Journal of Al-Azhar University Engineering Sector

Vol.15, No. 56, July, 2020, 810-827

VANET SECURITY: DEFENSE AND DETECTION, A REVIEW

Manal S. Gamal*[1], Abdurrahman A. Nasr,[2] and Sayed A. Nouh[2]
[1]Department of Electrical Engineering, Faculty of Engineering, 6th of October University, Giza, Egypt.
[2]Department of Computers and Systems Engineering, Faculty of Engineering, Al-Azhar University, Cairo, Egypt
*Corresponding Author E-mail: Manal.shehab@gmail.com

ABSTRACT
Vehicular Ad Hoc Networks (VANETs) are networks that deal with transferring data between moving vehicles in order to avoid accidents and to provide journey comfort and traffic safety. Like all other networks it is subjects to vulnerable attacks, hence, security is a hot topic to consider. This article provides a review on the researches and publications focusing on how to secure the communication between vehicles while transferring the data. Different attacks could take place within the communication scenario; the most harmful of them is Sybil attack. Therefore, in this paper, we shed lights on the researches dealing with the different types of attacks with a focus on Sybil attacks. Sybil detection and defense techniques and methodologies are reviewed in more details.

KEYWORDS: Vanet, Vanet Security, Sybil Attack, Sybil Attack Detection, and Sybil Attack Defense

تأمين الشبكات اللاسلكية للمركبات، الحماية والاكتشاف، مراجعة

منال شهاب جمال*[١] وعبد الرحمن على نصر[٢] وسيد عبد الهادي نوح[٢]
[١] قسم الهندسة الكهربية، كلية الهندسة، جامعة ٦ أكتوبر، الجيزة، مصر
[٢] قسم الهندسة النظم والحاسبات، كلية الهندسة، جامعة الأزهر، القاهرة، مصر
*البريد الإليكترونية للباحث الرئيسي: E-mail: Manal.shehab@gmail.com

الملخص
الشبكات اللاسلكية للمركبات (**فانيت**) هي الشبكات التي تعمل على نقل البيانات بين المركبات المتحركة من أجل تجنب الحوادث وتوفير الراحة أثناء الرحلة والسلامة المرورية. مثل جميع الشبكات الأخرى، فهي عرضة للتعرض للهجوم، وبالتالي يجب النظر بأهمية لكيفية حمايتها. هذا المقال يقدم توضيح للأبحاث والمنشورات التي تركز على كيفية تأمين الاتصال بين المركبات أثناء نقل البيانات. يمكن أن تحدث هجمات مختلفة أثناء سيناريو الاتصال، وأكثرها ضررًا هو هجمات **سيبل**. لذلك، في هذه المقالة، سلطنا الضوء على الأبحاث التي توضح الأنواع المختلفة من الهجمات مع التركيز على هجمات **سيبل**. تقنيات وطرق الكشف والحماية ضد هجمات **سيبل** يتم توضيحها بمزيد من التفاصيل.

الكلمات المفتاحية: الشبكات اللاسلكية للمركبات، تأمين الشبكات اللاسلكية للمركبات، هجمات سيبل، اكتشاف هجمات سيبل، والدفاع ضد هجمات سيبل

INTRODUCTION

Vehicular ad hoc Network (VANET) has been recently taken a growing interest as a promising technology in a ubiquitous environment. VANETs is a specific type of Mobile ad hoc Network (MANETs) where the mobile nodes are replaced with vehicles equipped with Onboard Unit (OBU) communications devices. VANETs architecture is designed for Vehicle-to-Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication, containing two communication devices called Roadside Unit (RSU) and Onboard Unit (OBU). Each vehicle is a node equipped with communication device which allow sending and receiving messages through wireless communication, these installed devices are used to gather environmental and road information.

VANETs are recently used in many different useful applications (Zaidi and Rajarajan 2015)(Faezipour et al. 2012)(Haas, Hu, and Laberteaux 2009)(Sarika et al. 2016)(V. Kumar, Mishra, and Chand 2013). Some of such applications are:

1. **Convenience applications**: Examples are: navigation, personal routing, congestion advice, toll collection, parking availability information. Another critical set of applications that are helpful in case of disastrous situations such as power failure and network breakdown, where the vehicular network can offer an emergency substituting communication mechanism via utilizing the onboard batteries of vehicles. Similarly, road and weather conditions can be obtained via sharing the data from onboard sensors of vehicles.
2. **Commercial applications**: Examples are: vehicle diagnostics exchanges for avoiding possible car problems, location-based services such as advertisements and entertainment, e.g., data/video relay, social networking updates, etc.
3. **Safety applications**: Examples are: crash notification, hazards on slippery roads, traffic violation warnings, curve speed warnings, emergency electronics brake light, pre-crash sensing, and cooperative forward collision warnings. This could also include generating warning messages to inform drivers of approaching emergency vehicles.

Studying VANETs security show that both packet security and driver's liability are key to detection and defense of attacks. VANET packets contain critical information; hence, it is necessary to make sure that these packets are not maliciously manipulated by an attacker. On the other hand, driver's' liabilities should be established so that they be held accountable for the correctness and the timeliness of their messages within the traffic environment.

There are several reasons to attack VANETs, such as modifying a message content, e.g., some kind of rotation in the contents also some identity related issues. There are different types of attackers such as selfish drivers that are authorized but because of their own needs they give false information also there are malicious drivers that are unauthorized, and they harm the system by different means and for different reasons. There are several attacks that may affect VANETs such as denial of service, spamming, Sybil, malware, black hole and etc..(A. Singh and Kad 2016). In fact, Sybil attacks are considered the root cause of many security problems; therefore, this article pays enough attention to Sybil attacks with a focus on the defense and detection algorithms.

In many VANET based applications, the cooperation of vehicles is required to draw a unified picture on a traffic situation, e.g., cooperative collision warning, local hazard notification, enhanced route guidance, and navigation. In such applications, the identical views sensed by multiple distinct vehicles for a certain traffic situation provide a trustable correctness and a reliable proof about the traffic situation to other vehicles. However, if there are many faked nodes in the network that send malicious messages, the drawn traffic situation will, of course, be inaccurate if not incorrect and totally misleading. In a Sybil attack, a malicious sender creates multiple faked identities, called Sybil nodes, to impersonate as normal nodes, hence, invalidating the traffic situation picture. For this reason, Sybil attack is particularly harmful because it violates the fundamental assumptions of VANETs communication protocols.

As most of the other review articles shown in table 1 and table 2 concentrate on the details of VANETs and/or on a specific type of attacks, this article focuses on:

- Reviewing some of the important aspects about VANETs and VANETs security,
- Special characteristics of Sybil attacks, and
- Sybil attacks detection and defense algorithms.

