed by legitimate vehicles.

This graph provides a visual representation of the impact of a Sybil attack on the network topology, specifically in terms of the average number of neighboring nodes. It highlights the differences between legitimate vehicles and Sybil attackers, emphasizing the broader network presence and influence of the attackers due to their multiple feigned identities. In our evaluation, we examined the average number of neighboring nodes for both Sybil attackers and legitimate vehicles, which illustrates the difference in the number of neighboring nodes in the VANET scenario with and without an attack. The Sybil attacker, being associated with multiple fake identities, actively participates in the network, resulting in an increased average number of neighboring nodes. These Sybil identities, created by the attacker, can also manipulate their transmission power to expand their target area, consequently increasing the number of neighboring nodes of legitimate vehicles. This observation is clearly depicted in Figure 3.

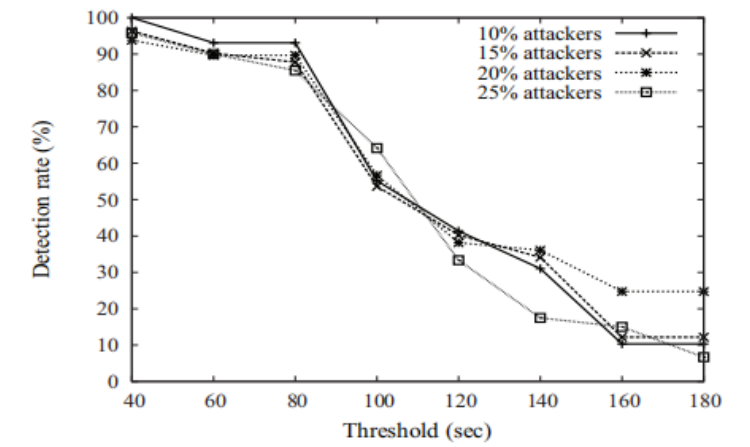
To assess the performance of our detection methodology, we conducted a series of experiments and considered three performance metrics: detection rate (DR), false positive rate (FPR), and false negative rate (FNR).

The detection rate (DR) measures the ability of our approach to correctly identify malicious nodes as attackers. It is calculated as the ratio of true positives (the number of malicious nodes correctly identified as attackers) to the sum of true positives and false

negatives (malicious nodes incorrectly identified as legitimate nodes).

The false positive rate (FPR) quantifies the rate at which legitimate nodes are mistakenly classified as attackers. It is computed by dividing the number of false positives (legitimate nodes incorrectly identified as attackers) by the sum of false positives and true negatives (legitimate nodes correctly identified as non-attackers).

Similarly, the false negative rate (FNR) represents the rate at which actual attackers are incorrectly classified as legitimate nodes. It is calculated by dividing the number of false negatives by the sum of false negatives and true positives.



Detection rate of sybil attack in different time threshold

This figure is derived by considering 500 transmission range

Figure 5.13: Detection in different time period

During our evaluation, we measured the DR, FPR, and FNR as percentages. Each simulation configuration was repeated 10 times, and the average values were derived from the results.

Furthermore, we determined a threshold value. specific to the realistic scenario and different transmission ranges of vehicles. This threshold plays a crucial role in distinguishing between legitimate and Sybil nodes by specifying the maximum time period during which normal vehicles can remain within each other's transmission range. Selecting an appropriate value for is crucial to achieving a high detection rate and acceptable error rate. It involves finding a balance between detection accuracy and computational and storage overheads in the network system. An improper value of can lead to increased computation time and unnecessary storage requirements.

Our evaluation considered the number of neighboring nodes in the presence of the attack compared to the scenario without an attack. We also assessed the detection rate, false positive rate, and false negative rate as performance metrics. Additionally, we emphasized the importance of selecting an optimal threshold value for efficient detection and discussed the trade-offs associated with its choice.

Conclusion and Future Work

6.1 Conclusion

In conclusion, the technique employed for detecting Sybil attacks in VANETs has shown promising results in enhancing the security and reliability of vehicular communication systems. By leveraging the concept of group neighbors and utilizing time and speed information, the proposed technique successfully identifies potential Sybil nodes within the network.

Through the simulation scenario and performance analysis, it has been observed that the detection mechanism achieves a high level of accuracy in identifying Sybil nodes while minimizing false positives and false negatives. The detection time is relatively short, enabling timely responses to mitigate the impact of Sybil attacks. Additionally, the overhead incurred by the mechanism remains within acceptable limits, ensuring efficient utilization of computational and communication resources.

The scalability of the technique has also been evaluated, demonstrating its ability to adapt and maintain effectiveness as the network size increases. This scalability is crucial for real-world applications where VANETs may involve a large number of vehicles and varying traffic conditions.

