Internet of Vehicles: Architectures, Applications and Challenges - Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2018, Vol. 14(12)

DOI: 10.1177/1550147718815054
journals.sagepub.com/home/dsn
SAGE

Systematic literature review on Internet-of-Vehicles communication security

Manar Abu Talib[1], Sohail Abbas[1], Qassim Nasir[2] and Mohamad Fouzi Mowakeh[2]

Abstract

Currently, the popularity of Internet-of-Vehicles technology and self-driving cars are increasing rapidly. Several companies are investing in this field and are competing to release the latest and safest autonomous cars. However, this rapid Internet-of-Vehicles development also creates many security problems, which are considered a significant threat both to industry and to consumers. As a result, there is an urgent need to study the possible security threats and different solutions that can ensure the safety of drivers and also the security of industry. This research article focuses on examining the systematic literature on Internet-of-Vehicles and security. It also provides comprehensive and unbiased information regarding various state-of-the-art security problems, solutions, and proposals in vehicular ad hoc networks and Internet-of-Vehicles. Systematic literature review is used for more than 127 different research articles published between the years 2010 and 2018. The results of the systematic literature review used are categorized into the following three main categories: (1) the different types of attacks on Internet-of-Vehicles, (2) the different solutions that can be implemented to solve the threats, and (3) the performance outcomes.

Keywords

Internet-of-Vehicles, security, authenticity, integrity, confidentiality, availability

Date received: 30 June 2018; accepted: 2 October 2018

Handling Editor: Syed Hassan Ahmed

Introduction

Vehicular ad hoc network (VANET) is a special type of network evolved from mobile ad hoc network (MANET) and is formed in a fully self-organized manner. It is composed of mobile vehicles and is constructed in ad hoc fashion. Communication in VANETs is facilitated by various short and long-range wireless technologies in order to establish inter-vehicle and vehicle-to-roadside communication.[1–4] Some of the prominent applications of VANETs include efficient traffic management, congestion monitoring, and drivers' safety and comfort. Since their inception, these networks have been an active area of research in both industry and academia. VANETs are mostly appropriate for small-scale services or for short-term applications, such as congestion avoidance, and hazard and accident prevention. However, due to their lack of processing and communication capability for handling global information collected from other vehicles and systems, VANETs have limited contemporary applications. In order to accommodate a broad range of contemporary applications, vehicles in VANETs are

[1]Department of Computer Science, University of Sharjah, Sharjah, UAE
[2]Department of Electrical and Computer Engineering, University of Sharjah, Sharjah, UAE

Corresponding author:
Manar Abu Talib, Department of Computer Science, University of Sharjah, 27272 Sharjah, UAE.
Email: mtalib@sharjah.ac.ae

required to communicate with infrastructure, Internet, and people. These evolved VANETs are called Internet-of-Vehicles (IoV) or Internet-of-Connected Vehicles (IoCV), which basically follows the Internet-of-Things (IoT) paradigm. In IoV, each network entity may act as a "smart" object and may enjoy ubiquitous connectivity to the Internet enabling the integration of humans, things, vehicles, networks, and infrastructures in order to establish an intelligent network that will support various services for large cities or even for a country (i.e. intelligent transport system for a city, road conditions, safety services).[5–8] According to recent research, billion things, where vehicles are considered, many of these things, will be connected to the Internet by 2020. IoV connects between vehicles and living things allowing them to send and receive data. There are three communication types of IoV: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-cloud (V2C). IoV has played a vital role in the emergence of smart cities by introducing better navigation, benefits for managing real-time traffic information, and by managing the safety of drivers and passengers.[9–13] However, the rapid pace of IoV development creates many security problems, which are considered a major threat to both industry and consumers' lives. As a result, there is an urgent need to do a detailed study on the possible security threats and the different solutions that can guarantee the safety of both drivers and industry as well. In this article, we will discuss the different types of attacks that autonomous cars might face, and the possible solutions for all or some of these problems and how these solutions may affect performance in general.

We have started collecting papers and have now reached 127 different research papers, which we then started filtering according to our requirements, by removing the papers that are related to physical security or to other vehicles than cars. We were then left with 74 different research papers that address the security risks and solutions for IoV and VANETs communication and protoco. In the following literature review section, the security and privacy issues in VANETs and IoV, as well as the related work on solving these issues in the connected vehicles arena, are demonstrated. In the "Methodology" section, we explain the systematic literature review (SLR) which consists of planning, conducting the research, and reporting. In section "Survey results," we discuss our findings on the predefined research questions. A survey conducted based on papers from 2010-2018 discusses the security challenges and the solutions in the IoV's (or VANET) protocols and how the performance will be affected after applying a solution. Then in section "Discussion and future directions," we present further discussions and possible future directions. Finally, we conclude in the last section.

Literature review

Security and privacy issues in VANETs and IoV

In this section, we discuss the security and privacy issues that are present in both VANETs and IoV. Because the IoV is evolved from VANETs, there may be significant overlap in the attack spectrum. However, we discuss both of these domains separately.

In VANETs, vehicles can disseminate valuable information regarding various important events, such as road conditions, traffic congestion, accident notifications, for efficient and distributed traffic management. Vehicles can get this sort of information from neighboring vehicles or from the environment in order to detect traffic congestion or collisions. In such a critical situation, the presence of malicious and misbehaving nodes causing falsified and fabricated information dissemination in the network can lead to drastic situations, thereby compromising the safety, security, and privacy of potential users.

Since VANETs are evolved from MANETs, the vulnerabilities posed by VANETs are largely inherited from the MANETs' ad hoc architecture, which usually attacked from the limited range because vehicles may not necessarily be connected to the Internet. We can mainly divide the attacks against VANETs as inter-vehicle and intra-vehicle.

Inter-vehicle attacks. Since in VANETs, there is no centralized administration or control; security protocols that require centralized trusted third party (TTP) or require all time connectivity, such as public key infrastructure (PKI), may not be used, which opens door for serious attacks at various levels. Similarly, the lack of a proper identity management system makes VANETs an appealing target for identity attacks, such as Sybil attacks. A Sybil attacker can create and manage multiple phony identities which share false information in the network in order to craft a false impression of nonexistent events. For example, the dissemination of falsified information generated by Sybil attackers about nonexistent road congestions or accidents can maliciously divert traffic for robbery, kidnapping, or car stealth purposes which are detrimental to drivers and/or vehicles safety and security. Similarly, an attacker can steal others' innocent nodes credentials to enjoy maliciously the rights and privileges associated with those identities or to commit malicious or misbehaving acts (such as denial of service (DoS) attacks) in the network without being accountable for those acts. This is called a masquerading or impersonation attack. VANETs are also vulnerable to packet dropping attacks, such as black hole, gray hole, and wormhole attacks, causing DoS attacks for individual vehicles or groups of vehicles. Vehicles are connected via wireless

communication links to other vehicles in the network, making them vulnerable to various kinds of attacks, such as traffic analysis, jamming, and eavesdropping attacks. These are some of the attacks launched against VANETs (note: discussion on complete spectrum of attacks is out of the scope of this article).

Intra-vehicle attacks. Currently, modern vehicles have a group of sensors which are responsible for undertaking various tasks, such as checking inter-vehicle distance and road conditions, smoke and fire detection, vehicle acceleration/deceleration system, obstacle detection radar, and so on. Intra-vehicle attacks are detrimental to safety and security of the driver and the vehicle, that is, misleading a sensor may harm the vehicle and/or the driver. For instance, disabling the braking system or the steering wheel by an attacker in an autonomous vehicle may endanger the driver's life.

On the other hand, in IoV, there will be a high level of heterogeneity caused by the amalgamation of various technologies, standards, and services; therefore, the demand for security and privacy will tend to increase. Connecting vehicles to the outside world may cause enormous threats and expose a wider attack spectrum to the IoV than the VANET. There are numerous security vulnerabilities in IoV resulting from the unprotected operation in V2I and V2C environments. Vehicles are connected to the Internet, which makes them globally accessible to individual hackers or malicious organizations. This exposes the vehicles and the network itself to attack by cyber criminals and attackers. Cyber attackers may cause devastating effects by exploiting vulnerable connection points or manipulating various vehicular data streams. For instance, even MP3 files can infect the whole network of cars very quickly.[14] Once the malicious users get control of the data system of the car using malwares or any other means, they can manipulate various subsystems of the vehicle, such as the steering wheel, safety system, braking system. This has been practically demonstrated at a recent Black Hat cybersecurity conference.[15]

The IoV's dependence on cloud services opens another door for cyber-attacks as cloud service providers are also potential targets for the cyber-attacks. For example, the cyber attackers may exploit ransomwares with the goal of creating revenue streams from cloud service providers or simply to launch DoS or distributed DoS (DDoS) attacks on the cloud to disrupt potential users. The situation will be aggravated if robot hackers capable of artificial intelligence (AI) and big data analytics are used against such service providers. Recently, defense advanced research projects agency (DARPA) conducted an all-machine hacking tournament,[16] which indicated that if the field progressed, robot hackers would be a big challenge for cyber space defenders. Furthermore, it has been shown that machines can identify software flaws and vulnerabilities faster than humans can[17] and they can launch more damaging and detrimental cyber-attacks than humans, such as botnets of machine hackers.

Related work

Recently, various attempts have been made to survey the existing body of work proposed to solve the security and privacy issues in the connected vehicles arena. These existing surveys contain some issues that motivated us to write this review article. First, some of the surveys at this point are now considered outdated, such as work in the La and Cavalli[1] surveys up to 2013. Second, some surveys are more threat-centric, meaning that the authors focused more on demonstrating the severity of the threats than on countermeasures. However, some of them follow a solution-centric approach, that is, focus more on describing the solution spectrum than that of the threats posed. In this article, we use a SLR in order to survey the existing proposed work related to securing connected vehicles. To the best of our knowledge, no previous work has systematically concentrated on the subject work. We use SLR to present comprehensive and unbiased information regarding various state-of-the-art security problems, solutions, and proposals in VANETs and IoVs. We briefly discuss these approaches as follows.

Engoulou et al.[18] surveyed the security issues and the challenges in VANETs and also introduced various architectures to address the security issues. The authors mainly focused on security problems and threats. The proposed work cited in the paper only goes to 2014 with no mention of Internet of connected vehicles. Similarly, the recent work in Contreras et al.[2] is related to IoV in that the authors discussed IoV protocols, architectures, and standards, but do not look comprehensively at security. A more recent work in this direction that focused more on threats is surveyed by Eiza and Ni[3] In their work, the authors focused on cybersecurity threats, such as malwares, auto mobile apps related threats, and on-board diagnostic (OBD) vulnerabilities, and also described the countermeasures proposed for them.

