International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

An Evaluation of Sybil Attack's Detection Approaches in Vehicular Ad-Hoc Networks (VANETs)

Muhammad Iqbal Younis[1], Rana M. Amir Latif[2], Izharul Haq[3], NZ Jhanjhi[4], Abdul Karim[5]

Submitted: 14/08/2022 **Accepted:** 11/11/2022

Abstract: Vehicular ad hoc networks (VANETs) are being used and progressively promoted for traffic control and accident prevention. A malicious node can be manufactured to be several vehicle nodes in a Sybil attack. It is generally agreed that vehicular ad hoc networks (VANETs) must rely heavily on peer-to-peer correspondence and malignant data traffic with the ultimate goal of achieving execution goals. The Sybil attack undermines attacks in which the aggressor deceives different nodes by the same incorrect ID or copy ID of the clients aware of the nodes in the WSN. Sybil attacks are named after an anecdotal personality with issues of dissociative uniqueness. The web-based social networking is under Sybil's attack, and it affects the entire system. By multiplying deceptive profiles using false characteristics, Sybil attacks are attacks against informal online organizations' reputations. In online social networks, bogus profiles have become a continuous and evolving danger. The line between the physical and online worlds is getting obscured as organizations and individuals grasp social networks. So, distinguishing, countering, and containing counterfeit records on online networks is critical. We collected datasets and performed a simulation to detect Sybil attacks. A dataset, which contains 1048576 records, is selected. A big data issue is a large dataset, so it was divided into chunks. The partitioned datasets are 11, and for detecting a Sybil attack, each is simulated. For detecting Sybil attacks in the network, a methodology is proposed. Sybil attacks have been detected by checking the similarity of each node's attributes to existing nodes.

Keywords: *Vehicular, Ad-Hoc Networks (VANETs), Sybil attacks, Social Networks, WSN*

1. Introduction

Today's world has connected objects, including watches, cameras, automobiles, and even medical equipment. For the progress and growth of humanity, these entities, which are described above, are significant. Vehicular ad-hoc networks or VANET consist of vehicles, also known as Nodes, RSUs (Road-Side Units), and CAs (Certification Authorities). This Vehicular network belongs to a category of MANET. With the frequent migration of nodes due to mobility, this MANET type can be classified as an (Ephemeral) Network. The vehicular ad-hoc network makes communication possible between:

- V – to-V (Vehicle-to-Vehicle)
- Vehicle-to-RSUs or Road Side Units

The ad hoc vehicle network is one of the easiest forms of creating ITS (Intelligent Transport System). What technology is used to apply ICT (information & communications technology) to transport infrastructures and automobiles (based on the WAVE standard IEEE 802.11)? These networks have no defined infrastructure and depend fully on themselves to facilitate network communication.

VANET has a decentralized feature, such that any node may function as a host. The density of the network would, therefore, shift with the change in traffic density. These VANET features make network security rather complicated. Security problems are data protection, safe communication, tamper-resistant hardware, and software, such that security can affect all components of the device due to this problem. VANET defence must be able to withstand all forms of attacks [1]. The protection of VANET is a little different from wireless network security and wired network security since it has specific characteristics of accessibility limitations, infrastructure-less framework, and limited length of the connection between nodes [2]. Before developing any defence strategy for VANETs, we should know numerous security and danger problems, their capacities to manage and avoid threats, and different forms of attackers [3].

Local attackers launch attacks with limited scope; attacks are restricted to a specific area. However, **Error! Reference source n ot found.** shows different ways of performing a Sybil attack in the context of VANET.

[1]*National College of Business Administration & Economics, Rahim Yar Khan, Pakistan, m.iqbalyounis@gmail.com*
[2]*Department of Computer Science COMSATS University Islamabad, Sahiwal Campus, ranaamir10611@gmail.com*
[3]*College Of Sciences and Human Studies Prince Mohammad bin Fahd University, Saudi Arabia, ihaq@pmu.edu.sa*
[4]*School of Computer Science and Engineering SCE, Taylor's University, Malaysia, noorzaman.jhanjhi@taylors.edu.my*
5Department of Computer Science & Electronics, University Gadjah Mada, Yogyakarta, Indonesia, abdullkarim@hotmail.com
** Corresponding Author Email: noorzaman.jhanjhi@taylors.edu.my*

Table 1 Methods of Sybil Attack

Sr.#	*Method of Sybil Attack*	*Description*
1	*Using Fake Identity to Perform a Sybil attack [1]*	*In the fake identity method, the attacker uses many pseudonymous identities to get influenced by the VANET on a massive scale.*
2	*Using Identity Theft to perform a Sybil attack [5]*	*In this attack, the Attackers use the stolen information from the accessible sources, access the vehicular network, join the network, and do wicked things.*
3	*Conspired Sybil Attack, sock puppets [7]*	*An identity used for description is a sock puppet. It portrays conversations that are used for the malicious attack but looking useful. In this method, the attackers of the Sybil attack victim the stakeholders to gain access to the vehicular ad hoc network.*
s4	*Compromise on Message Integrity [7]*	*Message/data consistency ensures that it has not been modified in any manner, like insertion or delete replay attacks or by frame addition or deletion. In this assault, the messages transmitted from one node to another network node are comprised and modified to trigger the attack.*
5	*Insider Attacker [10]*	*In an insider attack, an entity resides in the network with a harmful aim. Due to the reason that it uses the inside information about the system, its detection is not an easy task, and, in this way, the attacker negatively impacts the services of the vehicular network.*

The table generally describes that a malicious node makes many fake identities behave like genuine nodes and successful in harming the network. There is always needed for such a system that secures the network when communication of message occurs between source nodes to the destination node for the data confidentiality services. The following are some techniques used in the Sybil attacks system of detection shown in **Error! Not a valid bookmark self-reference.**.