In this article, Section 2 reviews some related work and few survey articles. Section 3 discusses the characteristics and constituent components of VANETs and VANET's security aspects. Section 4 discusses VANETs Vulnerability showing different possible types of attacks that affects VANETs highlighting the threats they cause, while Section 5 presents the Sybil attack in more details focusing on the defense and detection algorithms. Finally, Section 6 provides a summery.

1. RELATED WORK

There are different literatures that discussed the VANETs and the VANETs security showing the attacks that affect VANETs. Table 1 summarizes some of the surveys done on VANETs and VANET's security, while Table 2 focuses on articles reviewing Sybil detection and defense algorithms.

Table 1. Surveys Reviewing VANETs and VANETs Security.

Paper	Contribution
Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions (Karagiannis et al. 2011)	This survey and tutorial paper introduced the basic characteristics of vehicular networks, providing an overview of some applications and their associated requirements, along with challenges and some proposed solutions.
A Survey on Security in VANET (Salagar and Tangade 2015)	This paper presented the communication architecture of VANETs and outlined the privacy and security challenges that need to be overcome to make such networks safely usable in practice.
Survey on Security Issues in Vehicular ad hoc Networks (Mokhtar and Azab 2015)	This survey discussed the security features, challenges, and attacks of VANETs and classified the security attacks according to their network layers.
A Comprehensive Survey on VANET Security Services in Traffic Management System (Sheikh and Liang 2019)	This paper summarizes the state of VANETs by presenting the VANETs architecture, challenges and security, showing some security schemes and methods to provide secure communication focusing on the authentication schemes and showing how they protect vehicular networks from malicious nodes and fake messages.
VANET Routing Protocols: Pros and Cons (Varga et al. 2011)	This paper discussed and classified the different routing protocols in VANETs by studying the performance, advantages, and disadvantages of each.
Vehicular ad hoc networks (VANETS): Status, Results, and Challenges (Zeadally et al. 2012)	It reviewed some of the main areas that researchers have focused on, among which are security, routing, QoS, challenges, and broadcasting techniques. They highlighted the most salient results achieved to date.
A Survey on Authentication Schemes of VANETs (Mary Anita and Jenefa 2016)	In this paper, they summarized various authentication schemes which have been proposed for VANETs to establish secure communication. These schemes are discussed elaborately and then a comparison based on their security features and capabilities are carried out.

Table 2. Articles Surveying Sybil Attack Detection and Defense.

Paper	Contribution
Sybil Attack in VANETs Detection and Prevention (GROVER, GAUR, and LAXMI 2010)	It presented the Sybil attack as one entity controlling many different identities showing Sybil attack's challenges and applications. The main idea is to support VANETs with practical security solutions.
A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV (Sakiz and Sen 2017)	This paper aims to survey some possible attacks and their corresponding detection mechanisms that are proposed in the literature showing the advantages and disadvantages of each.
A Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs) (Al-Kahtani 2012)	This paper presented different security attributes and types of malicious nodes in VANETs showing different security attacks and their defending mechanisms with examples, showing the classification of the security and privacy approaches of VANETs.
A Survey of Techniques to Defend Against Sybil Attacks in Social Networks (Rangaswamy and Hegde 2014)	In this article, they discussed different kinds of Sybil attacks that can be applied on various applications; and also classified and summarized the different types of Sybil defense methods showing the advantages and disadvantages of each.

2. VANETS AND VANET'S SECURITY REQUIREMENTS

Vehicular Ad-Hoc Network (VANET) is a technology that uses moving vehicles as nodes in a network to create a mobile network. It enables the communication between the nodes to avoid accidents and provide journey comfort and traffic safety. In this section, we review the different components of VANETs, types of communication configurations, and the different routing protocols, which are the VANET elements affecting attacks analysis. Later, the security requirement is presented with an analysis of how these different elements relate to those requirements.

2.1. Components of VANETs

Three main components are involved in the VANET communication architecture (Zaidi and Rajarajan 2015)(Zeadally et al. 2012), as depicted by Figure 1. These are:

a. **Vehicles** that act as mobile nodes havi ng their own communication wireless network components.
b. **On-board Unit (OBU)** is installed in the vehicle and consists of:
   - Event Data Recorder (EDR) that records the transmitted and received messages, this recorded information can be retrieved and used later, e.g., as an accident evidence.
   - Global Positioning System receiver (GPS) that provides information about location, speed, directions of movement, and the acceleration of a node at a specific time.
   - Computing device that is used in taking actions according to the received messages.
   - Radar that is used to detect near-by obstacles.
c. **Road-side Unit (RSU)** which is a stationary device placed on rode sides, it may be installed at road intersection or at traffic lights. It helps in providing information for vehicles when needed.

2.2. Communication Configurations

Communication in VANET takes place by exchanging messages having different natures and purposes These communications can be classified into three main categories (S. Kumar and Verma 2015)(Zeadally et al. 2012):

a. **Pure cellular** communication, under which vehicles cannot communicate directly, but rather they communicate via infrastructures such as RSUs. The messages are sent either from a vehicle to the infrastructure "Vehicle to Infrastructure" (V2I) or from the

infrastructure to a vehicle "Infrastructure to Vehicle" (I2V) which are used as emergency or warning messages.

b. **Pure ad hoc** communication between vehicles Vehicle-to-Vehicle (V2V) in which the vehicles communicate directly with each other's by the help of sensors. In this type of communication, the messages are classified into 3 different types:

   1. *Beacon message*: messages are sent periodically carrying rapid information about traffic problems.
   2. *Group communication*: this communication takes place between vehicles of specific features.
   3. *Warning propagation*: sometimes messages should be sent directly to certain vehicles for the importance of the message, e.g., when there is an accident then the message should be sent directly to the vehicles heading at the accident zone.

c. **Hybrid** communication in which a mixture between both pure cellular and ad hoc communications take place. To explain, if an RSU is available then cellular communication takes place, otherwise, ad hoc communication is used.