La and Cavalli[1] surveyed attacks and their solutions in VANETs environments. However, the authors categorized and surveyed only cryptographic-based solutions for the attacks and the collected papers are not recent, that is, from 2007 till 2013. A more comprehensive work in this direction is Hamida et al.,[4] in which the authors discussed the characteristics, architectures, standards, and projects of intelligent transport systems. The authors also analyzed and classified security attacks. However, they discussed only cryptographic-based countermeasures for their proposed attacks. Similarly, the authors in Zaidi and Rajarajan[5]

discussed only cryptographic-based countermeasures; however, the positive point in their work is that they evaluated and compared those cryptographic-based methods. A more recent and comprehensive work in this direction is Azees et al.[6]

Some authors focused on intra-vehicle security issues, while others focused on inter-vehicle security issues. For instance, authors in Zhang et al.[19] addressed the unique challenges posed by different types of malwares in the intra-vehicle environment. The authors discussed the existing solutions for malware counteraction and the challenges posed to eliminate or quarantine malwares. On the other hand, in Sakiz and Sen,[7] the authors mainly focus on security attacks and their countermeasures in the inter-vehicle environment.

The authors in Othmane et al.[8] proposed taxonomy of security and privacy aspects for IoV. The authors named these aspects as data validity, device security, communication links' security, identity and liability, privacy, and access control. The authors surveyed the proposed schemes according to their taxonomy. The authors in Parkinson et al.[20] also categorized and surveyed the work related to securing connected vehicles from cyber threats. However, their main focus was on identifying and presenting knowledge gaps and future research directions in the field. Table 1 addresses other related work and shows the differences between our work and theirs.

We differ from related work in several aspects:

1. We include the communication types V2I, V2V;
2. Performance comparison of each solution;
3. Software-defined network (SDN) when it is used in IoV;
4. Comprehensive approach, which includes threats, attacks, and their solution in all network layers. Attacks on integrity, authenticity, confidentiality, and availability;
5. Cover the period from 2010 to 2018, which is quite recent;
6. SLR as a new way to do the literature review. Only Jowell reputed journal and conferences.

Methodology

In this survey, we conducted a SLR which consists of planning, conducting the research and reporting (see Figure 1). In the planning phase, the research questions were specified, while in the search phase the rules and strategy will be specified. At the end, the results were presented.

The objectives of this survey are designed to answer the question of what the vulnerabilities and threats in IoVs are. The following research questions were identified:

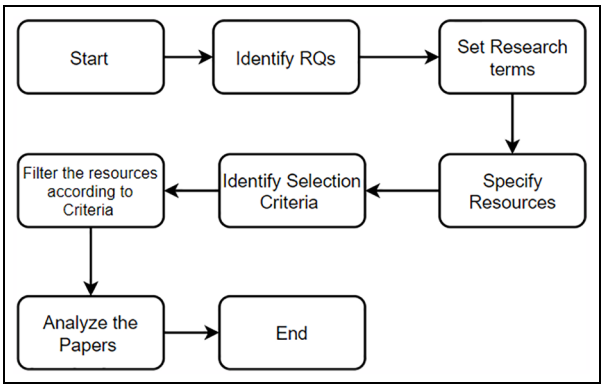

Figure 1. Review stages.

- RQ1: What are the different types of attacks on IoV and which security service is affected? The purpose of this question is to be able to categorize each threat, so it can be solved properly.
- RQ2: What are the different solutions that can be implemented to solve the threats discovered in RQ1? The purpose of this question is to see all the available solutions and choose the best one or the one that satisfies our needs.
- RQ3: How did each solution affect the performance of the system? The purpose is to make sure the performance will not decrease more than the standard with the use of any given solution.

Search strategy

The investigation was carried out to collect data using the following search term: ("IoV" OR "VANET" OR "Connected Cars") AND ("Threats" OR "Vulnerability "OR "Solutions") to answer the RQs mentioned above. As a result, all digital resources which discuss IoV or VANET or Cars Connections will be included and then filtered using threats, vulnerabilities, or solutions.

The following digital libraries were researched for the required articles (journals as well as conference papers):

- IEEE Explorer;
- Google Scholar;
- Science Direct;
- ACM Digital Library;
- Springer;
- Elsevier.

The resources considered in the survey are based on the following inclusion and exclusion criteria.

Table 1. Related work summary.

A survey on recent advances in vehicular network security, trust, and privacy[10]	In this survey, the main security services with their threats and their authentication schemes are surveyed. Three types of trust models are summarized as well as the significant properties to establish efficient trust management in VANETs. This survey is focusing on the novel privacy-preserving methods and trust models, and fills the gaps and reports the recent advances in VANETs	Covers threats and authentication only
Security issues in vehicular ad hoc network: a critical survey[11]	They threw light on the requirements of security, its implications, different attacks at different layers, and various techniques to cope up the attacks	Covers security and their implications on different layers
A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV[7]	In this article, a survey is presented on the attacks, together with their possible effects along with working principals. Then a survey was presented of solutions using different detection mechanisms proposed in the literature. Finally, a survey of solutions was presented with respect to the methods used, infrastructure, intrusion detection architecture, reputation, and response mechanisms	Covers attack detection and possible solutions
VANET security challenges and solutions: a survey[21]	This article presented an overview of the most of VANET security challenges and their causes as well as the existing. Some details of the security architectures and the well-known security standards and protocols were discussed	Covers security challenges and their causes till 2016
Security and attack analysis for vehicular ad hoc network—a survey[12]	Various threats to VANETs and the various entities that are discussed are very crucial factors for the proper implementation of the VANET and making it more reliable for the real world	Covers reliable VANET based on the study security and attack analysis
A comprehensive survey on security services in vehicular[6]	This article reviews the VANET system model, characteristics of VANETs, various security problems in VANETs, and various security services for VANETs. In addition, a summary of the security attacks and the related possible defense	Covers security in VANET services
Recent advances in VANET security: a survey[22]	This article is intended to provide a overview of the recent advances on VANETS security, surveying on security vulnerabilities, threats, and services	Similar to our work except it covers papers before 2015
Survey on security issues in vehicular ad hoc networks[23]	In this survey, an attack classification was introduced and their countermeasures on attacks facing the five layers discussed in this article	Covers attacks classification and their defenses till 2015
Survey on VANET security challenges and possible cryptographic solutions[24]	In this article, various recent aspects of VANETs sate of art such as standardization, routing protocols, projects, and applications are presented. In addition, it identifies various existing security issues in VANETs and classifies them from a cryptographic point of view	Covers standardization, routing protocols, and possible using crypto solution
VANET security surveys[18]	This article is composed of a comprehensive review of VANET security, security solution, threats, privacy, challenges, and addressing the attackers' profiles	Similar to our work except it covers papers before 2014
A systematic review on routing protocols for vehicular ad hoc networks[13]	This article provides a survey of various existing routing schemes with their relative advantages and disadvantages of each other	Only routing
Survey on security attacks in vehicular ad hoc networks (VANETs)[25]	This article presents several existing security attacks and approaches to defend against them, and discusses possible future security attacks with critical analysis and future research possibilities	Similar to our work except it covers papers before 2012

VANET: vehicular ad hoc network.

Inclusion criteria

- Date from 2010 to 2018;
- Only journals and conference papers which discuss IoV communications security, threats, and solutions are included.

Exclusion criteria

- Resources that include threats that are related to physical security of the communication inside the car;
- Exclude non-journal and non-conference articles;

- All digital resources which do not discuss the IoV communications and protocol threats and solutions.

Survey results

In this section, we discuss our findings on the predefined research questions. A survey conducted based on papers from 2010 to 2018 discusses the security challenges and solutions in IoV's (or VANET) protocol and how the performance will be affected after applying a solution.

In a world that is connected through Internet, we need to ensure that every new technology is as safe as possible and does not threaten the lives of the people using it. Most of the papers talk about the VANET protocol that is used in the communication.

IoVs are vulnerable to different kinds of attacks like jammers, for example, as they operate using wireless technologies. Jamming works by producing a signal that is similar to the vehicles' signals which will disrupt them as discussed in previous works.[21–24,26–32]

Different threats in IoV

Because of the broadcast nature of the IoV, cars will be easy to target and because of the continuous movement, it will be harder to track the attacker, so we must have a secure protocol and a mechanism that allows the cars to communicate safely and privately.

Just as with any other system, we are looking to implement four basic security features in our system:

1. Integrity: Making sure that the data transmitted is accurate, error free, and has not been modified during the transmission by a malicious party; a simple way to guarantee the integrity is using hashing algorithms.
2. Authenticity: Making sure that the person who sent the message is the person he claims to be, not someone impersonating him; a simple example to guarantee authenticity is a predefined password between the two parties that would be used to communicate.
3. Confidentiality: This is equivalent to privacy, where we need to make sure that the sensitive data are protected and only the right people can have access to that data; a simple example for that is encryption.
4. Availability: Making sure that the system is running perfectly, functioning as it is required to and is accessible at any time.

Table 2 summarizes the different targeted threats for each of the security features listed above. Figure 2

Table 2. Different threats.

Category	Attack	Purpose	Limitation
Integrity	• Message tampering • Masquerading • Black hole • Gray hole • Fabrication • Malware	Change the content of the messages to send wrong information or fake data	It can be detected easily using one-way encryption
Authenticity	• Sybil attack • Message tampering • Masquerading • GPS spoofing • Black hole • Worm hole • Gray hole • Fabrication • Replay attack • Malware	To allow unverified users to connect to the network along with communicating without the right ID	It can be defeated using default authentication
Confidentiality	• Eavesdropping • ID disclosure • Traffic analysis • Malware	To read and reveal the content of messages that travel through networks to implement different attacks	It can be defeated using encryption
Availability	• Denial of service • Black hole • Gray hole • Spamming • Jamming and malware	This allows the attackers to remove the vehicle from the network and make it unavailable to the rest of the vehicles	It can be defeated using vehicle ID–based cryptography and symmetric, hybrid, or public key encryption

Table 3. Different attacks on integrity.

Attacks on integrity	Referenced papers	Purpose
Message tampering	21, 22, 24, 27, 30, 33–43	Change the content of the messages to send wrong information or fake data
Masquerading	18, 21–25, 27, 29, 30, 33, 37, 38, 40–42, 44–52	Send fake data to the users as a trusted ID to create a chaos in the network
Black hole	21–26, 30, 33, 37, 38, 40, 42, 44, 47, 48, 52, 53	Not allowing any messages to pass which will increase the time to receive the packet and the vehicles might not have enough time to react
Gray hole	21, 22, 24, 30, 33–35, 38, 42, 44, 47, 50–52	To give the attacker the ability to join the network without the need to be physically there
Fabrication	21–25, 29, 35, 36, 38, 40, 41, 43–45, 47–50, 54, 55	To create fake messages without any meaning, either to slow the network or to create a chaos
Malware	19, 21, 22, 24, 37, 40, 42, 46, 48	Malwares can have multiple purposes, starting from spyware, viruses, bots till backdoors

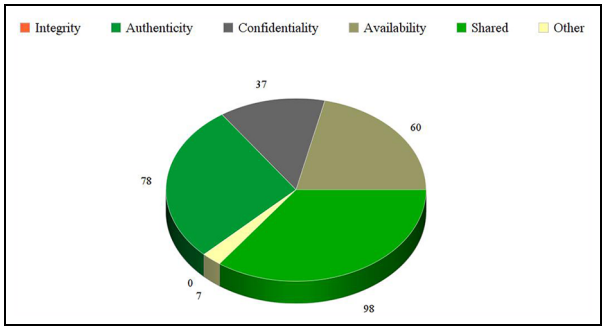

Figure 2. Number of papers that discuss the threat types of attacks on integrity.