Table 2 Detection Techniques of Sybil Attack

Sr. No	*Detection Technique of Sybil Attack*	*Description*	*Advantages/Merits*	*Disadvantages/Demerits*
1	*The technique of Mining of Data*	*It is a technique of coming across insights & know-how for a dataset that can assist in discovering the Sybil attack*	*It can be worked with several variables with or without some correlation.*	*Complex data sets overheads are the demerits of this scheme*
2	*Statistical Analysis Technique*	*In the technique of statistical analysis, data can be described, explained, and summarized, and based on these analyses; conclusions can be easily obtained.*	*The main advantage of this method is predictive analytics to mitigate future problems in the vehicular network*	*Massive sampling errors, validity constructs may not be accurate. Even though the excessive correlation is observed in factors, it may not prove that it is the far reason for the attacks.*
3	*Analysis of Data Stream*	*In this technique, the knowledge structures are extracted from rapids and continuous data records in a real-time frame.*	*This method can consider heuristic research data and get a real-time response before increasing the Sybil attack's adversity in the vehicular network more.*	*Limited offline analysis and the overhead of Large Data sets are some demerits of this technique.*
4	*Machine Learning Technique*	*The differentiation in this method is NOT in machine learning approach or data mining techniques but in the way to do with the results; we need patterns of datasets in the technique of machine learning to characterize abnormal and normal States to arrive at some type of decision.*	*This technique works for Sybil attack detection without illustrating the programming approaches.*	*It is challenging to deal with massive unstructured data with hidden, unknown patterns.*
5	*Techniques based on Probability*	*The probability method of detecting Sybil attack deals with detecting the issue related to whether some change occurs in the vehicular network or no change occurs and recognizing the times of some changes that may help detect Sybil attack in the network.*	*It can be used to make some decisions about Sybil attacks in the absence of the list of the exhaustive population present in real-time.*	*Time-consuming overheads and expensive*
6	*Sequence Mining Technique*	*assist in finding the patterns of most infrequent or frequent activities*	*Maybe helpful to tackle the Repeat-related issues*	*large dataset overhead in the shape of response/retrieval time and memory*
7	*Reputation, Trust in Voting Ranking Technique*	*In this technique, malicious nodes are detected using Trust points based on different types of algorithms. which helps to detection malicious nodes*	*Trust voting system based on man to machine and machine to machine voting may be built in this method*	*Trust system become failed in a network with compromised nodes*

8	*Thresholding Technique*	*With the help of heuristic evaluation and the algorithm of dynamic thresholding, Sybil attacks can be detected.*	*Having a simple implementation*	*The algorithm problem of numerical stability may occur due to the incorrect threshold calculation caused by extensive variability.*

Sybil detection and intrusion structures can be obtained from one of the strategies described above. However, these structures can also be characterized by storing location or data wherein the intensive computation algorithms are running. Table 3 given below illustrates this element.

Table 3 Intrusion Detection System (IDS) categories

Sr. No.	***Type ID system***	***Brief Description***
1	*Distributed IDS*	*No concept of client-server is present in Distributed IDS. In this approach, Multiple locations of analysis and detection of data for a network having multiple endpoints are present.*
2	*Central IDS*	*All nodes of the network communicate with the central node.*
3	*N –Tier IDS*	*In N-Tier, significant subnetworks and networks are present that have n-tier type of coordination between one another We are having n-tiers coordinating with each other. This coordination helps enhance the response to danger for the synchronization with one another and detect Sybil attacks.*

A robust cooperative system cannot blindly agree that its users will participate in the system. Malicious customers are seeking to take advantage of the machine for income. Egocentric users eat useful resources but avoid contribution. As an instance, adversaries have manipulated the voting system of Digg to sell their articles of dubious excellence. Selfish users in public BitTorrent communities go away from the system as quickly as they have completed downloading a file to keep away from uploading the report to others, ensuring critical overall performance degradation for these content distribution structures [4]. The most significant chance that cooperative systems face is the Sybil assault, wherein the adversaries create many Sybil identities (faux identities) and use them to disrupt the structures' ordinary operation. No security and incentive mechanism can work if it lacks secure identity management that could protect Sybil assaults [5].

There is no set infrastructure in an ad hoc network, such as base stations or moving engines. Shifting motors are taken into account as nodes that may be within any deferment's radio spectrum. They will speak without pause through Wi-Fi hyperlinks simultaneously, while the ones that far away depend upon separate nodes to transmit messages as routers. High node versatility in a vehicular ad-hoc network induces standard changes to the Network topology. VANET is built for a Vehicular node to the infrastructure node (V2I) and Vehicular node to Vehicular node (V2I), and vehicular to roadside gadgets (V2R) conversation [6]. Security in a vehicular network is important since one vehicle node's message data will have substantial consequences, including safety from roadside collisions. AODV (Reactive ad hoc network routing protocol) attempts to reduce the path discovery overhead to caching the course records for some period after a link expires. How lengthy any node has to hold this course knowledge is ready precedent, and usually randomly [7].

This architecture of VANET explains that motors are taken into consideration as nodes that could move freely with high mobility within a group and live connected, even if they are at high speed. Any car may talk with another automobile through DSRC (committed short variety of communication), as shown in Figure 1.

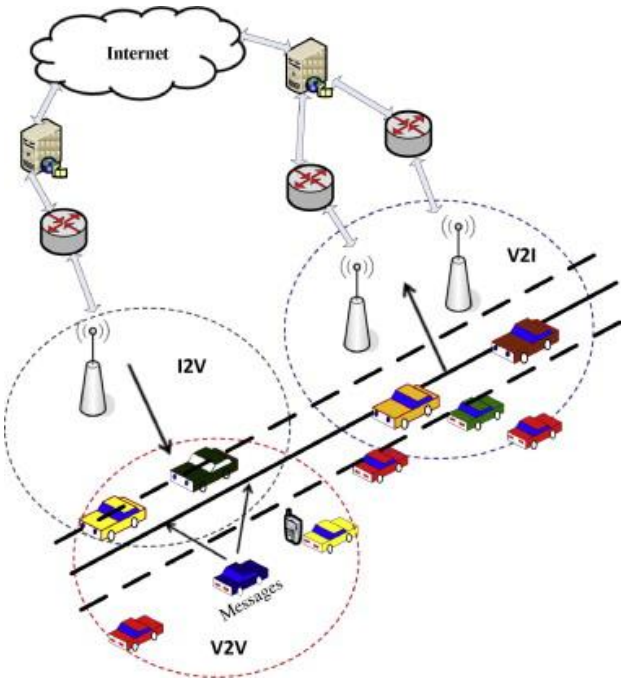

Figure 1 Architecture of VANET

The modern-day system of transportation has a vital function in people's day-by-day activities. Deficiencies and inefficiencies in transportation systems result in human life threats and wastage of time. Consequently, investigator s has attempted to introduce an Intelligent and smart system for transportation known as an intelligent transportation system (ITS). The vehicular ad-hoc network is a new transportation system that acquired a widespread interest in enterprise and studies areas. VANETs provide the basis for ITS an example is shown in Figure 2.

