# Security Threats in Intelligent Transportation Systems and Their Risk Levels

Besma Zeddini, Mohamed Maachaoui, Youssef Inedjaren

risks

MDPI

*Article*

# Security Threats in Intelligent Transportation Systems and Their Risk Levels

**Besma Zeddini [1,*], Mohamed Maachaoui [2] and Youssef Inedjaren [2]**

[1] SATIE Laboratory CNRS-UMR 8029, CY Tech, 95000 Cergy, France
[2] Quartz Laboratory EA7393, CY Tech, 95000 Cergy, France; mohamed.maachaoui@cyu.fr (M.M.); youssef.inedjaren@cyu.fr (Y.I.)
* Correspondence: besma.zeddini@cyu.fr; Tel.: +33-134251008

**Abstract:** Intelligent Transport Systems (ITSs) are part of road transportation sector evolution and constitute one of the main steps towards vehicle automation. These systems use technologies that allow vehicles to communicate with each other or with road infrastructure. By increasing information quality and reliability, ITSs can improve road safety and traffic efficiency, but only if cybersecurity and data protection is ensured. With the increase in the number of cyberattacks around the world, cybersecurity is receiving increased attention, especially in the area of transportation security. However, it is equally important to examine and analyze security in depth when it concerns connected vehicles. In this paper, we propose a qualitative risk analysis of ITSs based on Threat, Risk, Vulnerability Analysis (TVRA) methodology, and we focus on ETSI ITS communication architecture. We present a review of solutions and countermeasures for identified critical attacks.

**Keywords:** ITS; qualitative risk analysis; VANET; security threats; countermeasures; TVRA; communication



**Citation:** Zeddini, Besma, Mohamed Maachaoui, and Youssef Inedjaren. 2022. Security Threats in Intelligent Transportation Systems and Their Risk Levels. *Risks* 10: 91. https://doi.org/10.3390/risks10050091

Academic Editors: Michel Dacorogna and Marie Kratz

Received: 25 November 2021
Accepted: 12 April 2022
Published: 21 April 2022



## 1. Introduction

Intelligent Transport Systems are the solution to modern transportation problems such as congestion, accidents, etc. As mentioned in Rafiq et al. (2013), within an ITS, the drivers will be notified in advance of hazards on the road ahead before they are visible, and vehicles will be kept at a safe distance from one another by suggesting an optimum speed based on various parameters related to traffic conditions. For integrated communication technologies, users will be able to use vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. These communications provide system components with interaction capacity by exchanging real-time information on public transport services, real-time travel and traffic information (RTTI), as well as smart and seamless ticketing solutions.

Like any connected system, intelligent transport systems, especially vehicular ad-hoc network (VANET) systems, expose transport operators to increased risks in terms of cybersecurity. Indeed, these systems are often collaborative and communicate with each other, with equipment, or with heterogeneous information systems, and allow access to various networks such as the internet. The interconnection of these networks increases the vulnerability of attacks and can generate the possibility of being the target of intrusions and cyberattacks. Damage from these attacks can be dramatic. Protection of these systems requires a deep risk analysis (qualitative and quantitative) and the implementation of efficient methods adapted to critical environments while taking into account the ease of use and the real-time context. As ITSs propose critical road safety applications that may affect humans, security of ITSs is an important and emerging issue (U.S. Department of Transportation 2017; Sharma et al. 2017). These systems are based on vehicular communications that inherit traditional problems associated with wireless networks. ITS security is a complex task as it deals with various elements (applications, communication architecture and protocols). To guarantee this security, it is pertinent to identify the likely potential

threats to the ITS and then create apposite security solutions to mitigate threats. To achieve this, we conduct a risk analysis study to classify risks so as to understand the degree of seriousness of a particular threat and to be able to propose countermeasures for identified threats using the Threat, Risk, Vulnerability Analysis (TVRA) methodology.

Many risk analysis methods exist in the literature, such as Expression des Besoins et Identification des Objectifs de Securite (EBIOS). The aim of EBIOS is to formalize objectives and safety requirements adapted to the studied system and its context while taking into account business processes. The difference between EBIOS and TVRA is that EBIOS is a generic method, while TVRA is a detailed method usually used to determine specific vulnerabilities.

In this paper, we focus on ETSI ITS communication architecture, applying the Threat Vulnerability Risk Assessment (TVRA) method ETSI (2011). The results of our analysis is a list of vulnerabilities with the seriousness of their risk level. The rest of this paper is organized as follows: Section 2, provides an introduction to the ETSI ITS-S communication stack. Then, in the following section, we present the detailed risk analysis with applications and proposed vulnerabilities. In Section 5, we propose a review of countermeasures for identified critical attacks, and the last section concludes the paper.

## 2. ETSI ITS-S Communication Architecture

ITS communications are based on ITS-S architecture of communication described in ETSI EN 302 665 (ETSI 2010). ITS-S standards are based on a common communication architecture (ITS-S reference architecture ISO 21217). This is essential to ensure the interoperability of systems deployed in vehicles, road infrastructure, urban infrastructure and control centers available through the internet infrastructure. The communication architecture of ETSI ITS-S is structured in layers and is based on the OSI or TCP/IP communication models. ETSI ITS-S architecture supports wired and wireless communication technologies, versus to the IEEE WAVE communication architecture (IEEE 2010) (based on IEEE 802.11p). Separation into layers allows applications to be developed that operate independently of the underlying technologies, thus enabling portability across distinct hardware and software platforms, and allowing features or technologies to be replaced or added in the lower layers without impacting the higher layers. This is the model that made internet communication successful because it allows end-to-end exchanges between two remote peers that use separate means of communication (e.g., a vehicle connected only to the cellular network can communicate with another vehicle connected to the internet via WiFi). The "ETSI ITS-S" architecture includes (cf. Figure 1):

- *A lower "access technologies" layer (ITS-S access technologies layer)* allowing the integration of all existing and future access technologies, provided that each new access technology respects the rules of integration to the architecture (specified in ISO 21218). Today, vehicular WiFi (IEEE 802.11p, with ISO M5, ETSI ITS G5, IEEE P1609 variants), urban WiFi (IEEE 802.11n/b/g/ac), cellular (2G, 3G, 4G, etc.), satellite and 6LoWPAN sensor networks (IEEE 802.14) are already supported.
- *An ITS-S networking & transport layer* allowing both localized communications (ISO FNTP, ETSI GeoNetworking, IPv6) for direct exchanges between vehicles and infrastructure (V2V, V2R) and remote communications (IPv6) with distant peers. GeoNetworking is designed to use vehicular WiFi only; however IPv6 allows transmission over any locally available technology (IPv6 transmission can also be done over an existing IPv4 access network when IPv6 is not deployed).
- *A "services" layer (ITS-S facilities layer)* allowing applications to benefit from shared services, in particular standardized messaging, a database (LDM), datagram tagging services (time-stamping, geo-stamping), reliable positioning (fusion of data from several sources: GPS, roadside beacons, CAN bus, etc.). This layer also has the ability to direct datagrams to the most suitable communication stack according to the communication profile and the current capabilities of the ITS station.