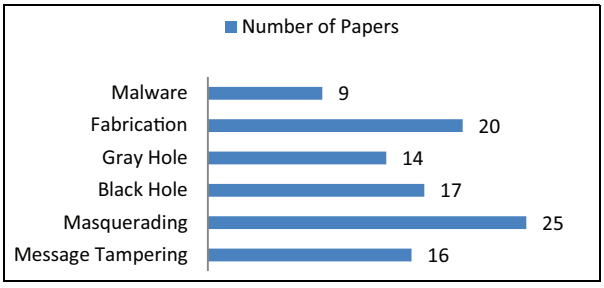

Figure 3. Number of papers that discuss the threats on integrity.

summarizes the big picture of research papers that discuss the threat types.

There are six main attacks on integrity discussed in SLR and they are summarized and demonstrated in Table 3 and Figure 3.

1. Message tampering: In this attack, the attacker modifies a message and claims that it came from an authenticated node. It can modify part of the data or all of the data by changing the content into fake alerts to create chaos.
2. Masquerading: The attacker will pretend to be another vehicle using that vehicle's ID and will start to send messages over the network to other cars so that the message will appear as if it came from an authenticated source.
3. Black hole: The attacker will be a node in the system, but it will participate in routing the data and will drop every packet that comes through him; the attacker can attract the messages to him by pretending that he is the shortest path by modifying his routing table.
4. Gray hole: This attack is a kind of black hole attack, where instead of dropping all the packets, the attacker will drop specific packets only, especially the ones that he is interested in and the ones that might be considered dangerous to drop, like warnings and accidental warnings.
5. Fabrication: Where the attack creates and sends false messages through the network, these messages might be to speed up the vehicles or to create traffic jams by sending slowing down requests.
6. Malware software that is planted in the vehicles or in the roadside unit (RSU) where it can disrupt the functionality of the whole network and even damage it.

Attacks on authenticity. There are four main attacks on authenticity discussed in SLR. They are summarized below and demonstrated in Table 4 and Figure 4.

1. Sybil attack: Where the attacker creates multiple nodes in the network and these nodes spread some wrong messages, warnings, or notifications or even drop packets.
2. GPS spoofing/position faking attack: The attacker will try to change the current location

Table 4. Different attacks on authenticity.

Attacks on authenticity	Referenced papers	Purpose
Sybil attack	21, 22, 24, 25, 30, 31, 33–38, 40–46, 48, 51, 52, 54, 55–57	Attackers use this method to overload the network
GPS spoofing/position faking attack	21, 22, 24, 25, 28–31, 33, 37, 38, 40, 42, 45, 52, 56, 57	This attack can be used to fool the autopilot system which might lead to a disaster
Worm hole	22, 23, 25, 29–31, 33, 37, 38, 40, 42, 45, 47, 56, 58	The attacker uses this attack to send messages to a network that is far away to create a chaos
Replay attack	21–24, 27, 30, 31, 35–38, 41–43, 45, 46, 50, 52, 54, 59, 60	This method is used to confuse the cars without the need to know the content of the messages captured

Table 5. Different attacks on confidentiality.

Attacks on confidentiality	Referenced papers	Purpose
Eavesdropping	18, 21–24, 27, 30, 32, 33, 38, 40, 44, 46, 47, 51, 54, 61	To see the content of messages and use it later in different attacks
Traffic analysis attack	21, 22, 24, 26, 29, 30, 39, 40, 46	To know the location of a person and follow him
ID disclosure	21, 23, 24, 29, 30, 34, 39, 41, 42, 44, 54, 55	To know the person in the vehicles that are connected to the network

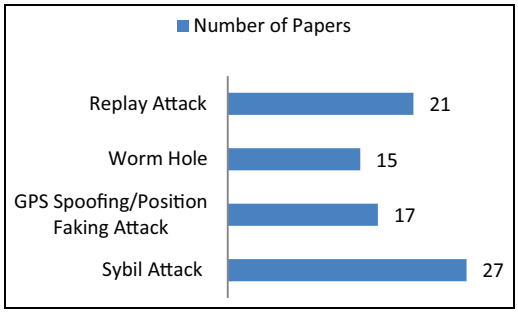

Figure 4. Number of papers that discuss the threats on authenticity.

of the victim and give him false information about his location, by generating signals that are more powerful than the satellite signals. He can then send the fake information to the victim.

3. Worm hole: In this attack, the attacker will route the messages to another network via a tunnel between two malicious nodes.
4. Replay attack: The attacker captures a packet transmitted on the network and analyzes each one of them along with their purpose. Then the attacker can retransmit any packet he had captured to the network to create fake alerts or accusations.

Attacks on confidentiality. There are three main attacks on confidentiality discussed in SLR. They are summarized below and demonstrated in Table 5 and Figure 5

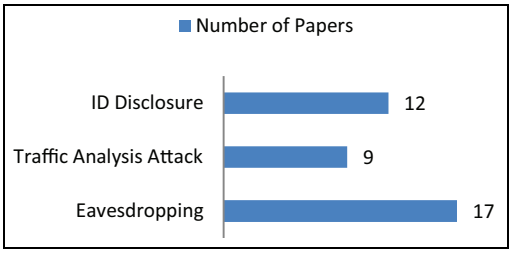

Figure 5. Number of papers that discuss the threats on confidentiality.

1. Eavesdropping: Because of the wireless nature of the IoV network, it is very easy to see the data and packets that go through the medium using the right tools. This means that the attacker can listen to the messages that travel over the network and can see the activity of the vehicles over the network. He then either saves the data to use later as a replay attack or to fabricate a message or launch different attacks.
2. Traffic analysis attack: This attack is against the anonymity between the V2V and V2R, where the attacker captures packets and some IDs.
3. Identity (ID) disclosure: Where the attacker obtains the ID of the vehicle or the user and then the attacker can track their location.

Attacks on availability. There are three main attacks on availability discussed in SLR. They are summarized below and demonstrated in Table 6 and Figure 6.

Table 6. Different attacks on availability.

Attacks on availability	Referenced papers	Purpose
Denial of service attack	18, 21–27, 29, 30, 33–38, 40–44, 46–48, 50–61	To make the network unavailable and create chaos between vehicles
Spamming	21, 22, 24–26, 30, 34, 37, 38, 40, 42, 46, 48	To increase the transmission time of messages between vehicle which will create a delay in reaction
Jamming the signal	21–24, 26–32	To not allow a vehicle or a network to send or receive any packet which will make it unavailable to the vehicles around it

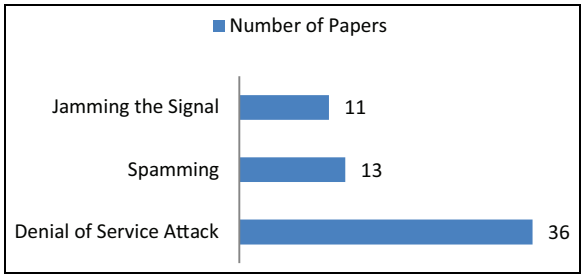

Figure 6. Number of papers that discuss the threats on availability.

1. DoS attack: This kind of attack is very dangerous on the VANET protocol where the attacker can overload the communication channel with fake messages or requests or with large messages that will overwhelm the devices. These devises then will not be able to process the messages in time, which will cause other messages that might be important to be dropped.
2. Spamming: The goal behind this kind of attack is to consume the bandwidth of the network and increase the transmission delay by sending messages that are not useful to the users, similar to sending spam emails.
3. Jamming the signal: This attack is a physical representation to the DoS attack, where the attacker transmits a signal to disrupt the communication between the devices.

Other attacks. A timing attack is very important in accidents and important notifications, because in this type of attack, the attacker will not forward the important message immediately and will instead waste some time and then it will forward the message later.[21,22,25,26,30,40,47,48,54,55]

All these problems need a solution, but before we implement any solution, we must know that we have some constraints in place to make sure that the system will keep running perfectly without any problems. The constraints are as follows:

1. Real time: One of the important constraints is the time, where all messages must be conveyed with a 100 ms transmission delay.[18,62]
2. Low tolerance for error: VANET uses life essential information, so any error in messages can cause real-life damage.[62]
3. 3 Key distribution: Distributing the keys in the system and knowing how to manage the certificates is a major constraint in IoV.[62]

Solutions for each problem

In this section, we briefly describe the solution proposed in the literature to counteract the above threats against the protocols of VANET or IoV. We also furnished them in Table 7.

1. Cryptographic digital certificates: One such example is vehicular public key infrastructure (VPKI), in which before sending a message, the vehicle must cryptographically sign it with its private key and the receiver will decrypt it with the sender's public key that it can get from certification authority (CA). In this way, the receiver is able to authenticate the message as well the sender. The schemes that use this approach in order to secure VANET and IoV include the previous works.[18,21,22,24,25,35,41,44,48,54,56,63–67]
2. Physical detection: The main idea behind this defense is to put a radar or signal receiver that detects the physical existence of the vehicles around it. Then, after performing some calculations on the message and fulfilling certain criteria, the message is accepted or rejected.[36,64]
3. Different encryption algorithms and methods like PKI, symmetric encryption, hybrid encryption, and group key (temporary key for the session derived from the master key) have been used to stop each attack that we have discussed earlier. Schemes in this connection include the previous works[18,21,24,25,35,41,44,48,53,54,56,58,60,66–78].

Table 7. Classification of threats, proposed solutions, and VANET Communication Mode 7.

