Scientific Research Publishing

Journal of Computer and Communications, 2016, 4, 38-62
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Systematic Approach for Cyber Security in Vehicular Networks

Farhan Ahmad, Asma Adnane, Virginia N. L. Franqueira

College of Engineering and Technology, University of Derby, Derby, UK
Email: f.ahmad@derby.ac.uk, a.adnane@derby.ac.uk, v.franqueira@derby.ac.uk

How to cite this paper: Ahmad, F., Adnane, A. and N. L. Franqueira, V. (2016) A Systematic Approach for Cyber Security in Vehicular Networks. *Journal of Computer and Communications*, **4**, 38-62.
http://dx.doi.org/10.4236/jcc.2016.416004

Received: November 21, 2016
Accepted: December 26, 2016
Published: December 30, 2016

Abstract

Vehicular Networks (VANET) are the largest real-life paradigm of ad hoc networks which aim to ensure road safety and enhance drivers' comfort. In VANET, the vehicles communicate or collaborate with each other and with adjacent infrastructure by exchanging significant messages, such as road accident warnings, steep-curve ahead warnings or traffic jam warnings. However, this communication and other assets involved are subject to major threats and provide numerous opportunities for attackers to launch several attacks and compromise security and privacy of vehicular users. This paper reviews the cyber security in VANET and proposes an asset-based approach for VANET security. Firstly, it identifies relevant assets in VANET. Secondly, it provides a detailed taxonomy of vulnerabilities and threats on these assets, and, lastly, it classifies the possible attacks in VANET and critically evaluates them.

Keywords

Vehicular Networks, Ad Hoc Networks, Cyber Security, Privacy, Vulnerabilities, Threats, Assets, Smart City

1. Introduction

1.1. Background

With large number of vehicles distributed around the world, traffic efficiency and driver safety have become relevant challenges of the modern age. According to the World Health Organization, approximately 1.25 million people die every year due to traffic accidents [1]. Traffic accidents are also responsible for creating massive road congestion which results in huge delays. The main goal of Vehicular Networks (VANET) is to solve part of these problems. In fact, VANET is the largest real life application of Mobile Ad Hoc Networks (MANET) where the nodes are replaced by moving vehicles with

sensing and communication capabilities [2] [3] [4].

VANET is a novel cutting-edge technology and is the future of Intelligent Transportation System (ITS). ITS will become more and more prevalent in the near future and it is expected that millions of vehicles will be connected through VANET by 2022 [5]. VANET plays a significant role in the success of emerging smart cities and Internet of Things (IoT) [6].

In VANET, the vehicles are equipped with various sensing and communication devices (e.g. camera, GPS). The sensors collect significant information from the vehicle, such as its location, speed and acceleration, and share it with other neighbouring vehicles and adjacent roadside units (RSU) through wireless interfaces (e.g., Long Term Evolution (LTE), Dedicated Short Range Communication (DSRC)) [7] [8]. RSU is a static entity, such as speed camera, mobile communication base station or relay nodes [9], positioned along the roadside; in the context of VANET, such units are considered as *infrastructure*. The messages generated are exchanged through two modes of communication, *i.e.*, 1) vehicle-to-vehicle (V2V) communication by utilising DSRC protocols; and 2) vehicle-to-infrastructure (V2I) communication by using mobile communication standards (e.g., 3G, LTE, or LTE-Advanced) to enable long distance communications. The main objectives of VANET include:

1) Ensuring vehicular traffic safety and high efficiency of ITS [10].

2) Assisting drivers in critical situations such as accidents and traffic congestion [11].

3) Providing infotainment to vehicular users on roads such as information about traffic, weather conditions and entertainment such as video [12] [13].

4) Monitoring fleet of vehicles remotely. Thus, VANET can be useful in logistics and transportation applications [14] [15].

Figure 1 highlights the architecture of VANET. It illustrates the accident scenario on highway where collision information is forwarded to the neighbouring vehicles through both V2V and V2I modes of communication, thus avoiding huge traffic jam on the highway as the approaching vehicles can take different route towards their destination.

VANET propagates critical and relevant information such as pre-crash, steep-curve ahead, or accident warnings. Ideally, this information must be shared with nodes (vehicles &RSU) without any alteration to its content. VANET heavily relies on cooperation and communication between nodes to ensure easy propagation of information. However, it is prone to various attacks (e.g., Denial of Service attacks, Man-in-the-Middle attacks, Message alteration attacks etc.) by malicious nodes and external malicious interference on the network, potentially affecting its application behavior and capability to perform in a desired manner. In fact, VANET is a large-scale, decentralized and highly dynamic network which contains both legitimate and potentially malicious nodes. Therefore, it becomes extremely challenging to ensure confidentiality, integrity, availability, authenticity and non-repudiation in such highly mobile network.

1.2. Motivation

According to the World Economic Forum (2015) [16], global environmental, societal,

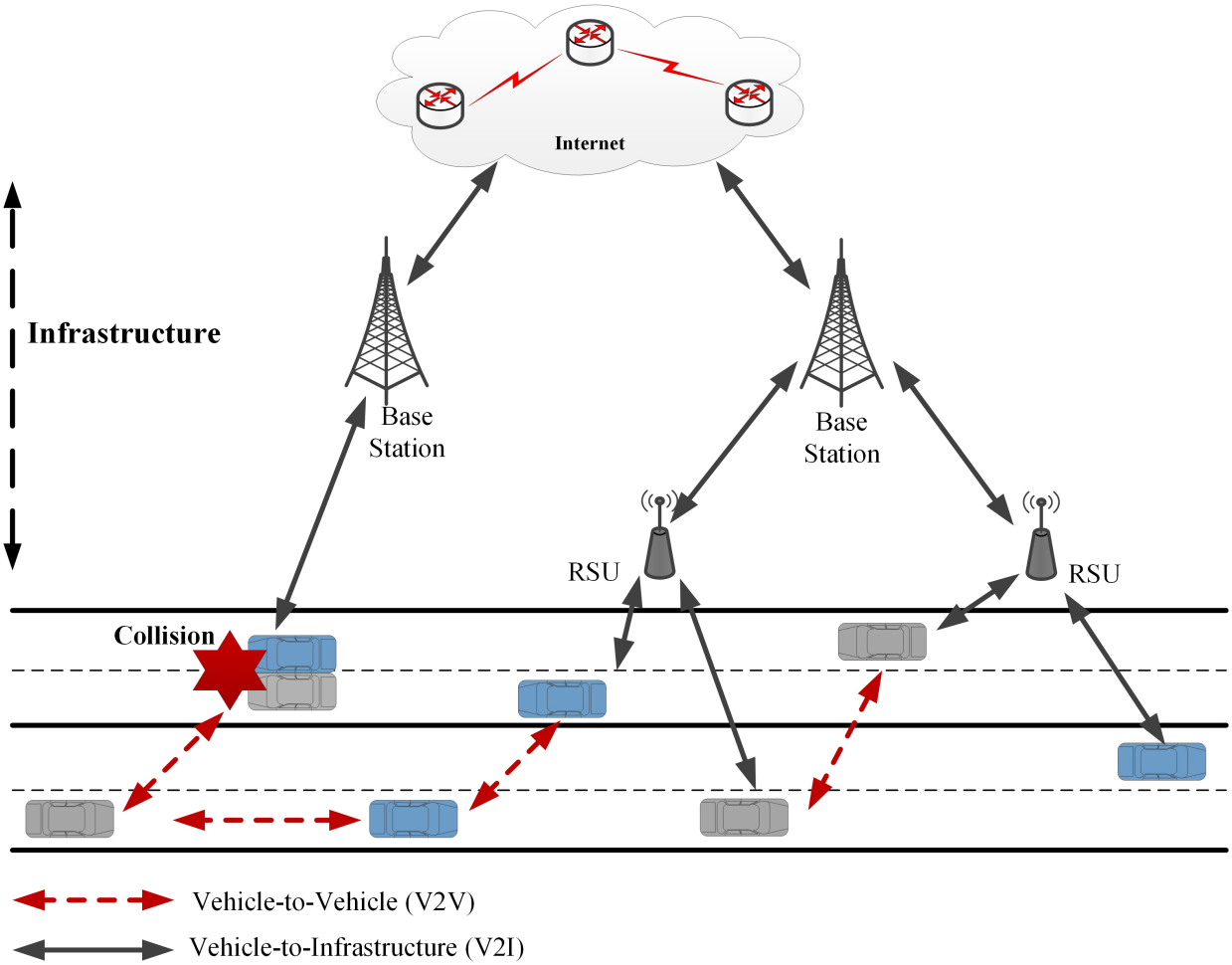

Figure 1. VANET Architecture; example of collision avoidance.

geopolitical and technological threats (*i.e.*, cyber attacks, data theft and technology misuse) are gaining more and more attention. Specifically, the risks caused due to cyber attacks will increase by 23.3% in 18 months and about 20.2% in the coming 10 years. Therefore, security becomes a crucial component in the design of new networking technologies. Especially in VANET, where vulnerabilities exploited in cyber attacks must be identified and addressed as quickly as possible (possibly in real-time) since an attack might have a severe impact on road users.

