applied sciences

MDPI

Article

The Security Perspectives of Vehicular Networks: A Taxonomical Analysis of Attacks and Solutions

Amandeep Verma [1], Rahul Saha [1,*], Gulshan Kumar [1] and Tai-hoon Kim [2,*]

[1] School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, Punjab, India; vermaaman78658@gmail.com (A.V.); gulshan3971@gmail.com (G.K.)

[2] Glocal Campus, Konkuk University, 268, Chungwon-daero, Chungju-si 27478, Korea

* Correspondence: rsahaaot@gmail.com (R.S.); taihoonn@daum.net (T.-h.K.)

Abstract: Vehicular networks are the combination of transport systems and the internet systems formed with the main motive to increase the safety of passengers, although non-safety applications are also provided by vehicular networks. Internet of Things (IoT) has a subsection called Mobile Ad hoc Network (MANET)m which in turn has a subsection called Vehicular Ad hoc Network (VANET). Internet of Energy (IoE) is a new domain that is formed using electric vehicles connected with VANETs. As a large number of transport systems are coming into operation and various pervasive applications are designed to handle such networks, the increasing number of attacks in this domain is also creating threats. As IoE is connected to VANETs extension with electric cars, the future of VANETs can be a question if security measures are not significant. The present survey is an attempt to cover various attack types on vehicular networks with existing security solutions available to handle these attacks. This study will help researchers in getting in-depth information about the taxonomy of vehicular network security issues which can be explored further to design innovative solutions. This knowledge will also be helpful for new research directions, which in turn will help in the formulation of new strategies to handle attacks in a much better way.

Keywords: VANET; security; networks; survey; attacks; solutions

check for updates

Citation: Verma, A.; Saha, R.; Kumar, G.; Kim, T.-h. The Security Perspectives of Vehicular Networks: A Taxonomical Analysis of Attacks and Solutions. *Appl. Sci.* **2021**, *11*, 4682. https://doi.org/10.3390/app11104682

Academic Editor: Gianluca Lax

Received: 22 March 2021
Accepted: 16 April 2021
Published: 20 May 2021

1. Introduction

Intelligent Transport System (ITS) is the present and future of vehicular communications. It is a framework that incorporates various innovative technologies in the classical transport system to make it smarter, safer, convenient, and congestion-free [1]. A similar motive is behind the formation of Vehicular Ad hoc Networks (VANETs) where communication takes place among vehicles and various other units of the infrastructure [2,3]. Initially, VANETs were used for communication among cars with the help of roadside units. Later, this communication level extended to connect other vehicles and units such as pedestrians and grids. At present, these networks are deployed in the metropolitan cities only to provide information about accidents, tolls, parking areas, and charging spots. Another motivation for the formation of these networks is to establish communication among all vehicles and the global classical network, i.e., the internet that connects VANET applications with the other users.

VANETs can be described as a hierarchy shown in Figure 1. It represents the relationship of the Internet of Things (IoT) with VANETs. It indicates that VANET is a sub-type of the IoTs and also adopts various attributes of IoTs and MANETs. With the rise in the availability of internet facilities and its speed, it is now possible to connect the devices that would not be possible earlier. Electric Vehicles (EVs) are also an important part of these vehicular networks. These vehicles can communicate with smart grids and charging spots. Vehicles having surplus electricity may pass to smart grids through charging spots (aggregators) [4]. This way a pool of energy from all the vehicles is created which can serve other vehicles. This creates a network of energy called the Internet of Energy (IoE) [5].

Not only vehicles are connected in IoE, but other appliances are also connected to it that use energy. IoE is also connected with the solar panels for the energy storage process for futuristic IoTs. The sustainable development of the technology has produced EVs. IoE is well connected with these EVs. In the future, most vehicles will be electric and this will use facilities provided by IoE. EVs, IoE, and vehicular networks are now closely coupled with each other, and this combination is exploring further possibilities.

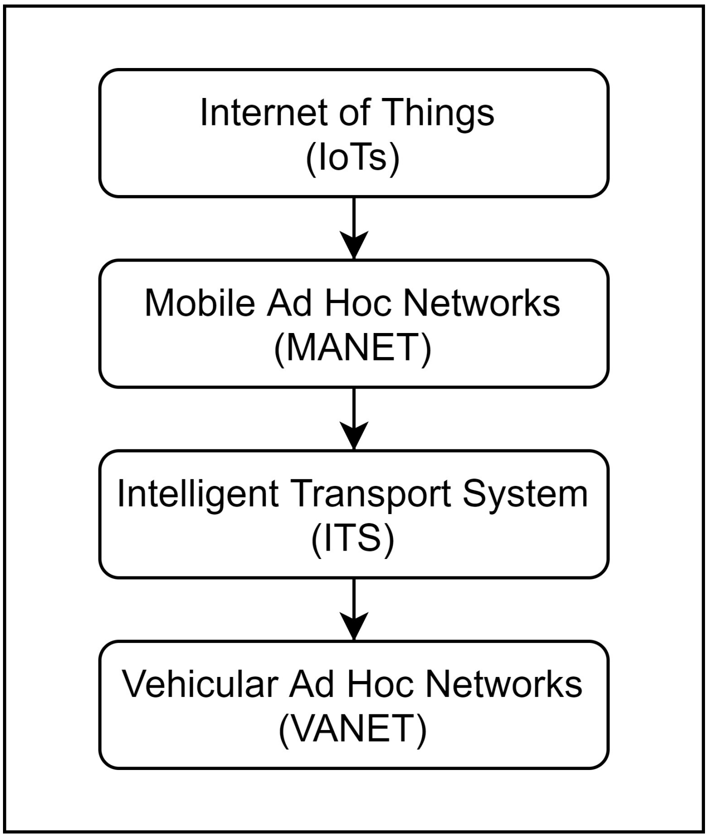
Internet of Things (IoTs)
Mobile Ad Hoc Networks (MANET)
Intelligent Transport System (ITS)
Vehicular Ad Hoc Networks (VANET)

Figure 1. Relationship of IoT and VANET: A hierarchical understanding.

1.1. Motivation and Contribution

VANETs and smart vehicles are connected to each other. The future of smart vehicles also urges the electric vehicles to connect in VANETs. Therefore, IoTs, VANETs, and IoE are closely connected. Rigorous research is going on these fields with the increasing demand of smart applications, seamless multimedia transfers, smart navigation, and others. This motivates us for the present study. Therefore, in this survey, we accumulate almost all the types of research dimensions related to VANETs. We provide a preliminary understanding of VANETs for the naive readers to trigger an interest in this domain. Further, we discuss various attacks on VANETs and also show different researched solutions to prevent such attacks. In a nutshell, this survey provides a pathway for understanding the research status in VANETs. We compare our survey with the existing surveys, and we find it complete in discussing the multi-dimensions of VANETs security attacks and solutions. We also note some important factors of VANETs for future research.

We have also compared our survey with the existing surveys in the literature. We have shown this comparison in the latter part of the survey. We have observed that, though there are various useful taxonomies in use, the complete classification as in our present survey is different from theirs. Moreover, the connection of EVs and IoE in the survey is a new direction in this survey. Our open research problems are also connected with the same. Therefore, our present survey is oriented for futuristic VANET development.

1.2. Organization

Section 2 explains some basic architectural knowledge, modules and applications, features, and security requirements of VANETs. Section 3 shows the taxonomy of the attacks on VANETs. Section 4 shows various solutions existing in the literature for vehicular networks. It provides a taxonomical classification of the solutions and also notifies the gaps in the existing solutions. We also compare our study with the existing surveys in this section. Section 5 shows some open research problems to motivate the research community in this direction and to enrich the domain with upcoming significant solutions. Finally, Section 6 concludes the survey.

2. Preliminary Understanding of VANETs

In this section, we initialize our discussion with the architecture of VANETs followed by the applications, features, and futuristic deployment.

2.1. Architecture of VANETs

The architecture of VANET can be described based on the components [6]. A generic VANET architecture is illustrated in Figure 2. It demonstrates various components and parties involved in a VANET and also shows communication techniques. VANETs are made up of many components like vehicles (electric and nonelectric), on-board units of vehicles, roadside units, and pedestrians, communication channels like Dedicated Short Range Communication (DSRC), cellular networks, and charging grids of electric vehicles [7–9]. Two types of communication can be observed in VANETs: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), and reversely, Infrastructure-to-Vehicle (I2V). Infrastructure-to-Infrastructure (I2I) communication takes place among roadside units and also with base stations. They use the internet as a backbone. To distribute the credentials or keys, trusted authorities also use this communication type. The components of the architecture are shown in Figure 3.

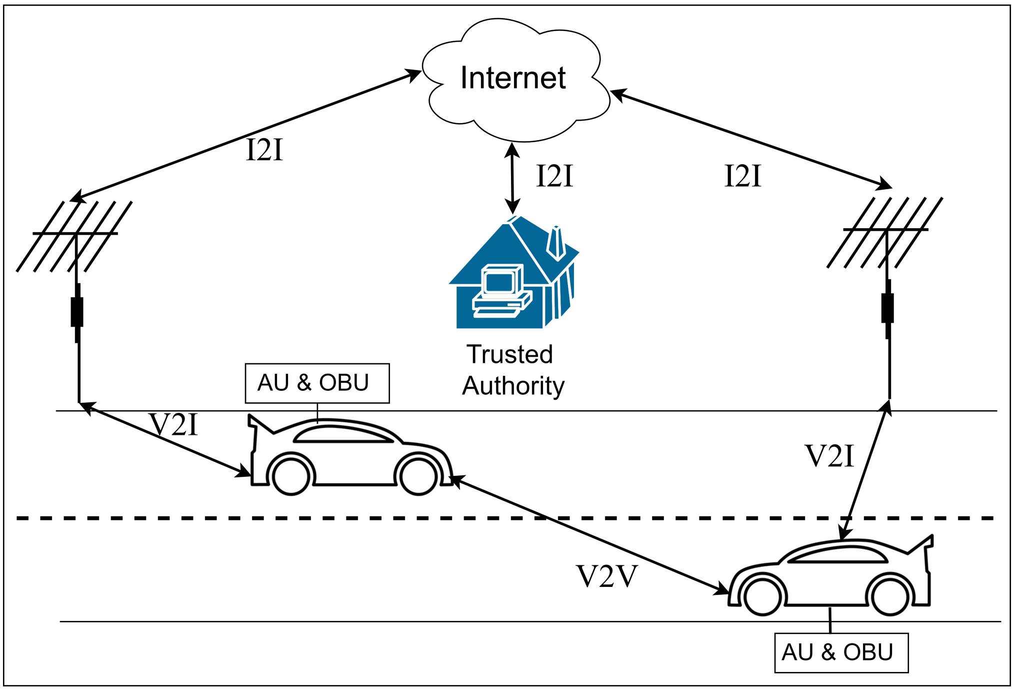

Figure 2. General architecture of VANET.