References	Threats	Solution	Communication type
21, 24, 34, 54, 58	Wormhole	• Time stamp • Temporal leash • TIK (TESLA with instant key) • Shared key distribution using public key • Use trusted hardware, by which is practically impossible to change existing protocols and values, except by authorized personnel	V2V and V2I
24, 47, 54	Replay	ARAN • Ariadne	V2I and V2V
24, 47	Traffic analysis	Anonymous key changing • Encrypt only data which has paramount importance and the manipulation of which puts at risk the privacy of the driver • Use algorithms such as VIPER for V2I communications	V2V and V2I
24, 47, 58	Denial of service (DoS)	Use bit commitment and signature-based authentication mechanisms, which reduces the impact of almost of DoS attacks • Digital signature and trustworthiness of a node • SEAD	V2V
58	Message tampering	Data correlation and challenge response	V2V
36, 47, 64, 84	Sybil attack	Address Resolution Protocol (ARP) • RobSAD • Active position detection • Deploy a central validation authority (VA), which validates entities in real time	V2V and V2I
47	Attacks on fabrication	Secure AODV (A-SAODV) • ECDSA	V2V
24	GPS spoofing	Signature with position data to authenticate	V2V
24	Jamming	Switch the transmission channel and use frequency hopping technique FHSS (frequency hopping spread spectrum) which involves cryptographic algorithms to generate pseudo-random numbers for the hopping algorithm. This proposal requires a modification of the current standard which allows only the OFDM	V2V and V2I
19, 24, 47	Masquerading	Use trusted hardware for which it is practically impossible to change existing protocols and values, except by authorized holistic protocol	V2V and V2I
19, 21, 24, 35	Attacks on authenticity	Secure routing protocol (SAODV)	V2V
25, 41, 45, 47, 48, 53, 54, 56, 60, 66, 67, 69, 71–76, 81, 85, 86	Attacks on integrity, confidentiality, and authenticity	ID-based cryptography • Symmetric, hybrid, or public key encryption • CoPRA	V2V and V2I

VANET: vehicular ad hoc network; TIK: TESLA with instant key; ARAN: authenticated routing for ad hoc network; V2I: vehicle-to-infrastructure; DoS: denial of service; SEAD: secure and efficient ad hoc distance; RobSAD: robust method for Sybil attack detection; ECDSA: elliptical curve digital signature algorithm; V2V: vehicle-to-vehicle.

4. Reply protocol: When the vehicle receives a message, the receiver will send it to the RSU to check the correctness of the message, and that the sender is not malicious.
5. Use of firewalls or intrusion detection system (IDS) for different components of the car to avoid attacks.[32,45]

6. VPKI: Relying on the public key encryption method, each car will have its own public and private key along with CA in order to authenticate the cars and the messages.[21,24,41,54,77]
7. Trust models: Create a trust model that will evaluate the truthfulness of the message and the vehicle that sent the message and according to the level of trust, it can be established whether to accept or reject and discard the message.[18,64,65,79,80]
8. Signature-based malware detection: By analyzing the malware, a signature can be produced which can be used later to detect that malware.[19]
9. Behavior-based and heuristic-based malware detection: By observing the behavior of the system against a normal profile of the system behavior, these algorithms can detect the abnormal behavior caused by an attack. The algorithms proposed in this category are mostly related to machine learning and data mining domain.[19]
10. Cloud-based service: providing a cloud based service that can detect and analyse the malwares and give the results to the vehicles.[11] Malware analysis usually employs machine learning and deep learning based algorithms that require too much computation power. The motivation behind this approach is to shift the processing load from the RSU to the cloud.
11. ID-based mechanism: The main idea is to use any known information to derive a digital signature for the vehicle and create encryption keys according to that information. This cryptographic-based ID information is used to counter identity-based attacks, such as Sybil attack and masquerading attacks.[21,22,25,48,54,68,76,77,79,81]
12. Temporal leash: By specifying a maximum distance for the packet to travel and synchronizing all the nodes to the maximum time synchronization error, then taking into account these two values, along with the power of the wireless, we can calculate the expiration time of a packet and based on this information decide whether to receive it or not.[58] Temporal leash approach is used to counteract the wormhole attack.
13. TESLA with instant key (TIK) uses the method of symmetric key cryptography, when all communication parties must be accurately time synchronized and each node should know just one public value for the sender node.[58] In this technique, a combination of RSA and symmetric are used by which the packets will be broadcasted from the source node to the destination nodes securely and efficiently. RSA is used to distribute the keys and node identifier (ID) between the nodes to assure secure key sharing.[58]
14. Shared key distribution using public key[21,58]: This method works as follows:
    (a) Compute the location of sending node and the time the packet has been sent.
    (b) Encrypt the location, time, and ID of sender node using the shared key distributed in the scenario described above.
    (c) Send the cipher text obtained from step 2 to the receiver.
    (d) Decrypt the cipher text using the shared key at the receiving side.
    (e) Compute the location of the receiving node and according to the calculations, check to see whether the message was secure or not.
15. Secure ad hoc on-demand distance vector (SAODV) is an extension of the basic routing protocol AODV that can be used to protect the route discovery mechanism providing security features like integrity, the authentication, and non-repudiation. SAODV assumes that each node has a signature key pair from crypto management system. It ensures the security of routing, thereby verifying multiple fields in routing messages by digital signature and using one-way hash function to verify the hop count. All routing messages are digitally signed to ensure authenticity. In this approach, intermediate nodes cannot send a route reply even if the fresh route is known to them.[45,47]
16. Authenticated routing for ad hoc network (ARAN): This routing protocol is an AODV-based protocol. ARAN basically has certification, authenticated route discovery, authenticated route setup, route maintenance, and key revocation steps of operation. In this method, a third-party CA provides signed certificates to nodes. Every new node will send a request to CA. The public key of CA is known to all authorized nodes. Public key encryption is used for authenticated secure route discovery and timestamps are used for freshness of route.[47,54]
17. Secure and efficient ad hoc distance (SEAD): This routing protocol is secure and efficient and works on the top of destination-sequenced distance-vector routing (DSDV). It is based on one-way hash function for authentication process to protect the systems against DoS, routing, and impersonation kind of attacks. It uses a destination-sequence number to ensure freshness of the route instead of long routes. At each intermediate node, hashing is applied to ensure the authenticity of routes.[21,47,54]

18. ARIADNE: ARIADNE (is another protocol which is an extension of DSR with the concepts of symmetric key cryptography. It uses the TESLA[3,32] security scheme for routing which adds a HMAC key for authentication of nodes. ARIADNE protects DSR from malicious attacks like replay attack and looping condition. It increases the end-to-end delay as security mechanism is included. It has a low packet overhead and average CPU processing. It uses combination of one-way hash function and MAC for authentication and communication between nodes using shared key.[21,47]
19. A-SAODV: It is an extension to SAODV which has the feature of adaptive reply decision. Each intermediate node in the network has the ability to decide whether to reply to the source node or not, depending on the queue length and threshold conditions.[47] It is basically used to protect the VANET against routing attacks, impersonation, and bogus information.
20. Elliptical curve digital signature algorithm (ECDSA): This algorithm uses a digital signature along with hashing and public key to provide authenticity in the system. Both the sender and the receiver need to agree on elliptical curve domain parameters.[21,47] ECDSA is variant of the digital signature algorithm (DSA) that operates on elliptic curve groups. In this system, the public key is generated using DSA. And signature generation for message is done using SHA algorithm. Signature verification for authentication is done using SHA algorithm.
21. Robust method for Sybil attack detection (RobSAD): The main concept behind this method is that two different vehicles cannot have the same motion pattern while driven by different drivers, since each person drives according to his comfort and needs. Identification of Sybil node is done by finding two or more nodes having the same motion trajectories.[47]
22. Holistic protocol: In this protocol, there is a registration phase where vehicles send Hello messages to RSU; then the RSU prepares the response with registration id (consisting of license numbers and vehicle registration numbers) and sends it back to the vehicle. The authentication process is conducted through a certificate provided by RSU. After the node is authenticated, the data can be shared, but otherwise the node is blocked.[47]
23. SDN: This method uses the concept of pseudonyms to avoid all kinds of vehicle tracking. This protects privacy in vehicular cloud computing. To ensure confidentiality, this mechanism utilizes elliptic curve cryptography using the ECIES encryption algorithm and ECDSA digital signature, which has the advantages of its shorter key and its higher efficiency, compared to the other public key cryptographies such as RSA. Finally, the security mechanism protects the vehicles, clients, and infrastructures from malicious nodes using revocation mechanism.[55]
24. A software-defined vehicular cloud controller (SDVC) maintains a global view of vehicles based on the information collected from vehicles. These formations will be shared to the vehicles once needed. Also, it will be to train multi-class support vector machine (SVM), and then the vehicles use an SVM classifier to detect various types of attacks in a more accurate manner.[82] The SDVC controller contains sufficient resources to train the multi-class SVM while the vehicle does not have enough computing resources to do such kind of classification.[82]
25. VANET-Big Data is causing a shift from technology-driven to data-driven VANETs. VANET- Big Data system is used to collect huge amounts of data that can contribute to improve the navigation and flexibility of geo applications by providing real-time information about traffic conditions and new traffic routes based on information collected from car sensors and. All the information that is exchanged will be encrypted by geolocation key of the RSU and processed by the big data.[83]
26. Event-based reputation system (EBRS) can defense against multi-source Sybil attacks, to ensure the integrity and preserve the privacy of vehicles. By establishing a reputation and trust threshold for each vehicle message, then the false message is restricted to legitimate identities. In EBRS, a trusted RSU is used to as CA.[84]

Table 7 shows the classification of the recent existing threats, suggested solution, and the VANET communication modes disrupted if the threats become reality (such as V2V, V2I, or both). This classification helps to identify the predefined threat on the hardware or software, members or authorities, and their effects on the VANET communication mode. The threats and solutions details are already explained in early sections. It is clear that many solutions existed in the literature for each kind of threat or attack.

Performance for nodes to build up trust in the network

In this section, we summarize the SLR discussion on performance. The details of the performance results taking into account certain countermeasures along with the performance metrics are shown in Figures 7–14.

Performance evaluation of proposed protocol or countermeasure is considered to be an important task in research. This phase indicates the actual working of the system and the embedded proposed protocol. It also demonstrates to the research community the underlying flaws and benefits of the proposed work in the form of results under some metrics following some evaluation methodology, such as real world experimentation, simulation, and theoretical modeling.

We have collected some protocols' evaluations from the literature in Table 8 (collection of Figures 7–14) in the subject area. It is quite evident from these evaluations that there is no standard way of evaluating the proposed security protocols. Various authors use different metrics for their secure protocols evaluation. This will further aggravate the situation when comparison among different schemes becomes inevitable. It is highly recommended that a standard way of evaluation in terms of metrics selection be outlined and then followed for the protocol design, evaluation, and comparison.

Discussion and future directions

As IoV's technology emerges and prevails in the near future, the demand for security features in the IoV protocols will also increase. Distributed, scalable, and robust security solutions are required in order to ensure that the IoV platform adapts with the legal necessities to the security and privacy of users and vehicles. In this article, we have surveyed various security solutions; however, there are still various directions which will be described in this section for future exploration.