VANET is an active research area and different studies were conducted on VANET security. Due to severity of impact, VANET security is becoming increasingly important. Raya *et al.* were the first to study this topic. They highlighted several challenges and gaps in accomplishing VANET security, for instance, privacy preserving of vehicular user in a highly mobile network and message propagation in a secure vehicular environment [17]. To address these challenges, Fuentes *et al.* identified distinct security requirements for VANET in terms of authenticity, integrity, availability, confidentiality, and non-repudiation [18]. Moreover, considering the security requirements in VANET, several studies proposed a variety of attacker models such as [19] [20] [21]. These at-

tacker models were classified into two distinct levels: high and low impact attackers. Similarly, various recent studies on VANET security identified different attacks based on the basic security requirements of confidentiality, integrity and availability [2] [22] [23] [24] [25]. Such classification is complex as a single attack might have several security requirements at a particular time. This also results in the overlapping the attacks in different components of VANET, thus making the attack classification very complicated. Bhargava *et al.* presented a study where a systematic approach is taken to analyse attacks focusing only on V2V communication in VANET [26]. The security of the in-vehicle communication was also the spotlight of other studies. For instance, Koshar *et al.* identified security gaps in Controller Area Network (CAN) of the vehicle by successfully launching different attacks (malware integration and spoofing attacks) [27]. Similarly, Checkoway *et al.* described the proof-of-concept of an attack which compromised in-vehicle communication resulting in an access to internal components of a vehicle [28]. The main limitation of these research studies is the very focused study of a particular component of VANET, as the implementation of same attacks have different requirements and consequences in other components (e.g., RSU or Central Entity) of VANET. Moreover, solutions to cater these attacks are missing in these studies.

Several recent research projects were entirely focused on VANET security and privacy. **Table 1** summarizes research projects relevant in regards to the focus of this paper. For instance, OVERSEE [29] and SeVeCOM [30] projects focused on the in-depth study of the security issues of the in-vehicular communication. Similarly, the main contribution of PRESERVE project was to design privacy-aware communication protocols for VANET [31].

The literature on VANET security either concentrates on particular VANET components only (e.g., V2V communication or in-vehicle communication) or on specific security requirements (e.g., confidentiality, integrity and availability), missing others. Therefore, these approaches do not guarantee a holistic and comprehensive analysis of security in VANET. It might be the case that components, not deemed relevant at first, represent a source of vulnerabilities, and that requirements, like availability of mobile and static nodes, are neglected. This paper fills this gap and presents an asset-based approach to analyse security of VANET.

In order to understand VANET security in depth, we followed a systematic approach which includes the following steps and are depicted in **Figure 2**.

1) Identification of assets in VANET,

2) Classification of assets,

3) Identification of vulnerabilities on the assets,

4) Identification of threats related to the assets,

5) Identification of possible attacks based on the threats and identified vulnerabilities, and

6) Identification of feasible solutions to cater these VANET attacks.

The remaining of the paper is organised as follows. Section 2 presents assets in VANET from a security point of view. Vulnerabilities and threats on the VANET assets

Table 1. Research projects on VANET security.

Project	Duration	Objectives
Open Vehicular Secure Platform Project (OVERSEE) [29]	01/2010-06/2012	To design a standardized platform for secure vehicular communication
Secure Vehicle Communication (SeVeCOM) [30]	01/2006-12/2008	To provide solutions for V2V and V2I communication security
Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) [31]	01/2011-16/2015	To design and implement a testbed for secure and privacy-aware V2X communication
E-safety vehicle intrusion protected applications (EVITA) [33]	07/2008-12/2011	To design a secure and trustworthy architecture for intra-vehicular communication for on-board devices
Satellite Applications for Emergency hamdling, traffic alerts, road safety and incident preventation (SafeTrip) [34]	10/2009-03/2013	To develop a platform, allowing third parties to integrate security applications
Privacy Enabled Capability In co-operative systems and safety applications (PRECOISA) [35]	03/2008-08/2010	To develop a privacy-aware application for ITS systems
Network on Wheels (NoW) [36]	05/2004-05/2008	To provide data security in V2V communications
Communication for eSafety (COMeSafety2) [37]	01/2010-10/2014	To develop standards for ITS security
Cooperative cars and roads for safer and Intelligent Transportation System (CopITS) [38]	10/2010-10/2013	To develop communication protocol for efficient data transfer in V2V and V2I scenarios in Doha City
Preventive and Active Safety Application (PREVENT) [39]	02/2004-01/2008	To design and implement safer early warning system on roads
Communication Network Vehicle Road Global Extension (CONVERGE) [40]	08/2012-10/2015	To design V2X architecture to provide real-time information directly in a secure and privacy-preserving environment
Advanced Safety and Driver Support for Essential Road Transport (ASSET ROAD) [41]	07/2008-12/2011	To develop an approach to provide security on roads and increase traffic efficiency
Engineering security and performance aware vehicular applications for safer and smarter roads (SafeITS) [42]	01/2015-01/2018	To design a security framework to integrate vehicular applications in VANET

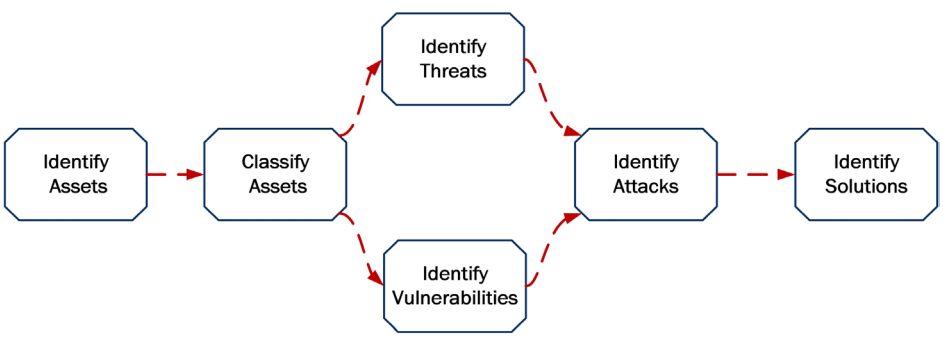

Figure 2. Systematic approach for VANET security.

are presented in Section 3 and 4 respectively. Section 5 introduces various attacks in VANET based on the identified vulnerabilities and threats. Finally, Section 6 draws conclusion of the paper.

2. Assets in VANET

Assets are the valuable components of the network [32]. Failure or misuse of these assets will cause damage to the entire network, thus affecting its users on a very large scale. A vulnerable asset is a threat to the whole network. The network can experience several attacks, if identified vulnerabilities are exploited by the attackers. Therefore, the process of identifying and securing the assets along with the access control of the users on the network is a crucial step in VANET security [18].

2.1. Identification of Assets in VANET

From a security point of view, the following are considered as assets in VANET because they have values for stakeholders:

1) VANET user
2) Exchanged data
3) Vehicles
4) Roadside units (RSU)
5) Network communication protocols
6) Central entity
7) Third parties

2.1.1. VANET User

As VANET is designed to provide safety and comfort to vehicular users, these users constitute the most important asset in VANET. Safety of users as well as the security of their identity is crucial. Moreover, user's privacy is considered to be the first VANET users concerns and need to be guaranteed [43] [44]. If the user is compromised, via a social engineering attack for example, all his private information is compromised and his vehicle become a point of failure to the networking system.

2.1.2. Vehicles

Vehicles, on the other hand are also one of the vital assets in VANET and they play different important roles in the network: 1) they generate critical data (e.g. traffic related information), 2) they route data for other vehicles, 3) and they store critical data (e.g. user identity, warning messages to be forwarded).

In VANET, every vehicle is composed of various components: 1) sensors, 2) Application Unit (AU) and 3) On Board Unit (OBU). Sensors collect information from surroundings and AU generate messages based on the gathered information. These messages are shared with neighboring vehicles via OBU. Compromising the vehicle, or any component in the vehicular system, will alter the generated messages as well as the routing operations, resulting in the propagation of compromised messages in the network. Therefore, the availability and the access to the vehicle must be guaranteed.

2.1.3. Exchanged Data

Important messages are transmitted and exchanged between different vehicles and nearby RSUs. As these messages can contain lifesaving information such as accident warning, or sensitive information like user private details (e.g. identity and location.), data security and privacy must be guaranteed in terms of confidentiality, integrity and availability (CIA).

2.1.4. Road Side Unit (RSU)

RSU acts as a bridge between the vehicles and the infrastructure during V2I communication. In RSU, the important components are its hardware, operating system (OS) and software residing on OS. This software communicates with vehicles on one hand and with infrastructure on the other. RSU, being static in nature, is more vulnerable to attacks and is one of the preferred passage for attackers to gain entry to VANET. If the RSU is compromised, the data stored in the RSU is compromised, and the communication with the infrastructure is not guaranteed.

2.1.5. Central Entity

The central entity is another static node in the VANET architecture which includes the application servers providing various applications such as collision avoidance application, weather and traffic updates etc. It is located in the infrastructure domain, and plays a vital role during V2I communication where all the messages are first received by the application server. It authenticates the received message and forwards it to other vehicles over a large geographical location. When the central entity is compromised (a compromised server or OS), all the V2I operations as well as the running services are affected, and the VANET operations are limited. Therefore, the access and the availability of the central entity are key requirements in VANET.

2.1.6. Third Parties

Third parties represents various authorities which resides in the infrastructure domain in VANET such as vehicle manufacturers and traffic police. These authorities have their own cryptographic tools which are integrated to the OBU of the vehicles. It should be made sure that these parties are free from bugs and malwares; they must be trusted and are referred to as trusted third parties (TTP).

2.1.7. Network Communication Protocols

After presenting the different nodes of VANET and their role in building the VANET security, we need to ensure a secured communication between them. This includes the following types of communications:

- In-vehicle communication between sensors, AU and OBU via Controller Area Network (CAN),
- Communication between two vehicles (V2V), and
- Communication between vehicle and adjacent RSU (V2I).