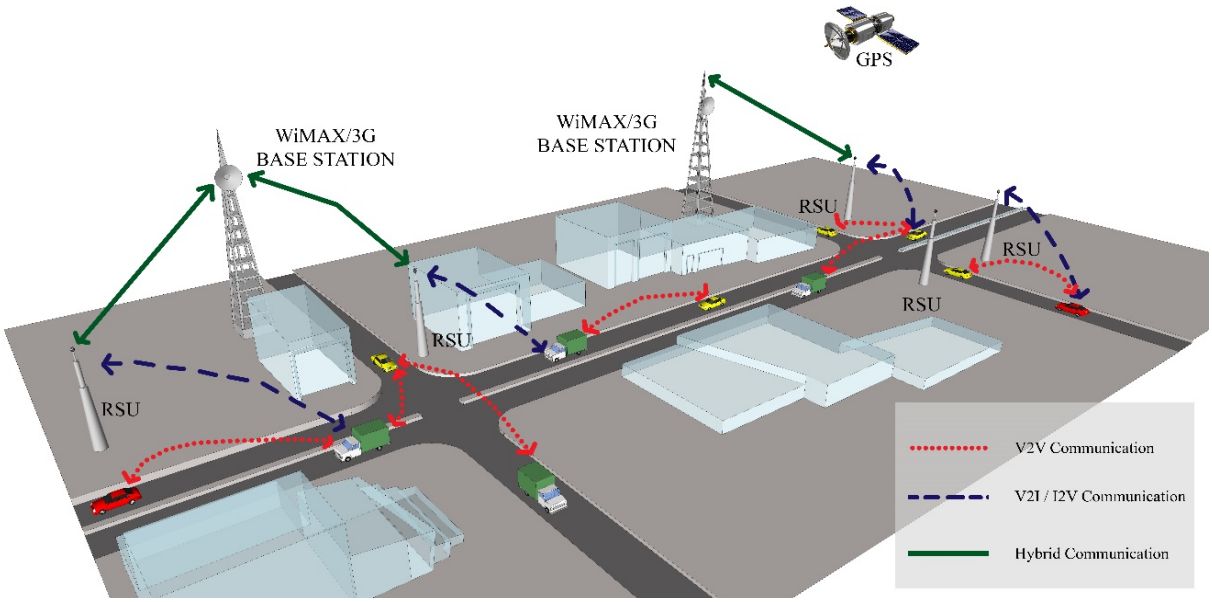

Figure 1. VANETs Structure

2.3. Routing protocols in VANETs

A routing protocol governs the way that two communication entities exchange information. It includes the procedures for establishing a route, deciding on forwarding, and maintaining the route, or recovering from routing failure (K. C. Lee, Lee, and Gerla 2010)(Ghori et al. 2018)(Zeadally et al. 2012)(S. Singh, Kumari, and Agrawal 2015). Main Routing protocols can be classified as in Figure 2.

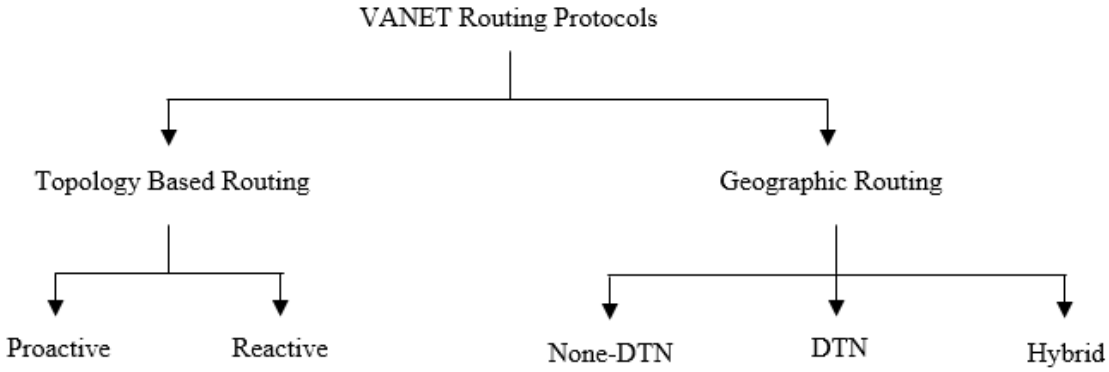

Figure 2. VANETs Routing Protocols

a. Topology based routing protocols: Links information within the network to send the data packets from source to destination. It is categorized into:

1. **Proactive (table driven) routing** is based on the shortest path algorithm and keeps information of all connected nodes in the form of tables that are shared with neighbors. Whenever there is a change in the network topology, every node updates its routing table. This protocol has low latency for real time applications and does not require route discovery. It has the advantage that its connection time is fast due to the presence of routing information when sending the first packet. It has the disadvantage that the unused paths occupy a significant part of the available bandwidth, therefore, the Communication routing information is continuously used while there is no traffic (Shete and Godse 2015).
2. **Reactive (on-demand) routing** initiates route discovery only when a source node request to find a route. It establishes a route for the source node to destination node only when it requests to communicate with another node and the source node do not have a route to the destination node. When any node tries to find the destination "on demand," the flooding technique is used to propagate the query. (Chowdhury et al. 2011). This protocol has the advantage of using the flooding technique that does not consume bandwidth for sending information. It consumes bandwidth only, when the source node starts transmitting the data to the destination node. It has the disadvantage that the route finding latency is high and excessive flooding of the network causes disruption of nodes communication.

b. Geographic (Position-based) routing protocol is based on three main assumptions: 1) all nodes can determine their own position; 2) all nodes know the positions of their direct neighbors, and 3) the source node knows the position of the destination (Varga et al. 2011). It is categorized into:

1. **Delay Tolerant Network (DTN)** uses the Carry & Forward strategy to overcome frequent disconnection of nodes in the network. In Carry & Forward strategy when a node cannot contact other nodes, it stores and forward the packet based on some metric of neighbors.
2. **Non-DTN** the fundamental principle in this greedy approach is that a node forwards its packet to its neighbor that is closest to the destination. Therefore, this forwarding strategy can fail if no neighbor is closer to the destination than the node itself; hence, we can say that the packet has reached the local maximum at the node since it has made the maximum local progress at the current node. The routing protocols in this category have their own recovery strategy to deal with such a failure.
3. **Hybrid** geographic routing protocol switches from non-DTN mode to DTN mode by estimating the connectivity of the network based on the number of hops a packet has

travelled so far, neighbor's delivery quality, and neighbor's direction with respect to the destination. The delivery quality of neighbors is obtained through Virtual Navigation Interface (VNI), which abstracts information from underlying hardware.

2.4. VANET Security Requirements

Securing the data transition between vehicles and other infrastructures in VANETs is an important issue as this data usually contain critical information that must be received correctly and timely. This section discusses the basic requirements to assure packet transfer security in VANETs.

In fact, may requirement conditions are required to maintain and elevate the security infrastructure of VANETs' communication (Salagar and Tangade 2015)(Mokhtar and Azab 2015)(Al-Kahtani 2012)(Samara, Al-Salihy, and Sures 2010) as discusses below:

a. **Authentication:** Only legitimate vehicles have the ability to communicate on the network, and therefore vehicles should not respond to messages that are not authenticated or that come from an unauthenticated vehicle.

b. **Data Integrity** is making sure that the message is received correctly. Thus, it is important to authenticate not only the senders (vehicles) but also the messages themselves that are received even from an authenticated sender. It ensures that data or messages received are the same as sent by the authorized node without any modification, deletion, or replay. This concept in VANETs often combines with the concept of authentication to guarantee that the receiver should be able to verify that a message is indeed sent and signed by another node without begin modified.

c. **Availability:** The networks should be available whenever it is required, e.g., the services provided by the RSU should be available to the vehicles whenever they require them.

d. **Privacy:** Driver's profile should be updated and maintained in a secured database that keeps such critical data away from unauthorized observers.

e. **Non-Repudiation:** it secures against the denial of an actual sender to the transmitted message whenever an investigation is required. Non-repudiation is of two folds, it protects against the sender's denial of sending a message (sender nonrepudiation) as well as the receiver's denial of receiving a message (receiver nonrepudiation).

f. **Real-time Constraints:** due to the high speed and movement of vehicles, which can affect the real time response and may cause delays in time. Therefore, most vehicular networks depend on Dedicated Short-Range Communication (DSRC), DSRC are one-way or two-way short-range to medium-range wireless communication channels specifically designed for automotive use.

g. **Confidentiality:** privacy and protection of both of the drivers' personal information and the messages they send should be protected and encrypted to make them unexposed to attackers and difficult to extract.