Trust

Trust is an important notion for interacting entities; especially if the interaction happens to be with strangers, that is, how much a node can trust the data shared by another node? The first requirement for any trust system to be viable is that the identities of nodes must be unique, persistent, and distinct. Non-persistent (having a short lifetime) identities cause loose accountability and nodes can change identities for upcoming interactions, whereas non-distinct identities are those that have no one-to-one identity to vehicle mapping, that is, more than one identity on a single vehicle: Sybil attack. The trust system designers need to devise strategies for these identity issues first; otherwise, there will be no use for nodes to build up trust in the network. Similarly, interaction experiences play a vital role in trust build up. In the IoV context, the question might be how to store and manage trust-related information on such a big scale? Or, how to utilize the trust information in a secure manner? The future trust models developed for IoV should fulfill identity requirements. The models need to be scalable and work in distributed manner. Finally, they should be efficient in terms of overhead and ensure accurate mapping of subjective to objective trust.

Resilience and self-adaptation

Another important direction that is worth looking at is a shift from eliminating vulnerabilities, and thereby augmenting resilience and self-adaptation. The IoV system should be robust enough to fully and rapidly recover from attacks and abnormal behaviors. Researchers need to explore and apply AI-based techniques like automated software patching[88] and self rewriting code[89] in the IoV domain for robustness.

Privacy preservation

The IoV applications mostly use cloud-based services. However, it is not always appealing to trust the third party cloud-based service providers for delegated operations. What is more enticing would be to use cloud-based services without the data being revealed. Current attempts at privacy preservation in cloud data processing are the techniques that use partially and fully homomorphic encryption algorithms. But these algorithms are very resource intensive; especially, when they are used to process a large volume of data generated by numerous vehicles from the IoV environment. A lightweight fully homomorphic encryption is needed in order to preserve data and user privacy in the IoV environment.

Another venue to explore in order to preserve privacy is to introduce controlled anonymity in the network. For example, at a cloud server, users' credentials must be authenticated but anonymized. By controlled anonymity, we mean that user anonymity must be within the bounds of accountability and privacy, that is, users should not be so anonymized as to compromise accountability, but should also not be so little anonymized as to compromise privacy.

Abstraction

The security of V2C link is crucial. One way to enhance V2C security and vehicle protection is to abstract the digital duplicate of a car out of a physical vehicle; this will prevent applications from directly interacting with the physical vehicle, rather all interactions will be made with the digital duplicate. The overhead may be reduced

Table 8. Performance outcomes.

In Yan et al.,[36] the time to defend against number vehicles is used to measure system performance in the case of cell based or flooding as shown in Figure 7(a). Also the author in Yan et al.[36] used average time to detect the attack as basis of performance as shown in Figure 7(b)

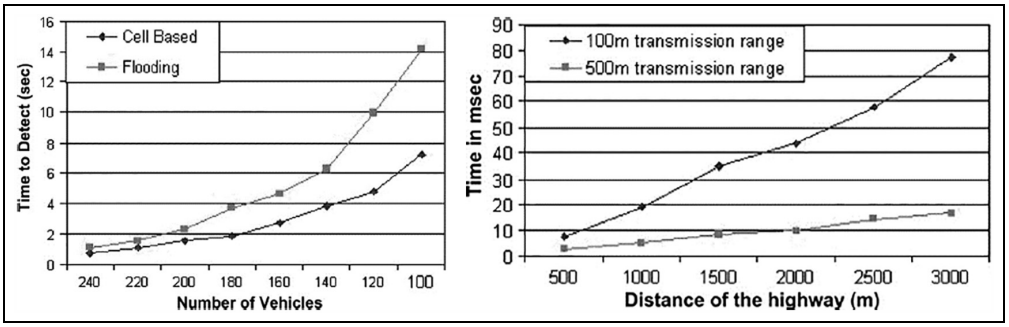

Figure 7. Time to defend against number of vehicles.

In Zhang et al.,[77] the author evaluates the proposed protocol performance by comparing it with efficient conditional privacy preservation (ECPP) as shown in Figure 8(a). The figure shows two time-cost ratio versus the number of vehicles existed in the range. Also the author shows the impact of authentication as rate of loss versus the message loss rate

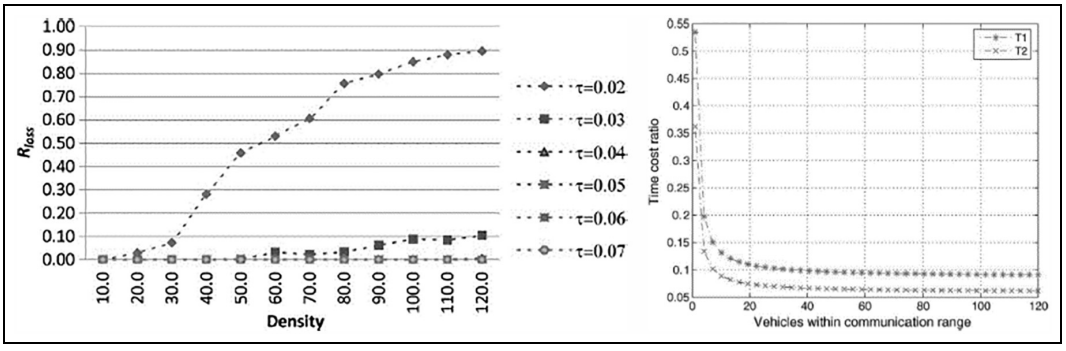

Figure 8. Impact of density on the message loss rate.

In Bißmeyer et al.,[70] the author used the latency of pseudonym resolution processes versus the number of pseudonyms to be resolved, contained in a single request as shown in Figure 9(a). Also the author used the mean, maximum, and minimum latency in the pseudonym resolution process with different numbers of database entries at the MEA, PCA, and LTCA versus increasing number of desired PC resolutions as shown in Figure 9(b)

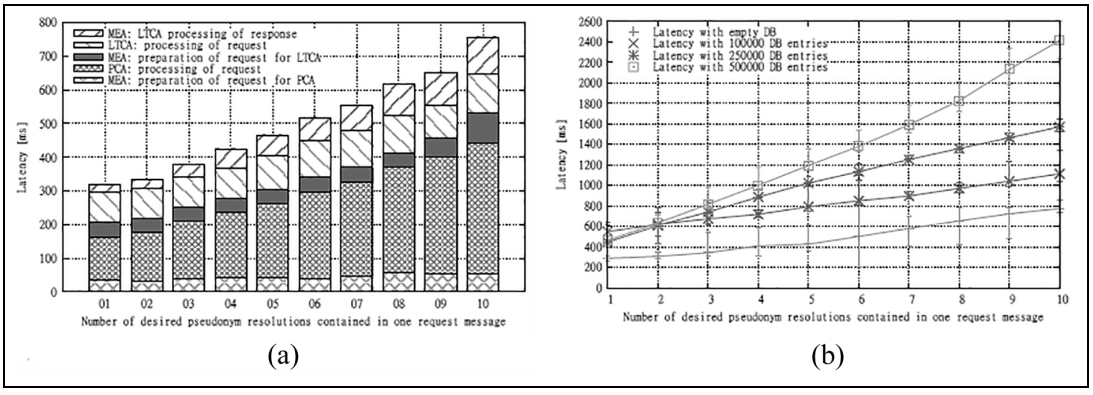

Figure 9. (a) Latency distribution in pseudonym resolution with empty database and (b) Latency of pseudonym resolution related to database size.

(continued)

In Figure 10, the author used various performance measures such as communication delay depending on number of vehicles, the delivery ratio, average event reputation value, and a comparison in communication overhead between TSA and DSAM[87]

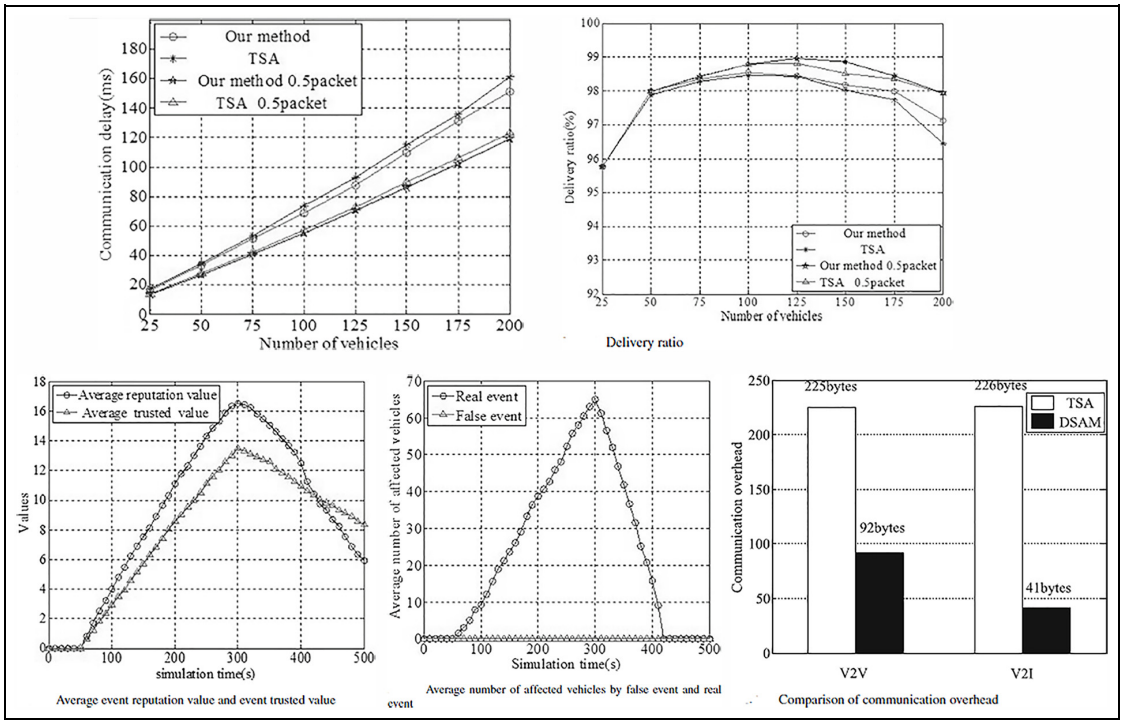

Figure 10. Various performance measures to compare the communication overhead between TSA and DSAM.