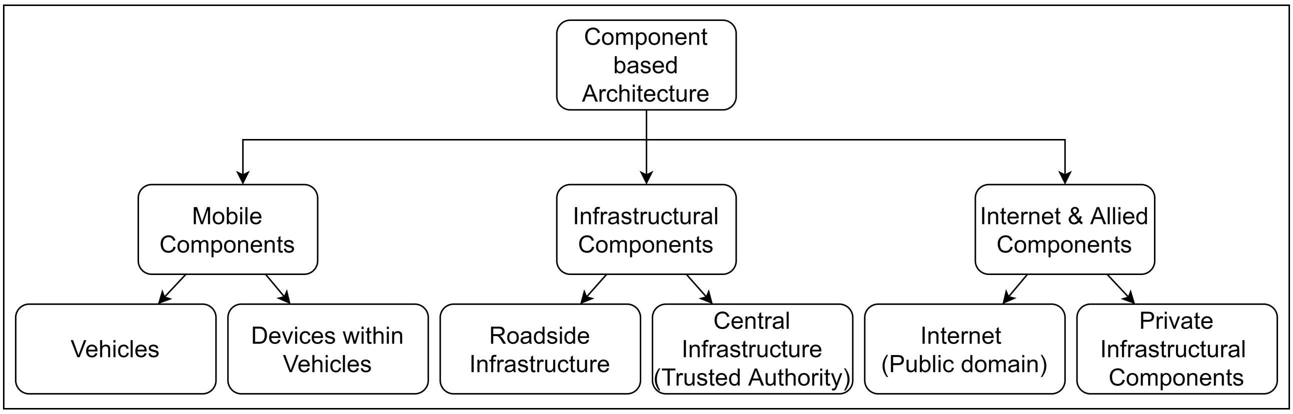
Component based Architecture
Mobile Components
Infrastructural Components
Internet & Allied Components
Vehicles
Devices within Vehicles
Roadside Infrastructure
Central Infrastructure (Trusted Authority)
Internet (Public domain)
Private Infrastructural Components

Figure 3. Component-based architecture of VANET.

Mobile component: All vehicles like cars, jeeps, trucks, buses, motorcycles, and pedestrians fall in this category. It also includes all those components or devices which are carried by passengers and those components which remain in the vehicle. Examples of these components and devices are on-board units, Personal Digital Assistant (PDA), navigation devices such as Global Positioning System (GPS), laptops, and smart mobile phones, etc.

Application Unit: It is the front end of the driver module. It is an application that is either provided by the manufacturer of the On-Board Unit (OBU), or it may be obtained from an external source. For example, in the case of PDA, applications may be downloaded from various resources using cloud applications.

Onboard Unit: An Onboard Unit (OBU) is a device that is placed in the vehicle used for communication with other vehicles using various communication technologies. It can also communicate with infrastructural components or Road-Side Units (RSUs) such as traffic lights, charging spots of electric vehicles, and trusted authority. For this, it may use some other mechanism of communication like 3G, LTE, VoLTE, or 4G networks. OBU further consists of multiple components like sensors, storage, GPS, a processor, and an interface for communication. Other components that may be used here are a Tamper-Proof Device (TPD) [10], event data recorder (EDR) [11], and GPS receiver [12]. OBUs are designed to consume less power so that the vehicles' functions can be executed smoothly.

Infrastructural components: These components don't move, but play important role in network communication. Some components are placed on the roads and are called the Road-Side Units (RSUs). For example, charging spots, poles, and traffic lights are considered as RSUs.

Road-Side Unit (RSU): These units are configured with antennas, processors, sensors, charging spots, and storage systems. They are generally placed alongside the road, but in many cases, these are also placed in parking areas and sometimes at other locations feasible for communication coverage.

Trusted Authority (TA): To implement security in VANETs, there is always a need for a trusted authority which handles the security issues. A trusted authority (TA) is a centralized or decentralized authority responsible for various activities like registration of vehicle users, OBUs, and RSUs [13,14]. These authorities are located in such a place where all the traffic is easily manageable. TAs have systems with high computational power, large storage capacity, and consume large amounts of power without any interruption. All these systems form the central infrastructure of the VANETs. These TAs can observe data traffic flowing in between various vehicles and can identify any suspicious activity. Various types of attacks may also be identified and stopped by taking appropriate action like removing a malicious node or stopping traffic from that malicious node. Different types of cryptographic keys are also initiated by these TAs.

Communication system: Vehicles can communicate with other vehicles using Dedicated Short Range Communication (DSRC) [15]. The information collected using this mechanism is not sufficient for managing vehicles and traffic. To get a wide range of information, the internet is used along with its infrastructure. Wireless Access in Vehicular Environment (WAVE) is also used for communication in VANETs [15]. On the other hand, 3G/4G/LTE cellular networks may be used for communication with other networks. Various types of communications take place in VANETs, which includes in-vehicle communication [16,17], vehicle to vehicle communication (V2V) [18,19], vehicle to infrastructure (V2I) [19], vehicle to pedestrians (V2P) [20], vehicle to grid (V2G) [21,22], vehicle to broadband cloud (V2B) [23], and vehicle to everything (V2X) [24]. Based on the above communication schemes one classification may be done which categorizes the VANETs in three types: pure ad hoc networks, cellular, and hybrid [25]. In pure ad hoc networks, vehicles and RSUs use DSRC for communication, and networks are completely transient. On the other hand, cellular networks are fixed and persistent even if these are used in VANETs or not. RSUs may use these cellular networks for communication with other RSUs or trusted authority. Hybrid VANET architectures use a combination of both the architectures.

2.2. VANET Applications

An application of VANET specifies where that VANET can be used. These networks are used for various purposes, and these applications can be categorized based on communication taking place between various entities. These entities may be vehicle to vehicle communication, vehicle to RSU communication, or any other [26]. Various applications are classified in four categories.

- *Safety applications* [27]: Safety applications include all those services which ensure the safety of vehicles and passengers traveling in these vehicles. Collision detection systems, real-time traffic information, and finding congestion-free paths are some of the services in this category.
- *Comfort applications* [28]: These applications are used for entertainment of the drivers and passengers in the vehicles such as audio and video facilities, and even gaming applications. On tolls, payment may be collected electronically, which saves time and fuel of customers and also saves the time of toll collectors. In big cities, parking is a big challenge, but with the help of VANET-based applications, it is easy to identify parking locations using VANET communications.
- *Commercial applications* [29]: Vehicles can download personalized settings of vehicles using the internet. Many companies use VANETs for providing security for rented cabs/vehicles. Commercial advertisements are used by companies to attract customers who are general drivers of vehicles. These advertisements may relate to restaurants, petrol pumps, hotels, etc.
- *Environmental applications* [30]: These applications use many sensors to get information from the environment, which proves beneficial to travelers. Vehicles may get information related to weather, and based on this information, traveling-related decisions are taken. For example, applications may suggest not using a path which may have snowfall, rainfall, or storm-like condition.

2.3. Features of VANETs

Security is important for all networks, but it is considered more crucial in VANETs, as it is related to human lives by providing congestion and the collision-free path to ambulances and vehicles. Various features of VANETs include the following [31,32].

- *Centralized security system*: In VANETs, a centralized security system is used, which is responsible for the implementation of security among all the nodes. Generally, servers are used for this. Packets are not monitored or rarely monitored in ad hoc networks, which make it more insecure. In these networks, either no security-protocol is used or used at very few occasions that make it more vulnerable to attacks.

- *Time constraint*: In critical situations, messages need to be forwarded within a specified time, otherwise collision cannot be avoided. On the other hand, the authenticity of these messages needs verification, which may lead to extra delays. Time constraint specifies that secure and authentic messages should be forwarded within a specified time.
- *Shared broadcast channel*: VANET is a wireless network that uses broadcast for transmission. Therefore, it is very easy for hackers to get the information traveling in these networks.
- *Volatility and no fixed topology*: Vehicles never move at the same speed and in the same direction, so it is not possible to maintain a network for a very long period. It is a short-lived communication network where an attacker may launch an attack and move from its location and escape. Moving vehicles leads to another issue of no fixed topology of the network. Without topology, routing becomes a difficult process to be implemented. Routes are frequently reconfigured, which increases routing overheads.
- *Infrastructure less*: VANET is an ad hoc network, and all the ad hoc networks do not contain any infrastructure. Although V2I communication considers RSUs and TAs as infrastructure, but still major infrastructure components like routers and servers are not used. Therefore, a trust relationship should be established among vehicles using reputation management systems. Other important features are Quality of Service (QoS), authentication, repudiation, scalability, heterogeneity, and multi-hop connection, etc.

2.4. Future of Vehicular Networks

Vehicular networks have the potential to safeguard the lives of millions of people all over the world. It can be implemented by all the developing countries and in all metropolitan cities of developed countries. It is expected that 64% of people of developing countries and 86% of people of developed countries will shift in urban areas by 2050 [33]. This increase in the population of urban areas will lead to an increase in traffic which may completely shut down the entire transport system if traffic will be regulated in an unmounted way. ITS with VANETs will surely replace the existing transport system and lots of advanced technologies and features will be included in it. Many countries have deployed various types of cameras and sensors at various locations for traffic regulations, e.g., cameras can find persons using mobile phones while driving. Moreover, in case of vehicle theft cases these cameras can immediately inform about their location after reading the number plate. In this way, the electric vehicles are also becoming part of IoTs [34]. Electric vehicles and automatic vehicles are going to play an important role in future vehicular networks. Many countries already have electric vehicle transport policies and many are considering them. Petrol pumps are also incorporating charging spots, and offices are also deploying these charging spots on their premises [35]. These vehicles can work in bidirectional mode by giving the electricity back to the electric grid with a good price [36]. For the sustainable growth of the world environment, these vehicles are going to be the soul of VANETs.

2.5. Security Requirements in Vehicular Networks

Security requirement specifies the attributes that should exist in any security solution. After observing various security aspects of VANET, services which are required by VANETs are discussed below [37,38].

Confidentiality: It is the process of making information visible only to those persons for whom this information is generated, and for other people it remains hidden. Sensitive information always requires confidentiality.

Integrity: It means receiving the same information that was sent by the sender. Information sent by the sender may be hacked in between, and may be re-transmitted after the alteration.

Availability: Requested services and resources should be always available to legitimate users whenever they require it.

Non-repudiation: It provides a kind of surety that data received by the receiver is sent by a genuine user and initiated from a protected source. It also makes sure that the integrity of data is also maintained.

Authentication: It ensures only authentic users are accessing that information or service, and only that section that belongs to them or for which they are authorized.

Authorization: It defines the kind and extent of information accessible by a particular user. In this, it is decided how much information may be accessed by the user, for what duration, and what other services the user can access.

Accounting: It means observing user activities and maintaining the record of it, like active time for which the user has used resources and services, and other relevant statistics. It is implemented using log files.

ID traceability: In this process, real identities of vehicles are identified, which locates the real source of the message [39]. In normal circumstances, these IDs are used to refer to the original sender and receiver.

Revocability: When any vehicle misbehaves in the network, central authority may revoke its certification and de-register it from the network. In this process, malicious nodes are removed from the network [40].

