Towards A Secure ITS: Overview, Challenges and Solutions

Lama Sleem[a,*], Hassan N. Noura[b], Raphaël Couturier[a]

[a] *FEMTO-ST Institute, UMR 6174 CNRS, Univ. Bourgogne Franche-Comté, France*
[b] *American University of Beirut, Department of Electrical and Computer*

Abstract

Intelligent Transportation Systems (ITS), the heart of the new revolution of smart transport, has evolved from the well-known Vehicular Ad-hoc Networks (VANETs) to become the Internet of Vehicles (IoV). In fact, the increase in the number of vehicles and the newly born technologies have stimulated the new Internet of Vehicles (IoV) or the Internet of Cars. In general, ITS aims at ensuring better traffic efficiency and reducing road accidents. However, due to different limitations and issues, these systems suffer from different security and privacy vulnerabilities. In fact, they are both vulnerable to various types of security and privacy attacks that may result in life-endangering situations. As a result, several solutions were presented to achieve the required levels of security and confidentiality. **In this paper, an overview of ITS is presented stating the reasons behind the evolution from Vanet to IoV. Then, the main threats/attacks that threaten ITS are classified according to their (1) security impact and according to the (2) network layer(s) they affect. Solutions for each attack are also well presented. In addition, a security and performance evaluation and summary tables are presented to provide an overview of these surveyed solutions.**

Keywords: ITS, IoV, VANET, Security attacks, Sybil attacks, Privacy

2010 MSC: 00-01, 99-00

1. Introduction

Intelligent Transportation Systems (ITS), the heart of the new revolution of smart transport, has evolved from the well-known Vehicular Ad-hoc Networks (VANETs) to become the Internet of Vehicles (IoV). Cars and vehicles are used by more and more people every day. The biggest problem regarding their increased usage is the increasing number of fatalities that occur due to accidents on the roads. Intelligent Transport Systems (ITS) have been developed rapidly all over the world. In general, IoV aims at ensuring better traffic efficiency and reducing road accidents. However, due to different limitations and issues, both technologies IoV and VANET suffer from different security and privacy issues. In fact, they are both vulnerable to various

*Corresponding author
Email address: lama.sleem@univ-fcomte.fr (Lama Sleem)

types of security attacks that may result in life-endangering situations. As a result, several solutions were presented to achieve the required levels of security and confidentiality.

Having a universal network connecting all the available heterogeneous networks has become one of the great challenges researchers are interested in. This fact comes from the highly growing number of everything: smartphones, vehicles, appliances, laptops, tablets, sensors used in the daily life, etc. This global network is nothing more than what is commonly referred to as the "Internet of Things". In IoT, the inter-operability among the heterogeneous devices is the major objective. In fact, Internet of Vehicles (IoV) is one of the main topics in IoT. IoV has evolved from what has been known as Vehicular Ad-hoc Network (VANETs). VANET is a special type of mobile ad-hoc network used for communication between vehicles and roadside units. It's objective is to improve road safety, traffic management and congestion monitoring. The great change in vehicular networks was initiated in 2002, when researchers investigated the use of VANETs to reduce safety problems and to ensure more comfortable driving. In Europe for example, several automobile manufacturers have had the courage to carry out a real inter vehicle communication such as **Audi, BMW, Fiat, Renault**. These companies have cooperated to create a *Car2car Communication Consortium (C2C-CC)* organization [1], dedicated to inter-vehicle problems and issues. In addition to security applications, there are other applications for VANET such as infotainment, new payment strategies and insurance billing using advanced wireless access technology enabled in vehicles with or without the help of roadside units. However, despite all efforts to ensure that VANET gains investor and commercial interest [2], VANET has so far failed to achieve this objective. The strong growth in the number of vehicles on the road is much greater than the capacity of the VANET technology. More than 125 million passenger cars with embedded connectivity are forecast to ship worldwide between 2018 and 2022. Currently, the connected car market is strongly aligned with 2G/3G networks, according to Neil Shah, research director at Counterpoint. However, he said that it is "moving swiftly" to 4G LTE connectivity, with the technology forecast to be installed in nearly 90 percent of connected cars by 2022 [3]. As seen, the purely ad-hoc nature of VANET [4], the lack of cloud computing and advanced computing despite all the ongoing attempts to integrate this functionality [5] and the lack of connectivity between the vehicle and personal devices [6] have meant that VANET has eclipsed its value. In addition, the main objective of VANET is to ensure driver safety, but safety solutions have not yet been developed at the time of writing this paper. Security has been one of the greatest challenges for VANET, and that's why researchers are trying to find the best reliable security solutions that can be used in IoV, since it has wider abilities [7] and more convincing arguments. IoV will enable the exchange of information between the vehicle and its surroundings using different communication means. Integrating the Internet of Things with VANET will create a new integrated network to support new applications, as intelligent traffic management, intelligent vehicle control, new information services [8], etc.

IoV will enable the vehicles to be continuously connected to internet making it easier to provide information for these different services. Information is exchanged between the vehicles themselves, the passengers, the infrastructures parties, drivers, different sensors and electric actuators. In fact, this is the main difference between these two technologies, since IoV focuses more on the interaction between vehicles, humans and the available infrastructure. As a result, research in the field of IoV is currently becoming extensive and very active as it involves several axes at the same time, namely: wireless communications, protocols for physical and MAC layers, routing protocols and security, all with the aim of ensuring safe driving for drivers, and a better future for the IoV.

1.1. Motivation

The main contribution of this work can be divided into two major points. First, since VANET evolved into the IoV, it is important to indicate the differences between these two platforms and what are the main motivations behind this evolution. The second contribution is related to the security of such systems which are both considered as Intelligent Transportation Systems. Using ad-hoc wireless communications, or 4G/5G communications makes these systems sensitive to a large number of threats. Unreliable multi-hop transmissions, willful intermediate packet forwarding, and sharing specific personal data (location information or any sensitive messages) will certainly require a specific level of security. Therefore, the practical benefits of such systems could be mitigated in the absence of appropriate safety systems and could have a negative reverse effect on traffic and drivers' safety. Thus, the main requirement to ensure is the security of these heterogeneous systems where several security requirements are needed to resist different kinds of existing attacks [9, 10, 11, 12, 13, 14, 15, 16, 17, 18]. Moreover, the existing security challenges are well presented. Almost all recent existing primitive security solutions are analyzed for each threat jeopardizing the safety of these platforms. Each attack usually aims at affecting at least one of the following security services: availability, authentication, integrity, confidentiality, privacy, and non-reputation. **Attacks are classified according to their security impact as well as the corresponding layer(s) in the Internet protocol stack layer they could affect**. In fact, a better classification of the existing attacks, threats on different network layers, and their countermeasures would allow researchers to find new and more effective security measures.

Section 2 is devoted to present an overview of VANET and IoV, stating the reasons that were behind this evolution and the main differences between them and the main challenges faced. Then, Section 3 shows the applications and standards deployed in these platforms. Then, in Section 4, security issues are presented, where the attacks/attackers are both classified and a risk analysis is shown, then modern security layers and characteristics of communication types are described. After that, in Section 5, the different existing security architectures are shown. Then, in Section 6, the limitations and the open issues in ITS are listed to broaden the horizon of the research. Finally, a conclusion is drawn in Section 7.

2. Background, Motivation and Overview

In this section of the survey, an overview of the conventional VANET is presented, followed by the motivations that encouraged the growth of the new platform IoV which will also be presented as a heterogeneous vehicular network.

2.1. VANET's architecture

Vehicular Ad-hoc Network (VANET) is a promising area of research and development as it has remarkable role in improving safety of vehicles on road, efficient traffic management, and providing comfort to commuters in an affordable way. VANET has three main entities which are described as follows and are demonstrated in Figure 1:

1. **OBU:** An On Board Unit is equipped with each vehicle to provide wireless communication, allowing it to communicate with other neighboring vehicles to share traffic information and road conditions to ensure the global safety.
2. **RSU:** A Road Side Unit is immobile, not fully trusted, and subordinated by the Trusted Authority (TA). It is used to exchange information with TA and OBUs and can be compromised by physical attacks.
3. **TA:** A Trusted Authority, the registration of immobile RSUs and mobile OBUs is done by TA. It requires sufficient storage and computation capability to enable it to issue the main keys of the network.

These stations will communicate using an infrastructure specialized for VANET and, as far as we know, cars are being sold with the ability to communicate. In addition to the OBU stated previously, there are other components that are also added into the smart vehicle's system. For example, a GPS (Global Positioning System) is used for navigation, sensors (ladar and radar) used to detect objects at a certain distance, Event Data Recorder (EDR) which is a computing unit that can ensure the process and storage of data, a unique ID like the electronic license plate, a wireless transceiver that provides V2X communication according to a standard; etc. In short, the smart vehicle is equipped with a communication system, a computing system, and a recorder box that records all the events exactly as a black box does in an airplane. In addition to all the aforementioned devices, each vehicle is equipped with a Tamper-Proof-Device (TPD) to store the secret information (private key) and is responsible for signing outgoing messages. To do that, a TPD contains a set of sensors that can detect hardware tampering. Once a tampering is detected, TPD removes all the stored keys, to prevent them from being compromised [19]. Moving to the communication side, vehicles communicate by node-to-node communication, where nodes establish connections with other nodes to exchange information in a short period of time. Communication in a VANET can occur through three kinds of vehicular communication methods [20] which are **vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I)** as shown in Figure 1. V2V communications can be