An insecure communication protocol will not guarantee the safe transmission of data between vehicular nodes in the network.

2.2. Classification of Assets

Asset classification is the key to various security measures that need to be implemented for asset optimization. In most security assessments reports, assets are divided in four categories: 1) Information, 2) Software, 3) Physical, and 4) Services [45]. In our point of view, this classification doesn't reflect the VANET operations and security requirements. For example, the vehicle and the central entity are both physical assets, but they use different communication protocols (vehicle is a mobile node using wireless communication protocols, and the central entity is static and part of the wired network), and they require different security implementations (the security of the wireless ad-hoc network is different compared to the wired network).

In this report, we have classified the assets into three broad classes according to their role, mobility and impact on the VANET. The purpose of this classification is to facilitate the security assessment and the threat analysis. Since, in VANET, the assets are distributed in different domains, therefore, we classify these assets into three classes as depicted in Figure 3. These are:

- *Vehicular System*: This class includes the vehicular user, vehicles and communication network.
- *Information*: This class contains the information carrying important messages.
- *Infrastructure*: This class includes the static entities along VANET, such as RSU, central entity and third parties.

In the following section, we will identify vulnerabilities in these classes of assets.

3. Vulnerabilities in VANET

Vulnerability is the weakness in the system which is exploited by the malicious users in the form of attacks for their own benefits. In this section, we identified vulnerabilities in VANET which are presented according to asset classification. The taxonomy of the vulnerabilities in depicted in Figure 4.

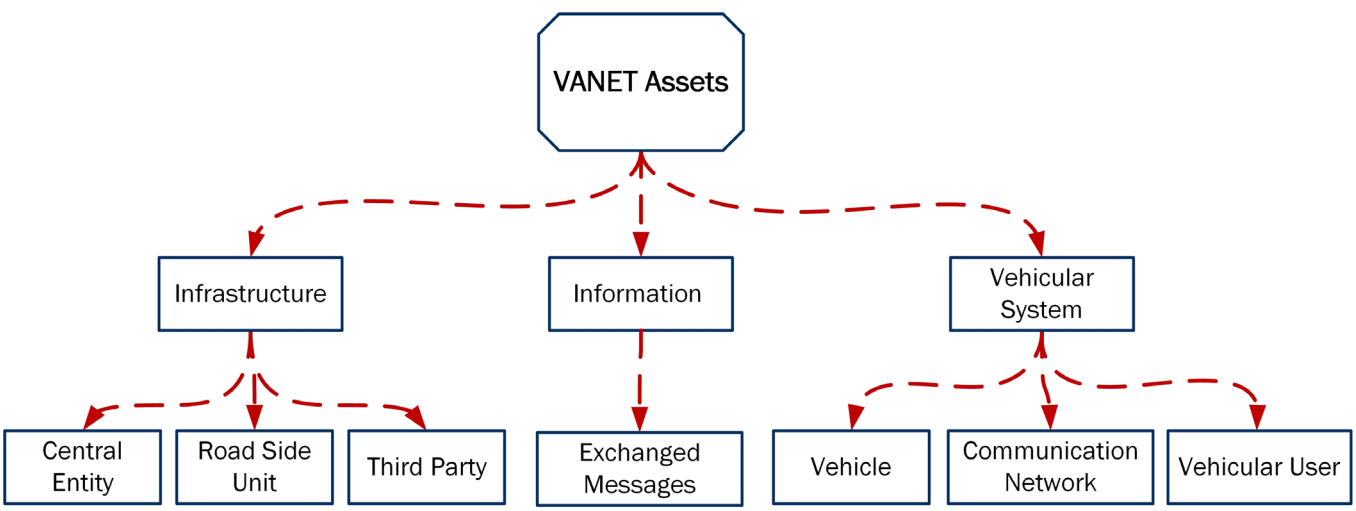

Figure 3. Assets in vehicular networks.

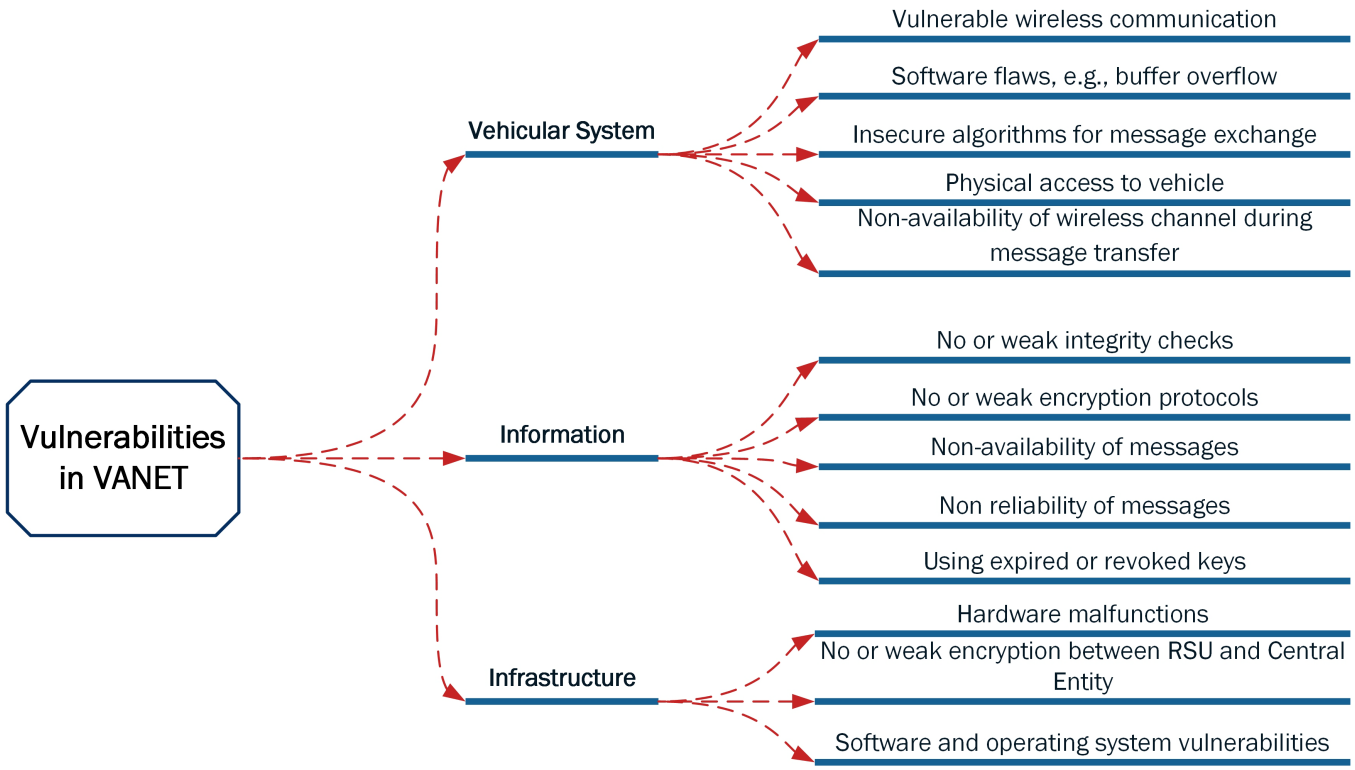

Figure 4. Taxonomy of vulnerabilities in VANET.

3.1. Vulnerabilities in Vehicular System

The vulnerabilities in this cluster include the physical access of an unauthorized person to the vehicle itself which poses direct risk on the vehicle's sensing and communication capabilities. Similarly, the use of insecure algorithms (weak passwords) to exchange significant information such as user information and credentials via wireless communication poses risk on the user's privacy. Moreover, software flaws such as buffer overflow, insecure cryptographic algorithms and key management failure offer vulnerabilities in the vehicular system which can be exploited by the attacker to launch several attacks. For instance, researchers from Tencent Keen Security Lab successfully implemented various attacks remotely on Tesla cars by accessing the CAN of vehicles [46].

3.2. Vulnerabilities in Information

Sensitive messages such as vehicular user personal information must be secured. If data is not encrypted and not signed, then the data is vulnerable to attacks by attacker where the attacker can modify the messages with bogus information. Similarly, no integrity checks on the data and routing messages offer vulnerabilities to be exploited by launching several attacks such as impersonation attacks, sybil attacks etc. Moreover, the manipulation of routing table with wrong routing information will result in the non-availability or alteration of these messages. As messages are of foremost importance in VANET, the non-availability or alteration of these messages can leave severe impact on the network.

3.3. Vulnerabilities in Infrastructure

Infrastructure as the static entity offers various vulnerabilities such as software and operating systems vulnerabilities. The back-end channel between RSU and central entity must be secured and encrypted. Any information sent on the un-encrypted communication channel is a vulnerability and can be interpreted and modified by the attacker. The attacker can also take advantage of the hardware malfunctions at RSU and central entity. e.g., an attacker can deceive a speed camera after stealing vehicular user information.

4. Threats in Vehicular System

This section introduces various potential threats according to VANET cluster. The taxonomy of threats in these VANET cluster is depicted in Figure 5.