Table 3 highlights the security requirments for the different types of comunication configurationsas discussed above (De Fuentes, González-Tablas, and Ribagorda 2011).

Table 3: The Security Requirements for the Different Types of Communication in VANETs.

Security requirements	I2V or V2I	V2V Beacon message	V2V Group communication	V2V Warning propagation
Authentication	√	√		√
Availability	√	√	√	√
Privacy	√	√	√	
Data integrity	√	√	√	√
Non-Repudiation	√	√		√
Real-time constraints		√		√
Confidentiality			√	

3. VANET'S VULNERABILITY

In this section, we start by discussing the types of malicious vehicles then move to understand how they can maliciously behave to threaten a VANET.

3.1. Malicious Vehicles in VANETs

Malicious vehicles affect the legitimate vehicles in different ways due to the type of the malicious vehicle. Malicious vehicles are classified as follows (Al-Kahtani 2012)(Salagar and Tangade 2015):

a. **Insider vs. Outsider Attackers:**

In a network, a member node who can communicate with other members of the network is known as an Insider. Outsiders cannot communicate directly with the members of the network. Both insider and outsider attackers can trick the *authentication* of the network.

b. **Malicious vs. Rational Attackers:**
A malicious attacker uses various methods to damage the member nodes and the network without gaining any personal benefits, while a rational attacker expects personal benefit from the attack. Thus, these attacks are more predictable and follow some patterns. Both breach the *confidentiality* of the network.

c. **Active vs. Passive Attackers:**
An active attacker can generate new packets to damage the network whereas a passive attacker only eavesdrops the wireless channel and do not necessarily generate new packets. Active attackers can affect the *availability* of the network

3.2. Security threats and attacks in VANETs

There are different targets for attackers to impact a VANET. Threats to the network are classified into three main groups—availability, integrity, and confidentiality (Mokhtar and Azab 2015)(Kushwaha, Kumar Shukla, and Baraskar 2014)(Sheikh and Liang 2019)(Sari, Onursal, and Akkaya 2015)(Zeadally et al. 2012).

The following are examples of attacks on three VANET security services, namely, availability, authenticity, and confidentiality.

a. Availability Threats:

Lack of availability affects the efficiency of the VANET. The following are some of the attacks that affect the VANET's availability:

- **Denial of Service (DOS) Attack** takes place when the attacker takes control of the resources of the vehicle and jams the communication channel used by the vehicular network causing the network to be unavailable to the authentic users. Malicious attackers are usually active insiders or active outsiders.
- **Black Hole Attack** is usually caused by a registered VANET user. The suspected node receives the packets from the network, but it declines the contribution in the networking operation. This may disrupt the routing table and may prevent an important message to the recipients due to the malicious node, which pretends to contribute in the non-practical event (Sheikh and Liang 2019).
- **Malware** virus or worm is entered to the VANET causing serious interference of flow operation, making the communication very slow due to eating of resources. It may be uploaded when a firmware update takes place in OBU and RSU.
- **Spamming (**or spam messages) in VANET causes an increase in the transmission latency due to the missing of centralized administration, which makes it difficult to control spamming.

b. Authenticity Threats

Authentication is mandatory to protect the VANET network from internal and external attacks. When malicious nodes join the network, they affect the network performance. The following are some of the attacks that relate to the VANET's authentication:

- **GPS Spoofing:** the attacker creates a false location on the GPS system of the network causing the vehicles think that this is the correct location. This is because the GPS satellite simulator usually generates stronger signals than those of the authentic or real satellite, hence, dominates.

- **Replay Attack:** attackers retransmit packets causing traffic jam and general network performance degradation.
- **Sybil Attacks:** a malicious driver creates multiple fake identities leading to different types of attacks such as position faking (reporting false positions), and masquerading (attackers join the network as legitimate vehicles). Sybil attack can be a serious threat because it causes great damage to a VANET's function**.**

c. Confidentiality Threats

Messages that are exchanged may be attacked with techniques such as illegitimate collection of messages through eavesdropping where attackers can collect information about users and use it, without the user's knowledge, in order to access confidential data. The following are some attacks that relate to VANET's confidentiality:

- **Eavesdropping Attack:** this attack affects the privacy of messages as it illegally acquires the information entailed that is supposed to be confidential and protected**.**
- **Timing Attack:** the attacker, without manipulating the actual content, adds time slots so that receivers get the message after the defined slots causing a message delay.
- **Man-in-the-Middle Attack:** This attack takes place in the middle of V2V communication to closely intervene and alter the message. The attacker gets access and control of the entire V2V communication, while the communication entities think that they are communicating in private

Table 4 summarizes and classifies the VANET attacks mentioned above depending on the security requirements they breach, the type of malicious vehicles performing the attack (Al-Kahtani 2012), and the affected components of the corresponding communication mode (Hasrouny et al. 2017).

Table 4. Classification of VANET Attacks

Attack	Security Requirement	Configuration Components	The Type of malicious vehicle
Denial of Service (DOS)	Availability	• V2V and V2I (infrastructure, hardware and software) • V2V (wireless interface)	Active, Insiders and Malicious
Black hole	Availability	• V2V (wireless interface, hardware and software)	Outsiders and Passive
Malware	Availability	• V2V (wireless interface) • V2I and V2V (hardware and software)	Malicious and Insider
Spamming	Availability	• V2V (hardware and software)	Passive, Malicious and Insider
GPS Spoofing	Authenticity	• V2I and V2V (hardware and software) • V2V (OBU)	Outsider and Rational
Replay Attack	Authenticity	• V2I and V2V (hardware and software)	Insider
Sybil Attacks	Authenticity	• V2V (wireless interface, hardware and software)	All
Eavesdropping	Confidentiality	• V2I and V2V (Infrastructure)	Rational, Insiders or Outsiders
Timing	Confidentiality	• V2V (hardware and software)	Malicious and Insider
Man-in-the-Middle	Confidentiality	• V2V (wireless interface) • V2I and V2V (hardware and software)	Passive and Insider

3.3. Security Approaches

There are different types of solutions to protect VANTs, as discussed below (Al-Kahtani 2012)(Li and Jain 2014)(Chen et al. 2018):

a. **Public Key Approaches:**

Under Public Key Infrastructure (PKI), each node in a VANET is provided with a pair of private and public keys. PKI is used in a scheme only if the vehicle has two extra hardware units: an Event Data Recorder (EDR) to record all events and a Tamper Proof Hardware (TPH) to run a cryptographic process. A public key infrastructure (PKI) is widely used to provide security in VANETs, which includes certificate revocation (i.e., terminating the membership of a vehicle) and ID-based cryptography.