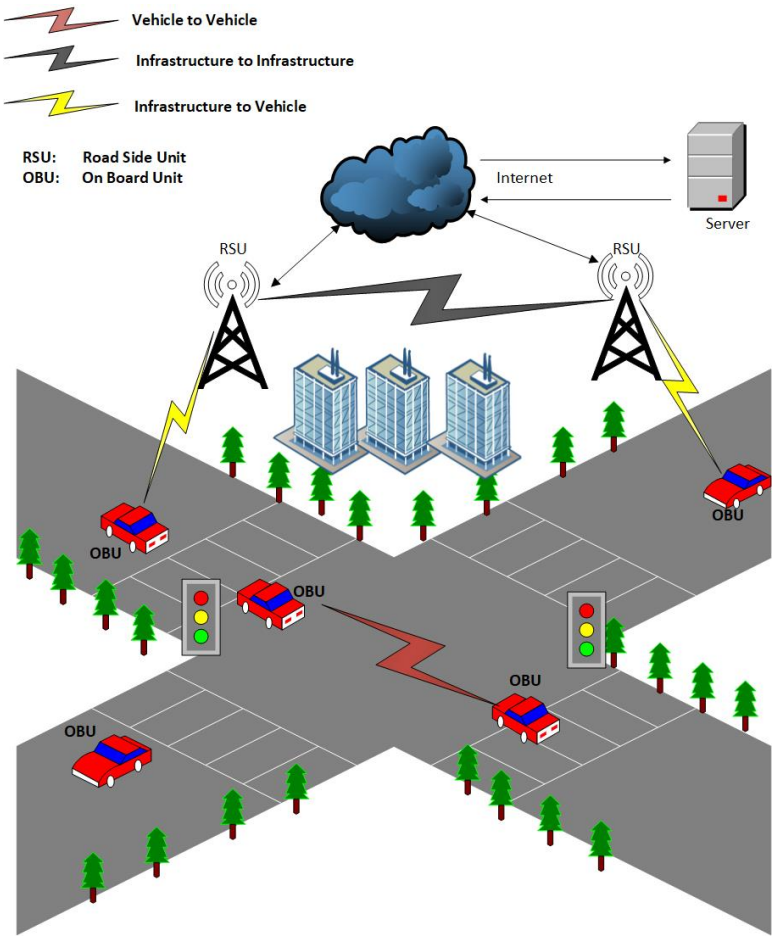

Figure 1: System architecture in VANET.

realized by employing IEEE 802.11p ad-hoc Network [21]. V2I communications are only based on ad-hoc communications (between the Vehicle and Roadside) or on generic wireless access network based Wi-Fi. In fact, V2I communication are less vulnerable to attacks and they require more bandwidth than V2V communication. This kind of connection requires a minimum lag and a low bit error rate. For this reason, it requires a reliable peer-to-peer channel, denoted by **Dedicated Short Range Communication DSRC** channel [22], that is presented by the **Federal Communication Commission** which allocates a 75 MHz of licensed spectrum for DSRC in US (30 MHz were allocated by the European Commission), and is used now by the **IEEE 802.11p**, enabling a high data rate, and a short-range communication with a minimal latency. Finally, I2I communications interconnect RSUs between each other and RSUs to central(s) and this is done via the Internet domain.

2.2. Motivations to launch Internet of Vehicles

Although VANET's aim is to enhance the safety of drivers with increased efficiency, the industry's interest in it was less than expected. In general, the commercial efforts in VANET were not enough [2]. Starting from the pure ad-hoc architecture that VANET has, the vehicle will lose all the services given by the network directly when it is disconnected. The collaboration with other networks is not an available feature in VANET [23]. In addition, commercial applications are not available in VANET due to the absence of continuous Internet connectivity [4]. In case of Internet loss, and due to the ad-hoc architecture, vehicles are not able to communicate with the driver's or the passenger's devices. In a world of Internet of Things, this feature will only affect the existence of VANET. Speaking of IoT, big data, and intelligent decisions, the common exchanged terms: edge computing, fog computing, or cloud computing are also not available in the current VANET architecture. And efforts are still being made to find a solution in spite of all the current challenges [24]. For these reasons, IoV was found to be more reliable and realistic in the big data era. Moreover, approximately 1.35 million people die each year as a result of road traffic crashes, and road traffic injuries are the leading cause of death for children and young adults aged between 5-29 years [25]. Due to these enormous numbers of deaths, there is an insistent need to start with an effective new solution based on safety applications without the need for continuous user intervention. A more reliable vehicular communication can be provided by IoV, thus decreasing the large number of road casualties. Finally, when talking about IoV, this opens the market to new demands. In fact, connected cars will turn into an increase in generated-revenue. Revenue projections from connected cars range from 40 billion dollars to worth of 100 billion dollars a year by 2020. Car manufacturers will benefit from connected vehicles and mobility services, but other industries are also in the process to benefiting from them. Mobile Network Operators will be the first to benefit from the connectivity required by IoV. In addition, the in-car technology will have the lion's share as new devices will be needed in the vehicles, new products and services will be adapted specifically to driving scenarios. Also, cloud services can help their businesses adapt to the accelerated development cycles and growing customer demands for connected cars. In addition, there will be a high demand for a higher processing power, thus the processor manufacturing will also have a new target. For example, currently, the NVIDIA Tegra X1 mobile processor for connected cars, used to demonstrate its Drive CX cockpit visualizations, can handle a trillion floating-point operations per second (flops) [26, 27].

2.3. IoV overview

Internet of Vehicles has become a special application of the Internet of Things. It will make drivers enjoy a safe, convenient and comfortable driving experience. IoV is especially important for autonomous vehicles as they can spontaneously communicate with other cars around them. This type of communication allows early notices of braking, changing lanes or turning and helps ensure smooth and safe transportation between autonomous vehicles [28]. Autonomous driving has been of great interest for many researchers in

the last few years. Additionally, new concepts are being proposed to predict the trajectories of the vehicles or to determine the driver's condition (i.e. as being drunk [29]). As an example for these technologies, consider blockchain [30, 31, 32, 33], Edge/Cloud computing [34, 35, 36] and Artificial Intelligence [37, 38]. Other technologies are also used like sensor technologies [39]. These technologies are all being proposed to find the best solutions that are needed for a secure, reliable and autonomous vehicular networks. The connectivity among vehicles occurs through an inter-communication between sensors and smart devices inside the vehicles, as well as smart systems in the environment as part of the Intelligent Transportation Systems (ITS). To achieve these goals, cars are enabled with modern electronics and an integration of the information to help maintain traffic flow, and to perform more effective fleet management and accident avoidance. The electronics used include special sensors, GPS, entertainment systems, brakes and throttles. There are five types of communication in heterogeneous IoV which can be summarized as following and as demonstrated in Figures 2 and 3:

V2V: Vehicle to Vehicle- using IEEE WAVE

V2R: Vehicle to Roadside unit- using IEEE WAVE

V2I: Vehicle to Infrastructure of the mobile networks- using WIFI/4G/5G

V2P: Vehicle to Personal devices (Laptops, smartphones..)- using CarPlay/NFC

V2S: Vehicle to Sensors- using Ethernet/MOST/Wi-Fi

A global network is enabled using Internet and other heterogeneous networks. The network includes IEEE WAVE for V2V and V2R, 4G/LTE, 5G and Wi-Fi for V2I, CarPlay/NFC for V2P, and MOST/WI-FI for V2S. It is obvious that due to the heterogeneous network environments in IoV, different wireless access technologies are utilized to establish connections. The vehicular networks are represented by different wireless access technologies. The V2V and V2R networks represents vehicular communications through WAVE/DSRC. The V2I network demonstrates the vehicular communications through Wi-Fi or 4G/LTE [40]. Adding to 4G/LTE, different works/plans and suggestions have been proposed to use 5G in IoV. For example, in [41] the authors proposed a satisfactory performance to the IoV communication requirements when adopting the 5G network with V2X communications. In fact, 5G will provide the basic infrastructure for building a smart IoV environment, which will push vehicle network performance and capability requirements to their extremes. The V2P network symbolizes the vehicular personal device communications using CarPlay of Apple or Android system of Open Auto-mobile Alliance(OAA) or Near Field Communication (NFC). The V2S network represents in-vehicle sensor communications through Ethernet, Wi-Fi or Media Oriented System Transport (MOST) [42]. This will add complexity to the architecture but will increase the interest in all industrial markets on contrary to VANETs. IoV will have a significant importance to supervise different

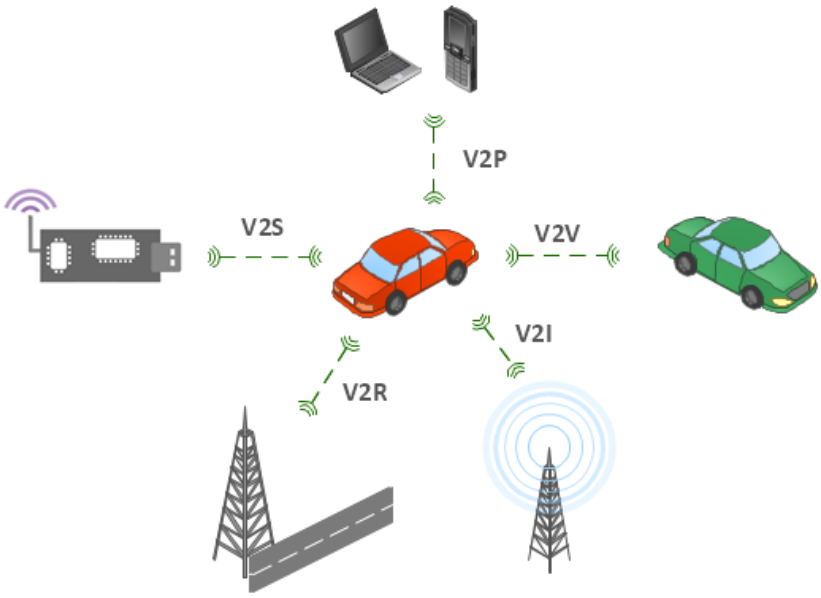

Figure 2: Types of vehicular communications in IoV.