- *An "applications" layer* where all applications can benefit from the shared or communication services of the lower layers without being constrained. To benefit from these services, the applications must make their communication needs known by providing the management entity with the characteristics of each of the data flows likely to be transmitted by the application.
- *Two cross-layers:* (1) A vertical (cross-layer) management entity, allowing management of the internal functionalities of the ITS-S (in particular the functionalities available in each layer) to determine which access technologies are available in a given place and at a given time, and to manage the data flows (ISO 24102-6) as best as possible. (2) A vertical entity (cross-layer) of security, allowing all layers to benefit from the mechanisms necessary to secure communications (encryption, authentication, etc.).

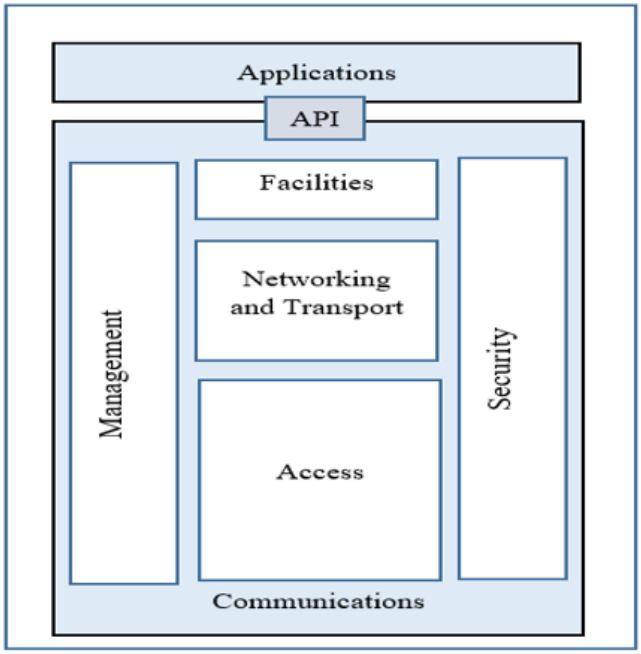


**Figure 1.** ETSI ITS Architecture.

## 3. Risk Analysis Study

Intelligent Transport Systems, even if they facilitate the gathering, processing and exchange of information, are not the guarantors in themselves, and raise issues of security and safety that require special attention: What are the main security measures that should be taken to address the risk of cyber attacks in ITS communications? In order to develop a complete security architecture with mechanisms adapted to ITS communications, we propose to use a risk analysis method to apprehend various attacks and to propose countermeasures according to the identified threat levels. Risk analysis is essentially used to identify potential vulnerabilities and threats related to the ITS, its interfaces and its environment in order to evaluate them and propose security solutions to remove, reduce or control them. There are many risk analysis methods in the literature, such as Expression of Needs and Identification of Safety Objectives (EBIOS), Analysis of Vulnerabilities, Threats and Risks (TVRA), etc. In this section, we present our analysis based on the TVRA methodology developed by ETSI to understand and measure the impact of the risk involved in ITSs and therefore to decide on appropriate measures and controls to manage them.

### *3.1. Risk Analysis Study in ITSs*

#### 3.1.1. TVRA Brief Description

The European Telecommunications Standards Institute (ETSI) has produced a methodology for practical assessment, known as the TVRA methodology, regarding three types

of system threats to be analyzed: (1) threats to the system, (2) system vulnerabilities and (3) risks related to system implementation. The ETSI assessment methodology that underlies the TVR analysis methodology is that any security-sensitive system should be assessed and tested against the security perimeter by which a system strengthens its properties.

Fundamentally, TVRA is used as a security analysis methodology designed to analyze and evaluate the characteristics of complex systems according to the probability of attacks or threats, vulnerabilities and possible risks. It first identifies the system assets and their associated threats, as well as the threat agent that will attack the system assets. Current TVRA methods focus on the behavior of the system enforced by countermeasures that are able to resist intelligent attacks. TVRA then provides risk for the identified threats, using estimated values for their likelihood and impact on the system. The results of performing TVRA are a measure of risk and the identification of countermeasures.

#### 3.1.2. Risk Analysis

In our analysis, we focus on the ETSI ITS-S communication architecture according to TVRA: we first model a system composed of assets and identify the components of the system and their associated weaknesses. An asset can be physical, human or logical and has vulnerabilities that can be attacked by threats. Thus, we identify attacks at each layer of the communication stack: access, network and transport, facilities and applications. TVRA consists of ten steps starting with identification of the Target of Evaluation (TOE), which leads to a high-quality specification of the main assets of the TOE and its context, as well as a statement of the objective, aim and reach of the TVRA. Then, we identify security purposes and requirements, and we classify threats in ITSs. Finally, we evaluate the risk by determining the likelihood and severity of the threats.

#### 3.1.3. Target of Evaluation (ToE)

**Assumptions**

We will consider the following assumptions:

- There is a passenger in the vehicle;
- Threats require between one day and one week to be identified and developed;
- Attackers are experts.

**System assets**

Taking into account the last assumption, an ITS system is composed of logical assets, physical assets and human assets.

As physical assets, we enumerate:

Vehicles: vehicles are essential entities of VANET that can play different important roles in the network: (1) generate critical data (information about traffic state), (2) route data to other vehicles and (3) store critical data (user identity, alert messages). In VANET, each vehicle is composed of: (1) sensors, (2) application utility (AU) and (3) on board unit (OBU). The sensors receive information on the environment and the AU generates messages based on collected information. These messages are shared with neighbors via the OBU. The compromise of vehicles or other ITS components will cause modification of messages as well as routing operations, leading to the propagation of compromised messages in the system.

Road Side Unit (RSU): an RSU, as a static component, is more vulnerable to cyberattacks, and constitutes one of the privileged passages for attackers to enter the VANET. An RSU serves as a link between vehicles and infrastructure (V2I). The important elements of the RSU are its hardware, its operating system (OS) and the software embedded in the OS. This software is used to interact with vehicles and infrastructure. If the RSU incurs a risk, the data stored in the RSU is compromised, and communication with the infrastructure is not secured.

To these physical assets, we associate these logical assets:

Shared Data: Important messages are communicated and shared between different vehicles and adjacent RSUs. Since these messages can be vital information, such as a

crash warning, or critical information, such as private user data (e.g., ID and location), the security and confidentiality of the data need to be ensured in terms of confidentiality, integrity and availability (Ahmad et al. 2016).

Network Communication Protocols: Once we have introduced the different nodes of the VANET and their security role, we should provide secure communication between them. This involves the following kinds of communication:

- 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.

For human assets:

VANET User: Since VANET is built to ensure the safety and convenience of vehicle users, the most important asset of VANET is the user. The safety of the users and their identity security are critical. In addition, the privacy of the user is considered the primary concern of VANET users and must be ensured. If the user is compromised, for example by a social engineering attack, all their personal information is compromised and their vehicle is a point of vulnerability for the entire VANET system (Ahmad et al. 2016).