Liability identification: It is based on the non-repudiation service, which makes drivers liable for the mistakes they have made (if any).

Real-time Constraints: Vehicular information should always be delivered in real-time for better performance. Any kind of delay may lead to serious consequences [41].

3. Classification of Attacks in VANETs

Many informational attacks are launched against the vehicles and smart grids [37]. These networks are less secure because of no or minimum-security standards maintained for them. Various types of attacks are launched on the different layers of the network. These attacks may be categorized based on the security service which targets integrity, confidentiality, or availability [38]. It is necessary to understand the nature of the attack and the attacker with the motive behind the attacks. We have classified the VANET security attacks based on security services, attacker types, VANET layers, and VANET components.

3.1. Classification Based on Security Services

- *Attacks on confidentiality*: When the information is exchanged between vehicles, various solutions like public keys and certificates are used to encrypt the information and make it confidential. Still, attackers launch various kinds of attacks on the confidentiality of information using novel attack methods. Some common and popular attacks launched on the confidentiality of information include man-in-the-middle attack, traffic analysis attack, social attack, and eavesdropping attack.
- *Attacks on data integrity*: With the help of integrity, it is made sure that the information transferred is not modified, delayed, or deleted during the transmission process. Attacks that may be launched against this security service include masquerading attack, replay attack, message tampering attack, and illusion attack.
- *Attacks on availability*: Availability defines that all the information should be available to legitimate users when they require it. If data is not available to the right person at the right time, then it means vehicular networks are not working efficiently. Attacks that may be launched against this security service include DoS/DDoS, sleep deprivation, jamming attacks, jellyfish attack, intelligent cheater attack, blackhole attack, greyhole attack, greedy behavior attack, spamming attack, etc.

- *Attacks on authentication*: Authentication is also a significant service that ensures that the information is provided to users after proper cross-checking. This way, with the help of authentication, the share of information that belongs to a specific user is provided to that particular user only. However, still many types of attacks may be launched against authentications include sybil attack, tunneling attack, GPS spoofing, free-riding attack, certificate/key replication attack, etc.
- *Attacks on non-repudiation*: With the help of this service, it ensured that once after sending any particular message, the sender cannot say that he has not sent any message. In case of any dispute, this service provides proof regarding the message sent by the attacker. Repudiation attacks and loss of event are attacks in this category.

Some of the attacks in this category are shown in Table 1.

Table 1. Attack classification based on security services.

Attacked Layer	Type of Attack	Reference(s)
Confidentiality	Man-in-the-middle attack	Ahmad et al. (2018) [42], Li et al. (2012) [43]
	Traffic analysis attack	Cencioni et al. (2008) [44]
	Social attack	Sumra et al. (2011) [45]
	Eavesdropping attack	Choudhari et al. (2019) [46]
Integrity	Masquerading attack	Malhi et al. (2016) [47]
	Replay attack	Junaid et al. (2018) [48], Malik et al. (2019) [49]
	Message tampering attack	Singh and Sharma (2019) [50]
	Illusion attack	Lo and Tsai (2007) [51]
Availability	DoS/DDoS	Komal et al. (2014) [52], Almori et al. (2012) [53]
	Sleep deprivation	Vimal et al. (2012) [54] Hasrouny et al. (2017)[55]
	Jamming attacks	Hasrouny et al. (2017) [55], Azer et al. (2014) [56]
	Jellyfish attack	Vimal et al. (2012) [54], Sakiz et al. (2017) [57]
	Intelligent cheater attack	Sakiz et al. (2017) [57]
	Blackhole attack	Kshirsagar and Patil (2013) [58]
	Grayhole attack	Sen et al. (2007) [59]
	Greedy behaviour attack	Mejri et al. (2014) [60]
	Spamming attack	Sumra et al. (2011) [45]
Authenticity	Sybil attack	John et al. (2015) [61], Doucear J.R. (2002) [62]
	Tunnelling attack	Sheikh et al. (2019) [63]
	GPS spoofing	Gamal et al. (2020) [41]
	Free-riding attack	Shilpa et al. (2015) [64]
	Certificate/key replication attack	Junaid et al. (2018) [48]
Non-repudiation	Repudiation attack	Li et al. (2014) [65]

3.2. Classification Based on Attacker Type

In vehicular networks, there may be different kinds of attackers that may launch an attack using different methods [11,66]. VANET attackers may be classified as follows. Basic attacker categories are active and passive attackers. Active attackers are those who actively take part in the attack, while on the other hand, passive attackers, which are considered relatively less harmful, don't participate actively in the attack and just monitor the information. Additionally, we can classify them as internal and external attackers. These attackers are also known as insider and outsider attackers. Internal attackers are part of the network and they have full information about the network, but external attackers are not part of the network and do not have any kind of information about network structure. Another classification can be malicious and rational attackers. Rational attackers are those who launch an attack for the sake of money or some other personal reason like revenge, and malicious attackers on the other hand launch attacks without having any personal benefits. Furthermore, some other categories can also exist. Timing attacker modifies the timing involved in communication or inserts unnecessary delays in the communication [67]. Communication attacker selects a particular type of communication like V2V or V2I as a target and launches an attack against the VANET systems. Area attacker launches an attack on a specific vehicle or set of vehicles or on specific areas with some predetermined objectives.

3.3. Classification Based on VANET Layers

Vehicular networks are made up of different layers just like the OSI model [68]. All these layers may also become vulnerable under some attacks.

- *Application Layer* [69]: This layer is responsible for receiving the inputs from the user and forwarding it to further layers. All the application-based attacks try to modify the basic functionalities of this layer. The heterogeneity of VANET modules make it a greater concern to create a security baseline for this layer.
- *Transport layer* [70]: This layer ensures process to process delivery of messages. It also ensures that these messages are sent in proper order without any alteration. Replaying, tunneling, session hijacking, or message sequence tampering are some of the attack examples of this category.
- *Network layer* [71]: It propagates data packets from one node to another node. In VANETs security, concerns are not the same as in the case of other networks. Because it has features like topology, mobility, and network size, attacks launched on this network are also different. Location revealing and routing attacks are some of the examples in this layer.
- *LLC Layer and MAC layer* [72]: It helps in congestion control using various algorithms. Congestion control may be proactive, reactive, or it may be a hybrid. This layer performs the tasks of scheduling and contention window adjustment. The jamming and identity impersonation are some of the examples of vulnerabilities in this layer.
- *Physical layer* [72]: DSRC uses 802.11p OFDM that works in the frequency spectrum of 5.9 GHz band (5.885–5.905) with a 10 MHz wide channel. This type of communication data rate is generally 3 Mbps with a 6 Mbps default data rate. Eavesdropping, signal loss, and jamming are some of the attack examples in this layer. Analysis of such frequencies, even with speech signal in a compromised environment, is also very easy [73].

A list of layer-wise attacks in VANETs is shown in Table 2. We also provide a short and summarized table for attacks in Table 3. It shows that the application layer and network layer of VANETs are more vulnerable.

Table 2. Attack classification based on VANET layers.

Attacked Layer	Types of Attack	Reference(s)
Application layer	DoS and DDoS	Komal et al. (2014) [52], Almori et al. (2012) [53], Porwal et al. (2014) [74]
	Message tampering	Singh and Sharma (2019) [50]
	Impersonation attack	Tyagi et al. (2014) [75]
	Repudiation attack	Li et al. (2014) [65]
	Replay attack	Junaid et al. (2018) [48], Malik et al. (2019) [49]
	Illusion attacks	Lo and Tsai (2007) [51]
	False position attacks	Gamal et al. (2020) [41]
	Sybil attack	John et al. (2015) [61], Doucear J.R. (2002) [62]

Table 2. *Cont.*

Attacked Layer	Types of Attack	Reference(s)
Transport layer	DoS and DDoS attack	Komal et al. (2014) [52], Almori et al. (2012) [53], Porwal et al. (2014) [74]
	Replay attack	Junaid et al. (2018) [48], Malik et al. (2019) [49]
	Tunnel attacks	Sheikh et al. (2019) [63]
	Man in the middle attack	Ahmad et al. (2018) [42], Li et al. (2012) [43]
	Message tampering	Singh and Sharma (2019) [50]
	Session hijacking attack	Hasrouny et al. (2017) [55]
	Sybil attack	John et al. (2015) [61], Doucear J.R. (2002) [62]
Network layer	Location disclosure	Mansour et al. (2018) [76]
	Packet dropping	Mansour et al. (2018) [76]
	Flooding attack	Vimal et al. (2012) [54]
	Replay attack	Junaid et al. (2018) [48], Malik et al. (2019) [49]
	DoS and DDoS attack	Komal et al. (2014) [52], Almori et al. (2012) [53], Porwal et al. (2014) [74]
	Message tampering	Singh and Sharma (2019) [50]
	Sybil attack	John et al. (2015) [61], Doucear J.R. (2002) [62]
	Wormhole	Sen et al. (2007) [59]
	Blackhole attack	Kshirsagar and Patil (2013) [58]
	Routing attack	Kong et al. (2003) [77]
LLC Layer and MAC layer	DoS and DDoS attack	Komal et al. (2014) [52], Almori et al. (2012) [53], Porwal et al. (2014) [74]
	Illusion attacks	Lo and Tsai (2007) [51]
	Signal jamming attack	Karagiannis and Argyriou (2018) [78]
	Replay attack	Junaid et al. (2018) [48], Malik et al. (2019) [49]
	Impersonation attacks	Tyagi et al. (2014) [75]
	Message tampering	Singh and Sharma (2019) [50]
	Sybil attack	John et al. (2015) [61], Doucear J.R. (2002) [62]
	Collision attack	Tolba Amr (2018) [79], Mayank et al. (2016) [80]
Physical layer	DoS and DDoS attack	Komal et al. (2014) [52], Almori et al. (2012) [53], Porwal et al. (2014) [74]
	GPS spoofing attack	Gamal et al. (2020) [41]
	Jamming attack	Hasrouny et al. (2017) [55], Azer et al. (2014) [56]
	Message tampering	Singh and Sharma (2019) [50]
	Passive eavesdropping	Choudhari et al. (2019) [46]

Table 3. Specific and common attacks on VANET layers.

Type of Attack	Attack Layer
DoS and DDoS	All layers
Message tampering	All layers
Impersonation attack	Application, MAC
Repudiation attack	Application
Replay attack	Application, transport, network, MAC
Illusion attacks	Application, MAC

Table 3. *Cont.*

Type of Attack	Attack Layer
False position attacks	Application
Sybil attack	Application, transport, network, MAC
Tunnel attacks	Transport
Man in the middle attack	Transport
Session hijacking attack	Transport
Location disclosure	Network
Packet dropping	Network
Flooding attack	Network
Wormhole	Network
Blackhole attack	Network
Routing attack	Network
Signal jamming attack	MAC and LLC
Collision attack	MAC and LLC
GPS spoofing attack	Physical
Jamming attack	Physical
Message altering attack	Physical
Passive eavesdropping	Physical

3.4. Classification Based on VANET Components

We can also categorize the VANET attacks based on the components attacked. Three categories exist here. They are as follows.