1. **Certificate Revocation:** Certificate revocation is performed by certificate authorities (CA) in two ways:
   - Centralized: a central authority is responsible only for taking the revocation decision.
   - Decentralized: a group of vehicles which are neighbors of the revoked vehicle take such a decision.

   Once a certificate is detected as invalid, certificate authorities (CA) issues messages to the RSU, which in turn, broadcasts messages to all vehicles to revoke that particular certificate and stop communication with it.
2. **ID-based Cryptography**: ID-based cryptography reduces the computational cost in the ID-based Signature (IBS) process for VANETs and is preferable for authentication using the ID-based Online/Offline Signature (IBOOS) scheme. IBOOS increases efficiency by separating signing process into an offline (executed initially at RSUs or vehicles) and online phase (executed in vehicles during V2V communication), in which the verification is more efficient than that of IBS.

b. **Symmetric Approaches:**

In a Symmetric scheme, nodes communicate after they share and agree on a secret key that is used for communication.

c. **Hybrid Approaches:**

A Hybrid scheme uses both Symmetric and PKI approaches together. It uses two types of communications: pairwise and group communication. Pair-wise communication is used when two vehicles need to communicate each other, whereas in group communication, more than two vehicles communicate. Hybrid approaches use symmetric keys for pairwise communications to avoid the overhead of using the key pair.

4. SYBIL ATTACKS

It is the type of attacks in which a malicious driver creates multiple faked identities, as shown in Figure 3. These identities are then used to play many type of attacks; consequently, every generated attack is played after spoofing the positions or identities of other nodes in the network (Sakiz and Sen 2017).

The attack through multiple Sybil nodes effects on network functioning (GROVER, GAUR, and LAXMI 2010). Such as:

- **Data aggregation**: A malicious node may contribute to alter the aggregation of data and change the results and calculations of the system, which may, in turn, affect the network performance.

- **Fair resource allocation**: Sybil nodes may impact the fairness of resource allocation. A malicious node eats a large share of the system resources. This may lead to a DoS.
- **Routing**: Sybil attacks are effective against the functioning of the routing protocols. For instance, in *Multiple routing protocol* (Malik and Sahu 2019), disjoint paths are used, so, the presence of Sybil identities on this path can impair routing. Another example, in *Geographic routing* (Varga et al. 2011) malicious nodes can appear in more than one place at the same time and that confuses the network.
- **Voting**: Sybil attack can update the output of voting scheme incorrectly.
- **Misbehavior detection**: An attacker can bypass a mechanism to detect a malicious node by spreading the blame through the Sybil nodes, even if the detection mechanism uses multiple observations to locate the malicious nodes, the attacker can still escape due to the multiple nodes that it created.

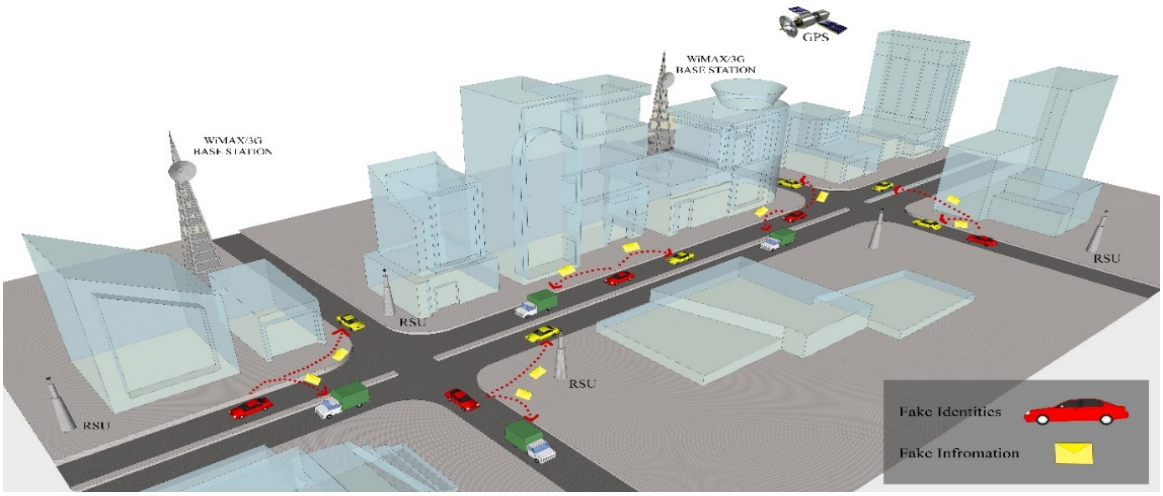

Figure 3. Sybil Attacks.

4.1. Forms of Sybil Attacks

Sybil attacks can be classified into three different categories (GROVER, GAUR, and LAXMI 2010) as shown in Figure 4, which are:

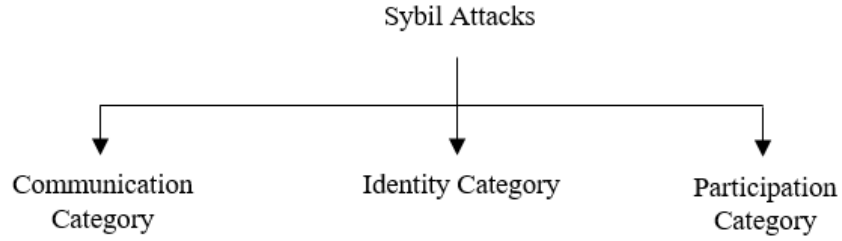

Figure 4. Forms of Sybil Attacks.

- **Communication category**: Communication to/from Sybil nodes can be direct or indirect.
  - In direct communication, all maliciously created Sybil nodes communicate with legitimate nodes.
  - In indirect communication, legitimate nodes reach the Sybil nodes through a malicious node.

- **Identity category**: In a Sybil attack, an attacker creates a new Sybil identity.
  - This identity can be a random 32-bit integer (*fabricated identity*), or
  - An attacker can spoof legitimate identity of one of its neighbors (*stolen identity*).
- **Participation category**: Multiple Sybil identities created by malicious nodes can be either simultaneously participated or presented one by one to share in an attack. In the latter case, a particular identity may leave and rejoin the network many times, that is, one identity is used at a time.