**Threat agents**

In our analysis, we adhere to the four dimensions of threat agents defined in Moalla et al. (2012):

- A threat agent with programmable radio transmitters/receivers.
- A valid ITS-S (node of a system)
    - used as an attack proxy by a remote threat agent;
    - providing false or misleading information;
    - using programmable radio transmitters/receivers.

#### 3.1.4. Security Objectives

Restricting to the system assets discussed below, we outline the security targets that must be addressed when specifying the security configuration and protocols. These security goals are Moalla et al. (2012): (1) secure V2X communications; (2) secure the physical entities of the VANET (ITS infrastructure).

To secure communication between ITS entities, multiple security requirements need to be guaranteed:

- Availability: ITS entities and applications require a high level of availability for data and services, and require that at all times, authorized entities should never be denied access to requisite services.
- Authentication: Authentication ensures that entities involved in communication are correctly identified and authentic. Entity authorization is necessary for applications that need definition of the rights that an entity (vehicle or infrastructure) has.
- Integrity: Integrity ensures that exchanged information and data used inside the vehicle (sensor data, data used by software, etc...) are not modified.
- Confidentiality: Confidentiality consists of preventing sensitive information from reaching the wrong people.
- Privacy: Privacy is a crucial security concern because ITS systems share private information, including positional data, via wireless communications. The key to developing an ITS security solution is to consider policies that guarantee the protection of private data.

#### Threats in ITSs

We classify threats in ITSs into two categories: attacks targeting authentication (Table 1) and attacks targeting availability (Table 2).

**Table 1.** Attacks targeting authentication.

| Attack | Asset | Vulnerability | Threat | Solution | Violated Security Requirement |
|---|---|---|---|---|---|
| Sybil Attack | Infrastructure communication | Flaws in the routing table and unencrypted messages | Data leakage on back-end channel | Verification of the position of neighboring nodes (Leinmüller et al. 2006), VANET PKI (Raya et al. 2006) | Authentication/ Availability |
| User privacy disclosure | Vehicle user | Vulnerabilities of OBU; unsecured wireless communication | Revelation of user identity | Holistic approach to data transmission (TamilSelvan and Rajendiran 2013) | Privacy/ Authentication |
| Eavesdropping | Information | Nature of message delivery via a wireless communication channel | Revelation of sensitive information and private user IDs | Strong encryption of messages for user communication | Privacy/ Authentication |
| Impersonation attack | Information | Unsecured wireless communication channel | Message changes Message modifications | Use variable MAC and IP addresses for V2V and V2I communications (Al-Kahtani 2012), Authenticate via digital certificates (Al-Kahtani 2012) | Authentication |
| Spoofing attack | Information | Vulnerable wireless communication channel | Manipulation and abandonment of messages | Multi-antenna system with known motions (Montgomery 2011); secure verification in the region (Song et al. 2008) | Authentication |
| Sensor impersonation | Vehicle | Defects of vehicle equipments | Disclosure of sensitive information | SPECS (Chim et al. 2011) | Authentication |
| Wormhole attack | Infrastructure communication | Unencrypted back-end communication channel | Delete messages | Packet leash (Hu et al. 2006); HEAP (Safi et al. 2009) | Confidentiality/ Authentication |

**Table 2.** Attacks targeting availability.

| Attack | Asset | Vulnerability | Threat | Solution | Violated Security Requirement |
|---|---|---|---|---|---|
| Jamming attacks at vehicle level | Vehicle | OBU vulnerabilities | Unauthorized manipulation of the routing table | Frequency hopping; multiple radio transceivers | Availability |
| Jamming attacks | Information | Vulnerabilities of OBU; unsecured wireless communication channel | Prevents vehicles from receiving sensitive information and using network services | Assign IP addresses to the vehicles and delete duplicate IP addresses when forwarding the message (Nguyen et al. 2013); DJAVAN (Mokdad et al. 2015) | Availability |
| Malware integration | Vehicle/vehicle user | Software fault (weak message propagation algorithm) | Leakage of sensitive private information | Update the antivirus; sandbox approach (Hortelano et al. 2010) | Availability/ authentication |
| MITM attacks | Information | Unencrypted messages; unsecured wireless communication channel | Editing message with incorrect information and compromised messages | Strong cryptographic techniques (Daeinabi and Rahbar 2013) | Availability |
| MITM attacks between RSU and cental entity | Infrastructure communication | Hardware malfunction; software defects; unencrypted communication channel | Modifications of messages transmitted to other vehicles via RSU and the central entity | Strong cryptographic techniques (Wahab et al. 2014) | Availability |
| JellyFish/ intelligent cheater | Information | Vulnerabilities of end-to-end congestion control protocols | Disorder, delay or periodically drop packets that are supposed to be transmitted | End-to-end control mechanisms with long-term monitoring | Availability |
| Flooding attacks | Vehicle/ infrastructure | Unsecured wireless communication channel | Network resources are no longer available to legitimate users | Flood-resilient broadcast authentication for VANET (Baiad et al. 2014) | Availability |
| Blackhole attack | Information | Unsecure communication protocols | Prevents vehicles and infrastructure from receiving important messages and alerts | Watchdog mechanism (Yao et al. 2017), Trust model based on weights (Hsiao et al. 2011) | Availability |

#### 3.1.5. Risk Analysis

TVRA methodology (ETSI 2011) calculates the risk of identified threats using estimated values for the likelihood of occurrence and impact of threat to the system using the formula: Risk = Likelihood * Impact (Moalla et al. 2012).

The risk is computed as the product of the numerical values of the likelihood and impact. The classes in which the risk is considered relevant are defined as: Critical (9,6)—countermeasures must be designed without delay; Major (4)— the threat will potentially need attention; Minor (3,2,1)—the threat can be ignored in the short term (cf. Table 3).

We used the definitions provided in ETSI (2003) to further break down the likelihood component into its two natural components: the technical difficulty in carrying out the threat and the motivation or potential gain on the part of the attacker for him or her to proceed. The values for technical difficulty (needed capabilities) can be defined in terms of whether or not the threat has previously been considered in theory or in practice.

The following factors are assessed during the analysis to identify the weight of the attack potential required to exploit a vulnerability: system knowledge, time, expertise, opportunity and facilities.

We define four levels for needed capabilities, according to Moalla et al. (2012): no rating (4); basic (3); moderate (2); extensive (1). The levels for motivation include: High—significant gains for attacker; Moderate—service disruption only; Low—no significant

gains (cf. Table 4). Three levels of likelihood are defined with an associated numerical value: Likely (3)—all elements in place; Possible (2)—some elements in place; Unlikely (1)—important elements missing (cf. Table 5). Necessary abilities and related motivation are used to determine the probability or likelihood assessment, as shown in Table 6.

For impact, we consider asset impact: Low (1)—the possible damage is low; Medium (2)—the threat concerns provider/subscriber interests and cannot be ignored; High (3)—a business base is under attack and serious damage may happen in this context as shown in Table 7. To obtain the threat impact, we then assess asset impact in light of the severity of the attack: single instance of attack (0); moderate level of multiple instances (1); high level of multiple instances (2); to obtain the threat impact.