(i) *Vehicles*: Vehicles are the mobile units which contain OBU and AU used in the communication. These mobile components may be easily targeted because these are the least secure units in the VANETs. Some of the attacks which may be launched against these units are social engineering attack, sensor impersonation attack, malware integration to vehicle attack, etc.

(ii) *Information*: Information which flows in all directions of the network is also targeted by the attacker by launching different novel attacks like eavesdropping, jamming spoofing, and false position attack, etc. These attacks may hamper both safety and non-safety applications of the network.

(iii) *Infrastructure*: It includes RSUs, central registration agency, charging spots of EVs, trusted authority, video cameras, and other components place alongside the road or at any other place like a parking place. Attacks that may be launched include network attack, DoS/DDoS, sybil attack, man in the middle attack, etc. The computer network software based attacks are also viable for VANET environment [81]. Component-based attacks are listed in Table 4.

Table 4. Attack classification based on different VANET components.

Attacked Component	Types of Attack	Reference(s)
Vehicles	Physical damage to the vehicle	Sumra et al. (2011) [45]
	Sensor impersonation attack	Rawat et al. (2012) [82]
	Bogus information attack	Singh and Sharma (2019) [50]
	Illegal remote firmware attack	Dennis and Larson (2009) [83]
	Jamming attack at vehicle level	Hasrouny et al. (2017) [55], Azer et al. (2014) [56]
	Social engineering attack	Sumra et al. (2011) [45]
	Malware integration	Hasrouny et al. (2017) [55]
	DoS and DDoS attack	Komal et al. (2014) [52], Almori et al. (2012) [53], Porwal et al. (2014) [74]
	Credential revelation	Whyte et al. (2013) [84]
Information	Fake information attack	Singh and Sharma (2019) [50]
	Impersonation attack	Tyagi et al. (2014) [75]
	False position attack	Gamal et al. (2020) [41]
	Message tempering	Singh and Sharma (2019) [50]
	Eavesdropping	Choudhari et al. (2019) [46]
	Man in the middle attack	Ahmad et al. (2018) [42], Li et al. (2012) [43]
	Spoofing attack	Gamal et al. (2020) [41]
	Jamming attacks	Hasrouny et al. (2017) [55], Azer et al. (2014) [56]
Infrastructure	Man in the middle attack	Ahmad et al. (2018) [42], Li et al. (2012) [43]
	GPS tracking attack	Singh and Sharma (2019) [50]
	Sybil attack	John et al. (2015) [61], Doucear J.R. (2002) [62]
	Network attacks	Sumra et al. (2011) [45]
	Bogus information	Singh and Sharma (2019) [50]
	DoS and DDoS attack	Komal et al. (2014) [52], Almori et al. (2012) [53], Porwal et al. (2014) [74]
	Wormhole attack	Sen et al. (2007) [59]

3.5. Attacks on Electric Vehicles

Electric Vehicles (EVs) [85] also play an important role in VANETs because these EVs can communicate with Smart Grids (SG) along with communication with vehicles and infrastructure. The automobile industry is concentrating on electric vehicles because in the future, all the vehicles are going to be electrical. These are not limited to few countries now, these are available across the globe, and these are increasing in numbers. Electric vehicles use smart charging to charge their battery in which data connection is shared by EV and charging device with the charging operator. Electric vehicles may use Grid to Vehicles (G2V) or Vehicle to Grids (V2G) systems for charging. Smart charging is a G2V charging system in which electricity moves in one direction that is from the charging point or grid to the vehicle. However, in the case of V2G charging, electricity moves in both directions. It means when the vehicle battery is low, it may be charged from the V2G point, and when the battery is having surplus electricity, then the V2G point may absorb that surplus electricity. This kind of electricity system works using smart grids [86]. A more advanced system of charging may be used in which smart grids are not used, instead a vehicle to vehicle charging system is used. In this method, vehicles meet at a particular location near to both and where these vehicles exchange electricity [87]. Various assets of electric vehicle which may be targeted by the attackers are access control policies, time, configuration data, software, firmware, and drivers, control commands, clock setting, meter data, tariff data, customer id, and location data, etc. [88]. All these assets are vulnerable to various kinds of threats that also affect other vehicular networks. Various ISO/IEC standards have been defined to provide security for the charging systems and the smart grids. All the attacks which may be launched against other vehicles may also be launched against electric vehicles. In addition to those attacks, many more attacks are possible against infrastructure used for vehicle charging and electricity distribution systems. So, additional security is required in the case of electric vehicles.

4. Security Solutions

To secure vehicular networks from the above-mentioned security issues, various solutions have been provided with help of different approaches [89,90]. A categorization of these solutions are described in the following subsections.

4.1. Identity-Based Solutions for VANETs

Identity-based security solution was first introduced by Adi Shamir in the year 1984, but implemented practically later in 2001 by Boneh and Franklin [90]. In identity (ID) based cryptography solutions, certificates are not used for verification of public keys as these are used in Public Key Infrastructure (PKI). In this system, identity information of an entity is used for generating the public keys. This information is publicly available like name, IP address, email address, etc. This was first used with bilinear pairings on elliptic curves. ID-Based Cryptographic (IBC) solutions are further divided into Identity-Based Encryption (IBE) and Identity Based Signatures (IBS). Some of the important solutions are mentioned here. An ID-based blind signature and ring signature are used in a solution [91]. It uses bilinear pairings for less computational overheads. Signatures are also used with Gap Diffie Hellman (GDH) groups [92]. Bilinear pairings are constructed for Computational Diffie-Hellman problem (CDHP). Small signature size increases the efficiency. Other ID-based ring signatures are used in [93,94]. Pairing computations are used with variable group size. The signature size is less, and therefore, computational complexity is less. Security frameworks based on cryptographic parameters are shown in [95,96]. No extra memory is used to map the pseudonymity. As VANETs are connected with IoE, security solutions are also important for grids. Such a solution is shown in [97]. It uses the Identity-based Key Infrastructure for Grid (IKIG) and uses gentry–Silverberg full HIBE and HIBS schemes. The least cost of computation and communication are the advantages of this solution. Privacy preservation with an ID-based scheme is shown in [98]. It observes a 92% improvement in various factors and also ensures less computation complexity. A solution using Elliptic Curve Cryptography (ECC) is shown in [99]. It uses general one-way hash functions in the process. It provides reduced single signature $cost = 0.4438$ ms and batch signature $cost = 0.442 + 0.0018n$ ms. A proficient message verification scheme is shown in [100]. It claims for less computational cost as compared to the traditional verification schemes. VANET-based Privacy-Preserving Communication Scheme (VPPCS) is shown in [101]. It uses ECC and ID-based encryption and ensures content and contextual privacy. A summarization of these solutions are listed in Table 5.

Table 5. List of ID-based solutions for VANETs

Reference(s)	Year	Service	Attack Type Handling	Research Gap
Zhang et al. [91]	2002	Anonymity, Privacy	Signature forgery	Implementation efficiency needs to be increased
Choon et al. [92]	2002	Confidentiality Authenticity	Forgery	Generic in nature and not for VANETs
Chow et al. [93]	2005	Confidentiality, Authenticity, Non-repudiation	Message and identity attack	Required improvement in signature generation and verification
Gamage et al. [94]	2006	Confidentiality, Authenticity	Forgery	Implementation efficiency needs to be increased

Table 5. *Cont.*

Reference(s)	Year	Service	Attack Type Handling	Research Gap
Kamat et al. [95]	2006	Authentication, Confidentiality, Non-repudiation, Integrity	Modification attack, Man-in-the-middle, Replay attack	Validation incomplete
Jinyuan et al. [96]	2010	Authentication, Non-repudiation, Integrity, Confidentiality	Forgery, Man-in-the-middle, Replay attack	Validation incomplete
Lim and Paterson [97]	2010	Confidentiality, Authenticity	Impersonation attack, Modification attack	More efficiency required in revoking public key certificates
He et al. [98]	2015	Confidentiality, Privacy	Impersonation attack, Modification attack, Man-in-the-middle, Replay attack, tolen verifier table attack	Validation is not successful in VANETs.
Ali et al. [99]	2019	Authentication	Forgery attack	Suitable only for V2V communication
Limbasiya et al. [100]	2019	Authentication, Privacy	Impersonation attack, Modification attack, Man-in-the-middle attack, Replay attack, Session key enclosure	Used only for V2ehicle to RSU communication
Al-shareeda et al. [101]	2020	Privacy	Impersonation attack, Modification attack, Man-in-the-middle, Replay attack	Validation incomplete

4.2. Key-Based Solutions for VANETs

This approach is more conventional than the ID-based cryptographic solutions. In this approach, public keys are used, which may be symmetric and asymmetric keys. These solutions are known as Public Key Infrastructure (PKI), but they also use private keys and hash functions as well. The main difference between these solutions and ID-based solutions is the use of certificates [102]. An Authenticated Routing protocol (ARAN) is shown in [103]. It uses certificates of authentication. Simplicity of the protocol make it significant to use in VANETs. Ariadne protocol is introduced in [104]. It uses initial route request timeout, maximum route request timeout, cache size, and cache replacement policy for the security purpose. 41.7% lower packet overhead has been achieved by this protocol. SEAD protocol is shown in [105]. Periodic route update interval, maximum packets buffered per node per destination, hash length (q), periodic updates: these parameters are used for the solution process. It claims to obtain a 95% packet delivery ration, which is very efficient. An explicit VANET oriented protocol is introduced in [44]. It enforces privacy in V2I communication; hence, it is named as Vehicle-to-Infrastructure communication Privacy Enforcement pRotocol (VIPER). It uses G (the group size), n (the message batch size), and pf (the probability of forwarding) for the security solution. VIPER is efficient in terms of low computations, reduced time delays, and less count of initialization messages. Another cryptography solution in this direction is noteworthy [43]. The solution named as Mobile Payment Protocol uses less communication and computation cost, and therefore, it is suitable for VANET applications. The summarization of this research is shown in Table 6.

Table 6. Authentication and authorization techniques for VANETs

Reference(s)	Year	Service	Attack Type Handling	Research Gap
Sanzgiri et al. [103]	2002	Authentication, Non-repudiation	Replay attack, Impersonation, Eavesdropping	Delays in route discovery
Hu et al. [104]	2002	Availability, Non-repudiation	DoS, Routing attack, Replay attack	More efficiency is required in PDR and computational overheads
Hu and Johnson [105]	2003	Authentication, Availability	DoS, Routing attack, Impersonation	Higher latency and overheads need to be improved.
Cencioni et al. [44]	2008	Confidentiality	Traffic Analysis Attack	Should be applicable in inter vehicle communication
Li et al. [43]	2012	Confidentiality	Man-in-the- Middle	Requirement of focus on time constraint

4.3. Trust-Based Solutions for VANETs

In dynamic VANETs condition, many vulnerabilities exist, as we have seen from the previous section. Therefore, it is very hard to make a decision on the parameter of trust, as the VANET environments are dynamic; vehicles can in and out on-the-fly leading to the frequent changes of the networks. However, trust in such networks is very much important and requires thorough development. Different existing trust models in VANETs can be segregated in two halves: data-oriented and entity-oriented. Data-oriented trust models focus on the data used while the communication and entity-oriented trust models focus on the trustworthiness of the drivers of vehicular entities. In [106], a solution for VANETs' security is provided with a trust-based system. It depends upon attack history and attack profiles. It can solve DoS/DDoS attack. Delay, average latency, packet delivery ratio, and energy consumption are considered as parameters. It claims for a detection rate 95.8%, average latency 30s, and packet delivery ratio is 86% in their obtained results. Another trust-based collaborative intrusion detection system is researched by Nandy et al. [107]. It is also able to provide security against DoS/DDoS attacks for availability services. Packet Drop Count (PDC), Packet Transfer Delay (PTD), and Packet Transfer Interval (PTI) are considered for experimentation. Intelligent cheater attacks can atill be launched in such trust-based environments.