4.1. Threats to Vehicular System

This category include threats to the vehicle, vehicular user and communication network *i.e.*,

4.1.1. Vehicle

Usually, VANET involve high speed mobility of vehicles and two vehicles communicate with each other for a very short span of time. However, there are still some threats to

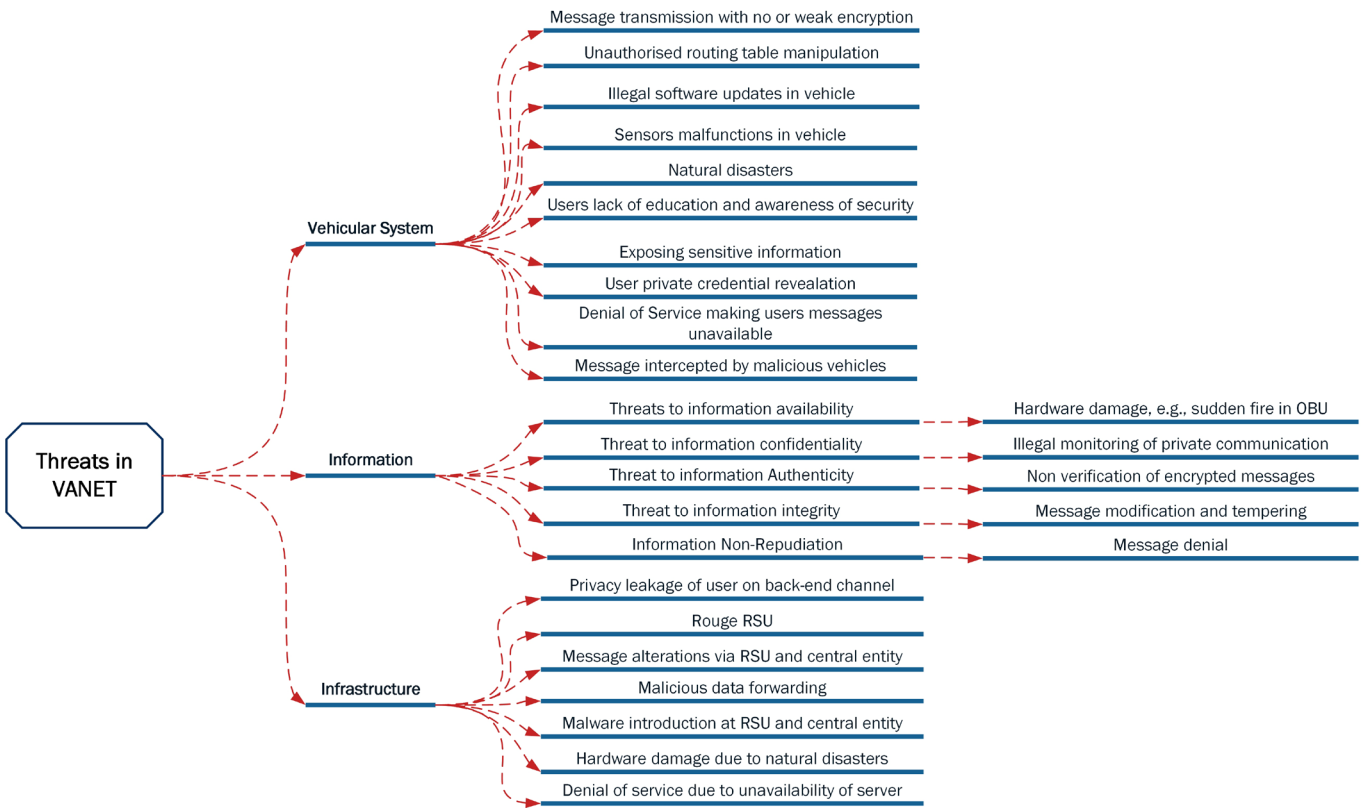

Figure 5. Taxonomy of threats in VANET.

vehicles and its different components. The attacker can plan to access the OBU or AU of vehicle and sensors. The threat also involves the attacker being able to install malware on AU and sensors. Firmware updates are also one of the targets where the attacker injects malicious code inside the in-vehicle network via CAN. This can lead to drastic results e.g., the attacker can misconfigure the sensor with its malicious code [47] [48].

4.1.2. User Privacy

Privacy is one of the important security aspects which aims to ensure that the identity of vehicular user is private and secure from unapproved person [49]. The threat includes revealing the vehicular user identity and its geographical location and sensitive information.

4.1.3. Communication Network

Wireless communication network is used for the transportation of messages in VANET. As this wireless medium is exposed to different vulnerabilities, it offer several opportunities which are exploitable by an attacker. For the in-vehicle network, the threats include the misconfiguration of OBU and sensors by an attacker via CAN. For V2V and V2I, it includes threats to different attacks such as Denial of Service (DoS), Man-in-the-Middle (MITM) attacks, altering the messages en-route and jamming the communication channel etc.

4.2. Threats to Information

Information contains important messages about a particular event, which is usually exchanged among the vehicles and RSUs during V2V and V2I communication. Threats to information always exist where the main interest of the attacker is to compromise its confidentiality, integrity and authenticity (CIA). The threats to information can be exploited in following different security aspects [50].

4.2.1. Threats to Confidentiality of Information

Information contains important messages about a particular event, which is usually exchanged among the vehicles and RSUs during V2V and V2I communication. Threats to information always exist where the main interest of the attacker is to compromise its confidentiality, integrity and authenticity (CIA). The threats to information can be exploited in following different security aspects [51].

4.2.2. Threats to Authenticity of Information

The routing of accurate and authentic information should be ensured in VANET as it involves several critical and lifesaving contexts. The source and destination in VANET must be known and verifiable. The threat lies to information from this perspective is the identity theft of vehicular user from an attacker. This can lead to severe and drastic results in VANET, especially during the event of an accident.

4.2.3. Threats to Integrity of Information

Information transmitted from source should arrive to destination without any altera-

tion to its content. The threat from this aspect is that the information can be tempered, modified or deleted from attacker in transit while carrying the transmission of information between two vehicles [52]. Therefore, integrity of information in both modes of communication (V2V and V2I) should be ensured.

4.2.4. Threats to Availability of Information

Since the main aim of VANET is to provide drivers' safety, it should be ensured that the information transmitted from any vehicle regarding particular context is available to neighboring vehicles and adjacent RSU.

4.2.5. Non-Repudiation

Non-repudiation ensures the information generated from sender and receiver is verifiable by the authorities. Therefore, the senders should be responsible for the messages generated. The threat from this category is the denial of message produced by sender or denial of message reception by receiver.

4.3. Threats to Infrastructure

Infrastructure refers to the static units present along the road in form of RSU. The probability of threats to infrastructure is high due to its non-mobile nature. The threats include damage to its hardware and access to RSU software.

4.3.1. Road Side Unit (RSU)

Usually network operators ensure high level of security in RSU but as RSU is mostly static in VANET, the major threat to RSU include physical damages to its hardware. Therefore, the physical security is mostly achieved via CCTVs. The other threats include illegal access of attacker to its software platform, DoS attack and rouge RSU. Rouge RSU must be identified intelligently and eliminated from the network.

4.3.2. Central Entity

Central entity is present in the infrastructure domain for transporting V2I messages over a long geographical area. The messages are first received at central entity, therefore, the threat exists to information itself where the attacker can modify its content. Other threats include DoS, MITM attacks and introduction of virus and Trojans to the OS of the central entity.

5. Attacks in VANET

5.1. Attacks

An attack is a sequence of calculated steps which are used to gain unauthorized entry to a system for an attacker's own interest. Attack is not a sudden process but is the result of continuous and repeated planning. The attacker needs prior knowledge of the system before planning and launching any attack. Attack steps are:

1) Monitoring the overall system
2) Collecting necessary information of the system
3) Preparing a plan for attack

4) Analyzing the attack methodology
5) Executing the attack against target system, and
6) Clear the attack tracks

Attackers are always in advantage as they have to find only a single vulnerability in the network. On the other hand, defenders have to think a step ahead of attackers to secure the whole network, *i.e.*, they have ideally to address all vulnerabilities.

5.2. Factors for Carrying Out an Attack in VANET

Pursuing and carrying-out an attack in VANET depends on various factors such as:

5.2.1. Attacker Motivation

Motivation of an attacker is one of the significant factor for carrying out an attack in VANET. The motivation of attacker is usually categorized into high, medium and low [53]. The higher the level of motivation of an attacker, the higher is the risk to VANET. The attacker can aim for any specific vulnerability he discovered in VANET and can have a major impact on the network. For example, OBU is one of the important entity of vehicle and is of great interest to every attacker. Any vulnerability in it will expose the VANET to high risk.

5.2.2. Target of Attack

Attack on VANET cannot be launched unless the attacker discovered any vulnerability in the network. The attacker can target any asset, for instance, misconfiguration of the hardware components like OBU, vehicle sensors and communication protocols which enable the sender and receiver to exchange important messages.

5.2.3. Budget for an Attack

Budget is another important factor to carry out an attack. Attackers need some resources to launch an attack against any specific component of the network such as hardware and software [54] [55]. Without any suitable resources, carrying an attack becomes very difficult, e.g., to block the communication channel, an attacker needs a signal jammer which can disturb the transportation of messages across the network. It should be noted that high budget for an attack can increase the motivation level of the attacker and therefore, the attacker can aim to launch more sophisticated attacks on VANET.

5.2.4. Time for an Attack

Time represents the total time taken by an attacker to launch an attack. This factor includes the time consumed for all attack steps such as time from gathering information until the successful execution of attack on the network [56]. Gathering information itself is a challenging and time consuming task, and in case of VANET, it is very crucial since the two vehicles meet for very small interval of time. Therefore, the attacker has to first gather information and then find a vulnerability in that short span of time.