**Table 3.** Risk Assessment.

| Threat Group | Attack | | | | | Impact | Risk |
|---|---|---|---|---|---|---|---|
| | **Factor** | **Range** | **Value** | **Potential** | **Likelihood** | | |
| Sybil attack | Time | ≤1 week | 1 | Moderate | Possible | High | Critical |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Restricted | 3 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Specialized | 3 | | | | |
| | Motivation | High (commited) | 3 | | | | |
| | Asset impact | High | 3 | | | | |
| | Intensity | High intensity | 2 | | | | |
| Eavesdropping | Time | ≤1 week | 1 | Moderate | Possible | Medium | Major |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Public | 0 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Specialized | 3 | | | | |
| | Motivation | Medium (interested) | 3 | | | | |
| | Asset impact | Medium | 2 | | | | |
| | Intensity | Single instance | 0 | | | | |
| Impersonation attack | Time | ≤1 week | 1 | Moderate | Possible | High | Critical |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Restricted | 3 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Specialized | 3 | | | | |
| | Motivation | High (commited) | 3 | | | | |
| | Asset impact | High | 3 | | | | |
| | Intensity | Moderate intensity | 1 | | | | |
| User Privacy Disclosure | Time | ≤1 week | 1 | Moderate | Possible | High | Critical |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Public | 0 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Specialized | 3 | | | | |
| | Motivation | High (commited) | 3 | | | | |
| | Asset impact | High | 3 | | | | |
| | Intensity | Single instance | 2 | | | | |
| Spoofing Attack | Time | ≤1 week | 1 | High | Unlikely | Medium | Minor |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Sensitive | 7 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Specialized | 3 | | | | |
| | Motivation | Medium (interested) | 3 | | | | |
| | Asset impact | Medium | 2 | | | | |
| | Intensity | Single instance | 0 | | | | |

**Table 3.** *Cont.*

| Threat Group | Attack | | | | | Impact | Risk |
|---|---|---|---|---|---|---|---|
| | **Factor** | **Range** | **Value** | **Potential** | **Likelihood** | | |
| Malware Integration | Time | ≤1 week | 1 | Moderate | Possible | High | Critical |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Sensitive | 7 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Standard | 0 | | | | |
| | Motivation | High (commited) | 3 | | | | |
| | Asset impact | High | 3 | | | | |
| | Intensity | Single instance | 0 | | | | |
| Jamming Attacks | Time | ≤1 week | 1 | Moderate | Possible | Medium | Major |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Public | 0 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Bespoke | 7 | | | | |
| | Motivation | Medium (interested) | 3 | | | | |
| | Asset impact | Medium | 2 | | | | |
| | Intensity | Single instance | 0 | | | | |
| Blackhole Attack | Time | ≤1 week | 1 | Moderate | Possible | High | Critical |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Public | 0 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Specialized | 3 | | | | |
| | Motivation | High (commited) | 3 | | | | |
| | Asset impact | High | 3 | | | | |
| | Intensity | Single instance | 0 | | | | |
| Flooding Attack | Time | ≤1 week | 1 | Moderate | Possible | High | Critical |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Public | 0 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Specialized | 3 | | | | |
| | Motivation | High (commited) | 3 | | | | |
| | Asset impact | High | 3 | | | | |
| | Intensity | Moderate intensity | 1 | | | | |
| MITM | Time | ≤1 week | 1 | Moderate | Possible | Medium | Major |
| | Expertise | Expert | 6 | | | | |
| | Knowledge | Public | 0 | | | | |
| | Opportunity | Moderate | 4 | | | | |
| | Equipment | Specialized | 3 | | | | |
| | Motivation | Medium (interested) | 3 | | | | |
| | Asset impact | Medium | 2 | | | | |
| | Intensity | Single instance | 0 | | | | |

**Table 4.** Motivation.

| | |
|---|---|
| Very low (indifferent) | 0 |
| Low (curious) | 1 |
| Medium (interested) | 2 |
| High (commited) | 3 |
| Very High (focused) | 4 |

**Table 5.** Likelihood Assessment.

| **Needed Capabilities** | **Motivation** | | |
|---|---|---|---|
| | **Low (1)** | **Moderate (2)** | **High (4)** |
| No rating (4) | Possible | Possible | Likely |
| Basic (3) | Unlikely | Possible | Likely |
| Moderate (2) | Unlikely | Possible | Possible |
| Extensive (1) | Unlikely | Unlikely | Possible |

**Table 6.** Factor and Values.

| **Factor** | **Range** | **Value** |
|---|---|---|
| Time | ≤1 week | 1 |
| | ≤2 week | 2 |
| | ≤1 month | 4 |
| | ≤2 months | 7 |
| | ≤3 months | 10 |
| | ≤5 months | 15 |
| | ≤6 months | 17 |
| | ≥6 months | 19 |
| Expertise | Laymen | 0 |
| | Proficient | 3 |
| | Expert | 6 |
| | Multiple experts | 8 |
| Knowledge | Public | 0 |
| | Restricted | 3 |
| | Sensitive | 7 |
| | Critical | 11 |
| Opportunity | Unnecessary/unlimited access | 0 |
| | Easy | 1 |
| | Moderate | 4 |
| | Difficult | 10 |
| | None | 999 |
| Equipment | Standard | 0 |
| | Specialized | 4 |
| | Bespoke | 7 |
| | Multiple bespoke | 9 |

**Table 7.** Asset impact.

| Impact | Explanation | Value |
|---|---|---|
| Low | The concerned party is not harmed very strongly; the possible damage is low | 1 |
| Medium | The threat addresses the interests of providers/subscribers and cannot be neglected | 2 |
| High | A basis of business is threatened and severe damage might occur in this context | 3 |

## 4. Risk Determination

We suppose that the identification and development of threats needs between one day and one week, the attackers are experts and the window of opportunity is moderate because of mobility. We also assume that the motivation of the attacker is related to the asset impact, so for physical assets such as RSUs and vehicles we associate high attacker motivation.

**Sybil Attack/ Impersonation Attack:** a vehicle pretends to be another vehicle, using information from dumpster diving, phishing, or from a third party to attempt to build a certain level of trust. The Sybil attacker needs to have restricted information, such as the identities of the target nodes (IPs); he also need to have some specialized equipment to be able to generate new IDs or to execute dumpster diving and/or phishing. For the intensity of the attacks, even if two attacks can be distributed, Sybil attack is more dangerous than impersonation attack.

**Eavesdropping/ID Disclosure:** Eavesdropping on wired and wireless networks is part of information gathering, where the attacker tries to capture the packets that cross the network. This type of attack can also perform radio frequency monitoring to determine the vehicles and the type of communication techniques used in the network. For a successful eavesdropping attack, no matter where the attacker is located, he must use specialized tools to easily capture and read encrypted information. The attacker captures the packets and records them, using Wireshark, for example, or records the packets and puts them in a capture file. Wireless networks can be captured and their encryption cracked to access the data using Aircrack, for example. For motivation of the attacker, information as an asset is not as important as infrastructure or vehicles, so for eavesdropping the motivation is medium, for ID disclosure, even though it is information, the motivation is high because the ID of the vehicle is private and very important. Since these attack cannot be distributed, a single instance is sufficient to launch it.