4.2. Sybil Attack Defense Techniques

There are several defense techniques against Sybil attacks. The defense methods can be classified into three different categories (Kushwaha, Kumar Shukla, and Baraskar 2014)(Rangaswamy and Hegde 2014)(Golle, Greene, and Staddon 2004)(Jayaraman, Kannimoola, and Achuthan 2014)(Kamesh and Sakthi Priya 2012), which are based upon resource testing, position verification, and encryption and authentication, as discussed below.

4.2.1. Defense Methods based on Resource Testing

Resource testing has few assumptions: 1) Every physical entity is equipped with limited computational resources, 2) each user has only one identity, and 3) each identity should work on a single machine. However, when Sybil attacks start, Sybil identities usually work on a single system.

Therefore, the Resource Testing defense method puts limitations and threshold constraints on the consumption of resources to each group of identities, such as time or resource consuming. In general, the goal of resource testing is to determine whether the selected identities have a reasonable amount of resources. Therefore, if a group of identities complete the work within the given threshold limit, then it is most likely that it is an honest nodes group; otherwise, it is most likely there is a suspect Sybil node within this group. Several methods can be used to test vehicle's resources, such as:

1. **Radio resources: Three assumptions about radio resources:**
   - Each entity has only one radio device.
   - Radio devices operate over a specified number of channels.
   - Radio devices cannot simultaneously transmit or listen on more than one channel.
2. **Computational and memory resources:**
   Vehicles failing to solve a puzzle are identified as fake vehicles. They can be detected by message tracking and monitoring vehicles to detect those using shared resources in sending messages and the processing of received signals.
3. **Identification resources:**
   If there are vehicles with IP addresses that are not recorded in the list, then they are identified as fakes. However, the operation of broadcasting the registered identities for legitimate vehicles violates privacy of the drivers.

4.2.2. Defense Methods based on position verification

The goal of these methods is to make sure that the position of the nodes are verified and that they are referring to only one identity.

1. **Passive Detection through Single or Multiple Observers:**
   - Single observers: A single vehicle monitors network traffic passively. It requires only a small amount of memory to record its observations.
   - Multiple observers: Multiple trusted nodes are requested to share their observations on the traffic with each other to improve the Sybil node detection rate.

2. **Sybil Node Detection through the Propagation Model:**
   The power of the signal received from a sending node is matched with that received from its same claimed position; if both (calculated and claimed) do not match, then there should be a Sybil node with a high probability.

3. **Sensor-Based Position Verification:**
   It uses multiple sensors rather than using fixed infrastructure to detect malicious behavior of the nodes in the network.

4.2.3. Defense Methods based on Encryption and Authentication

In the encryption and authentication methods, Sybil attack detection is based on:

1. **Authentication Mechanism:**
   Using trusted certificates has a high potential to eliminate Sybil attacks.

2. **Public key Cryptography:**
   Signatures are combined with digital certificates through asymmetric cryptography. Many of encryption and authentication methods are based on PKI.

3. **Trusted Certification**
   Sybil attacks can be avoided by using trusted certification authority, e.g., a central authority that can verify the validity of each user. Before a participant joins a peer-to-peer system, provides votes, and obtains services from the system, the identity must first be verified. Centralized trusted certification methods are often implemented by asymmetric (such as public/private keys) Cryptography. They assumed that each node shares a unique symmetric key with a trusted centralized base station. After checking the validity of each other, a pair of nodes can exchange their shared keys. During data transmission between adjacent nodes, they can use the key for mutual authentication, validation, and data encryption.
   Some problems may face central authority-based methods, such as:
   a. Single point of attack: The central authority can easily become a target.
   b. Performance bottleneck: If huge number of users access the central authority simultaneously, the central authority may fail (DOS).
   c. Communication cost: The authority should always be active during all data transmissions.

4.3. Detection methods for Sybil Attacks

The misbehavior of vehicles is important to be detected to save the VANETs environment and to protect the users and their messages from any malicious disruptions. Detection depends on different properties, such as time, position, cryptography protection, and the supporting resource. Accordingly, detection algorithms can be classified as in Figure 5.

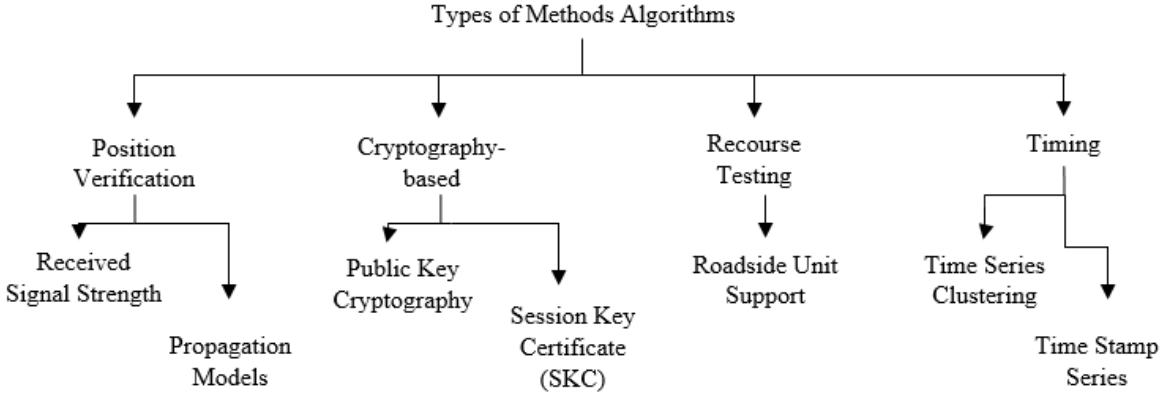

Figure 5. Sybil Attack Detection Classification

Table 5 highlights the advantages and disadvantages of such detection protocols (Al-Mutaz, Malott, and Chellappan 2014)(GROVER, GAUR, and LAXMI 2010)(Rahbari and Jabreil Jamali 2011)(Bruno 2019).

Table 5. Pros & Cons of the Detection Methods of Sybil Attacks.

Type of detection	About	Pros	Cons
Position Verification Methods:			
Received signal strength	• It Depends on the received signal strength • Signal strength is measured due to the last sent message.	• It does not require centralization. • Nodes can locally determine their locations through received signal strength variations.	• Signal strength of an individual transmission is not a simple function of distance. • Radio irregularity has a significant effect on the network layer protocols, especially location-based routing protocols. • Depends on the trust of the chosen nodes leading to limited accuracy.
Propagation models	• It Depends on the received signal strength • They use the received signal strength to calculate the inconsistencies between the power of the signal and the claimed position. • Received signal power can be used to calculate the position of the node	• Works very good on small scale, any change in signal strength will, therefore, be detected by a receiver. • More realistic radio propagation model is required to support high mobility of nodes in VANETs.	• Malicious node can use the same propagation model to compute the transmission signal strength required to fool detection system in estimating the next position of the node.
Cryptography-based Methods:			
Public key cryptography	• Signatures are combined with digital certificates and asymmetric cryptography is used. • Certificates are issued by CA and there is a hierarchy of these CAs.	• Signatures are combined with digital certificates and asymmetric cryptography is used. • Have a third parity (CA). • Certificates are changed from time-to-time.	• PKI is difficult to be deployed in VANETs, as there is no guarantee of the presence of infrastructure. • PKI consumes large memory, and time consuming as well.