5.2.5. Personal Reputation

The attacker can carry and pursue an attack with the intention of getting some fame

and reputation as a hacker [57]. This factor is also linked with the motivation of an attacker. To gain high reputation, the attacker can launch an attack with high level of sophistication.

5.3. Attack Steps in VANET

VANET is an important network which involves transportation of important and life-saving messages such as pre-crash warning. However, VANET is exposed to different vulnerabilities and types of attack. The attack steps in case of VANET are shown in Figure 6. These steps are as follows:

1) The attacker monitors the VANET network including every asset *i.e.*, available vehicles in the network, target wireless network and available infrastructure.

2) Attacker collects all the possible information of every available entity in VANET. For instance, the attacker tries to get information regarding the OBU of vehicle or V2V and V2I communication protocols. The main motivation of this step is to find known vulnerabilities in the network which can be targeted by an attacker.

3) Attacker plans the strategy of an attack in VANET, *i.e.*, how and which asset of VANET will be an easy target for him. This planning can be against:

a) *Vehicular System*: One component which attacker can aim is the wireless network of the vehicular system. Since important messages are carried through wireless medium such as DSRC and IEEE 802.11 technology, the wireless network is exposed to different vulnerabilities, providing many opportunities to the attacker to plan an attack against it. Other targets in vehicular system includes different components of vehicle such as OBU and sensors.

b) *Information*: One of the targets of an attacker is the information in transit from one vehicle to its neighbor vehicles and RSUs.

c) *Infrastructure*: The lowest priority of these attacks will be the adjacent infrastructure, *i.e.*, RSU and mobile communication base stations like Relay Nodes and LTE base station. Usually, the network operators ensure high level of security, therefore, gaining access to these infrastructure usually requires high level motivation and high engagement of attackers.

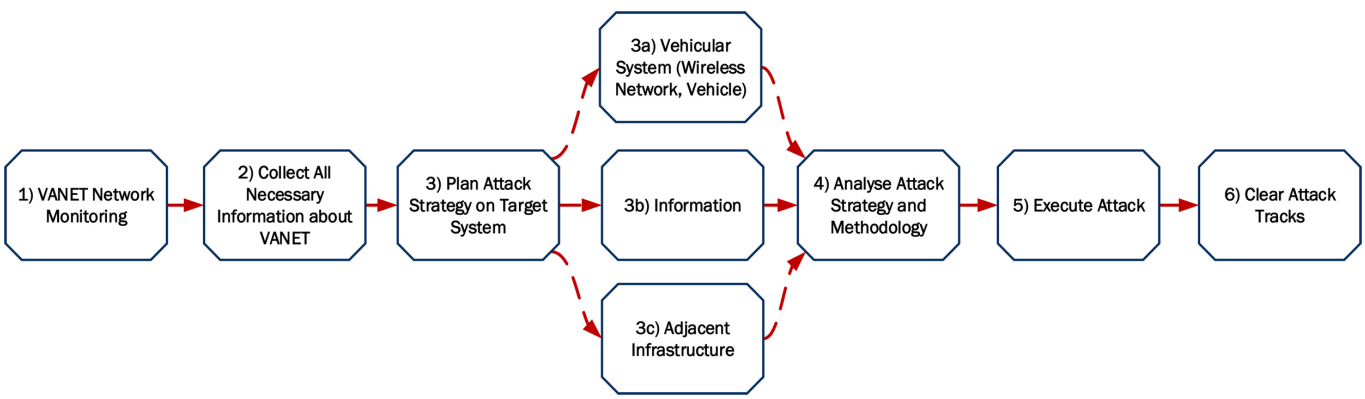

Figure 6. Attack steps in VANET.

4) Attacker analyses the strategy and the methodology of carrying an attack on VANET.

5) The attacker executes its plan by targeting the vulnerability discovered in the network

6) After execution of an attack, the main focus of the attacker is to clear his attack tracks, so that no one can blame him out for that specific attack such as different anti-forensic techniques to deceive law enforcement agencies [48].

5.4. Attacks in VANET

This section is dedicated for the attacks categorized according to VANET assets. The detailed taxonomy of attacks in VANET is depicted in **Figure 7**.

5.4.1. Attacks on Vehicular System

Vehicular system constitutes an important asset in VANET. The attacks specific to vehicular system are:

1) Social Ethical Attacks

This attack deals with the moral ethics of vehicular users. The main aim of this attack is to play with the emotions of the user by transmitting non-moral and inappropriate messages [20].

2) Cheating Sensor Information Attack

These attacks focuses on hacking the OBU and AU of a vehicle. This results in the modification of the sensor information such that it can cheat the authorities by changing its different parameters like location and speed [49].

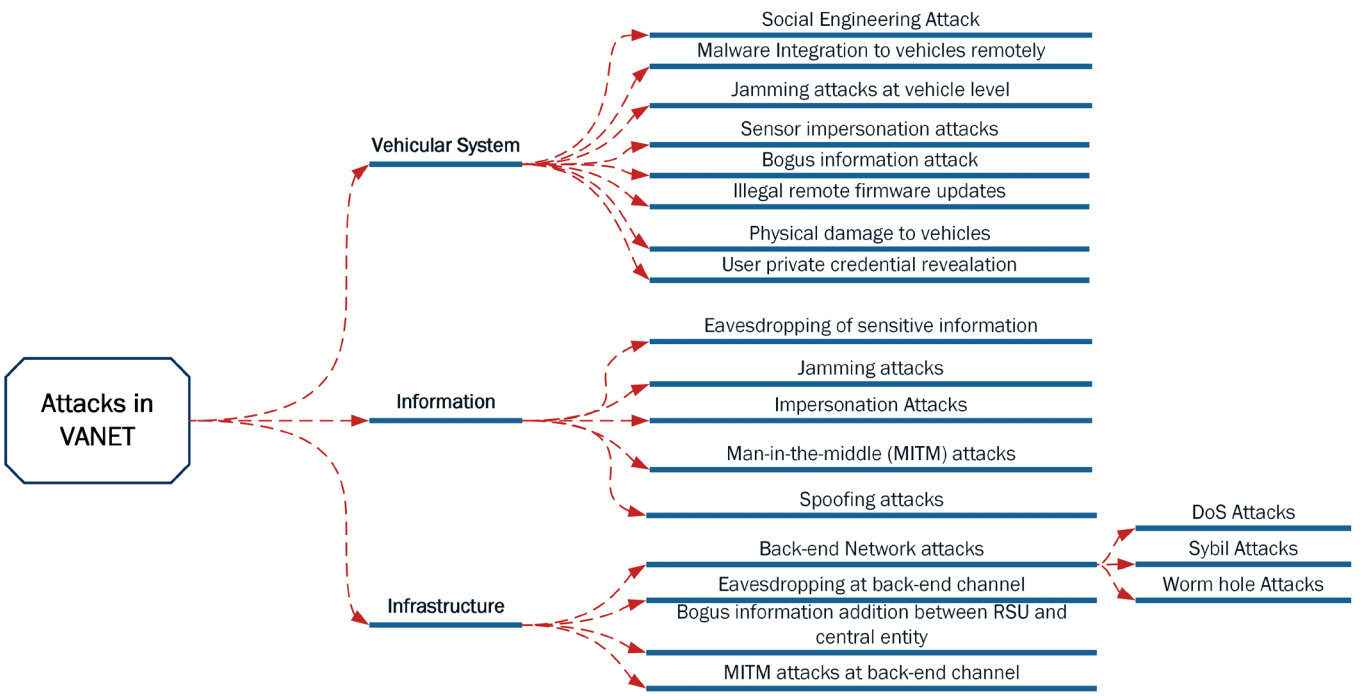

Figure 7. Taxonomy of attacks in VANET.

3) Jamming Attacks at Vehicle Level

The main focus of these attacks is to prevent communication between the internal components of vehicles by jamming its communication network. These attacks include Denial of Service (DoS) and Distributed DoS (DDoS) attacks [58].

4) Bogus Information Attack

In this attack, the attacker tries to affect the network by transmitting false and wrong information to other vehicles. For instance, the attacker can free the road for himself by creating congestion to neighboring vehicles by transmitting false information.

5) Sensor Impersonation Attack

In VANET, the vehicle is equipped with various sensors ranging from speed sensor to positioning sensor. Every vehicle is assigned a unique identity in the network. In this attack, the attacker impersonates the legitimate vehicle sensors to perform the desired operation for attackers benefits and then changes its identity [59]. For instance, if an attacker is involved in some accident, then he changes his identity and can deceive the law enforcement authorities. This attack is possible due to the hardware vulnerabilities of the OBU where the attacker can access the desired sensor and impersonates it and disable the functionality of particular sensor.

6) Physical Damage to Vehicular Components

Physical damage (e.g. vandalism) by an attacker can compromise the security of vehicle and its assets; thus resulting in the propagation of tempered messages in the network.

7) Malware Integration to Vehicles Remotely

In this particular cyberattack, the attacker introduces malware (virus, spam, and Trojans) to the vehicular system using one of the following assets: a) *In-Vehicle communication network*: The attacker adds malware to the information propagated between internal components of the vehicles, and b) *Wireless Communication:* where malware is integrated at the OBU of the vehicle by an attacker, thus resulting in the exchange of compromised messages between neighboring vehicles.

8) Network Monitoring Attack

In this attack, the attacker monitors the whole network and listens to the communication between vehicles and can pass this sensitive information to beneficiaries. For instance, an attacker can change the information of patient sent by an ambulance.