In Figure 11, the authors used the precision of the nearest neighbor SVM, the recall of the nearest neighbor SVM, recall and accuracy versus number of vehicles and alpha[82]
This graph specifies the average time to create a Diffie–Hellman key, depending on the speed of the vehicle[71]

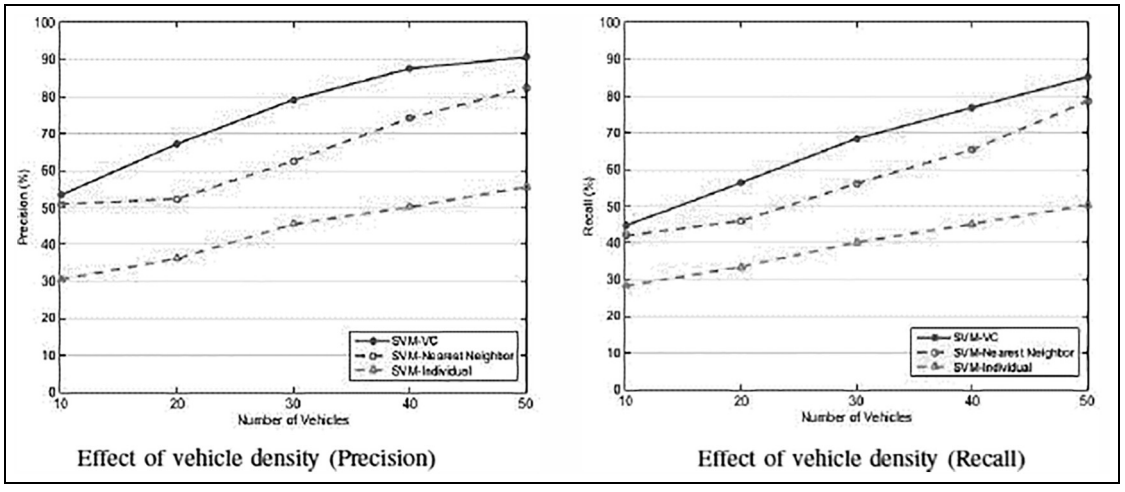

Figure 11. (Continued)

(continued)

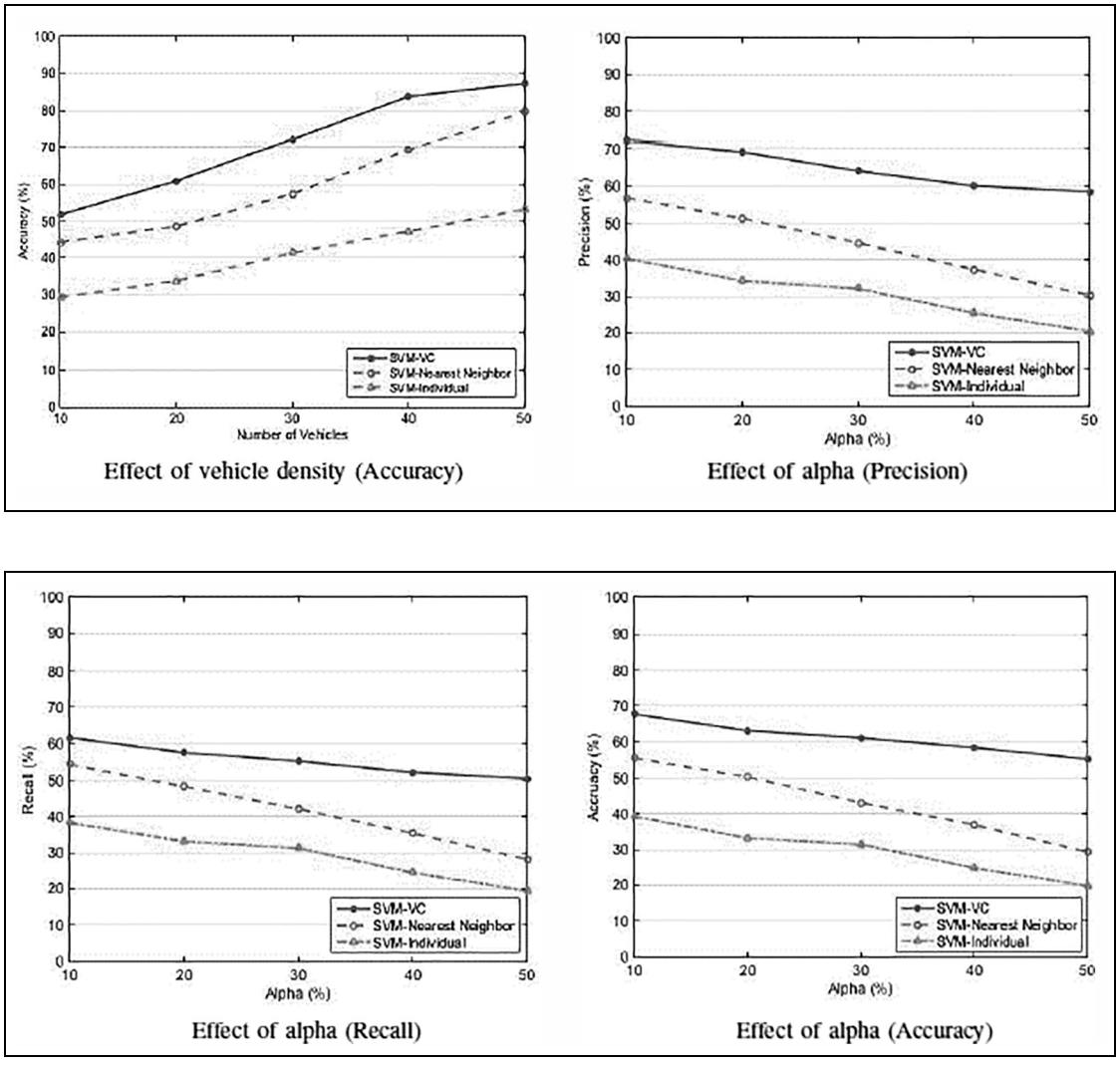

Figure 11. Precision of the nearest neighbor SVM, the recall of the nearest neighbor SVM, recall and accuracy versus number of vehicles and alpha.

In Figure 12, the author used the success rate, bandwidth used, average response time, dropping rate, dropping ratio versus vehicle density or versus speed are discussed[49]
This figure discusses the delivery ration for different sizes of message that are encrypted by different algorithms: AES and ECDSA[72]

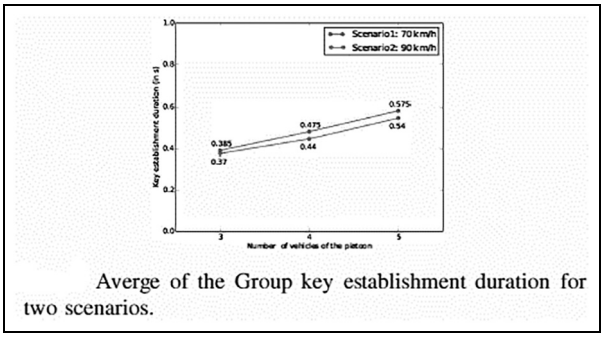

Figure 12. Average of Group Key Establishment duration.

SVM: support vector machine; ECDSA: elliptical curve digital signature algorithm.

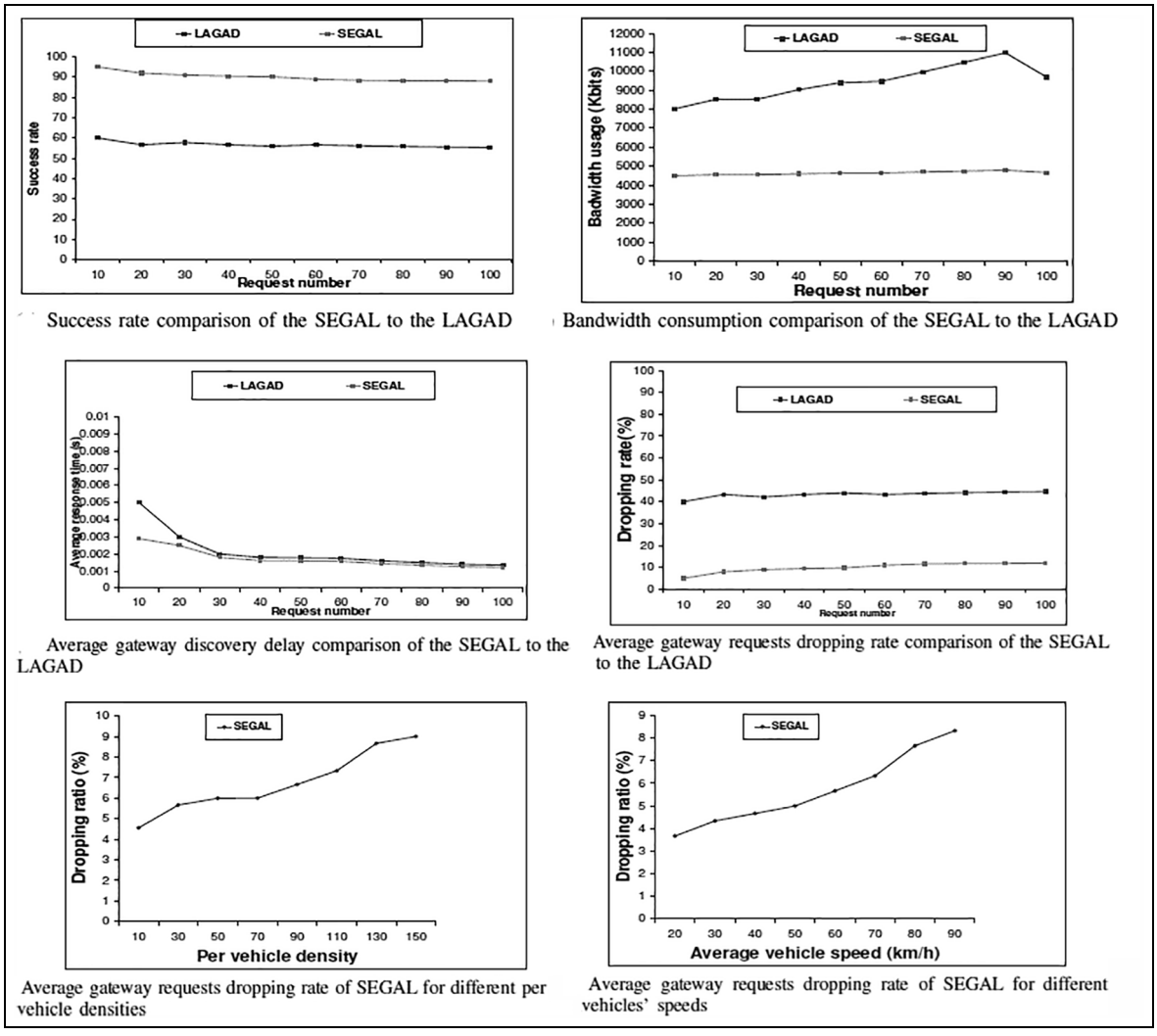

Figure 13. Success rate, bandwidth used, average response time, dropping rate, dropping ratio versus vehicle density or versus speed.