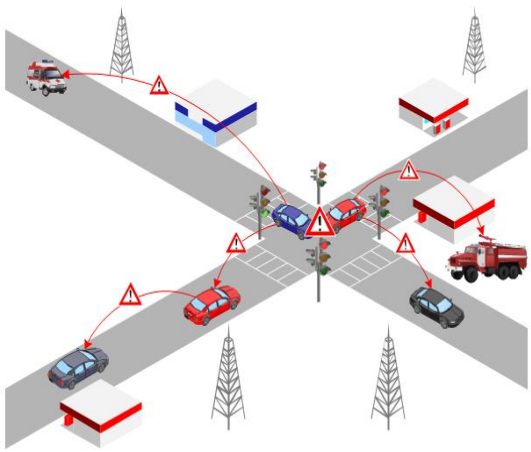

Figure 2 An Example of VANET

Due to the wireless nature of communications, VANET is at high risk of many network security threats associated with wireless networks with a highly dynamic nature. Sybil attacks are critical risks for the network, and Douceur defined it. Sybil attackers generate multiple fake copies of identities by stealing neighbour nodes' identities or deceiving them with new fake identities. Sybil attack is hazardous for the network's topologies, connectivity of networks, and consumption of bandwidth. Even, it has a few threats to the lives of human beings.

1.1. Importance of Sybil Attack Detection

Sybil detection is essential towards securing the network, and the following points bring into light the need to identify the Sybil attacks and defence strategies.

- Voting Tampering and Popularity structures: With multiple node identities, voting can be easily altered. The system can use voting to figure out the misbehaviour of nodes in a system report about roadside traffic and updated reputation rating.
- Routing Disturbance: A Multicast mechanism for packet routing might be disrupted by an attacker in a Sybil attack. If a Sybil node generates many malicious nodes within the network at some locations, in that case, separate paths that appear disjoint at the beginning may pass through the malicious entities of a single Sybil attacker.
- Taking most of the resources that are supposed to be similarly allotted among all of the motors inside the vehicular network and the bandwidth and radio channel in instances wherein valid automobiles use a shared channel.

In VANET, vehicles communicate with each other, as shown in Figure 3.

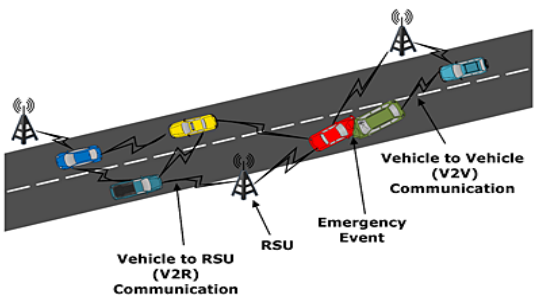

Figure 3 Communication in the Vehicular ad-hoc network (VAENT)

1.2. Sybil Attacks in Vehicular Ad-Hoc Network (VANET)

For a network's security assessment, an ad-hoc wireless network must fulfil some attributes conditions, i.e., integrity, availability, confidentiality, non-repudiation, and authentication.

1.2.1. Availability

Network availability offers a network's services, like connectivity services and bandwidth, to all the network nodes. Detection and prevention methods to secure the system from the issues regarding availability have been launched with an organization signatures scheme.

1.2.2. Authentication

Authentication means the identity verification among the automobile and Road Side Units and the validation of integrity during the exchange of messages between the wireless nodes. Also, it makes sure that everyone's network node is the valid vehicle node for communication purposes inside the wireless network.

1.2.3. Integrity

Data integrity is the warranty that information obtained utilizing Road Side Units, vehicle nodes, and AS is alike as produced at the time of message exchange. Virtual Signatures included with the password-based safe entry are used as a way to shield the message integrity.

1.2.4. Confidentiality

Confidentiality provides the services of confidentiality to communique the content. It ensures the private-ness of vehicle drivers to save them from unauthorized access. The most famous approach of pseudonyms is the most famous approach and used in VANET for privacy preservation.

1.2.5. Non-Repudiation

Non-repudiation services guarantee that the receiver and sender cannot refute ever receiving and sending a message, for example, a message about the accident. The term non-repudiation is also known as audit ability. The use of Road Side Units and the vehicle nodes have proven to send and receive the messages, respectively. A number of the network security attacks are described as under:

- Black-hole network attack

A network node rejects the neighbours' request to participate inside the vehicular network or when a longtime node drops out to form a black hole in a Black-hole network attack. The network receives redirected in the direction of a particular node that is sincere and leads to statistics lost.

- Sybil Attacks

A network node broadcasts more than one message to other nodes in a Sybil attack, and every message has a faked identity. The attacker's primary goal in the Sybil attack is to create misapprehension for other nodes via fake messages and to affect the other vehicle nodes for misusing them by the intruders.

- Disclosure of Identifications

Disclosure of IDs is a passive network assault. A malicious code sends to the target by the attacker to obtain the target vehicle node's information. Using this malicious code, information about the current location and the attacker node captures the vehicle's identity. Therefore, the privacy of the targeted node is damaged. In this way, route information and identities of the vehicles are accessed by the observers globally.

- Brute force

Safety of information is vital in VANET for the proper and effective functioning of vehicular network applications, and for this purpose, suitable approaches and algorithms of cryptography are needed. The attacker can access the cryptographic key by using

the brute force attack technique.

- Denial of service (DOS) attack

The aim of DOS is the unavailability of network applications and resources to the legitimate network nodes. VANETs have various personal life-saving and traffic efficiency applications, so it is crucial that every network node can have access to the network resources. In this aspect, DOS is the most dangerous attack as human lives can cause it. DOS jams network traffic and makes the network communication unavailable for the vehicle nodes that would bring about a variety of devastation in the applications of life savings in VANET.