4.4. Machine Learning and Deep Learning Solutions for VANETs

Among the available solutions for VAENTs, machine learning is well established and is proven to be very beneficial for prediction and analysis of the attacks. The machine learning and deep learning approaches are mostly used in preventing Denial of Service (DoS) and its variants. Various machine learning algorithms such as: Random Forest and Naïve-bayes [108–110], Support Vector Machine (SVM) [111–114], Artificial neural network (ANN) [115], K-clustering [109,116], neuro-fuzzy algorithms [117], decision tree based on features extracted [118], Markov chain integrated with ant-colony optimization [119], DeepVCM using CNN and LSTM [120,121] are used. Besides, some adaptive algorithms are also seen for intrusion detection in VANETs. For example, Heuristic-based adaptive IDS in [122]. Knot flow classification with spline implementation is shown in [123]. All these algorithms' performance are quite significant as they achieve approximately 90% of their accuracy related to their classification and detection of attacks. However, some of the limitations are also observed in these approaches. These solutions are summarized in Table 7.

Table 7. List of machine learning and deep learning-based solutions for VANETs

Reference(s)	Year	Service	Attack Handling	Research Gap
Grover et al. [108]	2011	Availability	DoS/DDoS	Not applicable for temporal attacks in a realistic scenario
Li et al. [111]	2015	Availability	DoS/DDoS	Validation not successful
Ghaleb et al. [115]	2017	Availability	DoS/DDoS	Validation is done without considering attacks of DoS/DDoS
Kim et al. [112]	2017	Availability	DoS/DDoS	Suitable only for software-defined VANET
Yu et al. [113]	2018	Availability	DoS/DDoS	Suitable only for software-defined VANET
Karagiannis and Argyriou [76]	2018	Availability	DoS/DDoS	Parametric evaluation not validated
Liang et al. [116]	2018	Availability	DoS/DDoS	Increased computational overheads
Kosmanos et al. [109]	2019	Availability	DoS/DDoS	Suitable for electric vehicles
Kaur et al. [117]	2019	Availability	DoS/DDoS	Parametric evaluation not validated
Aloqaily et al. [118]	2019	Availability	DoS/DDoS	The dataset is not VANET-based
Kolandaisamy et al. [119]	2019	Availability	DoS/DDoS	Parametric evaluation not validated
Zeng et al. [120]	2019	Availability	DoS/DDoS	Parametric evaluation not validated
Manimaran et al. [122]	2020	Availability	DoS/DDoS	Parametric evaluation not validated
Shahverdy et al. [121]	2020	Availability	DoS/DDoS	Non-reputational and non-trustable
Schmidt et al. [123]	2020	Availability	DoS/DDoS	Accuracy rate can be increased
Adhikary et al. [114]	2020	Availability	DoS/DDoS	Parametric evaluation not validated
Liu et al. [110]	2020	Availability	DoS/DDoS	Non-reputation and non-trustable

4.5. Hybrid Solutions for VANETs

Hybrid solutions use a combination of techniques to handle various vehicular attacks. Some of these attack solutions are provided in Table 8. Plausibility validation network is shown in [51]. Five sets of rules are used. Entropy-based solution for Distributed Denial of Service (DDoS) detection is shown in [60]. It uses data type and flag values for feature extraction. A secure genetic-based framework for VANETs is researched in [47]. It claims for 86.54% of accuracy in simulation. A mathematical model for security features for VANETs has been derived with features of lost packets, total busy time, total lost packets, etc. [124]. Attack vehicle detection is 100% accurate as claimed by the authors. A non-learning based method with drop-in packets feature is shown in [49]. With various types of vehicles and EV infrastructure, the VANETs are becoming heterogeneous in nature. A solution for such a network is shown based on communication framework with the hybrid information exchange [125]. Its uses waiting time, packet delivery ratio, and overhead analysis for the security measurements. All these algorithms are significant in VANETs, but having some limitations in their applicability or validation. A summarization of such problems and other security features are listed in Table 8.

Table 8. List of hybrid solutions for VANETs.

Reference(s)	Year	Services	Attack Handling	Research Gap
Lo and Tsai [51]	2007	Integrity	Illusion Attack	Performance not quantified
Mejri et al. [60]	2014	Availability	Greedy behavior attack	Handles only greedy behavior attacks
Malhi et al. [47]	2016	Integrity	Masquerade	Computational overheads reduction
Lahrouni et al. [124]	2017	Availability	DDoS attack	Root mean square (RMS), Mean Absolute Values (MAV) and Mean Squared Error (MSE) are not good evaluators
Malik et al. [49]	2019	Integrity	Replay Attack	Suitable in case of voice based systems only.
Li et al. [125]	2020	Availability	DoS/DDoS	Suitable only for EV infrastructure

4.6. Solutions for EV Infrastructure

EVs are the part of the vehicular networks and future generation transportation systems; it is necessary to provide security solutions for EV-based vehicular networks. Though the amount of research is less in this direction, some of the significant contribution are mentioned here. A privacy preserving scheme for EVs is researched in [126]. It uses Randomized Anonymous Credentials (RAC). The committed hashchains are used as one of the parameters. Some blockchain-based feasibility in security solutions of EV infrastructure are studied in [127,128]. Spatio-temporal parameters, roles, sessions, and environment of operation have been considered as parameters. A flatness control and rule-based algorithm for EVs are shown in [129]. It uses fuzzy logic to control the system and optimum value. It is more used for energy management in EV infrastructure. Use of lattice-based cryptography and SWIFFT hashing for EV communication is investigated in [130]. The use of lattice cryptography provides the less computational and communication complexity and moreover, the approach is post-quantum attack resistant. Another novel research has been found in this direction of EV-based security by using wavelet decomposition method [131]. A modified SVM is used for stability and proper classification of the security and insecurity of the incidents. The summarization of these solutions are shown in Table 9.

Table 9. List of security solutions for electric vehicles.

Reference(s)	Year	Service	Attack Type	Research Gap
Wan et al. [126]	2016	Authentication, privacy	Eavesdropping, Active adversaries	Suitable for V2G communication only
Liu et al. [127]	2018	Authentication, Non-repudiation	Tampering attack	Specific for cloud and edge computing
Kim et al. [128]	2019	Authentication	Replay attack, Man-in-the-middle	V2V communication needs to be discussed
Marzougui et al. [129]	2019	Availability	not specific	Used for energy management and not for communication
Kumar et al. [34]	2020	Confidentiality, Authentication, Non-repudiation	Authentication attacks	The trust management in aggregators requires focus.
Kavousi et al. [130]	2020	Availability, authentication	Message flooding	Computational overheads require more concentration

4.7. Comparison of Existing Surveys

Various surveys related to vehicular networks and related areas are observed in recent years. Attributes like architectures, attacks, and various solutions are mentioned in those surveys. In Table 10, we have shown the comparison of existing surveys along with our present survey to notify the potentials of our study. It shows that our study covers all the dimensions of the insecurity issues and security provisions, highlighting the significance of our study in the direction of VANETs.

Table 10. Comparison of various related studies in the timeline

Sr. No.	Author(s) & Reference	VANET Taxonomy	Attack Classifications	ID-Based Solutions	Key-Based Solution	Trust-Based Solutions	Machine Learning & Deep Learning Solutions	Hybrid Solutions	EV Solutions	Future Challenges
1	Cooper et al. (2017) [131]	Yes	No	No	No	No	No	No	No	Yes
2	Hasrouny et al. (2017) [55]	Yes	Yes	No	No	No	No	No	No	Yes
3	Manvi et al. (2017) [132]	Yes	Yes	No	No	No	No	No	No	No
4	Shahid et al. (2018) [133]	Yes	Yes	Yes	Yes	No	No	No	No	No
5	Tanwar et al. (2018) [89]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
6	Singh et al. (2018) [134]	Yes	No	No	No	No	No	No	No	No
7	Arif et al. (2019) [28]	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes
8	Sheikh et al. (2019) [63]	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes
9	Gamal et al. (2020) [41]	Yes	Yes	Yes	Yes	Yes	No	No	No	No
11	Present survey	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

5. Open Research Problems

VANETs are one of the concerning research domains as it is connected with IoTs and IoEs. The increasing number of vehicles, applications and sophisticated attack processes are making it hard to stabilize the security notions of VANETs. Therefore, with the technology progress, VANETs also require some futuristic developments for secure sustainability. In this section, we discuss some open research problems in a multi-dimensional way as future directions.

- *Dynamic topology*: Dynamic topology is an obvious feature of VANETs. When a vehicle sends a message, it passes through several intermediate nodes. The maliciousness of those nodes is always a question due to the ad hoc-ness. Therefore, research must be carried out to map these dynamic topologies in some directed acyclic graph and to compute some reputation system over it depending upon the past behavior or trust score. Another considerable aspect is that we can also try to use distributed ledgers for the transparency of the system transactions in this dynamic topology.
- *Real-time constraints*: The mobility of vehicular networks always has been a challenging issue. The real-time data monitoring, prediction of anomalies with high accuracy, and low false rates always have attracted the research community. Various machine learning and deep learning methods exist for these; however, we should explore more for collaborative learning or federated learning to gather the attack knowledge from the environment adaptive. This would help to detect the zero-day vulnerabilities in VANETs. As VANETs majorly use Dedicated Short-Range Communication (DSRC), the novel futuristic methods must support the short range communication maintaining the QoS of the networks.