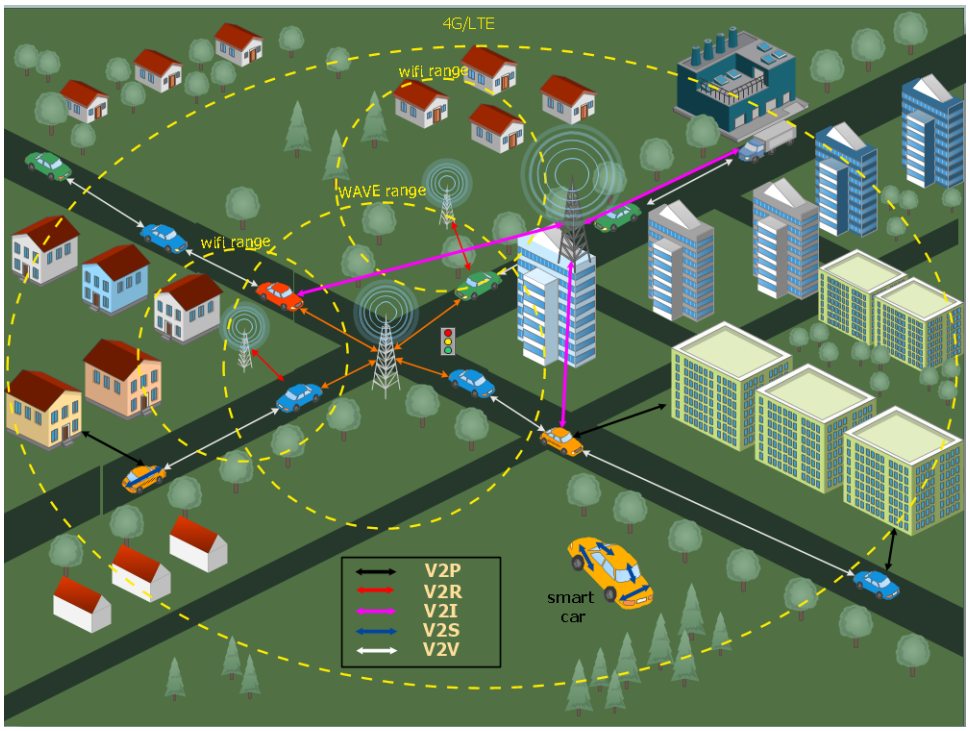

Figure 3: IoV and heterogeneous networks.

vehicles with the intervention of all different available networks. It will provide a more reliable platform for Internet and multimedia applications related to safe driving. More precisely, the main difference between both is relying on the 5G in IoV as stated earlier. The 5G wireless cellular network architecture is basically composed of only two logical layers: (1) a **radio network** and (2) a **network cloud**. The network function virtualization (NFV) cloud consists of a User Plane Entity (UPE) and a Control Plane Entity (CPE) that perform higher layer functionalities related to the User and Control plane, respectively. By this vision, future 5G wireless networks are no longer tied by hardware or even software limitations. The authors in [43] explained the everything-as-a-service (XaaS) taxonomy to light the way towards service-oriented wireless network design. Special network functionality as a service (XaaS) will provide service as per need, resource pooling is one of the examples. XaaS is the connection between a radio network and a network cloud.

2.4. Challenges in ITS

Employing ITS applications suffers from several obstacles and constraints that are discussed in the following:

1. **Big data:**A major challenge is the processing and storage of big data created in IoV due to the large number of connected vehicles. For instance, autonomous cars are expected to process 1 GB of data per second. Mobile cloud computing and edge computing; available in IoV; will play an important role in handling the big processed data especially when using the network virtualization concept.
2. **High mobility:** Since we are dealing with mobile nodes, the prediction of these nodes is a difficult task to fulfill in terms of location and specifying the directions [44]. The positions of nodes can join or leave a network quickly and in a very short period of time, hence, different topologies are investigated with every new node position, making the network topology very dynamic and subjected to frequent changes causing a continuous link breakage between nodes.
3. **Hard-delay constraints:** Information related to safety such as the location of other cars must be sent as fast as possible to avoid any collision, therefore, the network must be very sensitive to delays to avoid catastrophic results. Safety related applications mainly needs a real-time response. However, these real-time constraints make the applications vulnerable to Denial of Service attacks (DoS), therefore, detection of real-time attacks is critical when insiders evades existing protection mechanisms.
4. **Scalable network:** ITS can be applied in urban or rural areas thus the network's size is not limited to a defined area [45]. In addition, the number of vehicles is estimated to exceed 250 million by 2020 [46], and until today, no global authority has provided the security for such large systems. A cooperation between worldwide local authorities is needed to achieve the standardized authority.
5. **Using wireless Communication:** As explained, the nodes communicate with others by wireless communications, so here comes the major role of security to ensure the safety of the information.

In fact, data can be disseminated by the vehicles' communication, making the network vulnerable to attacks as bogus information attack.

6. **Different types of communication modes and technologies**: As stated earlier, there are different types of communication modes, so the connected vehicles must support a wide range of communication technologies such as IEEE 802.11p, Wi-Fi, Bluetooth, /4G/LTE/5G, etc. Therefore, the vehicle must be equipped with the convenient hardware/software to support these heterogeneous platforms.
7. **Ensure high level of security and privacy:** All the information will be sent to different parties, thus the integrity, authentication, and availability must be considered. In this context, security protocols must be implemented with low communication overhead due to time constraints, and low computation complexity to exchange quick and safe information. A trade-off between latency and QoS must be ensured and having a lightweight encryption scheme is necessary to be able to respond to all requests at the same time at once avoiding any lags that can cause catastrophic accidents.
8. **Network Management:** Due to the large scale of the vehicular network that consists of millions of vehicles, and generates a huge amount of data that must be stored and distributed across the network, an effective network management must be used to deal efficiently with the network size and network produced data [47].
9. **Localization system:** Ensuring safety property requires a reliable and very accurate localization system. Normally, GPS is used to enable the localization process. But satellite-based positioning systems are not always available, especially when passing through tunnels, which makes the system vulnerable to several types of attack such as spoofing and blocking attacks. To deal with this problem, a number of localization techniques have been investigated such as Map Matching [48], Dead Reckoning [49], and Cellular localization [50]. Until now, there is no technique that can meet all of ITS requirements, such as time sensitivity, availability, and reliability. Here comes the need to build a reliable localization system, whilst satisfying all the critical points.
10. **Spectrum issues:** V2V communication system is intended to be used for at least 20 years and within this time the spectrum availability has to be guaranteed. In the US, the FCC has allocated 75 MHz of spectrum at 5.9 GHz (from 5.850 to 5.925 GHz) for C2C and C2I communications. VSC and VII Consortium agreed that the best technology available for the communications systems using this spectrum would be a derivative of IEEE 802.11, thus, the development of the IEEE 802.11p and ISO TC204. However, when the number of nodes sending periodic broadcasts is too large due to high traffic volume, some specific messages like emergency warning messages need a greater amount of time to be received, since bandwidth availability is minimal in wireless networks. Thus, the bandwidth must have a good management to prioritize the exchanged messages.

3. Applications and Standardization efforts

3.1. Applications in ITS

The main target of ITS is to create a more efficient transportation infrastructure by employing vehicular communications that must improve **(1) Road Safety, (2) Traffic Efficiency and Management,(3) Comfort and Infotainment, and (4) Autonomous Driving and (5) Driving Anomaly Detection** in transportation systems. In this context, several explored applications vary from a simple exchange of vehicle status to a complex large-scale traffic management.

3.1.1. Road safety applications

These kinds of applications are primarily employed to avoid dangerous collisions which may cause losses of drivers' lives. They provide drivers with all kind of messaging assistance to avoid collisions with other vehicles. Communicating and sharing information between vehicles and roadside units are two ways used to predict and avoid collisions. This shared information can be a vehicle's position, intersection position, car speed and distance heading. Moreover, locating dangerous locations on roads, such as slippery sections or avalanches can be easier. These applications can be classified into two classes:

"Driver Assistance Applications (DAA)" inform and assist drivers to avoid road dangers or accidents. Three applications are being standardized by ETSI for DAA:

- Cooperative Awareness Applications (CAA) [51];
- Longitudinal Collision Risk Warning (LCRW) [52];
- Intersection Collision Risk Warning (ICRW) [53].

"Actions on Vehicle Applications (AVC)" that can provide necessary information for vehicles' systems to avoid or reduce accidents (Lane change assistance, pre-crash sensing/warning, emergency electronic brake lights, stationary vehicle warning, control Loss warning [54]).

3.1.2. Traffic efficiency and management

Traffic efficiency applications improve and facilitate the management of the traffic flow and provide a cooperative navigation. Typical examples of these types of applications are (1) Speed limit navigation to help the driver control the speed of his/her vehicle for easy driving and to avoid unnecessary stopping, (2) Traffic information and recommended itineraries provisioning to enhance the traffic efficiency by managing the navigation of vehicles through cooperation among vehicles and road side units. These applications use several V2X messages like control messages such as Service Announcement Message (SAM).

3.1.3. Comfort and infotainment

This kind of application aims at adding valued services. These services are mainly offered by service providers and are downloaded by drivers on their application units. There are mainly two kinds services available: (a) Cooperative local services which focus on infotainment that can be offered by locally based services such as point of interest notification, media downloading, local electronic business (b) Global Internet services which are mainly communities services (insurance and financial services, rapid management and parking zone arrangements, ITS station life cycle which is software and data updates).

3.1.4. Autonomous driving

A robot car driving autonomously is all about using Artificial Intelligence. Driving a vehicle is a mission that usually needs high level of skill, attention and experience from a human driver. Although computers are more capable of sustained attention and focus than humans, fully autonomous driving requires an advanced high level of intelligence achieved so far by AI agents. In general, autonomous driving needs 3 steps to be reached: (1) Recognition (knowing the surrounding environment), (2) Prediction (predict the future changes of the environment), (3) Planning (generate an efficient model that mixes both recognition and prediction to know the future sequence of driving actions enabling the vehicle to navigate successfully). Several works have been proposed to start considering this as a major goal, for example [55] takes a deep-learning proposal to achieve autonomous driving. Lately, autonomy has become a very topical issue. Cadillacs, BMW, Nissan can now drive themselves down highways hands-free, as long as the driver still pays attention and nothing out of the ordinary takes place; the new Mercedes-Benz S-Class can power through traffic circles, as long as you are actually doing the steering; and there are a few trials around the world of autonomous vehicles going on in severely controlled circumstances. In addition, augmented reality and virtual reality are both new concepts adapted in vehicles, where the user can enjoy his trip wearing a VR headset observing anything desired. In order to achieve that, new concepts should be adapted in vehicles to guarantee the safety of the driver [56]. This technology needs the vehicle to be equipped with ultrasonic sensors, 360 radars, 360 cameras, satellite systems, and the secure environment/standards that can enable this seem-less and autonomous driving.