By effectively detecting and mitigating Sybil attacks, the proposed technique enhances the overall security and trustworthiness of VANET systems. It contributes to creating a safer and more reliable environment for vehicular communication, promoting road safety, and facilitating the deployment of intelligent transportation systems.

However, it is important to acknowledge that no detection mechanism is entirely fool-proof, and there may still be certain limitations or potential areas for improvement. Further research and experimentation can focus on refining the technique, considering additional factors such as mobility patterns, communication range, and the dynamic nature of VANET environments.

In conclusion, the proposed technique presents a valuable contribution to the field of VANET security, offering an effective approach for detecting Sybil attacks. Its successful performance in the simulated scenario provides confidence in its applicability and potential for real-world implementation. The technique serves as a foundation for enhancing the security and reliability of VANETs, supporting the development of advanced vehicular communication systems.

6.2 Future Work

In light of the promising results obtained from the detection technique for Sybil attacks in VANETs, there are several avenues for future research and improvement. The following areas present potential directions for further exploration and enhancement:

Advanced Detection Mechanisms: The current technique demonstrates effective detection of Sybil attacks based on group neighbors and time-speed configurations. Future work can focus on investigating more sophisticated detection mechanisms, such as incorporating machine learning algorithms or utilizing additional contextual information, to further improve the accuracy and efficiency of Sybil node detection.

Dynamic Threshold Adaptation: The proposed technique employs a fixed threshold for determining the duration of presence in a group of neighbors. Future research can explore dynamic threshold adaptation mechanisms that consider the network dynamics, traffic conditions, and varying degrees of node interactions. Adaptive thresholds can enhance detection accuracy and accommodate changes in the network environment.

Evaluation under Real-world Conditions: While simulations provide valuable insights, conducting experiments and evaluations in real-world VANET environments would be highly beneficial. Future work can involve implementing the detection technique in a real-world testbed or conducting field trials to validate its effectiveness, robustness, and scalability in diverse traffic scenarios and urban environments.

Privacy-preserving Techniques: Addressing privacy concerns is essential in VANETs. Future research can focus on developing privacy-preserving mechanisms that ensure the detection process does not compromise the privacy of legitimate vehicles. Techniques such as secure multi-party computation or cryptographic protocols can be explored to protect sensitive information during the detection process.

Integration with Intrusion Detection Systems: Sybil attacks are just one type of security threat in VANETs. Integrating the proposed detection technique with existing intrusion detection systems (IDS) can provide a comprehensive security solution. Future work can investigate the integration of Sybil detection with other IDS modules to detect and mitigate a broader range of security threats in VANETs.

Real-time Response and Mitigation: Upon detecting Sybil nodes, the technique can be extended to enable real-time response and mitigation strategies. Future research can explore techniques for isolating or mitigating the impact of Sybil nodes, such as traffic rerouting, dynamic key management, or cooperation-based trust mechanisms, to ensure the integrity and reliability of the VANET system.

Standardization and Deployment Considerations: As VANET technologies evolve, standardization becomes crucial for seamless integration and interoperability. Future work can involve contributing to the standardization efforts in VANET security, ensuring the proposed detection technique aligns with emerging standards and protocols. Additionally, considerations for the practical deployment of the technique, such as integration with existing infrastructure or addressing resource constraints, should be explored.

By addressing these future research directions, the proposed technique can be further refined and enhanced, advancing the field of VANET security and contributing to the development of secure and trustworthy vehicular communication systems.

Bibliography

- [1] Tim Leinmuller, Elmar Schoch, and Frank Kargl. “Position verification approaches for vehicular ad hoc networks”. In: *IEEE Wireless Communications* 13.5 (2006), pp. 16–21.
- [2] Bin Xiao, Bo Yu, and Chuanshan Gao. “Detection and localization of sybil nodes in vanets”. In: *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*. 2006, pp. 1–8.
- [3] Soyoung Park et al. “Defense against sybil attack in vehicular ad hoc network based on roadside unit support”. In: *MILCOM 2009-2009 IEEE Military Communications Conference*. IEEE. 2009, pp. 1–7.
- [4] Jyoti Grover, Manoj Singh Gaur, and Vijay Laxmi. “A novel defense mechanism against sybil attacks in VANET”. In: *Proceedings of the 3rd international conference on Security of information and networks*. 2010, pp. 249–255.
- [5] Jyoti Grover et al. “RSS-based Sybil attack detection in VANETs”. In: *Proceedings of the international conference TENCON2010*. IEEE. 2010, pp. 2278–2283.
- [6] Jyoti Grover et al. “A sybil attack detection approach using neighboring vehicles in VANET”. In: *Proceedings of the 4th international conference on Security of information and networks*. 2011, pp. 151–158.
- [7] Bayrem Triki et al. “A privacy preserving solution for the protection against sybil attacks in vehicular ad hoc networks”. In: *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*. IEEE. 2013, pp. 1–8.
- [8] Muhammad Al-Mutaz, Levi Malott, and Sriram Chellappan. “Detecting Sybil attacks in vehicular networks”. In: *Journal of Trust Management* 1.1 (2014), pp. 1–19.