- Middle Man attack

The attacker in this attack is seated between 2 vehicle nodes communicating with one another and releasing it. In this form of attack, the control of communication is in the attacker's hand, but the communicating nodes are unaware of this. An attacker can listen to all the communications between them and modify, delete, or insert a new message in the communication.

- Sybil attack

Sybil assault is a type of impression, which includes more than one Sybil node's identities. Different forms of identities are pretended as different vehicle nodes by the Sybil attacker. It falsifies present incorrect records to the other vehicles by exchanging messages with other physical network nodes and false information on road traffic. A Sybil node can pretend itself at various locations in the same period so that this situation can be destroyed for the entire vehicular network and network routing.

Sybil assaults may invite severe security risks to the vehicular ad-hoc network. First of all, the attacker can create an illusion to misguide the other vehicles about the traffic jams, so they choose another clear path for their destination. In this way, the attacker can lead the vehicle/s on the attacker's desired path or road for some illegal purpose. Secondly, a Sybil attack can disturb data consistency in the network by inserting false information indirectly/directly into the vehicular network. It may disturb the voting process for making some traffic rules or creating informative traffic reports. The Sybil attacker may also launch some other DOS assaults like message suppression and channel jamming. Extensive research is an issue to defend and detect the Sybil attacks in a network [8]. The simplest elucidation to defend the system against Sybil attacks is Vehicle Public Key Infrastructure (VPKI). The network can be secure from the Sybil attack as there will be a unique certificate for each automobile node. However, despite this, vehicular ad-hoc networks are still vulnerable to a security breach if the attacker uses some authentic certificate issued to a valid vehicle [9]. The scheme of multifactor authentication can solve this problem by providing an advanced and modified security certificate. Various physical sets of attributes recorded by the certification authority are included in this certificate and the public key information. These attributes are transmitter coverage, fingerprint radio frequency, and many other attributes. This way makes the steal of keys and certificates of the valid vehicle nodes much hard to achieve.

2. Literature Review

Sybil attack is the most elusive and dangerous attack in inter-vehicular communication. Sybil attacks detection is a privacy risk for VANETs nodes. In a Sybil attack, a malicious node misuses the pseudonyms and pretends to be more noses in the network at the same time. ETSI and IEEE standardized many security mechanisms for VanETs over recent years. Despite these protection services, VANERTs are still vulnerable to Sybil attacked [10].

If a Sybil node uses more than one pseudonym, each pseudonym is considered a separate node by other vehicles. VANETs are highly vulnerable to security attacks than the conventional ad-hoc network due to their independent infrastructure and dynamic nature. Sybil detection methods can be divided into four categories. Transportation authorities and vehicle manufacturers invest money for safety requirements on the roads. With the vehicular network's help, the author can improve traffic efficiency, road safety, and infotainments, the author writes. Back to the pageYou came from: The author is happy to help you understand this article and share our understanding of Sybil and its techniques [11].

Vehicular Networks directly affect human life due to their crucial public safety role. ETSI and IEEE standardized various security services that are based on PKI, cryptography, and pseudonyms. The author [12] proposed a Vehicle driving pattern-based Sybil attacks detection method for urban areas. Vehicles communicate beaconing messages and based on these messages, Driving Pattern Matrices (DPM) are constructed. Unusual patterns are detected by evaluating the vehicle's driving patterns with the help of minimum distance classifiers. Sybil attacks can damage both the network and application layers.

Old schemes to detect Sybil attacks in vehicular ad hoc networks (VANETs) have a high risk of privacy loss. A malicious vehicle can send multiple messages by using many different pseudonyms. It is difficult for RSBs and vehicles in the network to identify that the messages are broadcast by either a single vehicle or several vehicles because they do not know the pseudonym's pool. One possible solution is the expiry time for pseudonyms, and a new pseudonym is taken from a nearby RSB when the previous one is expired. Another approach identifies the current position of the vehicle by using directional antennas. However, localization error may be occurred in the dense network and creates a lot of false positives results. The hackers may misuse the directional antennas and deceive the network nodes regarding their location [13].

The author [14] proposed a better scheme to detect the Sybil attacks with low privacy risk. No additional hardware is needed in this scheme. RSBs do not need to compromise any privacy risk. The author introduced an approach to detect a Sybil attack by using infrastructure and node localization. Privacy-preserving schemes can increase the risk of Sybil attacks. In the way of detecting this attack, the author has to compromise some privacy.

The author [15] proposes the L-P2DSA scheme for the privacy preserved detection of Sybil attacks. It is a modified form of C-P2DAP and reduced the load on DMV. RSUs coordinate with each other's to identify a malicious node location in VANET. In L-P2DSA, vehicle nodes do not disclose their identity, so privacy is preserved. Vehicles should have sufficient data to make immediate decisions for road safety and efficiency. VANETs have many challenges like traffic density, vehicle mobility, privacy and security issues, and non-repudiation, ensuring issues. A Sybil attack is a malicious attack in which a node claims itself as several nodes and deceives vehicles and agencies.

The author assigned vehicles a pool of pseudonyms hashed to some standard value for preventing Sybil attack. This scheme has two levels. RSUs overhear the communication between vehicles and identify their position with the help of other adjacent RSUs. If RSUs find the distinguishability degree more than a threshold, it reports this vehicle to DVM as a suspicious vehicle. DVM separates the actual attack from a false positive by fine-grain hash computing [16].

The author proposed a distributed Sybil detection method based on neighbourhood information. In this detection approach, a node is

considered as a malicious node (Sybil Node) if it is not acknowledged by one of two nodes within an intersected area. This approach works better in a scenario with high numbers of neighbour nodes. Researchers categorized detection techniques of Sybil attacks into three groups, i.e., position-based, resource-based, and certificate-based techniques. In a detection technique, the researcher uses the strength of the received signal for verifying the position of a node. The claimer node broadcasts the beacon messages to other nodes, and the verifier is a node that received these messages [17].

The author [18] uses a detection method for a Sybil attack based on the Support Vector Machine (SVM) is proposed. Many protocols and security services for vehicular networks have been proposed in recent years based on Pseudonyms, PKI, and Cryptography. The author proposed a classifier; based on three support vector machines kernel function for detecting the malicious node with the help of variance evaluation in Vehicle's Driving Pattern Matrix (DPM). The authors evaluate their proposed scheme's effectiveness by MATLAB and SUMO simulator, which shows that this scheme has a better detection rate in a dynamic environment.