3.2. Driving Anomaly Detection

Another important application in ITS, mainly in IoV is the detection of any unusual behaviour from the driver, or the trajectory. This kind of application tends to make driving safer in terms of the driver's physical safety, or even can be used by insurance companies (for judging the driver's behaviour). Collecting parameters as speed and engine parameters, from a large number of vehicles is characterized as large volume, multi-frequency, and multi-source data. This will largely reflect the vehicle status and thereby are widely used to

evaluate driving behaviors [57]. Real-time abnormal driving behaviors monitoring is a corner stone to improve driving safety. Several works have been proposed to detect such behaviours. For example, in [58] the authors addressed the problem of performing abnormal driving behaviors detection (coarse-grained) and identification (fine-grained) to improve driving safety. In [59], the authors proposed an adaptive driving maneuver detection mechanism that iteratively builds a statistical model of the driver, vehicle, and smartphone combination using a multivariate normal model taking into account the different vehicle characteristics. This is the main limitation of existing sensing platforms, which are principally based on fixed thresholds for different sensing parameters. SafeDrive is an online driving anomaly detection from Large-Scale Vehicle Data [28]. In [60] iBOAT was proposed which is an isolation-based online anomalous trajectory detection. It focuses on the problem of detecting anomalous routes by comparing the latter against time-dependent historically "normal" routes. It is an online method that is able to detect anomalous trajectories "on-the-fly" and to identify which parts of the trajectory are responsible for its anomalousness. Another proposal related to trajectory is TrajCompressor [61], but with adding the compression technique. In fact, massive and redundant vehicle trajectory data are continuously sent to the data center via vehicle-mounted GPS devices, causing a number of sustainable issues, such as storage, communication, and computation. Online trajectory compression becomes a promising way to surpass these issues. In the TrajCompressor proposal, authors presented an online trajectory compression framework running under the mobile environment. In order to detect any anomaly in trajectories, authors in [62] presented a two-step algorithm to measure the behavior of drivers. First, the algorithm finds abrupt movements considering abrupt accelerations, decelerations, and abrupt changes of direction. Second, according to different characteristics related to the abrupt movements as repetitive anomalies, events/episodes, and speed above street speed limit the driver is classified in levels of danger. Additionally, almost all people have been charged by a taxi driver that surprises us with the amount of charge they have to pay. In [63], authors have shed the light on this problem and proposed a method to collect the actual data (distance covered) by a taxi using Global Positioning System (GPS) which is implemented in the taxis. The secret trick that taxi drivers usually use i.e., modifying the taximeter to a smaller scale is taken into consideration. As a result, it not only makes the service distance larger but also makes the reported taxi speed larger. Fortunately, the speed information collected from the GPS reports is accurate. Hence, the speed information is used to design a system called the Speed-based Fraud Detection System (SFDS), to model taxi behaviors and detect taxi fraud. Bus trajectory anomalies also took part of the researchers' interest which is clearly explained in [64]. Authors proposed (1) LoTaD to find long-term traffic anomalous regions in urban city, (2) a novel method to partition the whole city based on the transportation stations, and finally they evaluated the method with real bus trajectory data in Hangzhou. Finally, detecting the drunk driver can decrease the number of victims drastically (in Europe, 25% of all driver deaths in road accidents were attributed to drunk driving). In [65] authors used driving performance measures that were

collected from a test in a driving simulator located in the Traffic Research Center, Beijing University of Technology. Lateral position and steering angle were used to detect drunk driving. Then, multivariate time series analysis was performed to extract the features. The proposed approach achieved an accuracy of 80.0%.

3.3. Standardization efforts

Two ITS standards had been defined for ITS communication architecture: IEEE Wireless Access in Vehicular Environments (WAVE) [66] and ETSI (European Telecommunications Standards Institute) organizations [67]. The architecture of each standard follows the seven layers of the OSI (Open System Interconnection) reference model as all the recent communication technologies such as LTE. A common part between both standards is composed of the physical and medium layers known as IEEE 802.11. Both ITS standards (IEEE 1609 [68] and ETSI TC ITS [67]) are very similar in several terms such as offered networking, application management functionalities, and security. The entire protocol stack of ITS standards consists of DSRC (Dedicated Short Range Communications) [69], the common part IEEE 802.11p [70], and WAVE (Wireless Access in Vehicular Environments) [71] or ETSI standards, which are described in the following.

3.3.1. DSRC

The ITS network uses a specific frequency band between 5850 to 5925 GHz (75 MHz bandwidth), which is known as Dedicated Short Range Communications (DSRC) [69]. This band can be divided into seven channels of 10 MHz, numbered 178, 172, 174, 176, 180, 182, and 184 respectively. The CCH channel (Control Channel) corresponds to channel 178. The other channels are used for SCH channels (Service Channels). Two service channels (172, 184) are reserved for high Availability and low Latency, and for high power and public safety. In Europe the situation is different. The DSRC band in Europe is regulated by the ETSI, and 5 channels are used; CCH uses channel 180 and the rest (172, 174, 176, and 178) is used for SCH.
Recent work has been proposed as "Vehicular Communications for ITS: Standardization and Challenges" by Sherali Zeadally, Muhammad Awais Javed and Elyes Ben Hamida [72]. The authors provide a review of the current standardization efforts for Dedicated Short-Range Spectrum (DSRC) and Cellular Vehicle-to-everything (C-V2X) technologies. The intention is to provide readers with insights about the evolution of Medium Access Control (MAC) and Physical (PHY) layers for both of the mentioned technologies.

3.3.2. WAVE

IEEE published in [66] the latest ITS standards fact sheets, which declare the WAVE IEEE 1609 family (Standard for Wireless Access in Vehicular Environments). They introduced different services and interfaces in addition to security architecture that should protect the WAVE stations from various attacks. In addition,

operation in an ITS environment and establishment of an efficient and secure V2X communication are both guaranteed. The WAVE architecture of the different 1609 standards and their integration with the OSI reference model are illustrated in Figure 4. Let us indicate that WAVE standards define the basis for the implementation of a wide set of applications in the ITS that include the safety of vehicles, traffic management, automatic tolls, improved navigation, and several other applications. The latest version (amended) is introduced lately 1609.2a in 2017 and 1609.2b in 2019.

Standard	**WAVE definition**
IEEE P1609.0	Architecture of WAVE
IEEE P1609.1	Resource Manager.
IEEE Std 1609.2	Security Services
IEEE Std 1609.3	Networking Services.
IEEE Std 1609.4	Multi-Channel Operations.
Draft IEEE P1609.5	Layer Management.
Draft IEEE P1609.6	Remote Management Services.
IEEE Std 1609.11	Data Exchange Protocol Over-the-Air
IEEE Std 1609.12	Provider Service Identifier Allocations (PSID).

Table 1: List of of standardized protocols of WAVE

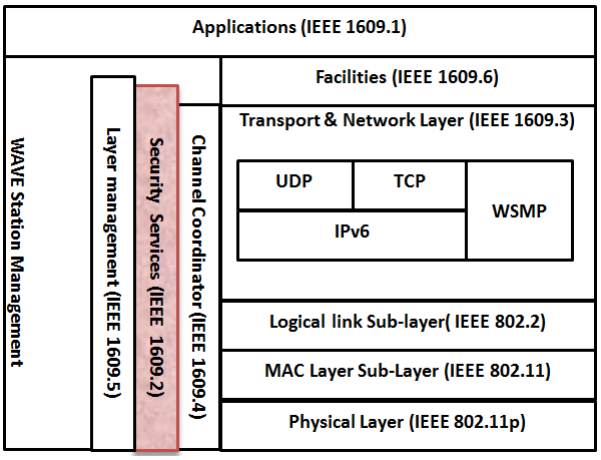

Figure 4: WAVE standards for ITS Layered Architecture for V2X Communications (US)

3.4. ETSI ITS standard

A standard of ETSI is presented in [73] and describes the European ITS communication architecture and specifies the comparison with the traditional OSI layered model. This standard consists of four layers: Applications, facilities, networking/transport, and access in addition to two cross layers, which are security and management are illustrated in Figure 5.

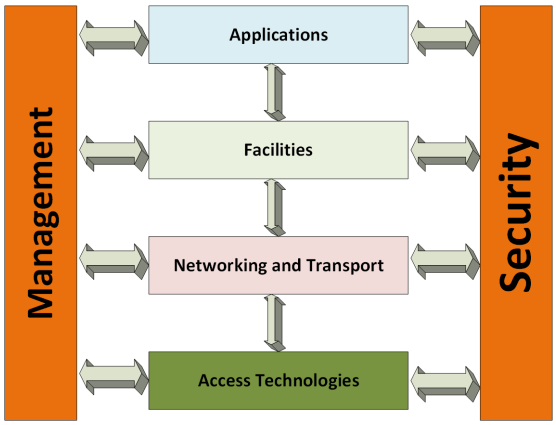

Figure 5: ETSI standard architecture.

Application layer: It is responsible for the execution and the implementation of one or several ITS applications such as road safety and efficiency.

Facilities layer: Its objective is to be a middle communication layer between application and network layers.

Networking & transport layer: It ensures the data transport between source and destination stations of ITS. In fact, it can be composed of two parts: ITS transport and TCP/UDP connection and includes the support of GeoNetworking, IPv6 networking, TCP/UDP transport protocol, etc.

Access layer: It makes it possible to ensure wired and wireless communication technologies that are available in an ITS station. The access technology used for Safety applications for ETSI is ITS G5 which appears as the European profile of IEEE 802.11p.

Management cross layer: It manages the communications depending on the requirements of ITS applications and it manages the features of the whole ITS architecture layers.