SKC (Session Key Certificate)	• Certificates are given using symmetric cryptography. • It generates anonymous IDs, session Key and session key expiration date.	• There is an expiration date for the session key.	• It is difficult to determining the number of attackers when there are multiple adversaries collectively use the same identity to launch malicious attacks.
Resource Testing Methods:			
Roadside Unit support	• Depends on RSU certificate authority • Vehicles must be authenticated to participate in the communication therefore the Sybil attack is detected if no authentication	• It needs neither vehicular based public key infrastructure nor internet accessible RSUs • Uses digital certificates that are only issued by RSUs.	• Limited number of roadside units (insufficient to sustain the load).
Timing Methods:			
Time series clustering	• Depends on the trust of the neighbors • Sybil attack may be detected by other vehicles	• Does not require any additional hardware or infrastructure support. • Time is an important parameter.	• Depends on human recourses.
Time stamp series	• Sybil attack can be detected if multiple traffic messages contain very similar series of timestamps. • Time stamps are certified by each RSU they pass by	• Changing the time stamp several times	• Depend on the RSU then if RSU is attacked then the whole system is attacked • If the RSU is located in the intersection, then detecting the Sybil attack is difficult to be detected

Table 6 lists articles and work related to the Sybil attack detection methods, as classified above, with an indication of the type of detection algorithms used.

Table 6. Detection Methods Related Work.

Paper	Detection algorithm	Contribution
Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs (Yao et al. 2017)	Received signal strength	This article proposes a Sybil attack detection method based on Received Signal Strength Indicator (RSSI) and Voice print to conduct a widely applicable, lightweight and full-distributed detection for VANET attacks due to inaccurate position estimation according to radio propagation models. Voiceprint adopts the RSSI time series as the vehicular speech and compares the similarity among all received time series.

A Modified RSA Cryptography Algorithm for Security Enhancement in Vehicular Ad Hoc Networks (Chyne, Kandar, and Paul 2018)	Public key cryptography	It proposes a modified version of the Rivets–Shamir–Adelman RSA algorithm, which they called it, MRSA. MRSA is an asymmetric key cryptography system to protect information. It prevents security as well as increasing the brute force attack time.
A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET (B. K. Lee, Jeong, and Jung 2013)	Session Key-based Certificate	This article proposes a DTSA (Detection Technique against a Sybil Attack) protocol so that it can provide vehicles with a more secure information for the road situation and the traffic flow among vehicles. The DTSA uses SKC (Session Key-based Certificate) to verify the IDs among vehicles to detect the Sybil attack.
RSS-based Sybil Attack Detection in VANETs (Grover et al. 2010)	Roadside Unit support	In this paper, the researchers presented a distributed solution based on the use of Received Signal Strength (RSS) for detecting Sybil nodes in VANET. This approach relies on similarity of RSS values of nodes instead of inferring the position of nodes using RSS. This technique is lightweight as it considers only a single parameter RSS value for detecting Sybil attacks.
A Time-series Clustering Approach for Sybil Attack Detection in Vehicular Ad hoc Networks (Dutta and Chellappan 2013)	Time series Clustering	In this paper, they proposed a fuzzy time-series clustering based approach that does not require any additional hardware or infrastructure support for Sybil attack detection in VANETs. The proposed technique leverages the dispersion of vehicle platoons over time in a network and detects Sybil nodes as those that are traveling closely in a cluster for an unreasonably long time.

5. SUMMARY

Vehicular Ad hoc Networks (VANETs) are becoming popular in transportation systems since they provide road safety, traffic management, and Internet access on highway via distributing safety information to drivers and passengers. In this article, we have reviewed VANETS from different perspectives, especially VANETs security. We shade light on the VANETs requirements, VANETs components, and VANETs communication. The article reviewed several types of attacks and threats affecting VANETs communication. In this article, the focus was on Sybil attack as it is the most harmful attack on VANETs. In Sybil attack, a malicious sender creates multiple faked identities and multiple faked messages; therefore, Sybil attack is particularly harmful because it violates the fundamental assumptions of VANETs communication protocols. In addition, this article reviewed most of known defense and detection algorithms for Sybil attacks in VANETs.

REFERENCES

1. Al-Kahtani, Mohammed Saeed. 2012. “Survey on Security Attacks in Vehicular Ad Hoc Networks (VANETs).” In *the Proceedings of the 6th International Conference on Signal Processing and Communication Systems, ICSPCS 2012* -.
2. Al-Mutaz, Muhammad, Levi Malott, and Sriram Chellappan. 2014. “Detecting Sybil Attacks in Vehicular Networks.” *Journal of Trust Management* 1(1): 4.
3. Bruno, Latour. 2019. “DEFENSE AGAINST SYBIL ATTACK IN VEHICULAR AD HOC NETWORK BASED ON ROADSIDE UNIT SUPPORT.” *Journal of Chemical Information and Modeling* 53(9): 1689–99.
4. Chen, Yingyang et al. 2018. “NOMA in Vehicular Communications.” In *IEEE Wireless Communications*, 333–66.
5. Chowdhury, Shaikhul Islam et al. 2011. “Performance Evaluation of Reactive Routing Protocols in VANET.” In the Proceedings of *International Journal of Future Generation Communication and Networking*, , 559–64.
6. Chyne, Phidahunlang, Debdatta Kandar, and Babu Sena Paul. 2018. “Intrusion Detection System for Software-Defined Networks Using Fuzzy System, A Novel Weighted Vehicular Network Clustering Scheme.” In *International Conference on Computing and*