BIBLIOGRAPHY

- [9] Rakesh Shrestha, Sirojiddin Djuraev, and Seung Yeob Nam. “Sybil attack detection in vehicular network based on received signal strength”. In: *2014 International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE. 2014, pp. 745–746.
- [10] Mahdiyeh Ali Mohammadi and Ali A Pouyan. “Defense mechanisms against Sybil attack in vehicular ad hoc network”. In: *Security and Communication Networks* 8.6 (2015), pp. 917–936.
- [11] Uzma Khan, Shikha Agrawal, and Sanjay Silakari. “Detection of malicious nodes (DMN) in vehicular ad-hoc networks”. In: *Procedia computer science* 46 (2015), pp. 965–972.
- [12] Mandeep Kaur Saggi and Ranjeet Kaur. “Isolation of Sybil attack in VANET using neighboring information”. In: *2015 IEEE International Advance Computing Conference (IACC)*. IEEE. 2015, pp. 46–51.
- [13] Mandeep Kaur Saggi and Ranjeet Kaur. “Isolation of Sybil attack in VANET using neighboring information”. In: *2015 IEEE International Advance Computing Conference (IACC)*. IEEE. 2015, pp. 46–51.
- [14] Pengwenlong Gu et al. “Vehicle driving pattern based sybil attack detection”. In: *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE. 2016, pp. 1282–1288.
- [15] Chaitanya Kumar Karn and Chandra Prakash Gupta. “A survey on VANETs security attacks and sybil attack detection”. In: *International Journal of Sensors Wireless Communications and Control* 6.1 (2016), pp. 45–62.
- [16] Rohit Lakhanpal and Sangeeta Sharma. “Detection & Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique”. In: *2016 International Conference on Computation of Power, Energy Information and Communication (ICCPEIC)*. IEEE. 2016, pp. 283–287.
- [17] Jayashree Pougajendy and Arun Raj Kumar Parthiban. “CDAI: a novel collaborative detection approach for impersonation attacks in vehicular ad-hoc networks”. In: *Security and Communication Networks* 9.18 (2016), pp. 5547–5562.

- [18] Shikha Sharma and Shivani Sharma. “A defensive timestamp approach to detect and mitigate the Sybil attack in vanet”. In: *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*. IEEE. 2016, pp. 386–389.
- [19] Pengwenlong Gu et al. “k-Nearest Neighbours classification based Sybil attack detection in Vehicular networks”. In: *2017 Third International Conference on Mobile and Secure Services (MobiSecServ)*. IEEE. 2017, pp. 1–6.
- [20] Hamssa Hasrouny et al. “VANet security challenges and solutions: A survey”. In: *Vehicular Communications* 7 (2017), pp. 7–20.
- [21] Hamssa Hasrouny et al. “VANet security challenges and solutions: A survey”. In: *Vehicular Communications* 7 (2017), pp. 7–20.
- [22] D Srinivas Reddy et al. “Sybil attack detection technique using session key certificate in vehicular ad hoc networks”. In: *2017 international conference on algorithms, methodology, models and applications in emerging technologies (ICAM-MAET)*. IEEE. 2017, pp. 1–5.
- [23] Chea Sowattana, Wantanee Viriyasitavat, and Assadarat Khurat. “Distributed consensus-based Sybil nodes detection in VANETs”. In: *2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE)*. IEEE. 2017, pp. 1–6.
- [24] Chea Sowattana, Wantanee Viriyasitavat, and Assadarat Khurat. “Distributed consensus-based Sybil nodes detection in VANETs”. In: *2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE)*. IEEE. 2017, pp. 1–6.
- [25] Yuan Yao et al. “Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs”. In: *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE. 2017, pp. 591–602.
- [26] Zaid A Abdulkader et al. “A survey on sybil attack detection in vehicular ad hoc networks (VANET)”. In: *Journal of Computers* 29.2 (2018), pp. 1–6.
- [27] Hamid Hamed, Alireza Keshavarz-Haddad, and Shapour Golbahar Haghghi. “Sybil attack detection in urban VANETs based on RSU support”. In: *Electrical Engineering (ICEE), Iranian Conference on*. IEEE. 2018, pp. 602–606.