Security cross layer: Its objective is to provide the security services.

Table 2: 5G networks development and standardization [41]

Institution	Projects	Goal(s)	Contributions
ITU [74]	International Mobile Telecommunications for 2020and Beyond (IMT-2020)	Radio regulations; Operational aspects; Protocols and test specifications; Performance, QoS and QoE; Security	Recommendations (standards)
3GPP [75]	5G specifications	Radio access network; Service and systems aspects; Core network and terminals	Releases; Technical specifications
ETSI [76]	5G technologies	mmWave transmission; Next generationprotocols; MEC; NFV	Technical specifications
NGMN [77]	Next Generation MobileNetworks (NGMN) 5GInitiative	Technology evolution towards 5G	White Papers
ATIS [78]	Technical forum	Incubator of new business models	White Papers
5G-PPP [79]	Working groups and various5G Public Private Partnership(5G-PPP) projects	5G infrastructure; 5G architecture	White Papers
IEEE Future Networks [80]	Technical community	Providing practical, timely technical and theoretical content; Development and deployment of 5G	Research publications
5G Americas [81]	5G network development on Americas	Support and promote the full development of wireless technology capabilities	White Papers
5GMF [82]	5G research and development by industry	5G radio access technologies; Networktechnologies for 5G	5GMF White Paper
Verizon 5G TF [83]	Forum and technical specifications	Specifications for physical layer, MAC,RLC, PDCP, and RRC	5G specifications
5TONIC [84]	Open research laboratory	SDN; NFV; Physical and MAC layer	5G technologies
5GAA [85]	Mobility and transportation services	Use cases and technical requirements; System architecture; Standards andspectrum; Business models	White Papers

Table 3: IoV vs Vanet

Parameters	Vanet	IoV
Goals to achieve	Traffic safety to reduce accidents and increase the efficiency	Enhance traffic safety, effectiveness and commercial infotainment for passengers to enhance the driving experience
Communication	V2V and V2I	V2V, V2R,V2I,V2S,V2P
Compatibility	Not compatible with smartphones or personal devices (i.e. single network)	Compatible with smartphones and personal devices (heterogeneous network)
Usage Range	Local and discrete (limited scale applications)	Global, and sustainable applications due to the presence of AI
Market	Did not gain the attention of the market for its limitations	Gained the attraction of market for the variety of services
Network	Singleton network architecture (no collaboration with other existing networks)	Flexible and heterogeneous network.
Internet availability	Not available due to the shortage in infrastructure	Connect any time with any target.
Data size	Limited data size (no collaboration)	No limitations in terms of data size
Network efficiency	Frequent perturbations in network	Very rare disconnections
Taking Decisions	Not applicable	Due to AI and other technologies, this is available
Cloud computing	Not available	Available due to Due to the presence of vast real-time traffic information

3.5. Towards Service-Oriented 5G

5G is now being the fuel that shifts the Vanet to IoV. 5G Standardization and Development is being studied by the Standard Development Organizations (SDOs), by some consortia, by government and by different industries. In Table 2, 5G development and standardization efforts are presented with their main contributions.

3.6. IoV Vs Vanet

In Table 3 a comparison is made between IoV and Vanet to shed the light on the importance of moving to IoV in order to achieve all the goals set today. It can be seen that IoV has gained the interest of industries and researchers at the same time. When incorporating all these technologies in one platform, the targets set can see the light.

4. Attacks/ Attackers modeling and ITS risk analysis

ITS were investigated for providing safe and fast rides, but because of the wireless network, several kinds of hackers can attack the system, degrade it and eventually cause accidents. Since the safety of people is involved, providing better security is mandatory. Vital information in ITS should be protected

to prevent an attacker from modifying or deleting them. Secure transportation systems must also be able to determine the responsibility of drivers while maintaining their privacy [16]. Data exchanged through a vehicular network, information about the vehicles and their drivers must be secured and protected to ensure the reliable functioning of intelligent transportation systems [86]. However, such systems are known as a highly dynamic environment with short connection period duration that prevents the deployment of a complete and practical security solution. Ensuring the security in ITS can be considered as a complicated task and any security breach leads to critical and dangerous consequences. In fact, security breaches are likely to occur when using wireless media, dynamic network topology, high mobility, and diverse involved entities. In the following, the different security requirements and threats are described.

4.1. Parties involved in security

The different parties involved in the security of ITS system are:

The driver: Drivers are receiving the information, so they are the most important element and their safety is a priority. Any wrong information sent to drivers can lead to their death.

The Road side Unit: We can distinguish between normal RSU terminals, which operate in a normal way, and malicious RSU terminals.

The vehicle (OBU): The driver and the vehicle are both referred to at the same time. Two types of vehicles can be distinguished : normal vehicles that are found between the network nodes and operate normally, and ambiguous vehicles.

Third parties: Third parties can be trusted or semi-trusted, and are responsible for RSU and OBU certificates and have the diverse secrets/public key pairs. They can be the regulators of transport, vehicle manufacturers, traffic police, and judges.

The attacker: An attacker's target is to violate successfully the security of normal vehicles.

4.2. ITS security requirements

To ensure a practical deployment of ITS, diverse security requirements must be reached to ensure safe driving and secure communication. Below, the requirements of ITS security are detailed.

Data confidentiality: The sender station must be sure that the exchanged message can only be decrypted by authorized users. However, the confidentiality in ITS is not essential compared to other kinds of MANET network such as WSN, because safety messages should be shared [19]. However, several applications in ITS transmit sensitive important information that require confidentiality such as in [87] by using anonymous key pairs that can ensure privacy. In fact, the security in ITS requires a lightweight yet secure cryptographic solution.

Data integrity: It ensures that the exchange of information is not changed during forwarding from the sender to receiver.

Authentication: It can be classified into three sub-requirements: (a) user authentication to prevent Sybil attacks and prevent attackers from threatening the security of the system; (b) source authentication to validate that the messages are generated by trusted entities; and (c) location authentication to validate the relevance of the received information.

Privacy: It is the most important security requirement, especially for ITS application since personal data are exchanged over wireless communications. An important requirement is to preserve the privacy of the driver against un-authorized observers. For that purpose, privacy should be ensured by protecting personal data and the design of ITS security solution must ensure this requirement with a lower latency. For example, if a node presents its certificate to one RSU at location x, then it presents the same certificate to another RSU at location y. Therefore, any attack observer can simply know that the owner of this certificate traveled from location x to y.

Availability: Exchanged information should be processed and made available [88, 89, 90]. These kinds of attacks are very dangerous for real-time applications since a small delay can make the message useless.

Traceability and revocation: The malicious entities that are attacking the system must be monitored, in order to block them at the right moment. The trust authority should be able to trace the attacker and reveal its true identity. In addition, in case of a dispute or when a malicious entity is detected, the TA must abolish it and add its true identity to the blocking list.

Authorization: It is necessary to define the rights and authorization of different entities (vehicle or infrastructure) for several applications to prevent entity attack.

Non-repudiation: It is necessary to get the proof of the message originator for several applications such as in road safety where crucial information should be exchanged and could lead to dangerous consequences. It may be crucial in some cases (e.g. wrong information that causes an accident) not only to identify a sender but also to get the proof of the originator of the message (for accountability).

Immunity against physical attacks: ITS entities should be immune against external attacks, such as availability attacks.

Scalability: The term scalability implies that despite the fact that the activity volume gets expanded, there should not be any performance degradation or even network blackout, without changing the system components or protocols.

Delay constraints: In some situations, the delivery of emergency messages on time is essential to preserve the safety of the driver.

Mobility: As one of the characteristics of VANET is dynamic topology, a perfect mobility model is required to develop VANET environment effectively and efficiently.

4.3. Attacker profiles

The network attackers' profiles should be specified when security issues are addressed in addition to the possible kinds of attacks. Attackers can be classified into five different categories. (1) Global vs local, (2) active and passive, (3) inter-vehicle and intra-vehicle (4) malicious and rational, (5) internal vs external. In the following, these categories are briefly elaborated.

4.4. Global vs. local:

Usually global attackers aim at damaging the whole system, or platform. There is no specific target rather than causing the maximum damage for the whole latter. While for a local attack, it either damages one vehicle, driver or cell. Even, it can damage few cells or a specific geographical area. The impact of a global attacks are much higher than the impact of local one.

4.4.1. Active vs. passive

An active node is a node that can send messages to cause harm to different nodes or to a part of the network. Mainly, this attacker is authorized to operate in the network, and in other cases it is not. The aim of this attack is to alter/delete the information sent between two entities, without their knowledge. On the contrary, passive nodes simply eavesdrop communications that occur between nodes in a network in a hidden manner. Passive attackers do not have any authorization. They will monitor the network and try to find some information that can be used for future more harmful attacks. Even though this will not cause any real damage to the network, the collected data can be used by the attacker for other attacks later on.

4.5. Inter-vehicle vs Intra-vehicle

For the inter-vehicle attacks, the vehicles in an ITS network share information among each other through wireless communication. This information has an important role in providing the functionalities associated with an IoT network, including traffic congestion control, accident warnings, etc. If an attacker (a local attacker from inside the network), provides false information, it could cause large disturbances and can cause loss of money and or loss of life. Thus, this kind of attack aims at collecting data by eavesdropping, packet manipulation or traffic manipulation attacks preventing important data from reaching appropriate entities or even falling into the wrong hands. However, intra-vehicle threats affect the on-vehicle or on-device attacking various components. These components can be sensors that use information such as speed,

location, proximity, acceleration, and giving these information to the OBU. This kind of attack can be achieved by leveraging from the wireless network (like the Internet) in ITS to cause damage to the vehicle or the environment. Also, it can lead to taking control of the vehicle through the Electronic control Unit (ECU) that is used to help in driving. This kind of attack is very dangerous since it can lead to enabling/disabling the braking system, manipulating the airbags by falsifying the collision information [91].