**Spoofing Attack:** There are several types of spoofing: IP address spoofing; MAC address spoofing; application or service spoofing (DHCP, DNS, routing protocols, email, etc.). Spoofing is when the attacker pretends to be something he is not (fake web server, fake DNS server…); for example, for email address spoofing, the sending address of an email is not really the sender. An example of MAC spoofing would be when an attacker changes the MAC address of an interface to appear like another vehicle in the network. Another type of spoofing is IP spoofing, which take the IP address of a legitimate vehicle and acts as if an update is coming from that vehicle, comparable to ARP poisoning or DNS amplification. The spoofing attacker needs to capture the MAC address and the IP address of the vehicles, which are sensitive information, so he needs specialized software and equipment such as simulators to generate false position messages. In this type of attack, the asset is the information, thus the motivation of the attacker and the impact of the attack are medium. They can be launched from a single instance.

**Malware Integration:** Malware is malicious software that can gather information (keystrokes), participate on a botnet, show you advertising or act as a virus or worm. There are several types of malware: viruses, crypto-malware, ransomware, worms, Trojan horses,

rootkits, keyloggers, adware/spyware and botnets. To integrate malware, an attacker needs to: (1) find a vulnerability (OS, user...); (2) install malware that includes a remote-access backdoor; finally, (3) a bot may be installed later. Before executing the malware integration attack, the attacker needs to know where exactly the vulnerability is, then he needs to install the malware by sending emails, web page pop-ups or worms; therefore, he doesn't need specialized equipment. These types of attacks can be distributed and target physical assets, so the motivation of the attacker and asset impact are high.

**Jamming Attack:** Jamming a radio frequency (RF) is a type of denial-of-service (DoS) attack that prevents wireless communication by transmitting interfering wireless signals in order to decrease the signal-to-noise ratio at the receiving vehicle, preventing it from hearing the good signal. There are many types of jamming attacks: legitimate frames, data sent at random times and reactive jamming. In order to be efficient, the attacker needs to be somewhere close. The jammer does not need specific information about the network; knowing that the radio frequency is open, he can simply broadcast interfering wireless signals. In reactive jamming, he needs to hear the network to know when communication has been launched. To generate interfering wireless signals, he needs to use bespoke equipment. This attack can be distributed, its intensity is therefore high as the asset to be protected is physical, which increases the attacker's motivation.. Therefore, the attack has a high impact.

**Flooding Attack:** Flooding is a type of DoS attack that forces a service to fail or causes a system to be unavailable by overloading the service through taking advantage of a design vulnerability or a failure in software. In flooding, the attacker is able to track how much traffic is coming to the network and how much there is of what type. There are different types of floods: SYN floods, ping floods/ping scans, port floods/port scans (while identifying a machine, the attacker tries to identify which server is running on that machine: webserver, email server...). The result is that the attacker will know what is happening on the network and/or be able to deny services. There is some information that the attacker needs to know before launching a flooding attack: he needs to identify what infrastructure, servers and vehicles are running on the network. For the equipment needed to launch a flooding attack, the attacker needs specialized equipment to create useless data and useless control requests. These types of attack can be distributed and target physical assets, so the motivation of the attacker and asset impact are high.

**Blackhole Attack/Man in the Middle:** In these two types of attack, the the cyber hacker will receive information from one vehicle, read it, and forward it on to another vehicle (MITM) or drop it (blackhole). The problem with this type of attack is that the attacker is completely invisible to the sender and receiver. They use ARP poisoning to create a man in the middle attack while sitting in the same IP subnet as other vehicles. For blackhole attacks in VANETs, an attacker vehicle could exploit routing protocols, such as claiming that it has the best path for the destination vehicle/RSU. The attacker needs to know the IP addresses of the sender and the receiver; he also need to have some specialized equipment to be able to execute the phishing. For a blackhole attack, even though the asset is information, the motivation and the asset impact are high because the information is dropped. A single instance can launch a blackhole or man in the middle attack.

Based on this analysis, identified threats are ranked as shown in Table 3.

## 5. Countermeasures

In the following, we focus on the specific threats to ITS communications that we classify as critical. In addition to the solutions mentioned in the previous tables (Table 1 and 2), new countermeasures have been proposed in the literature to deal with the different critical attacks identified. In order to protect against Sybil Attack, Impersonation Attack and User Privacy disclosure, traditional countermeasures include session-key based mechanisms (Lee et al. 2013) and public key infrastructure (Rahbari and Jamali 2011). Among the recent solutions proposed, we cite the work proposed in Baza et al. (2022). Mohamed (Baza et al. 2022) propose an approach based on signed time-stamped tags posted by roadside units

(RSUs) as proof of the vehicle's anonymous location. The author proposes the execution of a proof-of-work (PoW) algorithm to prevent vehicles from setting multiple trajectories in the case of low-density RSUs. Pengwenlong Gu et al. (2017) present three SVM kernel functions-based classifiers to distinguish malicious nodes from benevolent nodes by measuring the deviation of their driving pattern matrices (DPMs). The proposed security services are implemented using three main techniques: encryption algorithms, public key infrastructure (PKI) and pseudonyms. The authors of Zhou et al. (2020) proposed a privacy-preserving detection scheme without the need for vehicles to disclose their infrastructure information by relying on a set of pseudonyms instead of assigning a specific identifier to each vehicle. In Mahmood et al. (2019), the authors developed a solution to detect a Sybil attack based on the similarity of the movement paths of Sybil nodes, assuming that Sybil nodes always have the same position and movement paths, which is inconvenient and unsuitable in the real world. The solution detects a Sybil attack separately for each vehicle. Eziama et al. (2018) propose an approach based on computing trust in VANETs. The authors use the Bayesian neural network (BNN) model framework for predictive analysis, classification and node detection. Compared to a neural network (NN), a BNN keeps high performance by providing a robust distribution and the integration of the uncertain weights in the network. The solution developed in Stępień and Poniszewska-Marańda (2021) is based on time stamps and node identification information. A vehicle/node crosses an intersection each time with a given timestamp consisting of the current day and time. When the node arrives at another intersection, its timestamp is updated after checking whether the vehicle was able to travel the given path at the specified speed. To protect the network against the possibility of counterfeit tags, it must be possible to verify vehicle authenticity, for example by including a digital signature. In the same context, Reddy et al. (2017) suggest a cryptographic digital signature certificate method to set up trust between participating nodes. The asymmetric cryptography technique is used to combine the digital signatures. Each mobile vehicle in a VANET is allocated a set of public/private key pairs through which the vehicle identifies itself to the receivers by digitally signing the messages. The verification procedure is based on a local certificate session key. Gu et al. (2017) propose three SVM kernel functions-based classifiers to discriminate malignant nodes from benevolent ones by assessing the divergence in their driving pattern matrices (DPMs). The proposed security services are based on three major mechanisms: encryption algorithms, public key Infrastructure (PKI) and pseudonymous. They evaluate vehicle driving patterns in neighborhood road traffic situations and consider the possibility of detecting Sybil attacks based on the variation of their driving patterns. The main intention is to estimate the resemblance of vehicle driving patterns, then use SVM classifiers to distinguish malicious nodes from benign ones. As a countermeasure for impersonation attacks between two authentic device-to-device (D2D) users, in Tu et al. (2021), the authors propose a reinforcement learning-based technique that guarantees impersonator identification based on channel gains. They relate the performance of this technique in terms of false alarm rate, miss detection rate and average error rate. In Savekar and Thorat (2020), the authors present a comparison between K-nearest neighbors (KNN) and support vector machine learning algorithms to overcome impersonation attacks in VANETs. The experimental results showed that KNN gives better accuracy in detecting impersonation attacks compared to the SVM approach. In order to overcome impersonation attacks, Raghav1 et al. (2013) proposes a framework based on the cryptographic techniques to detect the impersonating node. Each node is given a unique identifier ID or pseudonym, and this information will be collected by a central authority to ensure confidentiality and privacy. Recently, two approaches have been used to provide anonymous services: group signature and pseudonymous authentication. Furthermore, there are hybrid methods that combine both group signing and pseudonymous authentication schemes. Both methods handle the problem of authentication and privacy. In group signature schemes, a vehicle receives a group private key with which it signs a message, whereas in pseudonymous authentication schemes (Memon et al. 2018), individual vehicles store a set of identities. In Zhong et al. (2019), the authors propose