The author [19] contributes to Sybil detection in two ways. Firstly, by designing DPM, a data format to describe the driving pattern of VCANETs. Secondly, by extending the detection method of Sybil attack using machine learning techniques into more dynamic networks. The author proposed a novel Received Signal Strength Indicator (RSSI) voiceprint-based detection technique for the Sybil attacks. It is a lightweight method, widely applicable, and fully distributed method. Most RSSI detection methods compute relative distance or absolute position according to average values of RSSI or RSSI distribution based on statistical testing. In voiceprint, the RSSI time series is used as vehicular speech, and similarity amongst RSSI time series is compared by vehicular speech.

VANETs supports a lot in cooperative and intersection collision warnings, Electronic Emergency Brake Lights, Enhancing Navigation, and Route Guides. VANET inherits many security vulnerabilities, which is a significant hurdle to apply as practice. Many Sybil nodes (virtual nodes) generate fake identities through malicious nodes in a Sybil attack and violate those applications' fundamental assumptions. The method of trusted certification generally relies on detection algorithms in a centralized way that is unsuitable for vehicular networks due to the dynamic topology of VANets. The method of position verification by physical measurement has high availability, low cost, and decentralized nature, so it is better to detect Sybil attacks in the early state of VANets [20].

Authors observed that attacker nodes insert fake statistics and then release numerous types of attacks. They also proposed techniques to evade the vehicle's misbehaviours in a vehicular network. Each vehicle in this technique takes a decision independently about the validity of the received information, i.e., either bogus or accurate [21].

The author in [22] "In signature-based Rule Matching approach in network Intrusion Detection machine" confirmed that signature is the pattern that is inside the facts packet-typically, for detecting an intruder actively; Intrusion Detection System (IDS) relay on the signatures. The most time crucial function in the intrusion detection system is pattern matching. In this system, the sample of recognized attacks is saved in the database of IDS.

The project is designed to develop a robot for remote control using an android application attached to the wireless camera. Camera surveillance can help the soldier team to develop strategies in the long run. This type of robot can be useful for spying in warfare fields. This robot can detect mines, detect objects, locate GPS and navigate and use a gun to fire the enemy against the enemy. The security system then follows these commands and answers the user. The camera and the motion detector are connected via ZigBee and Bluetooth protocols to the remote surveillance system [23].

The wireless sensor network is an emerging technology that offers many communication, energy and cost advantages. When a vehicle enters a passage after sensing its entry into a region, street lights turn on. The energy consumption of street light is low at daylight, moderate when average road traffic and high when high traffic is on the roads [24].

IoT plays a remarkable role in human life, with IoT services reducing workload and reducing life pressure. Human life is an important factor that human beings themselves always ignore. These new IoT concepts can be used with RFID technologies in smart homes. The RFID reader reads the information from home devices and sends it to an Android device, allowing users to play more intelligently in homes and reducing human efforts more accurately. This technology offers us advantages in cost to save human life, energy and complexity [25].

The Internet of Things (IoT) is a "things" network that is connected to the Internet for the collection and exchange of data. Sensors, actuators, smartphones, wearables, computers, or any object can be these "things." As part of IoT, Wireless Sensor Network (WSN) transmits the collected data after sensing any event. IoT's scalability and heterogeneity offer limited protection and are susceptible to various attacks, including WSN-inherited attacks. Researchers have suggested different mitigation mechanisms for secure IoT networks and routing [26].

Vehicle ad-hoc network (VANET) presents drivers with brilliant applications for transport, road safety, comfort and luxury. For the efficient implementation of VANet, it is extremely important to find a suitable and efficient routing protocol. The AOMDV protocol enhances network overall performance with maximum throughput and a minimum end-to-end delay, the study says. The research presents a practical assessment of VANET topology features in terms of time in high traffic situations. The simulation results show that AOMVV performs better in high traffic density areas than DSDV and AODV protocols [27].

The lack of resources and services coincides with urban development. To compensate for this shortage, the modern use of technology has become necessary. The Internet of Things is one of the most reliable solutions technologies. The problem of cyber-attack securing this data is increasing because it contains important information on people. For several reasons, designers are unable to encrypt the entire IoT device approach [28].

3. Research Methodology

The approach for this study consists of several steps to perform the research in a structured way. Firstly, existing papers will be gathered and sought about Sybil attacks, their detection and prevention schemes, privacy and security challenges, and current research states in the field of Vehicular Ad hoc Networks security. For evaluating the performance of different approaches, an active research methodology is needed in VANETs to quickly check the possible drawbacks of this technology and ensure the availability of proposed approaches. Experimental implementation for the introduction of new technology in VANETSs is expensive. There are two essential steps before the market introduction of new technology in VANETs. The first is the evaluation and analysis by the use of simulation, and the second is the verification by

operational testing in the field. Traffic simulators and network simulators are used for simulation in VANETs. Dataset is downloaded and divided into small chunks of one hundred thousand records each. Linux and JSON library is installed. Java source file is compiled to extract the dataset in Comma-separated values (CSV) format. R Studio is installed, and a method is written in the R language to analyze the dataset.

3.1. Methods Assessment

Researchers working on Sybil attacks divided the detection of Sybil attacks into three categories of techniques as a defence system against Sybil. A suitable technique selection for the implementation depends on the characteristics of strategies in each approach and the policies and expected cost in this area in a specific geographic area. Therefore, firmly selection of a single technique or method is not feasible. A terrific approach to detect the Sybil attack in the vehicular network in real scenarios should have the following necessities:

- A vital thing in the detection of Sybil nodes is the Time factor. The time necessary for the disposing and discovery of Sybil nodes must be minimum. It is necessary due to the high mobility of automobiles that response time should be short. (Computation complexity plays an important role and works as an essential factor for the above purpose)
- Having the detection capacity, a high proportion of malicious nodes reduce the level of destruction in Vehicular Networks.
- The risks of Road Side Units against compromising should be considered
- Preserving the privacy of the vehicle's driver is an outstanding service and should be maintained.
- The exchange of messages does not increase within the network.
- Hardware overheads should be minimal while implementing the defence mechanism.
- Scalability should be considered while using both overcrowded and less dense roads. Defence mode is one of the efficient features of scalability in assault detection procedures. Within primary mode for roads having heavy traffic, bottleneck advent is to be expected, and due to the reason, scalability is restrained. However, the network's scalability is more in the distributed model to cover more vehicle nodes.
- Some limitations in communication and the velocity of the automobile's nodes must not be considered. In some approaches, the detection rate depends upon the mobility of vehicles.