- *Privacy*: Maintaining the privacy of user information is also an important research area. In today's VANETs or ITS, multimedia transmission is another issue. Users always prefer the seamless multimedia data transfer while moving from one place to another. These multimedia are controlled and stored by various clouds and service providers, and therefore, cloud security must be enhanced. On the other way, VANET security can also affect the cloud security. In both the cases, users' privacy must be protected. For example, the GPS-based location in taxi services must not unnecessarily reveal the user's travel behavior to a third party. The information that is sensitive and requires confidentiality, if leaked, may impact organizations by losing its credibility. Even users' personal information stored on a device from which multimedia is getting transferred using a VANET may be misused for financial frauds. Such vulnerabilities must be checked thoroughly, and necessary solutions need to be developed by all the possible stakeholders.
- *Liability and revocability*: It is based on the non-repudiation service which makes drivers liable for the mistakes they have made (if any). There may be vehicle drivers which can disturb the network or may launch some kind of attack. It includes a process of ID traceability in which real identities of vehicles are identified, which also locates the real source of the message. It is a real challenge to find the real attacker or malicious vehicle in the network due to camouflage identities; however, if such messages are detected, the network can be protected with prediction. Moreover, from the drivers' point of view, sentiment analysis of the drivers and the behavioral aspects can also work as attack enablers in VANETs, which needs to be explored further. When an attacker is identified or any vehicle user misbehaves in the network, central authority may revoke its certification and de-register it from the network. In this process, malicious nodes are removed from the network. In trust-based networks, it is very difficult to find the misbehaving node and then revoke the assigned privileges, and therefore, some suitable methods need to be developed.
- *Safe and economical hardware*: Vehicles should be deployed with tamper-proof hardware which will have more security as compared to software issues. These hardware components should be economical and within the budget of all the users. Though this is not directly technically connected, it is for making awareness to the VANET users to always go for validated trusted platforms of security hardware.
- *Network scale*: The increasing number of vehicles in VANETs are a concerning parameter. Many security solutions exist in the literature that are unable to address the scalability of the VANETs. For example, the generic security models use traditional PKIs, which are time consuming as compared to the advanced security provisions. Therefore, the progress of lattice based cryptography should be explored rigorously to enhance the performance of VANET security. The lightweight and less complex methods should be developed to scale the network efficiently.
- *Information authenticity*: In vehicular networks, there are different kinds of attacks in which the attacker may send fake messages using a spoofed identity. So the authenticity of the information is also an important research area. With the increasing number of multimedia forms and the increasing demand of the users, the information authenticity process also faces problems. For example, a user of a vehicle may be interested in some infotainment or it may be a simple document from their google drive; in such cases, different authenticity mechanisms are required, as infotainment requires seamless authentication and continuous availability of data stream.
- *Jamming*: There are various kinds of attacks in which radio interference are used to block the communication. These attacks may be launched against any wireless device. Therefore, it is perfectly suitable for VANETs. Jamming may be further classified into four categories, which are constant, deceptive, random, and reactive. In the existing literature, this jamming problem is less addressed, and therefore, it can be explored further with the new technologies.

- *Handling data*: With the increase in vehicular networks, it is expected that a massive amount of data will exist in these networks. These data are heterogeneous and distributed in nature and are stored in clouds. This growing amount of data and the size of the vehicular networks will lead to new and unique challenges in handling this data. Therefore, cloud storage security and backup security, and recovery and maintenance, should be some of the concerns to look out for in future ventures.
- *Access control*: VANETs consist of various layers of data communication such as V2V, V2I, or I2V. In each of these communications, proper access control is required. For example, a vehicle running on a road must not be able to access the other vehicle's infotainment system in V2V communication. Similarly, a vehicle must not be able to include its data in EV charging machine or RSUs. Only some controlled access must be allowed. Some decentralized mechanisms of access control and their verifiability must be researched.
- *Heterogeneity*: In vehicular networks, there are different kinds of OBUs, cellular transmitters, sensors, digital audio systems, GPS, etc. Therefore, the data is heterogeneous. A standard security model or the benchmark for VANET security is a missing link. It will be very much beneficial for VANETs to have such a baseline security attempting to detect the anomalies and adapting itself to increase the knowledge base for analysis of new vulnerabilities.
- *Attacks solution*: From the literature, we have observed that DoS/DDoS attacks are the major consideration in VANET security. This is true, as these attacks are executed in all the layers of VANETs and may take various forms. However, the other categories of attacks need to be explored for developing optimized security method.
- *IoE consideration*: The future of VANETs is closely connected with IoE that is connected with power generation units with various resources. The connection of vulnerabilities between VANETs and IoEs must be explored in all possible directions. Appropriate solutions must be developed to mitigate the risk of attacking energy infrastructure through VANET components.
- *Blockchain aspects*: The decentralization and distribute computing is one of the major enablers in the present technologies. Blockchain ensures these features efficiently. Therefore, such blockchain-based solutions can be beneficial for VANET security. The VANET infrastructural components can work in a transparent and decentralized way to account the transactions of data. However, methods should be developed to enhance this feature along with maintaining the required security services.

6. Conclusions

This survey is an attempt to cover different types of attacks in vehicular networks with security solutions. As an additional feature, we have added the electric vehicles for the future generation transport systems. Various attacks are classified according to attack layers, security services, types of attackers, and types of components targeted providing a multidimensional taxonomy of attacks. Relevant studies related to the solution approaches are compared to identify the advantages and disadvantages. Lastly, the open research problems are accumulated to give a future direction to the researchers in the directions of VANETs.

Author Contributions: A.V. derived the conceived the idea and analyzed the data. He also wrote the manuscript in consultation with R.S., G.K. and T.-h.K.; R.S. and G.K. supervised the work. All authors have read and agreed to the published version of the manuscript

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sirohi, D.; Kumar, N.; Rana, P.S. Convolutional neural networks for 5G-enabled Intelligent Transportation System: A systematic review. *Comput. Commun.* **2020**. [CrossRef]
2. Choffnes, D.R.; Bustamante, F.E. An integrated mobility and traffic model for vehicular wireless networks. In Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '05), Cologne, Germany, 2 September 2005.
3. Kumar, G.; Saha, R.; Rai, M.K.; Kim, T.H. Multidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication. *IEEE Access* **2018**, *6*, 46558–46567. [CrossRef]
4. Gkatzikis, L.; Koutsopoulos, I.; Salonidis, T. The Role of Aggregators in Smart Grid Demand Response Markets. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1247–1257. [CrossRef]
5. Bui, N.; Castellani, A.P.; Casari, P.; Zorzi, M. The internet of energy: A web-enabled smart grid system. *IEEE Netw.* **2012**, *26*, 39–45. [CrossRef]
6. Mohammad, S.A.; Rasheed, A.; Qayyum, A. VANET Architectures and Protocol Stacks: A Survey. *Commun. Technol. Veh.* **2011**, 95–105. [CrossRef]
7. Tomar, R.; Prateek, M.; Sastry, G.H. Vehicular Adhoc Network (VANET)—An Introduction. *Int. J. Control. Theory Appl.* **2016**, *9*, 8883–8888.
8. Balu, M.; Kumar, G.; Lim, S.-J. A review on security techniques in vanets. *Int. J. Control. Autom.* **2019**, *12*, 1–14. [CrossRef]
9. Paranjothi, A.; Khan, M.S.; Nijim, M.; Challoo, R. MAvanet: Message authentication in VANET using social networks. In Proceedings of the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 20–22 October 2016.
10. Papadimitratos, P.; Buttyan, L.; Holczer, T.; Schoch, E.; Freudiger, J.; Raya, M.; Hubaux, J.-P. Secure vehicular communication systems: Design and architecture. *IEEE Commun. Mag.* **2008**, *46*, 100–109. [CrossRef]
11. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]
12. Purkait, R.; Tripathi, S. Fuzzy Logic Based Multi-criteria Intelligent Forward Routing in VANET. *Wirel. Pers. Commun.* **2020**, *111*, 1871–1897. [CrossRef]
13. Salem, F.M.; Ali, A.S. SOS: Self-organized secure framework for VANET. *Int. J. Commun. Syst.* **2020**, e4317. [CrossRef]
14. Silva, C.M.; Masini, B.M.; Ferrari, G.; Thibault, I. A Survey on Infrastructure-Based Vehicular Networks. *Mob. Inf. Syst.* **2017**, *2017*, 1–28. [CrossRef]
15. Ho, K.Y.; Kang, P.C.; Hsu, C.H.; Lin, C.H. Implementation of WAVE/DSRC devices for vehicular communications. In Proceedings of the International Symposium on Computer, Communication, Control and Automation, Tainan, China, 5–7 May 2010; pp. 522–525.
16. Pauzie, A. In-vehicle communication systems: The safety aspect. *Inj. Prev.* **2002**, *8*, 26–29. [CrossRef]
17. Neumann, A.; Mytych, M.J.; Wesemann, D.; Wisniewski, L.; Jasperneite, J. Approaches for In-vehicle Communication—An Analysis and Outlook. *Commun. Comput. Inf. Sci.* **2017**, 395–411. [CrossRef]
18. Yang, X.; Liu, L.; Vaidya, N.H.; Zhao, F. A vehicle-to-vehicle communication protocol for cooperative collision warning. In Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), Boston, MA, USA, 22–26 August 2004.
19. Jurgen, R. V2V and V2I Technical Papers. In *V2V/V2I Communications for Improved Road Safety and Efficiency*; SAE: Warrendale, PA, USA, 2012.
20. Anaya, J.J.; Merdrignac, P.; Shagdar, O.; Nashashibi, F.; Naranjo, J.E. Vehicle to pedestrian communications for protection of vulnerable road users. In Proceedings of the 2014 IEEE Intelligent Vehicles Symposium Proceedings, Dearborn, MI, USA, 8–11 June 2014; pp. 1037–1042.
21. Guille, C.; Gross, G. A conceptual framework for the vehicle-to-grid (V2G) implementation. *Energy Policy* **2009**, *37*, 4379–4390. [CrossRef]
22. Loisel, R.; Pasaoglu, G.; Thiel, C. Large-scale deployment of electric vehicles in Germany by 2030: An analysis of grid-to-vehicle and vehicle-to-grid concepts. *Energy Policy* **2014**, *65*, 432–443. [CrossRef]
23. Heddebaut, M.; Rioult, J.; Ghys, J.P.; Gransart, C.; Ambellouis, S. Broadband vehicle-to-vehicle communication using an extended autonomous cruise control sensor. *Meas. Sci. Technol.* **2005**, *16*, 1363–1373. [CrossRef]
24. Campolo, C.; Molinaro, A.; Iera, A.; Menichella, F. 5G Network Slicing for Vehicle-to-Everything Services. *IEEE Wirel. Commun.* **2017**, *24*, 38–45. [CrossRef]
25. Qureshi, K.N.; Abdullah, A.H.; Anwar, R.W.; Anwar, M.; Awan, K.M. Aegrp: An enhanced geographical routing protocol for vanet. *J. Teknol.* **2016**, *78*. [CrossRef]
26. Kumar, V.; Mishra, S.; Chand, N. Applications of VANETs: Present & future. *Commun. Netw.* **2013**, *5*, 12. [CrossRef]
27. National Highway Traffic Safety Administration (NHTSA). *Vehicle Safety Communications Project Task3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC*; Technical Report DOT HS; US Department of Transportation: Washington, DC, USA, 2005; pp. 809–859.
28. Arif, M.; Wang, G.; Zakirul Alam Bhuiyan, M.; Wang, T.; Chen, J. A Survey on Security Attacks in VANETs: Communication, Applications and Challenges. *Veh. Commun.* **2019**, 100179. [CrossRef]