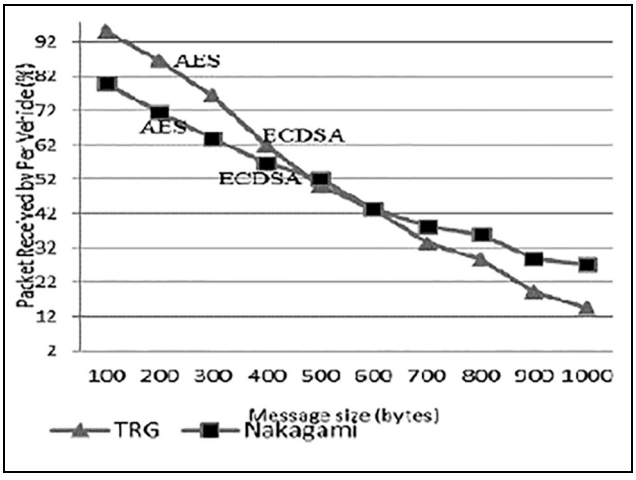

Figure 14. Packet delivery ratio versus message size.

using "Data Proxies," which would allow for abstraction and would also shift data handling to the cloud.[90]

AI-based detection

At the present time, a lack of human resources for cybersecurity is a big challenge throughout the world. In future, more reliance on robotics and autonomous systems will be seen. An AI-based immune system would be needed that could autonomously deal with unknown threats, use intelligent technologies to protect against unseen threats and anomalies, and respond to AI-based malwares, cognitive hackers, and so on. One such example is the IBM Watson project (https://www.ibm.com/watson/).

Conclusion

This survey explores security threats and their countermeasures in the VANETs and IoV domain, extracted from papers between 2010 and 2018. We have satisfied the goals of this survey and answered the following research questions:

- RQ1: What are the different types of attacks on IoV and which security service do they threat.
- RQ2: What are the different solutions proposed in the literature that can be implemented to solve the threats discovered in Q1?
- RQ3: How did each solution affect the performance of the system?

This study is restricted to journal and conferences papers in the field of IoVs and VANET. By applying a careful search filtration strategy, we obtained a good number of articles, but some were found to be irrelevant. The reason behind considering this number of papers is to ensure that the papers selected match our research questions. In addition, we applied rigorous matching criteria to select only the relevant articles that could provide meaningful results.

In addition to surveying various security solutions, we also provided some future directions for the novice researchers to start with. Those directions mainly include trust-based models, resilience and self-adaptation, privacy preservation, abstraction, and AI-based detection.

Acknowledgements

The authors would like to thank the University of Sharjah, Dubai Electronic Security Center (DESC), and OpenUAE Research and Development Group for funding this research study. The authors are also grateful to our research assistants who helped in collecting, summarizing, and analyzing the 127 research papers used in this SLR study.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

1. La VH and Cavalli AR. Security attacks and solutions in vehicular ad hoc networks: a survey. *IJANS* 2014; 4: 1–20.
2. Contreras J, Zeadally S and Guerrero-Ibanez JA. Internet of vehicles: architecture, protocols, and security. *IEEE Internet Things J* 2017; 5: 3701–3709.
3. Eiza MH and Ni Q. Driving with sharks: rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehic Tech Magazine* 2017; 12: 45–51.
4. Hamida EB, Noura H and Znaidi W. Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures. *Electronics* 2015; 4: 380–423.
5. Zaidi K and Rajarajan M. Vehicular Internet: security & privacy challenges and opportunities. *Future Internet* 2015; 7: 257–275.
6. Azees M, Vijayakumar P and Deborah LJ. A comprehensive survey on security services in vehicular ad-hoc networks. *IET Intel Trans Syst* 2016; 10: 379–388.
7. Sakiz F and Sen S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Networks* 2017; 61: 33–50.
8. Othmane LB, Weffers H, Mohamad MM, et al. A survey of security and privacy in connected vehicles. In: Benhaddou D and Al-Fuqaha A (eds) *Wireless sensor and mobile ad-hoc networks*. London: Springer, 2015, pp.217–247.
9. Butt TA, Iqbal R, Shah SC, et al. Social Internet of vehicles: architecture and enabling. *Comp Electr Eng* 2018; 69: 68–84.
10. Lu Z, Liu W, Wang Q, et al. A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access* 2018; 6: 45655–45664.
11. Arif M and Ahmad S. Security issues in vehicular ad hoc network: a critical survey. In: Shakhovska N (ed.) *Advances in intelligent systems and computing*, vol. 624, pp.527–536. Singapore: Springer.
12. Chauhan KK, Kumar S and Kumar S. The design of a secure key management system in vehicular ad hoc networks. In: *2017 conference on information and communication technology (CICT)*, Gwalior, India, 3–5 November 2017, pp.1–6. New York: IEEE.
13. Dua A, Kumar N and Bawa S. A systematic review on routing protocols for vehicular ad hoc networks. *Vehic Comm* 1: 33–52.
14. Reger L. Addressing the security of the connected car. *NXP blog*, 2014, https://blog.nxp.com/automotive/addressing-the-security-of-the-connected-car
15. Hackers demonstrate how to take control of cars. 20 jobs that will be replaced by technology. https://www.msn.com/en-gb/video/healthandfitness/hackers-demonstrate-how-to-take-control-of-cars/vi-BBlsiab (accessed 1 September 2018).
16. Feature: in first all-machine hacking tournament, computers battle to make world safer. Profile: Peru's engineer-turned-president Martin Vizcarra—Xinhua. *English.news.cn*, 5 August 2016. http://www.xinhuanet.com/english/2016–08/05/c_135567414.htm (accessed 1 September 2018).
17. Simonite T. Pentagon epic bot battle shows software could automatically fix security flaws. *MIT Technology Review*, 8 August 2016. https://www.technologyreview.com/s/602071/pentagon-bot-battle-shows-how-computers-can-fix-their-own-flaws/ (accessed 20 September 2018).
18. Engoulou RG, Bellaïche M, Pierre S, et al. VANET security surveys. *Comp Comm* 2014; 44: 1–13.
19. Zhang T, Antunes H and Aggarwal S. Defending connected vehicles against malware: challenges and a solution framework. *IEEE Internet Things J* 2014; 1(1): 10–21.
20. Parkinson S, Ward P, Wilson K, et al. Cyber threats facing autonomous and connected vehicles: future challenges. *IEEE Trans Intel Transport Syst* 2017; 18: 2898–2915.

21. Hasrouny H, Samhat AE, Bassil C, et al. VANet security challenges and solutions: a survey. *Vehicular Comm* 2017; 7: 7–20.
22. Bariah L, Shehada D, Salahat E, et al. Recent advances in VANET security: a survey. In: *2015 IEEE 82nd vehicular technology conference (VTC2015-Fall)*, Boston, MA, 2015, 6–9 September 2015, pp.1–7. New York: IEEE.
23. Mokhtar B and Azab M. Survey on security issues in vehicular ad hoc networks. *Alexandria Eng J* 2015; 54(4): 1115–1126.
24. Mejri MN, Ben-Othman J and Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. *Vehic Comm* 2014; 1(2): 53–66.
25. Al-Kahtani MS. Survey on security attacks in vehicular ad hoc networks (VANETs). In: *2012 6th international conference on signal processing and communication systems*, Gold Coast, QLD, Australia, 12–14 December 2012, pp.1–9. New York: IEEE.
26. Sumra IA, Ahmad I, Hasbullah H, et al. Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET). In: *2011 3rd international congress on ultra modern telecommunications and control systems and workshops (ICUMT)*, Budapest, 5–7 October 2011, pp.1–8. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6079000&isnumber=6078843
27. Amoozadeh M, Raghuramu A, Chuah CN, et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Comm Magazine* 2015; 53(6): 126–132.
28. Petit J and Shladover SE. Potential cyberattacks on automated vehicles. *IEEE Trans Intel Transport Syst* 2015; 16(2): 546–556.
29. Kim M. A survey of vehicular ad-hoc network security. In: Kim J and Joukov N (eds) *Proceedings of the mobile and wireless technologies 2017*. Singapore: Springer, pp.315–326.
30. Abdelgader AMS, Shu F, Zhu W, et al.Security challenges trends in vehicular communications. In: *2017 IEEE conference on systems, process and control (ICSPC)*, Malacca, Malaysia, 15–17 December 2017, pp.105–110. New York: IEEE.
31. Bhoi SK and Khilar PM. Vehicular communication: a survey. *IET Networks* 2014; 3(3): 204–217.
32. Thing VLL and Wu J. Autonomous vehicle security: a taxonomy of attacks and defences. In: *2016 IEEE international conference on Internet of Things (Ithings) and IEEE green computing and communications (Greencom) and IEEE cyber, physical and social computing (Cpscom) and IEEE smart data (Smartdata)*, Chengdu, China, 15–18 December 2016, pp.164–170. New York: IEEE.
33. Upadhyaya AN and Shah JS. Attacks on vanet security. *Int J Comp Eng Tech* 2018; 9(1): 8–19.
34. Al-Raba'nah Y and Samara G. Security issues in vehicular ad hoc networks (VANET): a survey. *Int J Sci Appl Res* 2015; 2(4): 6.
35. Samara G, Al-Salihy WAH and Sures R. Security analysis of vehicular ad hoc networks (VANET). In: *2010 second international conference on network applications, protocols and services*, Kedah, Malaysia, 20–23 April 2010, pp.55–60. New York: ACM.
36. Yan G, Olariu S and Weigle MC. Providing VANET security through active position detection. *Comp Comm* 2008; 31(12): 2883–2897.
37. Manjunath PS and Reddy N. A review on security and challenges for vehicular ad hoc. *Int J Emerg Tech Adv Eng* 2014; 4(5): 67–72.
38. Hezam Al, Junaid MA, Syed AA, Mohd Warip MN, et al. Classification of security attacks in VANET: a review of requirements and perspectives. *MATEC Web Conferences* 2018; 150: 06038.
39. Yan G, Wen D, Olariu S, et al. Security challenges in vehicular cloud computing. *IEEE Trans Intel Transport Syst* 14(1): 284–294.
40. Tyagi P and Dembla D. Investigating the security threats in vehicular ad hoc networks (VANETs): towards security engineering for safer on-road transportation. In: *2014 international conference on advances in computing, communications and informatics (ICACCI)*, New Delhi, India, 24–27 September 2014, pp.2084–2090. New York: IEEE.
41. Manvi SS and Tangade S. A survey on authentication schemes in VANETs for secured communication. *Vehic Comm* 2017; 9: 19–30.
42. Sabahi F. The security of vehicular adhoc networks. In: *2011 third international conference on computational intelligence, communication systems and networks*, Bali, Indonesia, 26–28 July 2011, pp.338–342. New York: IEEE.
43. Samara G, Al-Salihy WAH and Sures R. Security issues and challenges of vehicular ad hoc networks (VANET). In: *4th international conference on new trends in information science and service science*, Gyeongju, South Korea, 11–13 May 2010, pp.393–398. New York: IEEE.
44. Kumar A and Sinha M. Overview on vehicular ad hoc network and its security issues. In: *2014 international conference on computing for sustainable global development (INDIACom)*, New Delhi, India, 5–7 March 2014, pp.792–797. New York: IEEE.
45. Sun Y, Wu L, Wu S, et al. Security and privacy in the Internet of vehicles. In: *2015 international conference on identification, information, and knowledge in the internet of things (IIKI)*, Beijing, China, 22–23 October 2015, pp.116–121. New York: IEEE.
46. De La Torre P, Rad G and Choo K-KR. Driverless vehicle security: challenges and future research opportunities. *Future Generat Comp Syst*. Epub ahead of print 11 January 2018. DOI: 10.1016/j.future.2017.12.041.
47. Mishra R, Singh A and Kumar R. VANET security: issues, challenges and solutions. In: *2016 international conference on electrical, electronics, and optimization techniques (ICEEOT)*, Chennai, India, 3–5 March 2016, pp.1050–1055. New York: IEEE.
48. Hasan ASA, Hossain MS and Atiquzzaman M. Security threats in vehicular ad hoc networks. In: *2016 international conference on advances in computing, communications and informatics (ICACCI)*, Jaipur, India, 24–27 September 2016, pp.404–411. New York: IEEE.
49. Abrougui K, Boukerche A, Wang Y, et al. Secure gateway localization and communication system for vehicular ad hoc networks. In: *2012 IEEE global communications conference (GLOBECOM)*, Anaheim, CA, 3–7 December 2012, pp.391–396. New York: IEEE.