Communication Systems, Springer Singapore, 433–40. http://dx.doi.org/10.1007/978-981-10-6890-4_62.
7. Dutta, Neelanjana, and Sriram Chellappan. 2013. "A Time-Series Clustering Approach for Sybil Attack Detection in Vehicular Ad Hoc Networks." *VEHICULAR 2013 : The Second International Conference on Advances in Vehicular Systems, Technologies and Applications* (February): 35–40.
8. Faezipour, Miad, Mehrdad Nourani, Adnan Saeed, and Sateesh Addepalli. 2012. "Progress and Challenges in Intelligent Vehicle Area Networks." *Communications of the ACM* 55(2): 90–100.
9. De Fuentes, José María, Ana Isabel González-Tablas, and Arturo Ribagorda. 2011. "Overview of Security Issues in Vehicular Ad-Hoc Networks." In *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, , 894–911.
10. Ghori, Muhammad Rizwan et al. 2018. "Vehicular Ad-Hoc Network (VANET): Review." *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*: 1–6.
11. Golle, Philippe, Dan Greene, and Jessica Staddon. 2004. "Detecting and Correcting Malicious Data in VANETs." *VANET - Proceedings of the First ACM International Workshop on Vehicular Ad Hoc Networks*: 29–37.
12. GROVER, JYOTI, M GAUR, and V LAXMI. 2010. "Sybil Attack in VANETs Detection and Prevention." *Security of Self-Organizing Networks* (July): 269–94.
13. Grover, Jyoti, M S Gaur, Nitesh Prajapati, and Vijay Laxmi. 2010. "RSS-Based Sybil Attack Detection in VANETs."*IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS* (December 2015): 2278–83.
14. Haas, Jason J., Yih Chun Hu, and Kenneth P. Laberteaux. 2009. "Real-World VANET Security Protocol Performance." *GLOBECOM - IEEE Global Telecommunications Conference*: 6–12.
15. Hasrouny, Hamssa, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. 2017. "VANet Security Challenges and Solutions: A Survey." *Veh. Commun.* 7(January): 7–20. http://dx.doi.org/10.1016/j.vehcom.2017.01.002.
16. Jayaraman, Bharat, Jinesh M. Kannimoola, and Krishnashree Achuthan. 2014. "Sybil Attack Detection in Vehicular Networks." *Computer Science and Information Technology* 2(4): 197–202.
17. Kamesh, and N. Sakthi Priya. 2012. "A Survey of Cyber Crimes Yanping." *SECURITY AND COMMUNICATION NETWORKS* 5: 422–37.
18. Karagiannis, Georgios et al. 2011. "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions." *IEEE Communications Surveys and Tutorials* 13(4): 584–616.
19. Kumar, Sushil, and Anil Kumar Verma. 2015. "Position Based Routing Protocols in VANET: A Survey." *Wireless Personal Communications* 83(4): 2747–72. http://dx.doi.org/10.1007/s11277-015-2567-z.
20. Kumar, Vishal, Shailendra Mishra, and Narottam Chand. 2013. "Applications of VANETs: Present & Future." *Communications and Network* 05(01): 12–15.
21. Kushwaha, Deepak, Piyush Kumar Shukla, and Raju Baraskar. 2014. "A Survey on Sybil Attack in Vehicular Ad-Hoc Network." *International Journal of Computer Applications* 98(15): 31–36.
22. Lee, Byung Kwan, Eun Hee Jeong, and Ina Jung. 2013. "A DTSA (Detection Technique against a Sybil Attack) Protocol Using SKC (Session Key Based Certificate) on VANET." *International Journal of Security and its Applications* 7(3): 1–10.
23. Lee, Kevin C., Uichin Lee, and Mario Gerla. 2010. "Survey of Routing Protocols in Vehicular Ad Hoc Networks." In *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*, , 149–70.
24. Li, Mohan, and Raj Jain. 2014. "Security in VANETs." *http://www.cse.wustl.edu/~jain/cse571?14/ftp/vanet_security/index.html*.
25. Malik, Suman, and Prasant Kumar Sahu. 2019. "A Comparative Study on Routing Protocols for VANETs." *Heliyon* 5(8): e02340. https://doi.org/10.1016/j.heliyon.2019.e02340.
26. Mary Anita, E. A., and J. Jenefa. 2016. "A Survey on Authentication Schemes of

VANETs." In *2016 International Conference on Information Communication and Embedded Systems, ICICES 2016*.
27. Mokhtar, Bassem, and Mohamed Azab. 2015. "Survey on Security Issues in Vehicular Ad Hoc Networks." *Alexandria Engineering Journal* 54(4): 1115–26. http://dx.doi.org/10.1016/j.aej.2015.07.011.
28. Rahbari, Mina, and Mohammad Ali Jabreil Jamali. 2011. "Efficient Detection of Sybil Attack Based on Cryptography in Vanet." *International Journal of Network Security & Its Applications* 3(6): 185–95.
29. Rangaswamy, Shanta, and Vinay Hegde. 2014. "A Survey of Techniques to Defend Against Sybil Attacks in Social Networks." *International Journal of Advanced Research in Computer and Communication Engineering* 3(5): 6577–80.
30. Sakiz, Fatih, and Sevil Sen. 2017. "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV." *Ad Hoc Networks* 61(October): 33–50.
31. Salagar, Praveen G, and Shrikant S Tangade. 2015. "A Survey on Security in Vanet." *International Journal For Technological Research In Engineering* 2(7): 1397–1402.
32. Samara, Ghassan, Wafaa A.H. Al-Salihy, and R Sures. 2010. "Security Analysis of Vehicular Ad Hoc Networks (VANET)." In *Proceedings - 2nd International Conference on Network Applications, Protocols and Services, NETAPPS 2010*, , 55–60.
33. Sari, Arif, Onder Onursal, and Murat Akkaya. 2015. "Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)." *International Journal of Communications, Network and System Sciences* 08(13): 552–66.
34. Sarika, S., A. Pravin, A. Vijayakumar, and K. Selvamani. 2016. "Security Issues in Mobile Ad Hoc Networks." *Procedia Computer Science* 92(June): 329–35.
35. Sheikh, Muhammad Sameer, and Jun Liang. 2019. "A Comprehensive Survey on VANET Security Services in Traffic Management System." *Wireless Communications and Mobile Computing (Hindawi)* 2019.
36. Shete, Omkar, and Sachin Godse. 2015. "VANET Security against Sybil Attack by Using New SRAN Routing Protocol." *International Journal of Computer Applications Technology and Research* 4(7): 535–39.
37. Singh, Amandeep, and Sandeep Kad. 2016. "A Review on the Various Security Techniques for VANETs." *Procedia Computer Science* 78: 284–90.
38. Singh, Surmukh, Poonam Kumari, and Sunil Agrawal. 2015. "Comparative Analysis of Various Routing Protocols in VANET." In *International Conference on Advanced Computing and Communication Technologies, ACCT*, , 315–19.
39. Varga, András et al. 2011. "VANET Routing Protocols Pros and Cons." *WEIRD workshop on WiMax, wireless and mobility* 25(3): 2456–60. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4448631%5Cnhttp://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5426207%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:distributed+robust+geocast+multicast+routing+fo.
40. Yao, Yuan et al. 2017. "Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs." In *Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017*, , 591–602.
41. Zaidi, Kamran, and Muttukrishnan Rajarajan. 2015. "Vehicular Internet: Security & Privacy Challenges and Opportunities." *Future Internet* 7(3): 257–75.
42. Zeadally, Sherali et al. 2012. "Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges." *Telecommunication Systems* 50(4): 217–41.