29. Mak, T.K.; Laberteaux, K.P.; Sengupta, R. A multi-channel VANET providing concurrent safety and commercial services. In Proceedings of the 2nd ACM International Workshop on Vehicular Adhoc Networks, Cologne, Germany, 22–26 September 2005.
30. Hartenstein, H.; Laberteaux, K. (Eds.) *VANET: Vehicular Applications and Inter-Networking Technologies*; John Wiley & Sons: New York, NY, USA, 2009; Volume 1.
31. Sadatpour, V.; Zargari, F.; Ghanbari, M. A Collision Aware Opportunistic Routing Protocol for VANETs in Highways. *Wirel. Pers. Commun.* **2019**, *109*, 175–188. [CrossRef]
32. Zhu, L.; Zhang, C.; Xu, C.; Du, X.; Guizani, N.; Sharif, K. Traffic Monitoring in Self-Organizing VANETs: A Privacy-Preserving Mechanism for Speed Collection and Analysis. *IEEE Wirel. Commun.* **2019**, *26*, 18–23. [CrossRef]
33. Englund, C.; Chen, L.; Vinel, A.; Lin, S.Y. Future Applications of VANETs. *Veh. Hoc Netw.* **2015**, 525–544. [CrossRef]
34. Kumar, G.; Rai, M.; Saha, R.; Buchanan, W.J.; Thomas, R.; Geetha, G.; Rodrigues, J. A Privacy-Preserving Secure Framework for Electric Vehicles in IoT using Matching Market and Signcryption. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7707–7722. [CrossRef]
35. Wang, M.; Liang, H.; Deng, R.; Zhang, R.; Shen, X.S. VANET based online charging strategy for electric vehicles. In Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; pp. 4804–4809.
36. Gago, R.G.; Pinto, S.F.; Silva, J.F. G2V and V2G electric vehicle charger for smart grids. In Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2), Trento, Italy, 12–15 September 2016; pp. 1–6.
37. Liu, J.; Xiao, Y.; Li, S.; Liang, W.; Chen, C.P. Cyber security and privacy issues in smart grids. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 981–997. [CrossRef]
38. Stallings, W. *Cryptography and Network Security: Principles and Practice*; Prentice Hall: Upper Saddle River, NJ, USA, 1999.
39. Mokthar, B.; Azab, M. Survey on security issues in vehicular ad hoc networks. *Alex. Eng. J.* **2015**, *54*, 1115–1126. [CrossRef]
40. Pathre, A.; Agrawal, C.; Jain, A. Identification of malicious vehicle in vanet environment from ddos attack. *Int. J. Glob. Res. Comput. Sci.* **2013**, *4*, 30–34.
41. Gamal, M.S.; Nasr, A.A.; Nouh, S.A. Vanet Security: Defense and detection, a review. *J. Azhar Univ. Eng. Sect.* **2020**, *15*, 810–827. [CrossRef]
42. Ahmad, F.; Adnane, A.; Franqueira, V.N.; Kurugollu, F.; Liu, L. Man-in-the-middle attacks in vehicular ad hoc networks: Evaluating the impact of attackers' strategies. *Sensors* **2018**, *18*, 4040. [CrossRef]
43. Li, W.; Wen, Q.; Su, Q.; Jin, Z. An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. *Comput. Commun.* **2012**, *35*, 188–195. [CrossRef]
44. Cencioni, P.; Di Pietro, R. A mechanism to enforce privacy in vehicle-to-infrastructure communication. *Comput. Commun.* **2008**, *31*, 2790–2802. [CrossRef]
45. Sumra, I.A.; Ahmad, I.; Hasbullah, H. Classes of attacks in VANET. In Proceedings of the 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC), Riyadh, Saudi Arabia, 24–26 April 2011.
46. Choudhari, D.P.; Dorle, S.S. Maximization of packet delivery ratio for DADCQ protocol after removal of Eavesdropping and DDoS attacks in VANET. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; pp. 1–8.
47. Malhi, A.K.; Batra, S. Genetic-based framework for prevention of masquerade and DDoS attacks in vehicularad hocnetworks. *Secur. Commun. Netw.* **2016**, *9*, 2612–2626. [CrossRef]
48. Hezam Al Junaid, M.A.; Syed, A.A.; Mohd Warip, M.N.; Fazira Ku Azir, K.N.; Romli, N.H. Classification of Security Attacks in VANET: A Review of Requirements and Perspectives. In Proceedings of the MATEC Web of Conferences, Lille, France, 8–10 October 2018.
49. Malik, K.M.; Malik, H.; Baumann, R. Towards Vulnerability Analysis of Voice-Driven Interfaces and Countermeasures for Replay Attacks. In Proceedings of the 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), San Jose, CA, USA, 28–30 March 2019.
50. Singh, K.; Sharma, S. Advanced Security Attacks on Vehicular AD HOC Network (VANET). *Int. J. Innov. Technol. Explor. Eng.* **2019**, *9*, 2278–3075.
51. Lo, N.; Tsai, H. Illusion Attack on VANET Applications—A Message Plausibility Problem. In Proceedings of the 2007 IEEE Globecom Workshops, Washington, DC, USA, 26–30 November 2007; pp. 1–8.
52. Komal, B.; Sahare, D.R.; Malik, L.G. An approach for detection of attack in VANET. In Proceedings of the International Conference on Industrial Automation and Computing (ICIAC), Strathclyde, UK, 2–4 September 2014.
53. Alomari, E.; Manickam, S.; Gupta, B.; Karuppayah, S.; Alfaris, R. Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *Int. J. Comput. Appl.* **2012**, *49*, 24–32. [CrossRef]
54. Bibhu, V.; Roshan, K.; Singh, K.B.; Singh, D.K. Performance Analysis of Black Hole Attack in Vanet. *Int. J. Comput. Netw. Inf. Secur.* **2012**, *4*, 47–54. [CrossRef]
55. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]
56. Marianne, A.; Noha, G.; Sherif, M.; Ahmed, E. Jamming Attacks on VANETs. In Proceedings of the International Conference on Big Data Science and Computing, Beijing, China, 4–7 August 2014.
57. Sakiz, F.; Sen, S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Hoc Netw.* **2017**, *61*, 33–50. [CrossRef]

58. Kshirsagar, D.; Patil, A. Blackhole attack detection and prevention by real time monitoring. In Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 4–6 July 2013; pp. 1–5.
59. Sen, J.; Chandra, M.G.; Harihara, S.G.; Reddy, H.; Balamuralidhar, P. A mechanism for detection of gray hole attack in mobile Ad Hoc networks. In Proceedings of the 2007 6th International Conference on Information, Communications & Signal Processing, Singapore, 10–13 December 2007; pp. 1–5.
60. Mejri, M.N.; Ben-Othman, J. Entropy as a new metric for denial of service attack detection in vehicular ad hoc networks. In Proceedings of the 17th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems-MSWiM '14, Montreal, QC, Canada, 21–26 September 2014.
61. John, R.; Cherian, J.P.; Kizhakkethottam, J.J. A survey of techniques to prevent sybil attacks. In Proceedings of the 2015 International Conference on Soft-Computing and Networks Security (ICSNS), Coimbatore, India, 25–27 February 2015; pp. 1–6.
62. Douceur J.R. The Sybil Attack. In *Peer-to-Peer Systems. IPTPS 2002*; Druschel, P., Kaashoek, F., Rowstron, A., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2429.
63. Sheikh, M.S.; Liang, J.; Wang, W. A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). *Sensors* **2019**, *19*, 3589. [CrossRef]
64. Shilpa, P.; Patil, R.B. Cooperative message authentication and resisting free riding attacks in VANETS. *Int. Res. Eng. Technol.* **2015**, *4*, 127–131.
65. Li, J.; Lu, H.; Guizani, M. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 938–948. [CrossRef]
66. Leinmuller, T.; Schmidt, R.K.; Schoch, E.; Held, A.; Schafer, G. Modeling Roadside Attacker Behavior in VANETs. In Proceedings of the 2008 IEEE Globecom Workshops, New Orleans, LA, USA, 30 November–4 December 2008.
67. Upadhyaya, A.N.; Shah, J.S. Attacks on vanet security. *Int. J. Comp. Eng. Technol.* **2018**, *9*, 8–19.
68. Liang. W.; Li, Z.; Zhang, H.; Wang, S.; Bie, R. Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends. *Int. J. Distrib. Sens. Netw.* **2015**. [CrossRef]
69. Wang, Y.; Ding, Z.; Li, F.; Xia, X.; Li, Z. Design and implementation of a VANET application complying with WAVE protocol. In Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017.
70. Shah, J.C.; Patel, K.; Trapasiya, S.D.; Rathod, J.M. Study for Implementation of VANET with Transport Layer Protocol. *Int. J. Comput. Appl.* **2014**, *975*, 8887.
71. Ilavendhan, A.; Saruladha, K. Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs. *ICT Express* **2018**, *4*, 46–50. [CrossRef]
72. Khan, U.A.; Lee, S.S. Multi-Layer Problems and Solutions in VANETs: A review. *Electronics* **2019**, *8*, 204. [CrossRef]
73. Kataeva, E.; Yakimuk, A.; Konev, A.; Shelupanov, A. Metric of Highlighting the Synchronicity of Time Series and Its Application in Analyzing the Fundamental Frequencies of the Speaker's Speech Signal. *Symmetry* **2020**, *12*, 1943. [CrossRef]
74. Porwal, V.; Patel, R.; Kapoor, D.R. An investigation of DoS flooding attack in VANET. *Int. J. Adv. Found. Res. Comput.* **2014**, *1*, 158–169.
75. Tyagi, P.; Dembla, D. Investigating the security threats in Vehicular ad hoc Networks (VANETs): Towards security engineering for safer on-road transportation. In Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, India, 24–27 September 2014; pp. 2084–2090.
76. Mansour, M.B.; Salama, C.; Mohamed, H.K.; Hammad, S.A. VANET Security and Privacy-An Overview. *Int. J. Netw. Secur. Its Appl.* **2018**, *10*. [CrossRef]
77. Kong, J.; Hong, X.; Gerla, M. A new set of passive routing attack in Mobile ad hoc networks. In Proceedings of the IEEE Military Communication Conference MILCOM, Boston, MA, USA, 13–16 October 2003.
78. Karagiannis, D.; Argyriou, A. Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning. *Veh. Commun.* **2018**, *13*, 56–63. [CrossRef]
79. Tolba, A.M.R. Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs. *IEEE Access* **2018**. [CrossRef]
80. Bhatt, M.; Sharma, S.; Prakash, A.; Pandey, U.S.; Jyoti, K. Traffic Collision Avoidance in VANET Using Computational Intelligence. *Int. J. Eng. Technol.* **2016**, *8*, 364–370.
81. Novokhrestov, A.; Konev, A.; Shelupanov, A. Model of Threats to Computer Network Software. *Symmetry* **2019**, *11*, 1506. [CrossRef]
82. Rawat, A.; Sharma, S.; Sushil, R. VANET: Security attacks and its possible solutions. *J. Inf. Oper. Manag.* **2012**, *3*, 301.
83. Dennis, O.; Ulf, L. A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure. *J. Netw.* **2009**, *4*. [CrossRef]
84. Whyte, W.; Weimerskirch, A.; Kumar, V.; Hehn, T. A Security Credential Management System for V2V Communications. In Proceedings of the IEEE Vehicular Networking Conference, Ulm, Germany, 16–18 December 2013.
85. Wang, M.; Zhang, R.; Shen, X. Mobility-Aware Coordinated EV Charging in VANET-Enhanced Smart Grid. *Mob. Electr. Veh.* **2015**, 21–54. [CrossRef]
86. Saxena, N.; Choi, B. State of the Art Authentication, Access Control, and Secure Integration in Smart Grid. *Energies* **2015**, *8*, 11883–11915. [CrossRef]