Designing an excellent technique with thinking about all of those requirements is a robust plan. However, what is essential in this region is to keep human beings' lives, eliminate any coincidence and damage to cars and people, and prevent losing time for human beings due to busy visitors. Therefore, an excellent method makes a tradeoff between all of those purposes by considering priorities. A few of the capabilities, advantages, and disadvantages of each approach had been described in this paper. However, for a better view and contrast, we compare these methods in short in table A1. This desk describes each applicable and sufficient mechanism; this is defined for assault detection in VANET. We have no longer considered a useful resource in checking out mechanisms on this desk because it is not always enough to implement Sybil attack detection with high accuracy in VANETs. Different types of attackers and their attacks in VANETs are shown in Table **4**.

Table 4 Attack and Attacker types in Vehicular Ad-Hoc Networks

Attack Types	***Attacker Types***					
	Active	***Passive***	***Malicious***	***Rational***	***Insider***	***Outsider***
Service Denial	□	□	□	□	□	□
Fake Information	□	□	□	□	□	□
Masquerade	□	□	□	□	□	□
Identification Disclosure	□	□	□	□	□	□
Position Cheating	□	□	□	□	□	□

Many feature verification approaches are easy, computationally less complicated, processed and scalable than authentication strategies. There are beautiful implementation skills. However, they do not use RSUs as reliable units that trigger privacy breaches or reveal areas and recognize automotive data. Also, the distributed loading by automobiles in these strategies results in the generation of overhead messages. Both authentication solutions include main delivery and revocation infrastructure. This VANET architecture is important for many uses, including comfortable communication changes and organizational communications, apart from attack detection. The greater importance of implementing the infrastructure was no longer taken into account in our comparisons. In these techniques, privacy and consistency protection is high, while their execution is difficult and usually less scalable than function assurance strategies.

3.2. Evaluation of Defense Mechanisms

Defence Techniques in Mobile Ad-hoc Networks and particularly in Vehicular Ad-hoc Networks can be classified as under:

- Authentication and encryption techniques
- Location Verification Techniques
- Techniques based on resources testing

3.3. A Defence Based on The Techniques of Resource Testing

In this defence against the Sybil attack, automobile resources like memory resources, radio resources, identification resources, and computational resources are tested. In the Sybil attack, resources like IP, memory, and computation resources. Are shared amongst the malicious node and its generated Sybil nodes.

We can find a vehicle node using shared resources to send and receive message data by vehicles monitoring and tracking the communication signals. In this way, we can detect a malicious node used for Sybil attack in a vehicular network.

The testing method via radio resources discussed and the postulations described in its limit using this method up to only a few wireless communication networks. The first assumption is that specified channels for radio devices' operations; the second is having just a single radio device for a wireless node. The third and last assumption is not listening or transmitting on two or more channels simultaneously.

Every node in the testing method of radio resources sends a message to all other nearby nodes for testing the possibility of a Sybil node. Different channels are used to send a message to the testing nodes. Because of the reason mentioned above in the 3rd assumption, one channel is randomly selected to listen to the responsive message. Response message sends on the preselected

channel only if the node is legitimated. If the neighbouring node is malicious, according to the 3rd assumption, it is unable to transmit the response message for its different Sybil nodes at the same time at multiple channels. In this way, a malicious Sybil node may be identified if a response message is not received on the testing node's listening channel. Different radio devices can be controlled and used simultaneously by the Sybil attacker; this is a violation of the 2nd assumption. Additionally, the Sybil attacker's multiple communication channels may be owned, which violates the 3rd assumption. Due to this fact, this technique is not suitable for the vehicular network for the detection of a Sybil attack.

The concept behind testing by storage and computational resources is that a physical node has limited storage and computational assets inside a network.

This method was proposed the first time as a fighting technique for junk emails. They were avowed that this method proved helpful for the defence of the system from DOS attacks.

In the technique of testing by computational resources, the network nodes which fail in puzzle solution within a specified time are marked as fake entities. As compared to the legitimated nodes, the Sybil attackers make more effort to solve the puzzles for their malicious nodes at the consumption of extra time and computational resources. This method can stumble on the attacker in a network with the nodes having equal computational resources (homogeneous network). The author [29] presented Computational Resources Test (CRT) is introduced as an instance of a resource testing method of detection. CRT allows the crypto puzzles to confirm that the participating network nodes own a predictable computational resource number. In CRT, participating network nodes crack the cryptographic puzzle of the robust moderate level that can solve only by the method of Brute Force within a prescribed period. The cryptographic puzzle with expensive and not intractable computations can detect the computational resources of the network nodes.

The authors discussed a few puzzles and the comparison between them. A network entity can solve limited numbers of the puzzle within a specific period because every network entity has confined computational resources. It limits the Sybil entities created by some Sybil attackers to a few ones inside a network. As described by the author, Computational Resources Testing methods are extensive in scalability compared to the method of testing by radio resources to implement on a large-scale vehicular network. However, the testing method via radio resources has a probability level of 1 in detecting and eradicating the malicious nodes, which cannot be provided by the testing method of computational resources.

The method of storage and computational resource testing can be effective inhomogeneous mobile ad-hoc networks but not suitable for VANETs due to the reasons:

- It may decrease the number of Sybil nodes but unable to eliminate them from the network
- As VANET is not a homogeneous network, the Sybil attacker can use a more storage and computational power device than the legitimate node.

Different Sybil attack detection techniques identify attacks in the network. The statistical analysis approach is selected to identify a Sybil attack due to large dataset availability, but the Data mining approach is also helpful in this regard. The performance comparison of both methods is shown in Table 5.