5.4.2. Attacks on Information

As mentioned earlier, information is the most important asset in VANET due to its critical and lifesaving messages. The attacks on the information can be categorized into following:

1) Eavesdropping of Sensitive Data

The attacker behaves passively in this attack, where the main focus of the attacker is to illegally listen to the communication in the network [60]. For instance, the communication between law enforcement authorities while chasing the criminals. The attacker can also compromise the privacy of the vehicular users where the attacker can reveal the private and useful credentials of the user such as user identity and location.

2) Jamming Attack

Jamming attacks are one of the severe attacks in VANET [61] [62] [63] where the communication channel is blocked by the attacker which stops the propagation of critical messages in the network. For example, the information of traffic jam on the highway to the following vehicles due to unavailability of communication channel can result in massive congestion on the road. Jamming attacks can be launched at following venues in the communication network: a) *Wireless Communication*: Jams the communication channel between two vehicles and neighboring RSU, and b) *Wired Communication*: Jams the communication between RSU and central entity.

3) Impersonation Attacks

In VANET, every vehicles and RSUs are assigned with a unique identity which can locate them in the network during accidents [64]. In this type of attack, the attacker changes his identity for his own benefits. For instance, if an attacker is involved in particular accident at certain location, then the attacker changes his identity, so that hecan deceive the law enforcement authorities. The attacker exploits the insecure wireless communication to impersonate the particular vehicle and alters the messages which are en-route to other vehicles.

4) Man-in-the-Middle (MITM) Attacks

MITM attacks represents an intermediate adversary node which can intercept and modify the messages en-route from RSU to vehicles and vice versa. These attacks can result in the violation of the integrity and confidentiality of the messages [65]. The attackers mostly exploit the non-encrypted nature of messages on the insecure wireless communication channel to launch these attacks. The main intentions of this adversary node is to capture the message, alter it and forward the bogus message or updated message with wrong information to other vehicles.

5) Spoofing Attacks

In this particular attack, the attacker steals the identity of a legitimate vehicle to become part of the network by transmitting wrong location information.

5.4.3. Attacks on Infrastructure

Infrastructure, being the static entity in VANET, is one of the favorite location for an attacker to launch different network attacks DoS and MITM attacks, message alteration on back-end channel and impersonation attacks.

1) Network Attacks

The attacker exploits the insecure wireless communication channel to launch illegal monitoring of the network containing significant messages such as traffic accident. The attacker can launch following attacks in the network,

a) *DoS attacks:* leaving a severe impact on the network by preventing vehicles to receive sensitive information such as road accident warnings. Two techniques are used to perform DoS attacks in VANET [66] [67]. 1) Transmission of random signal in a given frequency range of message communication, and 2) generation of messages in huge quantity at the physical layer of VANET to take down the communication channel.

b) *Sybil attacks:* which involves the generation of multiple identities by a malicious

Table 2. Attack mapping in VANET and their solutions.

Asset	Vulnerability	Threat	Attack	Solution	Violated Security Requirement
Vehicle/ Vehicular User	Software flaw (Weak message propagation algorithm)	Privacy leakage of sensitive information	Malware integration	Updating antivirus, Sandbox approach [70]	Availability/Authentication
Vehicle	OBU vulnerability	Unauthorised manipulation of routing table	Jamming attacks at vehicle level	Frequency hopping, Multiple radio transceivers	Availability
Vehicle	Vehicular hardware flaws	Disclosure of sensitive information	Sensor impersonation	SPECS [71]	Authentication
Vehicle	OBU vulnerabilities, Sensors malfunctions	Network flooding with wrong information	Bogus information	ECDSA [72]	Authentication/Integrity
Vehicle	Insecure cryptographic algorithms	Illegal software updates	Remote firmware updates	Secure firmware updates over the air (FOTA) [73]	Authentication
Vehicle/ Vehicular User	Software flaws, Weak Password	Privacy leakage of sensitive data	Social engineering attack	Encrypted and strong password for message communication	Integrity/Privacy
Vehicle	Ohysical access to vehicles	Damaging sensors to perform correctly	Physical damage to vehicles	Access control	Authentication
Vehicular User	OBU vulnerabilities, Inseucre wireless communication	Revelation of users identity	User privacy disclosure	Holistic approach for data transmission [74]	Privacy/Authentication
Information	Broadcast nature of messages via wireless communication channel	Revelation of sensitive information and user's private credentials	Eavesdropping	Strong encrypted message for user's communication	Privacy/Authentication
Information	OBU vulnerabilities, Insecure wireless communication channel	Prevents vehicles to receive sensitive information and use network services	Jamming attacks	Assign IPs to vehicles and drop duplicate IP during message transfer [58], Change packet delivery ratio (PDR) based on PDR rate decrease [75], DJAVAN [76]	Availability
Information	Insecure wireless communication channel	Messages alterations	Impersonation attacks	Identity-based batch verification scheme [77]	Authentication
Information	Non-encrypted messages, Insecure wireless communication channel	Message modification with wrong and compromised messages	MITM attacks	Strong cryptographic techniques	Availability/Confidentiality
Information	Vulnerable wireless communication channel	Message manipulation and dropping	Spoofing attacks	Multi-antenna system with known movements [78], Secure in-region verification [79]	Authentication
RSU, Wired communication, Central entity	Flaws in routing table and non-encrypted messages	Data leakage on back-end wired channel	Sybil attacks	Position verification of neighbouring nodes [80], VANET PKI [17], RobSAD [81]	Authentication/Availability

Continued

Wired communication channel	Un-encrypted back-end communication channel	Revelation of sensitive information	Eavesdropping between RSU and central entity	Use of encrypted messages	Confidentiality/Privacy
RSU, Central entity	Hardware vulnerabilities	Network flooding with compromised messages	Bogus information between RSU and central entity	ECDSA	Confidentiality/Authentication
Wired communication channel	Hardware malfunction, Software flaws,Un-encrypted communication channel	Message alterations en-route to other vehicles via RSU and central entity	MITM attacks between RSU and cental entity	Strong cryptographic techniques	Confidentiality/Availability
Wired communication channel	Un-encrypted back-end communication channel	Discarding messages	Wormhole attacks	Packet leash [82] [83], HEAP [84]	Confidentiality/Authentication

attacker [68]. Sybil attacks hinders the normal VANET operation as mobility of these vehicles reduces the network efficiency by increasing the difficulty of attackers identification.

c) *Worm hole attacks:* involving the tunnelling of packets between two nodes located at remote locations [69], and

d) *MITM attacks:* by creating a rogue entity between RSU and central entity.

2) Message Alteration at Back-end Channel

As infrastructure is responsible to disseminate verified information via RSU and central entity. Any attack on this information can leave a severe impact on the overall network. For instance, if the attacker can intercept and modify the message between RSU and central entity, then the whole network will be flooded with altered message, resulting in huge impact on the overall network.

Table 2 summarizes possible attacks in VANET based on assets, vulnerabilities and threats reviewed in section 2, 3 and 4 respectively. Moreover, the table also provides reasonable solutions to these identified attacks.

6. Conclusions

VANET is an important and promising technology which aims to increase safety on the roads by enabling vehicles to communicate with each other. However, this communication between vehicles via insecure communication channel exposes VANET to various threats and attacks. This paper reviews these attacks from cyber security aspects where a systematic methodology is proposed and adopted to identify attacks on VANET.

It can be concluded that attackers can exploit the threats reviewed in section 4 for their own benefits by identifying different vulnerabilities in infrastructure, information and vehicular systems to launch several attacks. However, the window of opportunity for an attacker to launch attacks on the information and vehicular system is very small. This is due to the fact that vehicles are highly mobile and diverse, providing a limited time for vehicles to interact via V2V communication. On the other hand, infrastructure

are exposed to various threats due to their static nature, thus resulting in high probability of attack occurrence. Although, network operators ensure high security in RSU, the potential for attacks are still significant enough, given a highly motivated attacker. These attacks can have a severe impact on VANET. Therefore, for secure transmission of information, access to the network for an attacker should be restricted. Moreover, a strong security framework for message routing is required for VANET due to the sensitive nature involved, such as collision avoidance messages.

This study provides a basic platform for identifying various parameters in the design of security frameworks (e.g., intrusion detection) in VANET. In our future work, we will design a security framework at the asset level in VANET to ensure secure routing of messages in an attack-free environment.

References

[1] World Health Organization (2015) Global Status Report on Road Safety.

[2] Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H. and Zedan, H. (2013) A Comprehensive Survey on Vehicular Ad Hoc Network. *Journal of Network and Computer Applications*, **37**, 380-392. https://doi.org/10.1016/j.jnca.2013.02.036

[3] Hu, B. and Gharavi, H. (2011) A Joint Vehicle-Vehicle/Vehicle-Roadside Communication Protocol for Highway Traffic Safety. *International Journal of Vehicular Technology*, **2011**, Article ID: 718048. https://doi.org/10.1155/2011/718048

[4] Bhoi, S. and Khilar, P.M. (2014) Vehicular Communication: A Survey. *Networks IET*, **3**, 204-207. https://doi.org/10.1049/iet-net.2013.0065

[5] Markets and Markets (2016) Intelligent Transportation System Market by Roadway (Hardware, Software, & Services), Aviation Tool (Kiosk, Multi-User Flight Information Display, and Smart Gate System), Railway, Maritime, Protocol, Application, and Geography—Global Forecast to 2022. http://www.marketsandmarkets.com/Market-Reports/intelligent-transport-systems-its-market-764.html

[6] Gerla, M., Lee, E., Pau, G. and Lee, U. (2014) Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds. *IEEE World Forum on Internet of Things*, Seoul, 6-8 March 2014, 241-246. https://doi.org/10.1109/wf-iot.2014.6803166

[7] Grassi, G., Pesavento, D., Pau, G., Vuyyuru, R., Wakikawa, R. and Zhang, L. (2014) VANET via Named Data Networking. *IEEE Conference on Computer Communications Workshops*, Castle Toronto, 27 April-2 May, 410-415. https://doi.org/10.1109/infcomw.2014.6849267

[8] Ahmad, F. and Adnane, A. (2015) Design of Trust Based Context Aware Routing Protocol in Vehicular Networks. Poster Presented at 9th IFIP WG 11.11 International Conference on Trust Management , Hamburg, 26-28 May 2015.