certificate-less, aggregate-signature-based mechanism to perform message authentication without generating overhead for the system resources. The proposed approach uses the pre-computation method to minimize computation during the signature phase. More recently, in Yang et al. (2021), a single-message cooperative authentication scheme based on certificate-less signatures is proposed. Several vehicles were randomly selected for new message authentication and construct the proof, which can be used for rapid message verification and is difficult to falsify.

Flooding attacks, malware integration and blackhole attacks are critical attacks targeting availability. The key objective of these attacks is to inhibit ITS unit use and autonomous vehicle use of network facilities. These attacks can be initiated in the system by mischievous core or peripheral nodes. Several countermeasures have been proposed in the literature to mitigate flooding attacks, such as packet marking (Verma et al. 2013), a trust model using transmission thresholds (Verma and Hasbullah 2015) and monitoring SYN packets (Kerrache et al. 2017). Recently, the authors of Aneja et al. (2018) proposed a hybrid intrusion detection system that enhances accuracy and other key performance metrics. The authors used a combination of artificial neural networks and a genetic algorithm and implemented two scenarios for computing performance metrics: misuse and anomaly. Moreover, in Kumar and Sinha (2019), the authors implement attacks such as flooding and blackhole using AODV routing protocol and improved AODV routing. Three different scenario were simulated and measured performance parameters such as end-to-end delay, packet overhead, packet delivery rate and packet drop ratio, which were analyzed and compared to existing protocols. Regarding malware integration, there are currently many types of malware, such as worms, computer viruses, ransomware, spyware, Trojans, rootkits, backdoors and botnets. Most malware works on computer systems or mobile devices. There are different infection vectors (Atanassov and Chowdhury 2021; Boukerche and Zhang 2019) depending on the characteristics of the specific malware.

In Wei et al. (2018), Lei Wei et al. proposed a two-layer model (named the coupled dynamic virus-traffic model) to study the propagation of viruses in V2V communication networks. This model constructed the virus propagation process in the upper layer using Susceptible–Infectious–Recovered (SIR) model KERMACK199133. Several results were obtained: (i) Communication range and travel distance of infected vehicles are proportional to the probability of virus infection. In contrast, increasing traffic density decreases the probability of virus infection. This result somewhat contrasts theories of disease-spreading. (ii) The higher the probability of virus infection, the shorter the time required for the virus to spread to the epidemic stage. This makes perfect sense in terms of epidemic models. (iii) There are certain minimum proliferation thresholds for viruses. (iv) Reducing the probability of virus infection is essential for virus management under various constraints of communication range and traffic levels.

In Le et al. (2021), the authors propose a mathematical model called SEIR-S (Susceptible, Exposed, Infectious, Recovered-Susceptible) based on VANET characteristics and the SIR disease propagation model. This model takes into account the possible behaviors of malware and provides the corresponding states of the vehicles: Susceptible (S), Exposed (E), Infectious (I) or Recovered (R).

Some studies focus on the impact of worm propagation and factors affecting malware propagation on V2X communications and propose similar worm models (Galluccio and Morabito (2019); Liu et al. (2018)).

In a blackhole attack, instead of relaying network traffic to destinations, the malicious node drops the packets and prevents traffic from flowing. Therefore, the goal of a blackhole attack (also referred to as a packet-drop attack) is to persuade as many nodes as possible to send their traffic through the malicious node. As a result, the communication between the source and the destination is blocked (Tobin et al. 2017; Kumar et al. 2019). To overcome this issue, a secure AODV routing protocol was developed for detection of blackhole attacks by Kumar et al. (2021). The proposed method is a modified version of the original AODV routing protocol with improvements in the RREQ packet and RREP packet protocols. For

added security, cryptographic function-based encryption and decryption is included to verify the source and destination nodes.

As this type of attack is classified as critical risk, the risk must be treated as urgent and appropriate countermeasures must be developed. After performing the ITS risk assessment using TVRA and determining the risk level of each threat, we chose the proposal in Inedjaren et al. (2021) as a trusted and secured extension of OLSR protocol to mitigate the risk of blackhole attacks in VANET. The system proposed in Inedjaren et al. (2021) provides all vehicles in the network with a commonly distributed, highly secure, tamper-proof framework for routing in VANETs using blockchain. We use Optimized Link State Routing (OLSR) as a characteristic routing protocol to integrate blockchain into VANETs. OLSR has various security issues because its routing mechanism is based on the availability of a small group of nodes called multi-point relays (MPRs), and the security mechanisms are executed at each node individually with repetitive processes. In our proposed contribution, we use blockchain, as a reliable and highly secure technology to solve the security problems of OLSR by motivating (rewarding) the vehicles to collaborate and avoiding repetitive detection processes.

## 6. Conclusions

Securing connected vehicles in VANET systems against cyber threats is becoming increasingly complex with the addition of connections, electronics and software-driven systems. In this context, we proposed in this paper a qualitative risk analysis of the different threats targeting VANETs. Our work focuses on the ETSI ITS communication architecture. Risk analysis was done using the TVRA methodology by defining the security environment as the first step, then security objectives and finally determining the threats. The risk analysis phase allowed us to determine the risk level of each threat to ITS entities. As future work, and in order to enhance security in ITSs, we propose the use of machine learning techniques. Data and its context are crucial to effectively secure connected vehicles. This data can provide contextual clues to reduce threats. Machine learning will enable deep predictive analysis of cyber risks, and the correct application of machine learning can provide contextual information to reduce the potential risks and costs associated with a security breach. Furthermore, we will propose countermeasures for these threats based on the risk level of each threat; then we will use the results of this analysis to develop a security framework to simulate different attacks targeting an ITS.