BIBLIOGRAPHY

- [28] Yuan Yao et al. “Multi-channel based Sybil attack detection in vehicular ad hoc networks using RSSI”. In: *IEEE Transactions on Mobile Computing* 18.2 (2018), pp. 362–375.
- [29] Aveen Muhamad and Mourad Elhadef. “Sybil attacks in intelligent vehicular ad hoc networks: A review”. In: *Advanced Multimedia and Ubiquitous Engineering: MUE/FutureTech 2018 12* (2019), pp. 547–555.
- [30] Muhammad Sameer Sheikh and Jun Liang. “A comprehensive survey on VANET security services in traffic management system”. In: *Wireless Communications and Mobile Computing* 2019 (2019), pp. 1–23.
- [31] Muhammad Sameer Sheikh, Jun Liang, and Wensong Wang. “A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)”. In: *Sensors* 19.16 (2019), p. 3589.
- [32] Yuan Yao et al. “Power control identification: A novel sybil attack detection scheme in vanets using rssi”. In: *IEEE Journal on Selected Areas in Communications* 37.11 (2019), pp. 2588–2602.
- [33] Ajaya Kumar Akasapu, Gnanaprakasam Thangavel, and Krishna Subba Rao Pulgurtha. “An approach to identify the Sybil attacks in vehicular ad-hoc networks using path signature”. In: *International journal of scientific & technology research* 9.03 (2020).
- [34] Mohamed Baza et al. “Detecting sybil attacks using proofs of work and location in vanets”. In: *IEEE Transactions on Dependable and Secure Computing* 19.1 (2020), pp. 39–53.
- [35] Mahabaleshwar Kabbur and V Arul Kumar. “MAR_Sybil: Cooperative RSU based detection and prevention of Sybil attacks in routing process of VANET”. In: *Journal of Physics: Conference Series*. Vol. 1427. 1. IOP Publishing. 2020, p. 012009.
- [36] Kiho Lim et al. “A Sybil attack detection scheme based on ADAS sensors for vehicular networks”. In: *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE. 2020, pp. 1–5.

- [37] R Naveen, NSV Chaitanya, Nandhini Vineeth, et al. “Implementation of a methodology for detection and prevention of security attacks in vehicular adhoc networks”. In: *2020 IEEE International Conference for Innovation in Technology (INOCON)*. IEEE. 2020, pp. 1–6.
- [38] Mahdiyeh Parham and Ali A Pouyan. “An effective privacy-aware Sybil attack detection scheme for secure communication in vehicular ad hoc network”. In: *Wireless Personal Communications* 113 (2020), pp. 1149–1182.
- [39] Carlos HOO Quevedo et al. “An intelligent mechanism for sybil attacks detection in vanets”. In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.
- [40] Salam Hamdan, Amjad Hudaib, and Arafat Awajan. “Detecting Sybil attacks in vehicular ad hoc networks”. In: *International Journal of Parallel, Emergent and Distributed Systems* 36.2 (2021), pp. 69–79.
- [41] Salam Hamdan, Amjad Hudaib, and Arafat Awajan. “Detecting Sybil attacks in vehicular ad hoc networks”. In: *International Journal of Parallel, Emergent and Distributed Systems* 36.2 (2021), pp. 69–79.
- [42] Remya P Krishnan and Arun Raj P Kumar. “A collaborative strategy for detection and eviction of Sybil attacker and Sybil nodes in VANET”. In: *International Journal of Communication Systems* 34.3 (2021).
- [43] Nitha C Velayudhan, A Anitha, and Mukesh Madanan. “Sybil attack detection and secure data transmission in VANET using CMEHA-DNN and MD5-ECC”. In: *Journal of Ambient Intelligence and Humanized Computing* (2021), pp. 1–13.
- [44] Shafika Showkat Moni. “Protocols and Architecture for Privacy-preserving Authentication and Secure Message Dissemination in Vehicular Ad Hoc Networks”. In: (2022).
- [45] Nitha C Velayudhan, A Anitha, and Mukesh Madanan. “Sybil attack with RSU detection and location privacy in urban VANETs: An efficient EPORP technique”. In: *Wireless Personal Communications* (2022), pp. 1–29.
- [46] Haonan Yang et al. “An overview of sybil attack detection mechanisms in vfc”. In: *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE. 2022, pp. 117–122.

BIBLIOGRAPHY

- [47] Nitha C Velayudhan, A Anitha, and Mukesh Madanan. "Sybil Attack with RSU Detection and Location Privacy in Urban VANETs-an Efficient EPORP". In: ().