[9] Jeong, J. and Lee, E. (2014) Vehicular Cyber-Physical Systems for Smart Road Networks. *KICS Information and Communications Magazine*, **21**, 103-116.

[10] Da Cunha, F., Boukerche, A., Villas, L., Viana, A. and Loureiro, A. (2014) Data Communication in VANETs: A Survey, Challenges and Applications. INRIA Technical Report RR-8498, Saclay.

[11] Moustafa, H. and Zhang, Y. (2009) Vehicular Networks: Techniques, Standards, and Applications. Auerbach Publications, Boca Raton. https://doi.org/10.1201/9781420085723

[12] Vegni, A.M., Biagi, M. and Cusani, R. (2013) Smart Vehicles, Technologies and Main Applications in Vehicular Ad Hoc Networks. In: Giordano, L.G., Eds., *Vehicular Technologies—Development and Applications*. Intech Open Access Publisher, Rijeka, http://dx.doi.org/10.5772/55492

[13] Hartenstein, H. and Laberteaux, K. (2010) VANET: Vehicular Applications and Inter-Networking Technologies. Wiley, Hoboken. https://doi.org/10.1002/9780470740637

[14] Khaliq, K.A., Qayyum, A. and Pannek, J. (2016) Methodology for Development of Logistics Information and Safety System Using VANET. *Proceedings of the* 5*th International Conference on Dynamics in Logistics*, Bremen, 22-25 February 2016, 185-195.

[15] Ahmad, F., Marwat, S., Zaki, Y., Mehmood, Y. and Goerg, C. (2014) Machine-to-Machine Sensor Data Multiplexing Using LTE-Advanced Relay Node for Logistics. *Proceedings of the* 4*th International Conference on Dynamics in Logistics*, Bremen, February 2014, 247-257.

[16] World Economic Forum (2015) Global Risks 2015 Report. 10th Edition, World Economic Forum, Geneva.

[17] Raya, M., Papadimitratos, P. and Hubaux, J.-P. (2006) Securing Vehicular Communications. *IEEE Wireless Communications Magazine*, **13**, 8-15. https://doi.org/10.1109/WC-M.2006.250352

[18] De Fuentes, J., González-Tablas, A. and Ribagorda, A. (2010) Overview of Security Issues in Vehicular Ad-Hoc Networks. In: Cruz-Cunha, M. and Moreira, F., Eds., *Handbook of Research on Mobility and Computing*: *Evolving Technologies and Ubiquitous Impacts*, IGI Global, New York, 894-911.

[19] Ahmad, F. and Adnane, A. (2016) A Novel Context-Based Risk Assessment Approach in Vehicular Networks. 30*th International Conference on Advanced Information Networking and Applications Workshops*, Crans-Montana, 23-25 March 2016, 466-474. https://doi.org/10.1109/waina.2016.60

[20] Sumra, I.A., Hasbullah, H. and Rehman, M. (2011) Trust and Trusted Computing in VANET. *Computer Science Journal*, **1**, 29-51.

[21] Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A. and Hubaux, J. (2008) Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communications Magazine*, **46**, 100-109. https://doi.org/10.1109/MCOM.2008.4689252

[22] Siddiqui, N.R., Khaliq, K. and Pannek, J. (2016) VANET Security Analysis on the Basis of Attacks in Authentication. *Proceedings of the* 5*th International Conference on Dynamics in Logistics*, Bremen, 22-25 February 2016, 491-502.

[23] Dak, A.Y., Yahya, S. and Kassim, M. (2012) A Literature Survey on Security Challenges in VANETs. *International Journal of Computer Theory and Engineering*, **4**, 1007-1010. https://doi.org/10.7763/IJCTE.2012.V4.627

[24] Hamida, E., Noura, H. and Znaidi, W. (2015) Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. *Electronics*, **4**, 380-423. https://doi.org/10.3390/electronics4030380

[25] Zheng, K., Zheng, Q., Chatzimisios, P., Xiang, W. and Zhou, Y. (2015) Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions. *IEEE Communications Surveys and Tutorials*, **17**, 2377-2396. https://doi.org/10.1109/COMST.2015.2440103

[26] Bhargava, B., Johnson, A., Munyengabe, G. and Angin, P. (2016) A Systematic Approach for Attack Analysis and Mitigation in V2V Networks. *Journal of Wireless Mobile Networks*,

7, 79-96.

[27] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B. anderson, D., Shacham, H. and Savage, S. (2010) Experimental Security Analysis of a Modern Automobile. *IEEE Symposium on Security and Privacy*, Oakland, 16-19 May 2010, 447-462. https://doi.org/10.1109/sp.2010.34

[28] Checkoway, S., McCoy, D., Kantor, B. anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. and Kohno, T. (2011) Comprehensive Experimental Analyses of Automotive Attack Surfaces. *Proceedings of the 20th USENIX Conference on Security*, Berkeley, 8-12 August 2011, 6-22.

[29] OVERSEE. Open Vehicular Secure Platform (OVERSEE). https://www.oversee-project.com/

[30] SeVeCOM. SEcure VEhicle COMmunication. http://www.transport-research.info/project/secure-vehicle-communication

[31] PRESERVE. Preparing Secure Vehicle-to-X Communication Systems (PRESERVE). https://www.preserve-project.eu/

[32] ISO (2009) ISO/IEC 27000:2009, Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. BSI Standard Publication.

[33] EVITA. E-Safety Vehicle Intrusion Protected Applications (EVITA). http://www.evita-project.org/

[34] SafeTrip. Satellite Applications for Emergency Handling, Traffic Alerts, Road Safety and Incident Prevention (SafeTrip). https://www.itu.int/dms_pub/itu-t/oth/06/41/T06410000300001PDFE.pdf

[35] PRECOISA. Privacy Enabled Capability in Co-Operative Systems and Safety Applications (PRECOISA). http://www.transport-research.info/project/privacy-enabled-capability-co-operative-systems-and-safety-applications

[36] Festag, A., *et al*. (2008) "NOW-Network on Wheels": Project Objectives, Technology and Achievements. *Proceedings of the 5th International Workshop on Intelligent Transportation*, Hamburg, 18-19 March 2008, 211-216.

[37] COMeSafety2. Communications for eSafety. http://cordis.europa.eu/project/rcn/97474 en.html

[38] Filali, F., *et al*. CopITS: The First Connected Car Standard-Compliant Platform in Qatar and the Region. Qatar Foundation Annual Research Forum Proceedings, **2012**, CSO8. http://dx.doi.org/10.5339/qfarf.2012.CSO8

[39] PREVENT. Preventive and Active Safety Application. http://www.transport-research.info/project/preventive-and-active-safety-application

[40] CONVERGE. Communication Network VEhicle Road Global Extension. http://www.converge-online.de/

[41] ASSET ROAD. Advanced Safety and Driver Support for Essential Road Transport. http://www.project-asset.com

[42] SafeITS. Engineering Security and Performance Aware Vehicular Applications for Safer and Smarter Roads. http://www.safeits.org/

[43] Doetzer, F. (2005) Privacy Issues in Vehicular Ad Hoc Networks. *5th International Workshop on Privacy Enhancing Technologies*, Cavtat, 30 May-1 June 2005, 197-209.

[44] Biswas, S., Haque, M. and Misic, J.V. (2010) Privacy and Anonymity in Vanets: A Con-

temporary Study. *Ad Hoc & Sensor Wireless Networks*, **10**, 177-192.

[45] Identifying and Classifying Assets (2002) Network Magazine. http://www.networkmagazineindia.com/200212/security2.shtml

[46] Keen Security Lab Blog (2016) Car Hacking Research: Remote Attack Tesla Motors. http://keenlab.tencent.com/en/

[47] Nilsson, D.K. and Larson, U.E. (2008) Combining Physical and Digital Evidence in Vehicle Environments. 3*rd International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland, 22 May 2008, 10-14. https://doi.org/10.1109/sadfe.2008.10

[48] Nilsson, D.K. and Larson, U.E. (2008) Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks. *Proceedings of the* 1*st ACM International Conference on Forensic Applications and Techniques in Telecommunications*, *Information*, *and Multimedia*, Adelaide, 21-23 January 2008, Article No. 8. https://doi.org/10.4108/e-forensics.2008.32

[49] Grover, J., Gaur, M.S. and Laxmi, V. (2013) Trust Establishment Techniques in VANET. In: Shafiullah, K. and Al-Sakib, K., Eds., *Wireless Networks and Security*: *Signal and Communication Technology*, Springer, Berlin, 273-301. https://doi.org/10.1007/978-3-642-36169-2_8

[50] Sumra, I.A., Ahmad, I., Hasbullah, H. and Ab Manan, J. (2011) Behavior of Attacker and Some New Possible Attacks in Vehicular Ad Hoc Network (VANET). 3*rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, Budapest, 5-7 October 2011, 1-8.