**Author Contributions:** Conceptualization, B.Z. and M.M.; methodology, B.Z. and M.M.; software, Y.I.; validation, Y.I.; formal analysis, B.Z., M.M. and Y.I.; investigation, B.Z. and M.M.; resources, B.Z., M.M. and Y.I.; data curation, Y.I.; writing—original draft preparation, B.Z., M.M. and Y.I.; visualization, Y.I.; supervision, B.Z. and M.M.; project administration, B.Z. and M.M. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## References

Ahmad, Farhan, Asma Adnane, and Virginia N. L. Franqueira. 2016. A systematic approach for cyber security in vehicular networks. *Journal of Computational Chemistry* 4: 38–62. [CrossRef]

Al-Kahtani, Mohammed Saeed. 2012. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). Paper presented at the 2012 6th International Conference on Signal Processing and Communication Systems, Gold Coast, QLD, Australia, December 12–14, pp. 1–9.

Aneja, Mannat Jot Singh, Tarunpreet Bhatia, Gaurav Sharma, and Gulshan Shrivastava. 2018. Artificial Intelligence Based Intrusion Detection System to Detect Flooding Attack in VANETs. In *Handbook of Research on Network Forensics and Analysis Techniques*. Hershey: IGI Global. [CrossRef]

Atanassov, Nikolay, and Md Minhaz Chowdhury. 2021. Mobile Device Threat: Malware. Paper presented at the 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, May 14–15, pp. 007–013. [CrossRef]

Baiad, Raghad, Hadi Otrok, Sami Muhaidat, and Jamal Bentahar. 2014. Cooperative cross layer detection for blackhole attack in vanet-olsr. Paper presented at the 2014 International Wireless Communications and Mobile Computing Conference (IWCMC), Nicosia, Cyprus, August 4–8, pp. 863–68.

Boukerche, Azzedine, and Qi Zhang. 2019. Countermeasures against Worm Spreading: A New Challenge for Vehicular Networks. *CM Computing Surveys* 52: 1–25. [CrossRef]

Baza, Mohamed, Mahmoud Nabil, Mohamed M. E. A. Mahmoud, Niclas Bewermeier, Kemal Fidan, Waleed Alasmary, and Mohamed Abdallah. 2022. Detecting Sybil Attacks Using Proofs of Work and Location in VANETs. *IEEE Transactions on Dependable and Secure Computing* 19: 39–53. [CrossRef]

Chim, Tat Wing, Sm Yiu, Lucas C. K. Hui, and Victor O. K. Li. 2011. SPECS: Secure and privacy enhancing communications schemes for VANETs. *Ad Hoc Networks* 9: 189–203. [CrossRef]

Daeinabi, Ameneh, and Akbar Ghaffarpour Rahbar. 2013. Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks. *Multimedia Tools and Applications* 66: 325–38. [CrossRef]

ETSI. 2003. *ETSI: Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis*. Technical Specification ETSI TS 102 165-1 V4.1.1. Sophia Antipolis: ETSI.

ETSI. 2010. *ETSI EN 302 665—Intelligent Transport Systems (ITS)*. Communication Architecture, v1.1.1. Sophia Antipolis: ETSI.

ETSI. 2011. *ETSI: 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 TS 102 165-1 V4.2.3. Sophia Antipolis: ETSI.

Eziama, Elvin, Kemal Tepe, Ali Balador, Kenneth Sorle Nwizege, and Luz M. S. Jaimes. 2018. Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning. Paper presented at the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, December 9–13, pp. 1–6. [CrossRef]

Galluccio, Laura, and Giacomo Morabito. 2019. Impact of worm propagation on vehicular sensor networks exploiting V2V communications. Paper presented at the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, October 21–23, pp. 1–6. [CrossRef]

Gu, Pengwenlong, Rida Khatoun, Youcef Begriche, and Ahmed Serhrouchni. 2017. Support Vector Machine (SVM) Based Sybil Attack Detection in Vehicular Networks. Paper presented at the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, March 19–22, pp. 1–6.

Hortelano, Jorge, Juan Carlos Ruiz, and Pietro Manzoni. 2010. Evaluating the usefulness of watchdogs for intrusion detection in VANETs. Paper presented at the 2010 IEEE International Conference on Communications Workshops, Cape Town, South Africa, May 23–27, pp. 1–5.

Hsiao, Hsu-Chun, Ahren Studer, Chen Chen, Adrian Perrig, Fan Bai, Bhargav Bellur, and Aravind Iyer. 2011. Flooding-resilient broadcast authentication for vanets. Paper presented at the 17th Annual International Conference on Mobile Computing and Networking, Las Vegas, NV, USA, September 19–23, pp. 193–204.

Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. 2006. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications* 24: 370–80.

IEEE. 2010. *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Networking Services*. IEEE Std 1609. Piscataway: IEEE.

Inedjaren, Youssef, Mohamed Maachaoui, Besma Zeddini, and Jean-Pierre Barbot. 2021. Blockchain-based distributed management system for trust in VANET. *Vehicular Communications* 30: 100350. [CrossRef]

Kerrache, Chaker Abdelaziz, Nasreddine Lagraa, Carlos T. Calafate, and Abderrahmane Lakas. 2017. TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs. *Vehicular Communications* 9: 254–67. [CrossRef]

Kumar, Ankit, and Madhavi Sinha. 2019. Design and analysis of an improved AODV protocol for black hole and flooding attack in vehicular ad-hoc network (VANET). *Journal of Discrete Mathematical Sciences and Cryptography* 22: 453–63. [CrossRef]

Kumar, Ankit, Vijayakumar Varadarajan, Abhishek Kumar, Pankaj Dadheech, Surendra Singh Choudhary, V. D. Ambeth Kumar, B. K. Panigrahi, and Kalyana C. Veluvolu. 2021. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems* 80: 103352. [CrossRef]

Le, Duc T., Khanh Q. Dang, Quyen L.T. Nguyen, Soha Alhelaly, and Ammar Muthanna. 2021. A Behavior-Based Malware Spreading Model for Vehicle-to-Vehicle Communications in VANET Networks. *Electronics* 10: 2403. [CrossRef]

Lee, ByungKwan, EunHee Jeong, and Ina Jung. 2013. A DTSA (detection technique against a sybil attack) protocol using SKC (session key based certificate) on VANET. *International Journal of Security and Its Applications* 7: 1–10.

Leinmüller, Tim, Christian Maihöfer, Elmar Schoch, and Frank Kargl. 2006. Improved security in geographic ad hoc routing through autonomous position verification. Paper presented at the 3rd International Workshop on Vehicular Ad Hoc Networks, Los Angeles, CA, USA, September 29, pp. 57–66.

Liu, Bo, Wanlei Zhou, Longxiang Gao, HaiBo Zhou, Tom H. Luan, and Sheng Wen. 2018. Malware Propagations in Wireless Ad Hoc Networks. *IEEE Transactions on Dependable and Secure Computing* 5: 1016–26. [CrossRef]

Mahmood, Adnan, Wei Zhang, Quan Z. Sheng, Sarah Ali Siddiqui, and Abdulwahab Aljubairy. 2019. Trust Management for Software-Defined Heterogeneous Vehicular Ad Hoc Networks. In *Security, Privacy and Trust in the IoT Environment*. Berlin: Springer.