Sr. No	***Sybil Detection Method***	***Description***	***Merits***	***Demerits***
1	*Data Mining*	*It is the way of discovering perceptions and information for the dataset, identifying the Sybil attack.*	*It works with the variables which did not correlate.*	*The large datasets overhead*
2	*Statistical Analysis*	*Data can be clarified, summarized, defined, and conclusions can be drawn.*	*With the help of prediction, future problems in the network can be anticipated*	*Extensive sampling errors may occur; validity construction may not be right. Even if the correlation is high, sometimes it does not guarantee that an attack occurs.*

Table 5 Performance evaluation of Sybil detection methods

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage**.** For example, write "15 Gb/cm^2 (100 Gb/in^2)." An exception is when English units are used as identifiers in trade, such as "3½-in disk drive." Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength *H* is A/m. However, if you wish to use units of T, either refer to magnetic flux density *B* or magnetic field strength symbolized as $\mu_0 H$. Use the center dot to separate compound units, e.g., "A·m^2."

4. Results and Discussion

A dataset is selected, which contains 1048576 records. The selected dataset is partitioned into small datasets because the original dataset is large, and it is a big data problem. The partitioned datasets are 11, and each is simulated to detect a Sybil attack. Residuals present the dependent variables. These are calculated by subtracting the fitted (predicted) values from the actual values of the residuals. A "decent" residual versus fitted (predicted) plot is moderately shapeless defined without clear examples in the information, no conspicuous outliers, and large symmetrically circulated the 0 lines without especially significant residuals, as shown in Figure 4. The red line is indicating to smooth out the two separate trends.

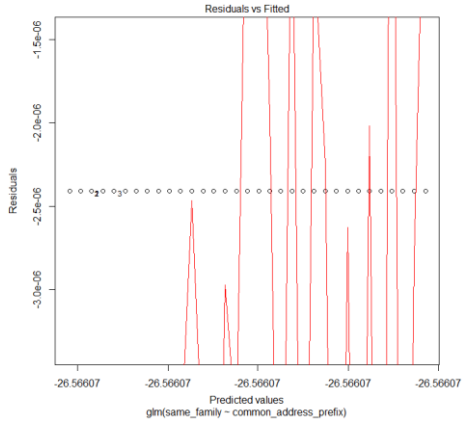

Figure 4 Relationship between actual and fitted values

The quantile-quantile (Q-Q) plot is a likelihood plot for comparing likelihood distribution by plotting their quantiles against each other. It is used to determine if dependent variables are normally distributed. The set of intervals for the quantiles is taken from the selected dataset. The unconventionality from a straight line in the normal quantile-quantile plot shows that the errors do not follow a normal distribution. The Q-Q plot provides an assessment of how properties, i.e., same-family, common-address-prefix, same_country, same_region, same_autonomous_system, etc., are similar or different in the two distribution which is used to detect the Sybil attack in the network as shown in Figure 5.

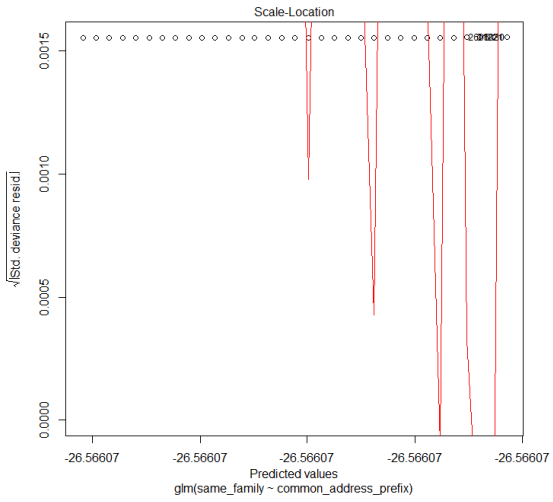

Figure 5 Location-based parametric detections

This plot is identifying possible outliers. Cook's distance attempts to detect points that have more impact than other points. These are detached points from other points in the dataset concerning the dependent variable or independent variables. Each observation is characterized as a line whose height tells the value of Cook's distance for that observation, as shown in Figure 6. The suspicious nodes are detected in the simulation, and Sybil nodes are filtered and blocked. This investigation estimates the impact of affected perceptions from the original dataset.

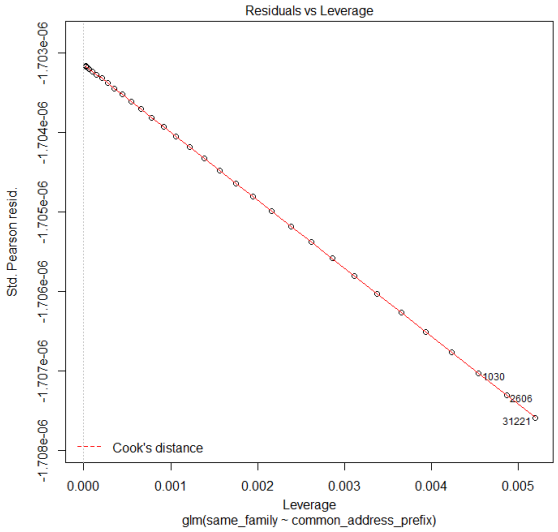

Figure 6 Detecting outliers' points from the dataset network

5. Conclusion

This research categorized the studies about Sybil attacks in three broad areas and then explained the features of the technique used in each area. Through light on each technique's inefficiencies and efficiencies, researchers use Sybil attacks' detection and mitigation. The mechanism of resource testing is not enough to secure the vehicular ad-hoc network from the Sybil attack due to its features. One thing that should be considered while selecting the best approach for detecting Sybil attacks is that there should not be extra overheads only for the detection of Sybil attacks in the VANETs. For both the verification objectives and the detection of positions, the localization technique is appropriate in the mentioned circumstances. So, the accuracy enhancement and improvement in the mentioned techniques regularly have a superb effect on the applications that are location dependents. Generally, techniques based on authentication are essential for legitimating the identities of the vehicle's nodes. The research shows how to detect the nodes in the network with similar identification within the same network, which leads to a Sybil attack. These attacks are hazardous for the network due to the overload of the same node. The results of this research show that one node is attempting the network with different identities. To preserve the nodes' privacy in the VANET, we must have preliminary authentication infrastructures to keep away the network from forging and altering traffic safety messages that greatly impact the vehicles' roadside safety. Therefore, detecting the Sybil attack in VANET can be used and the different safety packages in vehicular networks.