4.5.1. Malicious vs. rational

Malicious attackers do not have any specific goal and are not looking for any specific result. Their attacks are only conducted because it can be done, with no purpose in mind. Their main purpose is to damage the network by different ways like transmitting false information to different vehicles in a specific geographical area [92, 93]. In contrast, rational attackers have a specific target and can be dangerous [94], they are unpredictable and follow the passive class such as confidentiality attacks.

4.5.2. External vs. internal:

An internal attacker is mainly an evil node in the network, who aims at removing/modifying information just to cause a reputation attack to the infrastructure and make the users lose trust in this system. This can be a spy that is disguised as a legitimate node, and has succeeded in breaching all the security measurements. This kind of attack can be the first step in the way of more dangerous attacks such as external attacks (from outside the network).

On the other side, external attackers are mainly categorized as malicious hackers having a remote access to the network. This kind of attacker looks at gaining a high/unauthorized privilege access to the ITS system. He/she usually use malwares like worms, Spyware, Keylogger, or Remote Access Trojan attacks. Another example of external attack is the availability attacks such as DoS. Several kinds of DoS can be perpetrated and their main goal is to jam the network with fake messages since users in the network will receive these messages and the network will be unavailable.

4.6. Classification of ITS Attacks and their corresponding solutions

ITS is vulnerable to different kinds of threats and attacks as any communication system. In contrast to wireless sensor networks, the energy problem is absent and additionally, an OBU has the ability to harmonize dozens of microprocessors, which gives an important capacity of processing and computing to the vehicle [16]. Encrypting the sensitive message (or the sensitive part of the message) can provide better robustness and resistance against the passive attack and ensures the user privacy. Therefore, the transmitted data is protected from any unauthorized access. On the other hand, it is also necessary to ensure that

this data is only exchanged between legitimate parties and is not being altered at the intermediate nodes. Classifying attacks is the first step to have suitable security solutions. In [95] a classification of existing attacks have been proposed. Attacks are classified according to their target, whether they attack the vehicle or they attack the RSUs. As in [12], a cryptographic related classification is used and expanded to clarify the cryptographic solutions to VANETs security issues. In this paper, attacks are classified according to their impact on the existing modern security requirements which are: **Availability, Authentication and Identification, Integrity and Data trust, Confidentiality, Privacy and Non-repudiation.** Each attack will be classified according to what criteria of those it affects, stating also the layer it performs on. To satisfy these security services, several methods are used. For example, cryptographic algorithms mainly use encryption/decryption algorithms that generally include key generations and protocols to protect the exchange of shared data, hash functions that are widely used, digital signatures and many other tools. Attacks and their corresponding solutions are presented in the following.

4.6.1. Availability attacks and proposed solutions

Availability is the most crucial factor in transportation's security system. It means that the network is functional at any time to get useful data.

DoS attack: One of the most dangerous attacks in availability is the Denial-of-Service attack (DoS). Another kind of DoS is Distributed Denial-of-Service attack (DDoS). DDoS attack is a variant of DoS attack and is more serious than DoS because it is performed in a distributive manner. DoS attacks usually have three main properties: Malicious (the attack has a specific goal/target), Disruptive (disrupt the network) and Remote (attack is performed over the network). In a DDoS attack, multiple malicious nodes/vehicles attack on legitimate node unlike single attacker in DoS attack and it uses different time slots and locations to accomplish its objective of blocking the users from accessing the services of a network. This attack can also be launched both on vehicles/nodes and infrastructures (RSUs) [136]. The main intention behind DoS or DDoS attacks is to make a service unavailable and cause havoc rather than trying to breach the security perimeter of the target. In most cases, the methods of DDoS attacks aim at flooding the network and the results are always dreadful.

-Layers targeted: Multi-layer attack (Physical, Data Link, Network, Transport, Application layer)

-Solution: Few solutions are presented in Table 5 indicating the merits and demerits of each solution.

Jamming attack: This occurs by sending a noisy high-frequency signal in a channel which will result in a lower SNR preventing the vehicles from communication [137] [102].

-Layers targeted: It is based on producing an interference at the Physical Layer.

-Solution: Few solutions are listed in Table 6.

The effect of jamming for mobile ad-hoc networks can be reduced by using different techniques such

Table 4: Different types of availability attacks with their corresponding solutions.

Name of Attack	Communication Types	Proposed Solutions	Possible Reason(s)
Denial of Service	V2I/V2V	[96] [97][98] [99][100] [101]	OBU vulnerabilities,Insecure wireless communication channel
Jamming	V2I/V2V	[102] [103] [104]	OBU vulnerabilities,Insecure wireless communication channel
Sybil Attack	V2V	[105] [106] [107] [108] [109] [110] [111] [112] [113]	Flaws in routing table and unencrypted messages
Malware	V2V/V2I	[114] [115]	Software flaw and weak message propagation algorithm
Spamming	V2V	[116] [117]	Software flaw and weak message propagation algorithm
Black-Hole	V2V	[118] [119] [120] [121] [122]	Unencrypted backend communication channel
Grey-Hole	V2V	[123] [124]	Unencrypted backend communication channel
Worm Hole / Tunneling	V2V	[125] [126] [127]	Unencrypted backend communication channel
Sink Hole	V2V	[128] [129] [130] [131] [132]	Unencrypted backend communication channel
Greedy Behavior	V2V	[133] [134]	Broadcast nature of messages via communication channel
Hardware Tampering	V2V	[135]	Physical access to vehicles

Table 5: Few solutions for DOS attacks.

Year	Merits	Demerits	Technique used
2010[96]	Simple method as it is based on OBUs	Simulator not mentioned / results not compared with other existing methods	Depends on on the use of OBUs in vehicles
2012[98]	Efficiently detect invalid signatures	Simulator not mentioned	Pre-authentication process and the group rekeying scheme
2013 [97]	Method suits small scale as well as large scale DoS attacks	Manual setting of parameters for comparison which is time consuming	Distributed and robust approach based on bloom filter and IPCHOCK
2014 [101]	Detects the attacks prior to occurrence at node level	Simulator not mentioned	Request-Response detection algorithm (RRDA)
2018 [99]	Avoids traffic overloading, reduces overhead delay and enhances the communication speed	Performance not compared with other existing algorithms	Malicious and Irrelevant Packet Detection Algorithm (MIPDA)
2019[100]	Decreased the buffer usage, detects DDOS attacks, Comparison was made.	Extensive computing resources in a wider scale of the wireless framework.	Intrusion Detection Systems (IDS) Artificial Intelligence (AI) and Machine Learning (ML)

as in [102] and [103]. To reduce the effect of this attack, the frequency hopping technique FHSS (Frequency Hopping Spread Spectrum) of the used standard OFDM [104] should be randomized by the hopping algorithm. Furthermore, a pseudo-random generator should be used for this purpose on top of modifying the existing standard. In some cases, it is simply impossible to defend the system against jamming as an experienced attacker may have the ability to flood all available network frequencies. If the major concern was about malicious jamming, an intrusion prevention and detection system may be the best option. At the bare minimum, this type of system should be able to detect the presence of an RPA (Rogue Access Point) or any authorized client device in the wireless network.

Sybil attack: It is considered as one of the dangerous attacks in VANETs. In Sybil attack, malicious node can have multiple identities so it is hard to determine that the received information is from a legitimate and innocent node or from a malicious one. Because of multiple identities of each node, the network suffers from a huge security risk because one vehicle can deceive others by creating a deception of multiple vehicles on the road. Attacker can also send fake messages like non-existing traffic jam message, wrong route directions or even give false positions so the whole network which is risky for the passengers lives [138]. For example, in [139], an attacker creates a large number of pseudonyms, and fools vehicles to think that there is a traffic jam ahead of them and forces them to tell other vehicles that there is jam ahead, then makes them take an alternate route.

-Layers targeted: Data link, Network, Transport, Application and sometimes Physical Layer.

-Solution: Few solutions are listed in Table 6.

Malware attacks: Malware attacks [16, 17, 140], such as viruses, Spyware, Adware, Trojan horses, Logic bombs and Cookies, have the potential to cause serious disruption to its normal operation. Malware attacks are more likely to be carried out by a malicious insider rather than an outsider. These attacks may be introduced into the network when the vehicles or the roadside stations receive software updates.

-Layers targeted: Application Layer

-Solution: Software companies develop detection systems products at laboratories and keep track of new programs, analyzing them, putting the valid software in the whitelist and the malicious software in the blacklist. For the undecidable software, which is called the gray list, the scanners operate them in a controlled environment for more classification. When an analysis of a program in the gray list results in new malware, the company releases online updates for the new malicious software. Then, users can update their product databases by using remote access through an Internet connection. Signature-based and anomaly-based with artificial intelligence (AI) techniques were used to enhance their efficiency. Neural networks (NNs) have been adopted for their adaptability to environmental changes and their efficiency in prediction techniques [114]. In [115], authors discussed the importance of using IDS in such attacks, giving a fine taxonomy to malware threats.

Spamming attacks: The presence of spam messages like ads heightens the risk of increased transmission latency, and therefore might cause accidents. The lack of centralized administration causes serious problems. It is difficult to deal with spams because of the lack of infrastructure [16, 17, 141].

-Layers targeted: Application Layer

-Solution: Naive Bayes, Clustering and Decision trees are being used to improve the detection and

Table 6: Few Sybil detection proposals.