Manish Kumar, Vanita Jain, Achin Jain, Uttam Singh Bisht, and Neha Gupta. 2019. Evaluation of black hole attack with avoidance scheme using AODV protocol in VANET. *Journal of Discrete Mathematical Sciences and Cryptography* 22: 277–91. [CrossRef]

Memon, Imran, Ling Chen, Qasim Ali Arain, Hina Memon and Gencai Chen. 2018. Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks. *International Journal of Communication Systems* 31: e3437. [CrossRef]

Moalla, Rim, Houda Labiod, Brigitte Lonc, and Noemie Simoni. 2012. Risk analysis study of ITS communication architecture. Paper presented at the 2012 Third International Conference on The Network of the Future (NOF), Tunis, Tunisia, November 21–23, pp. 1–5. [CrossRef]

Mokdad, Lynda, Jalel Ben-Othman, and Anh Tuan Nguyen. 2015. DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks. *Performance Evaluation* 87: 47–59. [CrossRef]

Montgomery, Paul Y. 2011. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In *Radionavigation Laboratory Conference Proceedings*. Austin: The University of Texas at Austin.

Nguyen, Anh Tuan, Lynda Mokdad, and Jalel Ben Othman. 2013. Solution of detecting jamming attacks in vehicle ad hoc networks. Paper presented at the 16th ACM International Conference on Modeling, Analysis & Simulation of Wireless and Mobile Systems, Barcelona, Spain, November 3–8, pp. 405–10.

Rafiq, Gulzaib, Batool Talha, Matthias Patzold, Jose Gato Luis, Gianluca Ripa, Iacopo Carreras, Cristina Coviello, Stefano Marzorati, Gonzalo Perez Rodriguez, German Herrero, and et al. 2013. What? s new in intelligent transportation systems?: An overview of european projects and initiatives. *IEEE Vehicular Technology Magazine* 8: 45–69. [CrossRef]

Raghav1, R. S., R. Danu, A. Ramalingam, and G. K. Kumar. 2013. Detection of Node Impersonation for Emergency Vehicles in VANET. *International Journal of Engineering Research & Technology (IJERT)* 2: 3383–89.

Rahbari, Mina, and Mohammad Ali Jabreil Jamali. 2011. Efficient detection of sybil attack based on cryptography in VANET. *arXiv* arXiv:1112.2257.

Raya, Maxim, Panos Papadimitratos, and Jean-Pierre Hubaux. 2006. Securing vehicular communications. *IEEE Wireless Communications* 13: 8–15. [CrossRef]

Reddy, D. Srinivas, V. Bapuji, A. Govardhan, and S. S. V. N. Sarma. 2017. Sybil attack detection technique using session key certificate in vehicular ad hoc networks. Paper presented at the 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai, India, February 16–18, pp. 1–5. [CrossRef]

Safi, Seyed Mohammad, Ali Movaghar, and Misagh Mohammadizadeh. 2009. A novel approach for avoiding wormhole attacks in VANET. Paper presented at the 2009 Second International Workshop on Computer Science and Engineering, Qingdao, China, October 28–30, vol. 2, pp. 160–65.

Savekar, Mrugnayana S., and Sandeep A. Thorat. 2020. Identifying Impersonation Attack in VANET using KNN and SVM Approach. *International Journal of Future Generation Communication and Networking* 13: 1266–74.

Sharma, Prinkle, Hong Liu, Honggang Wang, and Shelley Zhang. 2017. Securing wireless communications of connected vehicles with artificial intelligence. Paper presented at the 2017 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, April 25–26, pp. 1–7.

Song, Joo-Han, Vincent W. S. Wong, and Victor C. M. Leung. 2008. Secure location verification for vehicular ad-hoc networks. Paper presented at the IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference, New Orleans, LA, USA, November 30–December 4, pp. 1–5.

Stępień, Krzysztof, and Aneta Poniszewska-Marańda. 2021. Security Measures with Enhanced Behavior Processing and Footprint Algorithm against Sybil and Bogus Attacks in Vehicular Ad Hoc Network. *Sensors* 21: 3538. [CrossRef] [PubMed]

TamilSelvan, Komathy Subramanian, and Rajeswari Rajendiran. 2013. A holistic protocol for secure data transmission in VANET. *International Journal of Advanced Research in Computer and Communication Engineering* 2: 4840–46.

Tobin, John, Christina Thorpe, and Liam Murphy. 2017. An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks. Paper presented at the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, Australia, June 4–7, pp. 1–7. [CrossRef]

Tu, Shanshan, Muhammad Waqas, Sadaqat Ur Rehman, Talha Mir, Ghulam Abbas, Ziaul Haq Abbas, Zahid Halim, and Iftekhar Ahmad. 2021. Reinforcement Learning Assisted Impersonation Attack Detection in Device-to-Device Communications. *IEEE Transactions on Vehicular Technology* 70: 1474–79. [CrossRef]

U.S. Department of Transportation. 2017. National ITS Architecture V8.0. Available online: http://local.iteris.com/arc-it/ (accessed on 20 February 2022).

Verma, Karan, and Halabi Hasbullah. 2015. Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET. *Security and Communication Networks* 8: 864–78. [CrossRef]

Verma, Karan, Halabi Hasbullah, and Ashok Kumar. 2013. Prevention of DoS attacks in VANET. *Wireless personal communications* 73: 95–126. [CrossRef]

Wahab, Omar Abdel, Hadi Otrok, and Azzam Mourad. 2014. A dempster–shafer based tit-for-tat strategy to regulate the cooperation in vanet using qos-olsr protocol. *Wireless Personal Communications* 75: 1635–67. [CrossRef]

Wei, Lei, Hongmao Qin, Yunpeng Wang, Zhao Zhang, and Guizhen Yu. 2018. Virus-traffic coupled dynamic model for virus propagation in vehicle-to-vehicle communication networks. *Vehicular Communications* 14: 26–38. [CrossRef]

Yang, Ming, Shuang Wei, Rongwang Jiang, Faizan Ali, and Boxiong Yang. 2021. Single-message-based cooperative authentication scheme for intelligent transportation systems. *Computers & Electrical Engineering* 96: 107390. [CrossRef]

Yao, Xuanxia, Xinlei Zhang, Huansheng Ning, and Pengjian Li. 2017. Using trust model to ensure reliable data acquisition in VANETs. *Ad Hoc Networks* 55: 107–18. [CrossRef]

Zhong, Hong, Shunshun Han, Jie Cui, Jing Zhang, and Yan Xu. 2019. Privacy-preserving authentication scheme with full aggregation in VANET. *Information Sciences* 476: 211–21. [CrossRef]

Zhou, Man, Lansheng Han, Hongwei Lu, and Cai Fu. 2020. Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant. *Computer Networks* 172: 107174. [CrossRef]