50. Wang P, Yu G, Wu X, et al. An extended car-following model to describe connected traffic dynamics under cyberattacks. *Physica A* 2018; 496: 351–370.
51. Qu F, Wu Z, Wang FY, et al. A security and privacy review of VANETs. *IEEE Trans Intel Transport Syst* 2015; 16(6): 2985–2996.
52. Mejri MN and Hamdi M. Recent advances in cryptographic solutions for vehicular networks. In: *2015 international symposium on networks, computers and communications (ISNCC)*, Hammamet, Tunisia, 13–15 May 2015, pp.1–7. New York: IEEE.
53. Karimireddy T and Bakshi AGA. A hybrid security framework for the vehicular communications in VANET. In: *2016 international conference on wireless communications, signal processing and networking (WiSPNET)*, Chennai, India, 23–25 March 2016, pp.1929–1934. New York: IEEE.
54. Deeksha N, Kumar A and Bansal M. A review on VANET security attacks and their countermeasure. In: *2017 4th international conference on signal processing, computing and control (ISPCC)*, Solan, India, 21–23 September 2017, pp.580–585. New York: IEEE.
55. Bousselham M, Abdellaoui A and Chaoui H. Security against malicious node in the vehicular cloud computing using a software-defined networking architecture. In: *2017 international conference on soft computing and its engineering applications (IcSoftComp)*, Changa, India, 1–2 December 2017, pp.1–5. New York: IEEE.
56. Tbatou S, Ramrami A, Tabii Y, et al. Security of communications in connected cars modeling and safety assessment. In: *Proceedings of the 2nd international conference on big data, cloud and applications*, Tétouan, 29–30 March. New York: IEEE.
57. Abumansoor O and Boukerche A. Preventing a DoS threat in vehicular ad-hoc networks using adaptive group beaconing. In: *Proceedings of the 8h ACM symposium on QoS and security for wireless and mobile networks*, Paphos, Cyprus, 24–25 October 2012. New York: ACM.
58. Ali S, Nand P and Tiwari S. Secure message broadcasting in VANET over Wormhole attack by using cryptographic technique. In: *2017 international conference on computing, communication and automation (ICCCA)*, Greater Noida, India, 5–6 May 2017, pp.520–523. New York: IEEE.
59. Dominic D, Chhawri S, Eustice RM, et al. Risk assessment for cooperative automated driving. In: *Proceedings of the 2nd ACM workshop on cyber-physical systems security and privacy (CPS-SPC'16)*, 28 October 2016, pp.47–58. New York: ACM.
60. Rizvi S, Willet J, Perino D, et al. A threat to vehicular cyber security and the urgency for correction. *Procedia Comp Sci* 2017; 114: 100–105.
61. Koscher K, Czeskis A, Roesner F, et al. Experimental security analysis of a modern automobile. In: *2010 IEEE symposium on security and privacy*, Oakland, CA, 22–25 May 2010, pp.447–462. New York: IEEE.
62. Agarwal P. Technical review on different applications, challenges and security in VANET. *J Multimedia Tech Recent Advance* 2017; 4(3): 11.
63. Balamurali R and Vimali JS. Certificate and message authentication acceleration in VANET. In: *International conference on innovation information in computing technologies*, Chennai, India, 19–20 February 2015, pp.1–4. New York: IEEE.
64. Grover J, Gaur MS, Laxmi V, et al. A Sybil attack detection approach using neighboring vehicles in VANET. In: *Proceedings of the 4th international conference on security of information and networks*, Sydney, NSW, Australia, 14–19 November 2011. New York: ACM.
65. Sumra IA, Hasbullah HB, Ab Manan JI, et al. Using TPM to ensure security, trust and privacy (STP) in VANET. In: *2015 5th national symposium on information technology: towards new smart world (NSITNSW)*, Riyadh, Saudi Arabia, 17–19 February 2015, pp.1–6. New York: IEEE.
66. Lim K, Tuladhar KM, Wang X, et al. A scalable and secure key distribution scheme for group signature based authentication in VANET. In: *2017 IEEE 8th annual ubiquitous computing, electronics and mobile communication conference (UEMCON)*, New York, 19–21 October 2017, pp.478–483. New York: IEEE.
67. Singh R and Miglani S. Efficient and secure message transfer in VANET. In: *2016 international conference on inventive computation technologies (ICICT)*, Coimbatore, India, 26–27 August 2016, pp.1–5. New York: IEEE.
68. Jiang W, Li F, Lin D, et al. No one can track you: randomized authentication in vehicular ad-hoc networks. In: *2017 IEEE international conference on pervasive computing and communications (Percom)*, Kona, HI, 13–17 March 2017, pp.197–206. New York: IEEE.
69. Mahagaonkar SV and Dongre N. TEAC: timed efficient asymmetric cryptography for enhancing security in VANET. In: *2017 international conference on nascent technologies in engineering (ICNTE)*, Navi Mumbai, India, 27–28 January 2017, pp.1–5. New York: IEEE.
70. Bißmeyer N, Petit J and Bayarou KM. Copra: conditional pseudonym resolution algorithm in VANETs. In: *2013 10th annual conference on wireless on-demand network systems and services (WONS)*, Banff, AB, Canada, 18–20 March 2013, pp.9–16. New York: IEEE.
71. Mejri MN, Achir N and Hamdi M. A new group Diffie-Hellman key generation proposal for secure VANET communications. In: *2016 13th IEEE annual consumer communications & networking conference (CCNC)*, Las Vegas, NV, 9–12 January 2016, pp.992–995. New York: IEEE.
72. Wagan AA and Jung LT. Security framework for low latency VANET applications. In: *2014 international conference on computer and information sciences (ICCOINS)*, Kuala Lumpur, Malaysia, 3–5 June 2014, pp.1–6. New York: IEEE.
73. Reddy DS, Bapuji V, Govardhan A, et al. Sybil attack detection technique using session key certificate in vehicular ad hoc networks. In: *2017 international conference on algorithms, methodology, models and applications in emerging technologies (ICAMMAET)*, Chennai, India, 16–18 February 2017, pp.1–5. New York: IEEE.
74. Nema M, Stalin S and Tiwari R. RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p. In: *2015 international conference on computer, communication and control (IC4)*, Indore, India, 10–12 September 2015, pp.1–5. New York: IEEE.

75. Shen C and Mu H. A roaming authentication protocol based on elliptic curve cryptography in IOV. In: *2017 3rd IEEE international conference on computer and communications (ICCC)*, Chengdu, China, 13–16 December 2017, pp.400–404. New York: IEEE.
76. Wang F, Xu L and Pan JS. Security analysis on "strongly secure certificateless key-insulated signature secure in the standard model." In: *2015 international conference on intelligent information hiding and multimedia signal processing (IIH-MSP)*, Adelaide, SA, Australia, 23–25 September 2015, pp.195–198. New York: IEEE.
77. Zhang L, Wu Q, Solanas A, et al. A scalable robust authentication protocol for secure vehicular communications. *IEEE Trans Vehic Tech* 59(4): 1606–1617.
78. Mamun MSI, Miyaji A and Takada H. A multi-purpose group signature for vehicular network security. In: *2014 17th international conference on network-based information systems*, Salerno, 10–12 September 2014, pp.511–516. New York: IEEE.
79. Rehman A, Ali A, ul Amin R, et al. VANET thread based message trust model. In: *Eighth international conference on digital information management (ICDIM 2013)*, Islamabad, Pakistan, 10–12 September 2013, pp.58–60. New York: IEEE.
80. Putra GD and Sulistyo S. Trust based approach in adjacent vehicles to mitigate Sybil attacks in VANET. In: *Proceedings of the 2017 international conference on software and e-business*, Hong Kong, 28–30 December 2017. New York: IEEE.
81. Sun J, Zhang C, Zhang Y, et al. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Trans Parallel Distr Syst* 21(9): 1227–1239.
82. Kim M, Jang I, Choo S, et al. Collaborative security attack detection in software-defined vehicular networks. In: *2017 19th Asia-Pacific network operations and management symposium (APNOMS)*, Seoul, South Korea, 27–29 September 2017, pp.19–24. New York: IEEE.
83. Contreras-Castillo J, Zeadally S and Guerrero Ibañez JA. Solving vehicular ad hoc network challenges with Big Data solutions. *IET Networks* 5(4): 81–84.
84. Gantsou D. On the use of security analytics for attack detection in vehicular ad hoc networks. In: *2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC)*, Shanghai, China, 5–7 August 2015, pp.1–6. New York: IEEE.
85. Bouabdellah M, Bouanani FE and Ben-Azza H. A secure cooperative transmission model in VANET using attribute based encryption. In: *2016 international conference on advanced communication systems and information security (ACOSIS)*, Marrakesh, 17–19 October 2016, pp.1–6. New York: IEEE.
86. Tripathi VK and Venkaeswari S. Secure communication with privacy preservation in VANET- using multilingual translation. In: *2015 global conference on communication technologies (GCCT)*, Thuckalay, India, 23–24 April 2015, pp.125–127. New York: IEEE.
87. Feng C-Y, Li D-X, Chen X, et al. A method for defensing against multi-source Sybil attacks in VANET. *Peer-to-Peer Networking and Applications* 10(2): 305–314.
88. Patch management with AI: never miss an update again. *SingleHop*, 11 October, https://www.singlehop.com/blog/patch-management-with-ai/ (accessed 20 September 2018).
89. AI learns to write its own code by stealing from other programs. *NewScientist*, https://www.newscientist.com/article/mg23331144-500-ai-learns-to-write-its-own-code-by-stealing-from-other-programs/ (accessed 1 September 2018).
90. Siegel J. *Data proxies, the cognitive layer, and application locality: enablers of cloud-connected vehicles and next-generation Internet of Things*. PhD Dissertation, Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA, June 2016.