Year	Merits	Demerits	Technique used
2015[105]	high accuracy to detect Sybil attacks low false positive	simulator is not mentioned; less evaluation parameters are used	Cross layer scheme based on hash key and public-key cryptography
2015[106]	Easy to implement; energy efficient, effecient network load, low delay and low packet loss	Simulator and node density not mentioned	Random waypoint model
2015[107]	Reduce computation time and a high detection accuracy	Dependent on RSUs	Distributed detection approach rely on the difference in the movement patterns
2016[108]	Cost efficient and blueuces the network overhead	Simulator and node density are not stated	Dynamic Certificate generation technique based on pseudo-certificates
2017[109]	Provides better accuracy even in sparse networks	Less evaluation parameters are considered	Electro-acoustic positioning with context-aware information
2017[110]	Simple implementation and no need for certification or hardware support	Decrease in the detection rate due to increase in number of nodes	Position based technique based on information of neighboring nodes
2018[111]	Decreases the delay by reducing the amount of messages exchanged with RSUs, and thus, simplifies the mobility management	Node density not mentioned as well as less evaluation parameters are considered	Symmetric key encryption and authentication between RSUs
2019[112]	varying transmission powers; propose PCISAD to identify Sybil nodes with or without power control using RSSI time series; high detection rate and low false positive rate	The work is based on assumption which can be changed	Sybil attack detection based on RSSI with power control.
2020[113]	ADAS a proposal which uses sensors installed on modern passenger vehicles; No assistance of trusted third party; low false positive.	Not enough evaluation done	Deep Learning to identify nearby objects for Sybilattack detection and multi-step verification process

prevention of spams [117]. Also, using digital signatures of software and sensor is crucial so that only authorized nodes can send and receive data.

Black-Hole attacks: In Blackhole attack, vehicles either drop packets in between or deny participating in communication which causes a black hole. A black hole is an area where entire traffic is targeted to a node which is not publicly known. It attacks the routing protocol by introducing itself as a node having the shortest path to a destination node. Therefore, instead of relying on the route discovery process, all nodes start trusting the fake route and then data packets are intercepted by this malicious node instead of forwarding it to the real destination. The loss of data may result in denial of service attacks or taking advantage of the location during the initial phase resulting in man-in-the-middle attacks [142].

-Layers targeted: Network and Transport Layer.

-Solution: Black hole attacks could be detected by using a quality control chart [143]. Few proposals are presented in Table 7.

Grey-Hole attack: Gray Hole Attack is a branch of blackhole attack and it is based on selective forwarding concept. That is, instead of dropping all the data packets, malicious nodes will select which packets to drop and other packets will be forwarded. Thus, it results in the degradation of packet delivery ratio of the network. This attack is difficult to be detected since the node can operate as a malicious one or even as legitimate node [144].

-Layers targeted: Network and Transport layer.

-Solution: Using Intrusion Detection System as proposed in Ahmed, M. et. al. [123], where every mobile node carries intrusion detection system which monitors the whole network structure with in-built mechanism. In [124], authors have proposed a solution to minimize the grey hole attacks. The solution depends on the improvement of Denial Contradictions with Fictitious Node Mechanism (DCFM) and is named as IMP (IMProvement). IMP strengthens the routing decisions by two contradiction rules of DCFM and therefore, the attacker is named as a multi-point relay node (MPR) as well as other nodes can also take routing decision rules based on the outcomes of defined rules. The merits in this proposal is that the Grey hole attack is drastically minimized by showing a decrease up to 51% in previously dropped packets. The disadvantages is to perform further minor adjustments in IMP to enhance effectiveness (it can be done as a future work).

Wormhole and Tunneling attack: A Wormhole attack requires two nodes at least to participate. It happens when an attacker A sends a false message to an attacker B who is technically far from him/her. This message shows to the neighboring nodes of B, that A is near them as well [145, 125]. In this way, the interchanged control packets among them [146] cause to create non-existing roads according to

Table 7: Few solutions for Black-hole attack.

Year	Merits	Dimerits	Technique used
2015[118]	IDS having a high detection rate and low error rate	Computationally heavy and system needs extra memory resources	Based on Proportional overlapping scores (POS) to reduce the features
2016[119]	Increased detection rate and minimized false positive rate	-	Novel cross layer based IDS and cooperative watchdog technique
2017[120]	Decreases end-to-end delay, packet loss ratio And high detection rate	-	LI-AODV (Lifetime improving AODV) method and HMAC-SHA3-384 algorithm
2018[121]	GPSR has better results than AODV in terms of throughput, end-to-end delay, overhead and energy	-	GPSR (Greedy Perimeter Stateless Routing) protocol
2020[122]	Easy to implement and does not require any modification to the 802.11p standard or the routing protocol as we will	Sample size taken is not enough, more tests are needed.	Variable control chart widely to monitor the quality of a given process. Identify malicious nodes in real time by deploying the monitoring system in each receiving node within the network.

Table 8: Few solutions for the wormhole attack.

Year	Merits	Demerits	Technique used
2012 [126]	Efficient in detecting wormhole attack in terms of true positive and true negative	Simulator and node-density not mentioned	Based on Intrusion Detection Scheme (IDS)
2017 [127]	AODV protocol and efficiency is attained from Heuristics for deciding the path of the packet. Efficient towards packet transfer and in avoiding the wormhole attacks.	-	heuristic based approach
2018 [99]	Simple and Cost-Effective because it is independent of position information, clock synchronization and any additional hardware	no comparison is conducted with other proposals	Based on Round Trip Time (RTT), usage level of links and count of neighbors

their neighbors. Tunneling attacks are like wormhole attacks [16] but with one difference which is using the same network to initiate a private connection (tunnel) in contrast with Wormhole attackers that use a different radio channel for the exchanging packets. An additional communication channel (tunnel) is used by the tunneling attack which establishes a connection between two far nodes in the vehicular network. Worm Hole attack restrains the operations of routing protocols like AODV and DSR in transmitting the messages in VANETs. Malicious nodes or warm holes might have unauthorized access to perform a denial of service attack, resulting in a security breach in the transmitted data packets.

-Layers targeted: Network and Transport layer.

-Solution: One solution is proposed in [146] by Safi et. Al which introduces a packet leashes method to defend against the wormhole attack. A leash [147] is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Additional solutions are listed in Table 8.

Sinkhole attack: Sinkhole attack degrades the network performance either by dropping packets or modifying them which leads to a degradation of network performance. The packets of neighboring nodes go through a malicious node, which can eliminate or modify the received packets before eventually re-transmitting them. Moreover, the Sinkhole attack can be used to mount other attacks as the grey-hole and the Black-hole attacks [148].

-Layers targeted: Network layer.

-Solution: In [128], a light-weight algorithm to detect sinkhole attacks and identify the intruder in

an attack is proposed. They examined multiple suspicious nodes and concluded the intruder based on majority votes. A sinkhole detection algorithm in wireless sensor networks is proposed by authors in [129] based on the random routes selected by minimum hop (RMHSD). RMHSD consists of multistep approach: Clustering the network, establishing the hop database, establishing the minimum hop paths and calculating the hop difference. A new measure known as the frequency of each node by establishing M routes with optimal hops is introduced based on dynamic programming. The positives in this proposal is that it has a better performance in terms of detection rate and false positive rate. While the disadvantage is the difficulty to detect Sinkhole attack in the presence of a number of attacks. Another proposal is stated in [130] by using the MD5 algorithm. They rely on the energy power consumption model in AODV routing protocol to detect the malicious nodes in the network. Energy consumption of each node is extracted/calculated and when the energy is reduced, then by using an external battery, energy is given to the required node. To increase the security, MD5 uses both public and private keys as each node is assigned with a signature. If the signature used by the attacker node is the same as the signature already used by another legitimate node, then the attack is detected by the proposed algorithm and then determines the shortest alternative path to sink and provides security. This solution provides a better performance compared to normal AODV routing. In [131], authors proposed a decentralized sinkhole detection mechanism. It is based on network density estimation (NDE). The strong points in this proposal are that the proposal reduces the overhead generated by distributed sinkhole detection process and increases the network throughput by increasing the best effort (BE) traffic. In [132], an Adaptive Sinkhole Aware Algorithm (ASA) is proposed. It considers the subjective logic framework to estimate the reliability of each node by gathering the required information and both positive and negative Monitoring algorithm is implemented on all monitor nodes. This can help to find the residual energy of all nodes thus query message is transmitted to all neighboring nodes and energy of each node is compared with average residual energy, if the difference is more, then suspicion is born. However, the Base station algorithm is embedded in the base station and has a timer to calculate the length of each iteration. This approach is robust to malicious byzantine nodes and false positives and false negatives are greatly reduced.

Greedy Behavior Attack: It is when greedy or selfish drivers aim to use network resources for their own benefit. It can cause an illusion of traffic congestion in its neighborhood. The attacker may also persuade the neighboring vehicles that there is a congestion in a specific route, thus they will use alternate routes and this will grant him/her a clear path to his/her destination [149].

-Layers targeted: Manipulate specific Data Link layer parameters.

-Solution: In [133], a detection algorithm for greedy behavior attacks is proposed based on a statistical method, linear regression and watchdog software. A proposal named GDVAN (Greedy Detection for

VANETs) [134] is proposed for greedy behavior attacks in VANETs. The proposed method mainly consists of two phases: the suspicion phase and the decision phase. The suspicion phase is based on linear regression mathematical concept while the decision phase is based on a fuzzy logic decision scheme. The proposed algorithm detects the existence of a greedy behavior and establishes a list of the potentially compromised nodes using three newly defined metrics. The major advantages of this technique is that it can be executed by any node of the network and does not require any modification of the IEEE 802.11p standard. Another proposal is UPPAAL model [150] which is interested in the contention access period of the beacon-enabled mode of the slotted CSMA-CA. The developed model shows it is suited to assess and identify both honest and greedy devices. However, the proposal misses the simulation to validate the proposal.

Hardware Tampering: Hardware tampering can occur at the manufacturing level or by other mechanical ways that manipulate the node physically [151]. If materials are physically damaged, communication is disturbed and becomes unavailable [152].

-Layers targeted: Physical Layer.

-Solution: One of the proposed solutions is using Trusted Platform Module (TPM) [135]. Here, a driver must perform a physical verification. Hardware tampering also includes sensor tampering which means alteration of the position, speed and the orientation of other cars by an attacker. In case of an accident, the responsibility will fall on the attacking node rather than on the attacker.

All availability attacks and their solutions are summarized in Table 4.