[51] Laurendeau, C. and Barbeau, M. (2006) Threats to Security in DSRC/WAVE. In: Kunz, T. and Ravi, S.S., Eds., *Ad-Hoc*, *Mobile*, *and Wireless Networks*, Springer, Berlin, 266-279. https://doi.org/10.1007/11814764_22

[52] Plossl, K., Nowey, T. and Mletzko, C. (2006) Towards a Security Architecture for Vehicular Ad Hoc Networks. 1*st International Conference on Availability*, *Reliability and Security*, Vienna, 20-22 April 2006, 374-381.

[53] Sanzgiri, A.M. and Upadhyaya, S. (2011) Feasibility of Attacks: What Is Possible in the Real World—A Framework for Threat Modeling. *Proceedings of* 2011 *International Conference on Security and Management*, Las Vegas, 18-21 July 2011. http://worldcomp-proceedings.com/proc/p2011/SAM3508.pdf

[54] Henniger, O., Apvrille, L., Fuchs, A., Roudier, Y., Ruddle, A. and Weyl, B. (2009) Security Requirements for Automotive On-Board Networks. *Proceedings of the* 9*th International Conference on Intelligent Transport System Telecommunications*, Lille, 20-22 October 2009, 641-646. https://doi.org/10.1109/itst.2009.5399279

[55] Boudguiga, A., Kaiser, A. and Cincilla, P. (2015) Cooperative-ITS Architecture and Security Challenges: A Survey. 22*nd World Congress on Intelligent Transport Systems*, Bordeaux, 5-9 October 2015, 1-22.

[56] ETSI (2006) TS 102 165-1 v4.2.1 (2006-12): Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN). Methods and Protocols, Part 1: Method and Proforma for Threat, Risk and Vulnerability Analysis. ETSI.

[57] PRESERVE (2011) Preparing Secure Vehicle-to-X Communication Systems, Security Requirements of Vehicle Secuirty Architecture, Deliverable 1.1. 7th Framework Programme.

[58] Verma, K., Hasbullah, H. and Kumar, A. (2013) Prevention of DoS Attacks in VANET. *Wireless Personal Communications*, **73**, 95-126. https://doi.org/10.1007/s11277-013-1161-5

[59] Vorugunti, C.S. and Sarvabhatla, M. (2014) A Secure and Efficient Authentication Protocol in VANETs with Privacy Preservation. *Proceedings of* 9*th International Conference on*

Wireless Communication and Sensor Networks, Nice, 21-26 July 2013, 189-201. https://doi.org/10.1007/978-81-322-1823-4_18

[60] Ekedebe, N., Yu, W., Lu, C., Song, H. and Wan, Y. (2015) Securing Transportation Cyber Physical Systems. In: Al-Sakib, K.P., Ed., *Securing Cyber-Physical Systems*, CRC Press, Boca Raton, 163-196. https://doi.org/10.1201/b19311-7

[61] Ahmad, F., Kazim, M., Adnane, A. and Awad, A. (2015) Vehicular Cloud Networks: Architecture, Applications and Security Issues. *IEEE/ACM 8th International Conference on Utility and Cloud Computing*, Limassol, 7-10 December 2015, 571-576.

[62] Ekedebe, N., Yu, W., Song, H. and Lu, C. (2015) On a Simulation Study of Cyber Attacks on Vehicle-to-Infrastructure Communication (V2I) in Intelligent Transportation System (ITS). *Proceedings of SPIE*: *Mobile Multimedia/Image Processing*, *Security*, *and Applications*, **9497**, 94970B.

[63] Ahmad, F., Kazim, M. and Adnane, A. (2016) Vehicular Cloud Networks: Architecture and Security. In Zhu, S.Y., Hill, R. and Trovati, M., Eds., *Guide to Security Assurance for Cloud Computing*, Springer, Berlin, 211-226.

[64] Mokhtar, B. and Azab, M. (2015) Survey on Security Issues in Vehicular Ad Hoc Networks. *Alexandria Engineering Journal*, **54**, 1115-1126. https://doi.org/10.1016/j.aej.2015.07.011

[65] Igure, V.M. and Williams, R.D. (2008) Taxonomies of Attacks and Vulnerabilities in Computer Systems. *IEEE Communications Surveys and Tutorials*, **10**, 6-19. https://doi.org/10.1109/COMST.2008.4483667

[66] Sanzgiri, A.M. (2013) A Comprehensive Threat Assessment Framework for Securing Emerging Technologies. PhD Thesis, the State University of New York at Buffalo, Buffalo.

[67] Lipinski, B., Mazurczyk, W., Szczypiorski, K. and Smietanka, P. (2015) Towards Effective Security Framework for Vehicular Ad Hoc Networks. *Journal of Advances in Computer Networks*, **3**, 134-140. https://doi.org/10.7763/JACN.2015.V3.155

[68] Guette, G. and Bertrand, D. (2007) On the Sybil Attack Detection in VANET. *IEEE International Conference on Mobile Adhoc and Sensor Systems*, Pisa, 8-11 October 2007, 1-6. https://doi.org/10.1109/mobhoc.2007.4428742

[69] Raya, M. (2009) Data-Centric Trust in Ephemeral Networks. PhD Thesis, Ecole Polytechnique Federale de Lausanne (EPFL), Lausanne.

[70] Nikaein, N., Datta, S.K., Marecar, I. and Bonnet, C. (2012) Application Distribution Model and Related Security Attacks in VANET. *International Conference on Graphic and Image Processing*, Singapore, 6-7 October 2012, Article CID Number: 876808. http://www.icgip.org/history/12FRONT_Part1.pdf

[71] Chim, T.W., Yiu, S.-M., Hui, L.C. and Li, V.O. (2011) SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs. *Ad Hoc Networks*, **9**, 189-203. https://doi.org/10.1016/j.adhoc.2010.05.005

[72] Manvi, S., Kakkasageri, M. and Adiga, D. (2009) Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approach. *International Conference on Future Computer and Communication*, Kuala Lumpur, 3-5 April 2009, 16-20. https://doi.org/10.1109/icfcc.2009.120

[73] Nilsson, D.K. and Larson, U.E. (2009) A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure. *Journal of Networks*, **4**, 552-564. https://doi.org/10.4304/jnw.4.7.552-564

[74] Tamil Selvan, K.S. and Rajendiran, R. (2013) A Holistic Protocol for Secure Data Transmission in VANET. *International Journal of Advanced Research in Computer and Communication Engineering*, **2**, 4840-4849.

[75] Nguyen, A.T., Mokdad, L. and Ben Othman, J. (2013) Solution of Detecting Jamming Attacks in Vehicle Ad Hoc Networks. *Proceedings of the* 16*th ACM International Conference on Modeling, Analysis & Simulation of Wireless and Mobile Systems*, Barcelona, 3-8 November 2013, 405-410.

[76] Mokdad, L., Ben-Othman, J. and Nguyen, A.T. (2015) DJAVAN: Detecting Jamming Attacks in Vehicle Ad Hoc Networks. *Performance Evaluation*, **87**, 47-59. https://doi.org/10.1016/j.peva.2015.01.003

[77] Zhang, C., Lu, R., Lin, X., Ho, P.-H. and Shen, X. (2008) An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks. *The* 27*th IEEE Conference on Computer Communications*, Phoenix, 15-17 April, 2008, 816-824. http://dx.doi.org/10.1109/INFOCOM.2008.58

[78] Montgomery, P.Y., Humphreys, T.E. and Ledvina, B.M. (2009) Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer. *Proceedings of the ION International Technical Meeting*, Anaheim, 26-28 January 2009, 124-130.

[79] Song, J.-H., Wong, V.W. and Leung, V.C. (2008) Secure Location Verification for Vehicular Ad-Hoc Networks. *IEEE Global Telecommunications Conference*, New Orleans, 30 November-4 December 2008, 1-5. https://doi.org/10.1109/glocom.2008.ecp.160

[80] Leinmuller, T., Maihofer, C., Schoch, E. and Kargl, F. (2006) Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification. *Proceedings of the* 3*rd International Workshop on Vehicular Ad Hoc Networks*, Los Angeles, 29 September 2006, 57-66. https://doi.org/10.1145/1161064.1161075

[81] Chen, C., Wang, X., Han, W. and Zang, B. (2009) A Robust Detection of the Sybil Attack in Urban VANETs. 29*th IEEE International Conference on Distributed Computing Systems Workshops*, Montreal, 22-26 June 2009, 270-276. https://doi.org/10.1109/icdcsw.2009.48

[82] Hu, Y.-C., Perrig, A. and Johnson, D.B. (2003) Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. 22*nd Annual Joint Conference of the IEEE Computer and Communications*, San Francisco, April 2003, 1976-1986.

[83] Hu, Y.-C., Perrig, A. and Johnson, D.B. (2006) Wormhole Attacks in Wireless Networks. *IEEE Journal on Selected Areas in Communications*, **24**, 370-380. https://doi.org/10.1109/JSAC.2005.861394

[84] Safi, S.M., Movaghar, A. and Mohammadizadeh, M. (2009) A Novel Approach for Avoiding Wormhole Attack in VANET. 1*st Asian Himalayas International Conference on Internet*, Kathmandu, 3-5 November 2009, 54-59. https://doi.org/10.1109/AHICI.2009.5340317