References

[1] M. Soni and A. Jain, "Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks," in *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, 2018, pp. 539-543: IEEE.

[2] M. Maleknasab Ardakani, M. A. Tabarzad, and M. A. Shayegan, "Detecting sybil attacks in vehicular ad hoc networks using fuzzy logic and arithmetic optimization algorithm," *The Journal of Supercomputing*, pp. 1-33, 2022.

[3] K. Hussain, S. J. Hussain, N. Jhanjhi, and M. Humayun, "SYN flood attack detection based on bayes estimator (SFADBE) for MANET," in

2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1-4: IEEE.

[4] C. Iwendi, M. Uddin, J. A. Ansere, P. Nkurunziza, J. Anajemba, and A. K. Bashir, "On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique," *IEEE Access*, vol. 6, pp. 47258-47267, 2018.

[5] S. S. Sefati and S. G. Tabrizi, "Detecting sybil attack in vehicular ad-hoc networks (vanets) by using fitness function, signal strength index and throughput," *Wireless Personal Communications*, vol. 123, no. 3, pp. 2699-2719, 2022.

[6] N. K. Chaubey and D. Yadav, "Detection of Sybil attack in vehicular ad hoc networks by analyzing network performance," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 12, no. 2, 2022.

[7] Z. Helmi, R. Adriman, T. Y. Arif, H. Walidainy, and M. Fitria, "Sybil Attack Prediction on Vehicle Network Using Deep Learning," *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, vol. 6, no. 3, pp. 499-504, 2022.

[8] M. S. Naveed and M. H. Islam, "Detection of Sybil Attacks in Vehicular Ad hoc Networks Based on Road Side Unit Support," *Int. J. Sci. Eng. Res*, vol. 6, no. 2, pp. 817-827, 2015.

[9] S. A. Asra, "Security issues of Vehicular Ad Hoc Networks (VANET): A Systematic Review," *TIERS Information Technology Journal*, vol. 3, no. 1, pp. 17-27, 2022.

[10] D. Singh and M. Kaur, "Mitigation of Sybil Attack Using Location Aware Nodes in VANET," *International Journal of Science and Research (IJSR)*, vol. 4, no. 11, 2015.

[11] H. Kaur and P. Bansal, "Efficient Detection & Prevention of Sybil Attack in VANET," *International Journal of Innovative Science, Engineering & Technology*, vol. 2, no. 9, 2015.

[12] M. Khalil and M. A. Azer, "Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks," in *Wireless Days (WD), 2018*, 2018, pp. 184-186: IEEE.

[13] S. S. Vinayagam and V. Parthasarathy, "A secure restricted identity-based proxy re-encryption based routing scheme for sybil attack detection in peer-to-peer networks," *Journal of Computational and Theoretical Nanoscience*, vol. 15, no. 1, pp. 210-221, 2018.

[14] M. Jain and R. Saxena, "VANET: Security Attacks, Solution and Simulation," in *Proceedings of the Second International Conference on Computational Intelligence and Informatics*, 2018, pp. 457-466: Springer.

[15] A. Balaram and S. Pushpa, "Sybil attack resistant location privacy in VANET," *International Journal of Information and Communication Technology*, vol. 13, no. 4, pp. 389-406, 2018.

[16] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A Survey of Anomaly Detection for Connected Vehicle Cybersecurity and Safety," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018, pp. 421-426: IEEE.

[17] I. Bhardwaj and S. Khara, "An Analytic Study of Security Solutions for VANET," *International Journal of Computer Applications*, vol. 132, no. 10, pp. 1-7, 2015.

[18] M. B. Shareh, H. Navidi, H. H. S. Javadi, and M. HosseinZadeh, "Preventing Sybil attacks in P2P file sharing networks based on the evolutionary game model," *Information Sciences*, vol. 470, pp. 94-108, 2019.

[19] A. N. Upadhyaya and J. Shah, "Attacks on VANET Security," *International Journal of Computer Engineering & Technology (IJCET)*, pp. 8-19.

[20] M. Alimohammadi and A. A. Pouyan, "Sybil attack detection using a low cost short group signature in VANET," in *Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on*, 2015, pp. 23-28: IEEE.

[21] P. Rawat and S. Sharma, "Review on sybil attack in vehicular ad hoc network," *International Journal of Science, Engineering and Technology Research (IJSETR) Volume*, vol. 5.

[22] S. Rakhi and K. Shobha, "Performance Analysis of an Efficient Data-Centric Misbehavior Detection Technique for Vehicular Networks," in *International Conference on Computer Networks and Communication Technologies*, 2019, pp. 321-331: Springer.

[23] L. B. Imran, M. Farhan, R. M. A. Latif, and A. Rafiq, "Design of an IoT based warfare car robot using sensor network connectivity," in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, 2018, pp. 1-8.

[24] L. B. Imran, R. M. A. Latif, M. Farhan, and T. Tariq, "Real-time simulation of smart lighting system in smart city," *International Journal of Space-Based and Situated Computing*, vol. 9, no. 2, pp. 90-98, 2019.

[25] R. M. A. Latif, M. Farhan, L. B. Imran, K. Manzoor, T. Tariq, and H. Raza, "Real-Time Simulation of IoT Based Smart Home System and Services Using RFID," *KIET Journal of Computing and Information Sciences*, vol. 2, no. 2, pp. 12-12, 2019.

[26] S. M. Muzammal, R. K. Murugesan, and N. Jhanjhi, "A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-based Approaches," *IEEE Internet of Things Journal*, 2020.

[27] R. M. Waseem, F. Z. Khan, M. Ahmad, A. Naseem, N. Jhanjhi, and U. Ghosh, "Performance Evaluation of AOMDV on Realistic and Efficient VANet Simulations," *Wireless Personal Communications*, pp. 1-20, 2021.

[28] M. Saleh, N. Jhanjhi, A. Abdullah, and R. Saher, "Proposing Encryption Selection Model for IoT Devices Based on IoT Device Design," in *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, 2021, pp. 210-219: IEEE.

[29] R. Mishra, A. Singh, and R. Kumar, "VANET security: Issues, challenges and solutions," in *Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on*, 2016, pp. 1050-1055: IEEE.