87. Li, G.; Sun, Q.; Boukhatem, L.; Wu, J.; Yang, J. Intelligent Vehicle-to-Vehicle Charging Navigation for Mobile Electric Vehicles via VANET-Based Communication. *IEEE Access* **2009**, *7*, 170888–170906. [CrossRef]
88. Falk, R.; Fries, S. Electric vehicle charging infrastructure security considerations and approaches. In Proceedings of the INTERNET, Helsinki, Finland, 17 August 2012; pp. 58–64.
89. Tanwar, S.; Vora, J.; Tyagi, S.; Kumar, N.; Obaidat, M.S. A systematic review on security issues in vehicular ad hoc network. *Secur. Priv.* **2018**. [CrossRef]
90. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil Pairings. In *Advances in Cryptology-Asiacrypt*; Springer: New York, NY, USA, 2001; pp. 514–532.
91. Zhang, F.; Kim, K. ID-based blind signature and ring signature from pairings. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, 1–5 December 2002; pp. 533–547.
92. Choon, J.C.; Hee Cheon, J. An Identity-Based Signature from Gap Diffie-Hellman Groups. In *International Workshop on Public Key Cryptography*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; pp. 18–30. [CrossRef]
93. Chow, S.S.M.; Yiu, S.-M.; Hui, L.C.K. Efficient Identity Based Ring Signature. In *International Conference on Applied Cryptography and Network Security*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; pp. 499–512. [CrossRef]
94. Gamage, C.; Gras, B.; Crispo, B.; Tanenbaum, A.S. An identity-based ring signature scheme with enhanced privacy. In Proceedings of the 2006 Securecomm and Workshops, Baltimore, MD, USA, 28 August–1 September 2006; pp. 1–5.
95. Kamat, P.; Baliga, A.; Trappe, W. An identity-based security framework For VANETs. In Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks—VANET '06, Los Angeles, CA, USA, 29 September 2006.
96. Sun, J.; Zhang, C.; Zhang, Y.; Fang, Y. An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks. *IEEE Trans. Parallel Distrib. Syst.* **2010**, *21*, 1227–1239. [CrossRef]
97. Lim, H.W.; Paterson, K.G. Identity-based cryptography for grid security. *Int. J. Inf. Secur.* **2010**, *10*, 15–32. [CrossRef]
98. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
99. Ali, I.; Lawrence, T.; Li, F. An Efficient Identity-Based Signature Scheme without Bilinear Pairing for Vehicle-To-Vehicle Communication in VANETs. *J. Syst. Archit.* **2019**, 101692. [CrossRef]
100. Limbasiya, T.; Das, D. Identity based proficient message verification scheme for vehicle users. *Pervasive Mob. Comput.* **2019**, *60*, 101083. [CrossRef]
101. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Yassin, A.A. VPPCS: VANET-Based Privacy-Preserving Communication Scheme. *IEEE Access* **2020**, *8*, 150914–150928. [CrossRef]
102. Paterson, K.G.; Price, G. A comparison between traditional public key infrastructures and identity-based cryptography. *Inf. Secur. Tech. Rep.* **2003**, *8*, 57–72. [CrossRef]
103. Sanzgiri, K.; Dahill, B.; Levine, B.N.; Shields, N.; Belding-Royer, E.M. A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12–15 November 2002; pp. 78–87.
104. Hu, Y.C.; Perrig, A.; Johnson, D.B. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of the MobiCom'02, Atlanta, GA, USA, 23–26 September 2002; pp. 23–26.
105. Hu, Y.-C.; Johnson, D.B.; Perrig, A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Netw.* **2003**, *1*, 175–192. [CrossRef]
106. Poongodi, M.; Hamdi, M.; Sharma, A.; Ma, M.; Singh, P.K. DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET. *IEEE Access* **2019**, *7*, 183532–183544. [CrossRef]
107. Nandy, T.; Noor, R.M.; Yamani Idna Bin Idris, M.; Bhattacharyya, S. T-BCIDS: Trust-Based Collaborative Intrusion Detection System for VANET. In Proceedings of the 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), Durgapur, India, 12–18 March 2020; pp. 1–5.
108. Grover, J.; Prajapati, N.K.; Laxmi, V.; Gaur, M.S. Machine learning approach for multiple misbehavior detection in VANET. *Commun. Comput. Inf. Sci.* **2011**, *192*, 644–653.
109. Kosmanos, D.; Pappas, A.; Maglaras, L.; Moschoyiannis, S.; Aparicio-Navarro, F.J.; Argyriou, A.; Janicke, H. A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles. *Array* **2019**, 100013. [CrossRef]
110. Liu, T.; Shi, S.; Gu, X. Naive Bayes Classifier Based Driving Habit Prediction Scheme for VANET Stable Clustering. *Mob. Netw. Appl.* **2020**. [CrossRef]
111. Li, W.; Joshi, A.; Finin, T. SVM-CASE: An SVM-based context aware security framework for vehicular ad hoc networks. In Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston, MA, USA, 6–9 September 2015; pp. 1–5.
112. Kim, M.; Jang, I.; Choo, S.; Koo, J.; Pack, S. Collaborative security attack detection in software-defined vehicular networks. In Proceedings of the 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), Seoul, Korea, 27–29 September 2017; pp. 19–24.
113. Yu, Y.; Guo, L.; Liu, Y.; Zheng, J.; Zong, Y. An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks. *IEEE Access* **2018**, *6*, 44570–44579. [CrossRef]
114. Adhikary, K.; Bhushan, S.; Kumar, S.; Dutta, K. Hybrid Algorithm to Detect DDoS Attacks in VANETs. *Wirel. Pers. Commun.* **2020**. [CrossRef]

115. Ghaleb, F.A.; Zainal, A.; Rassam, M.A.; Mohammed, F. An Effective Misbehavior Detection Model using Artificial Neural Network for Vehicular Ad hoc Network Applications. In Proceedings of the 2017 IEEE Conference on Application, Information and Network Security (AINS), Sarawak, Malaysia, 13–14 November 2017; pp. 13–18.
116. Liang, J.; Chen, J.; Zhu, Y.; Yu, R. A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position. *Appl. Soft Comput.* **2018**. [CrossRef]
117. Kaur, J.; Singh, T.; Lakhwani, K. An Enhanced Approach for Attack Detection in VANETs Using Adaptive Neuro-Fuzzy System. In Proceedings of the 2019 International Conference on Automation, Computational and Technology Management (ICACTM), London, UK, 24–26 April 2019.
118. Aloqaily, M.; Otoum, S.; Ridhawi, I.A.; Jararweh, Y. An Intrusion Detection System for Connected Vehicles in Smart Cities. *Ad Hoc Netw.* **2019**. [CrossRef]
119. Kolandaisamy, R.; Noor, R.M.; Zaba, M.R.; Ahmedy, I.; Kolandaisamy, I. Markov Chain Based Ant Colony Approach for Mitigating DDoS Attacks Using Integrated Vehicle Mode Analysis in VANET. In Proceedings of the 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP), Chennai, India, 4–6 July 2019.
120. Zeng, Y.; Qiu, M.; Zhu, D.; Xue, Z.; Xiong, J.; Liu, M. DeepVCM: A Deep Learning Based Intrusion Detection Method in VANET. In Proceedings of the 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 25–28 May 2019.
121. Shahverdy, M.; Fathy, M.; Berangi, R.; Sabokrou, M. Driver Behavior Detection and Classification Using Deep Convolutional Neural Networks. *Expert Syst. Appl.* **2020**, 113240. [CrossRef]
122. Manimaran, P. NDNIDS: An Intrusion Detection System for NDN Based VANET. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5.
123. Schmidt, D.A.; Khan, M.S.; Bennett, B.T. Spline-based intrusion detection for VANET utilizing knot flow classification. *Internet Technol. Lett.* **2020**. [CrossRef]
124. Lahrouni, Y.; Pereira, C.; Bensaber, B.A.; Biskri, I. Using Mathematical Methods Against Denial of Service (DoS) Attacks in VANET. In Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access-MobiWac '17, Miami, FL, USA, 21–25 November 2017.
125. Li, G.; Li, X.; Sun, Q.; Boukhatem, L.; Wu, J. An Effective MEC Sustained Charging Data Transmission Algorithm in VANET-Based Smart Grids. *IEEE Access* **2020**, *8*, 101946–101962. [CrossRef]
126. Wan, Z.; Zhu, W.T.; Wang, G. PRAC: Efficient privacy protection for vehicle-to-grid communications in the smart grid. *Comput. Secur.* **2016**, *62*, 246–256. [CrossRef]
127. Liu, H.; Zhang, Y.; Yang, T. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. *IEEE Netw.* **2018**, *32*, 78–83. [CrossRef]
128. Kim, M.; Park, K.; Yu, S.; Lee, J.; Park, Y.; Lee, S.W.; Chung, B. A secure charging system for electric vehicles based on blockchain. *Sensors* **2019**, *19*, 3028. [CrossRef] [PubMed]
129. Marzougui, H.; Kadri, A.; Martin, J.P.; Amari, M. Implementation of energy management strategy of hybrid power source for electrical vehicle. *Energy Convers. Manag.* **2019**, *195*, 830–843. [CrossRef]
130. Kavousi-Fard, A.; Jin, T.; Su, W.; Parsa, N. An Effective Anomaly Detection Model for Securing Communications in Electric Vehicles. *IEEE Trans. Ind. Appl.* **2020**. [CrossRef]
131. Cooper, C.; Franklin, D.; Ros, M.; Safaei, F.; Abolhasan, M. A Comparative Survey of VANET Clustering Techniques. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 657–681. [CrossRef]
132. Manvi, S.S.; Tangade, S. A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.* **2017**, *9*, 19–30. [CrossRef]
133. Shahid, M.A.; Jaekel, A.; Ezeife, C.; Al-Ajmi, Q.; Saini, I. Review of potential security attacks in VANET. In Proceedings of the 2018 Majan International Conference (MIC), Muscat, Oman, 31 October 2018; pp. 1–4.
134. Singh, D.; Ranvijay, N.A.; Yadav, R.S. A state-of-art approach to misbehaviour detection and revocation in VANET: Survey. *Int. J. Hoc Ubiquitous Comput.* **2018**, *28*, 77. [CrossRef]