4.6.2. Attacks on authenticity and identification

Authenticity is considered as a hard challenge in ITS security where the legitimate nodes should be protected against different kinds of attacks. It enables the receiver to validate the origin of data received. In fact, available services should only be accessed by the authenticated nodes and any fragility in the process of authentication or identification leads to perilous consequences in the network. An outside or inside attack can be prevented by ensuring the authentication using a falsified identity [16]. Whenever a vehicle needs to join the network or needs any service to allow the access, first it should pass through the process of identification-authentication. Let us note that the term of "authentication" from a cryptographic viewpoint means both authentication and integrity. Even though in this part, the focus is on authentication attacks, in the following part, integrity attacks are described. A list of these attacks is described in the following:

Node impersonation attack: In the impersonation attack, the attacker obtains the credentials for another legitimate vehicle in the network. Every vehicle has a network ID which allows to distinguish it among the other nodes [140]. The attacker can advertise fake routes to confuse others, forward a route message with false sequence numbers to delay other messages, and also is able to flood the network

by DoS attacks. In many networks, a malicious node could obstruct proper routing by injecting false routing packets into the network or by modifying routing information.

-Layers targeted: Network Layer

-Solution: Use Secure Ad-hoc On-Demand Distance Vector (SAODV) which depends on (1) **Hash chains** to secure mutable fields of the messages (hop count information is the only mutable field), and (2) **Digital signatures** to authenticate the non-mutable fields of the messages [153, 154]. Another solution was proposed in [155], which is a Double Authentication (DA) scheme which provides authentication to the routing information data carried by the link state routing packets. Every router needs to sign the routing data twice with two different keys using a group keying scheme, which is based on one-way hash function. In addition, in [156], they proposed the first group communication protocol to allow vehicles to authenticate and securely communicate with others in a group of known vehicles. A more recent solution is [157], where the authors proposed a framework to detect and prevent impersonation attacks. It relies on hypothetical examination of utilizing the spatial association of RSS inherited from remote hubs for assault identification. The authors used an unsupervised threshold methodology to split the RSS hint of hub character into two classes. It is not dependent on cryptography as the premise to catch mocking assaults. The strong point is that it effectively eliminates the adversaries from the network. Then, we see that EEPM (Efficient probabilistic packet marking) and RSS (Received signal strength) are the techniques availed by the authors in [158] for the prevention of impersonation attacks. Inter domain packet filter (IDPFs) architecture based on locally exchanged BGP updates is used and it looks for feasible route from source to destination to route the packets. This proposal is extremely effective with high detection rates.

Key and/or Certificate Replication attack: Duplicate keys or certificates are used as proof of identification to create ambiguity. Therefore, this prevents the authorities from recognizing a vehicle.

-Layers targeted: Network Layer

-Solution: Using certified and available keys will protect the exchanged data. In addition, checking the validity of digital certificates in real time via CRL (Certificate Revocation List) [19] can be used. Another method is to apply the cross certification that occurs between the different certified authorities in the security network [159].

Illusion attack: It is also an attack against integrity and data trust. Sensors are placed in the network to generate false data [160] and the vehicle it self needs to deceive its own sensors. As a result, false data can spread the network. In this attack, the protection process of authentication is not efficient, since the attacker is already authentic. These fake messages can be exchanged normally in the network and are capable of changing the decision of the drivers.

-Layers targeted: Application Layer

-Solution: In [161], they developed a new model, called plausibility validation network (PVN), to protect against fraud messages in traffic safety applications. Also, the signature can be used to detect only authentic location data [98]. Another solution is to use a reputation score for safety applications to detect the malicious nodes [162].

GPS spoofing/position faking attack: "Jamming just causes the receiver to die, spoofing causes the receiver to lie" say consultant David Last, former president of the UK's Royal Institute of Navigation. Here the attacker can change the geographical information retrieved by GPS satellites by producing stronger signals. Thus, drivers might think they are in the right place when they are not. Particularly in transportation systems, the location of information is a very critical point, it must be precise and true [17]. This attack is done when false location information is transmitted to the neighboring nodes. Locations and geographical positions of all vehicles in the network are maintained using the genuine GPS satellite. However, an attacker can use a GPS satellite simulator that is more efficient than traditional GPS satellite, and allows to produce stronger signals [163], to track the node locations. So, other vehicles believe that they are in different locations, which can potentially cause collisions. This threat poses a critical problem in the vehicular network. A successful GPS spoofing attack can open the door for other attacks such as the ones against applications which use the position of the node for identification [144].

-Layers targeted: Application Layer

-Solution: To avoid this attack, bit commitment and signature scheme can be used. These methods work with positioning systems that only accept authentic and real data location [98, 164, 165]. Recently, authors in [166] proposed a two-factor authentication method to prevent spoofing of vehicles based on time synchronization and a digital signature. To hash the GPS signal, a digital signature using RSA-1024 is generated, then the private key is used to encrypt the hashed signal so at last, the car will decrypt the signal using the public key. This proposal is a feasible method and ensures the safety of passengers. A future work can be done is to propose a more secure method to fight the hijacking of cars.

Timing attack: The timing attack is to delay the transmission of messages with high requirements on propagation delay, and transmits them, e.g. after adding time preventing their treatment in a normal way [167], thus making it a useless message. Some classifications such as in [168] and [140], also consider this category as a separate family of attacks. Another classifications has been proposed in [99, 169]. For example, timing attacks can be classified to (1) Vehicle-to-vehicle timing attack and (b) Vehicle-to-infrastructure timing attack which is much dangerous than the former.

-Layers targeted: Transport Layer

-Solution: This attack can be made inefficient by using the "time stamping mechanism" for packets

of delay-sensitive applications. However, this proposition encountered the problem of time synchronization between entities [170].

All authentication attacks and their solutions are summarized in Table 9.

Table 9: Different types of authentication attacks with their corresponding solutions.

Name of Attack	Communication Types	Proposed Solutions	Possible Reason(s)
Node impersonation attack	V2V	[153] [154] [155] [156] [157] [158]	Hardware flaws or insecure wireless communication
Key and/or Certificate Replication attack	V2I/V2V	[19] [159]	Weak certification methods and vulnerable wireless communication channel
Illusion attack	V2I/V2V	[98] [161] [162]	Insecure wireless communication
GPS spoofing/position faking attack	V2V	[98] [164] [165] [166]	Vulnerable wireless communication
Timing attack	V2V	[170]	Non-encrypted messages, Insecure wireless communication

4.6.3. Attacks on integrity and data trust:

The aim of integrity services is to make sure that any exchanged message has not been altered during transmission among the intermediate nodes. Additionally, integrity services immunize the system against destruction, unauthorized alteration or creation. External integrity attacks are not possible since a prior authentication process is required. In fact, this kind of attack is internal and integrity attacks mainly target V2V communications and not V2I communications because of the latter's fragility. Several possible methods exist and can breach the integrity property which will consequently make any transportation system defective [171]. Several examples of integrity attacks are briefly described in the following along with their possible solutions.

Masquerading: It is an active attack where the attacker masks his own identity to act as a legitimate node with the intention to produce false messages in the network or even modify the received message. For example, an attacker may receive a message from ahead vehicles that the road is clear, but he/she

Table 10: Different types of integrity attacks with their corresponding solutions.

Name of Attack	Communication Types	Proposed Solutions	Possible Reason
Masquerading	V2V	[19] [172] [173] [174]	Insecure Communication channel
Replay Attack	V2V	[16]	Vulnerable wireless communication channel
Message Tampering- Suppression- Fabrication- Alteration	V2V	[175] [116] [176] [177] [178]	Vulnerable wireless communication channel
Incorrect Data Injecting Attack	V2V	[16]	Non-encrypted message, Insecure wireless communication
Man in the middle attack	V2V	[179] [170] [180]	Non-encrypted message, Insecure wireless communication, Poor authentication scheme

would broadcast the wrong message causing an accidents or it may act as an emergency vehicle to slow down the entire traffic and the performance of network [181]. Masquerade attacks are ranked second on the top five lists of electronic crimes after viruses, worms or other malicious code attacks. The attacker seems to be an authentic user since he/she uses a valid identity which is known as a mask. This is done by forming a Black-hole or generating false messages which are then broadcast to the neighboring vehicles. This attack has different objectives such as slowing down the speed of a vehicle, changing lanes which may lead to an accident.

-Layers targeted: Network Layer

-Solution: To avoid this kind of attack, a Certificate-Revocation-List (CRL) is used containing the identity of detected malicious vehicles. Therefore, when malicious vehicles act in a malevolent way, their corresponding identities are distributed to the overall nodes within the network, and the CRLs are updated by introducing the identity of the new malicious cars into the list. This can reduce the effect of this attack [19], but also an efficient detection technique of malicious node is required to answer the constraints of ITS. In [172], they proposed using a combination key instead of a public key so that the throughput value is improved by 40%. Authors in [173] proposed an anomaly detection model to detect the masquerade attacks using signal strength fluctuation. At the time of dissemination, one-way hash chains are used with the aim to secure the RSS readings from being fabricated. To find the malicious nodes, two concepts are considered in the detection mechanism: time of reception for each RSS received and the maximum speed of nodes is assumed as Vmax. This proposal does not

depend on the fixed access point or air monitors and its results indicate a good detection accuracy. Another secure genetic-based framework is given by authors in [174] for prevention of masquerade and DDOS attacks. In this proposal, the genetic feeder acts as an intermediate between vehicles and RSUs and helps in sharing the genetic information between them. Genetic information consists of vehicle dynamics, RSU zone, and packet parameters. These genetic information is required to calculate the fitness function. The framework is adequate in enhancing the network accuracy, tracking the time of attackers, network recovery time and decreasing the percentage of the packets.

Replay Attack: Replay attack has a special trait that it can be conducted by illegitimate nodes. A replay attack is the broadcasting of messages again and again by the attacker which are already forwarded to the nodes with the intention of deceiving the other nodes in the network by dropping the priority messages from the queue. The efficiency of the system would be degraded by frequent replaying and the cost of bandwidth is also increased. The adversary replays the valid messages sent sometime before in order to disturb the traffic. The mechanism of a replay attack consists of broadcasting a previously transmitted message [182] to ensure the objective of the transmitted message at the moment such as manipulating the location and the nodes routing tables. Therefore, this leads to mystifying the authorities and to preventing the node from knowing the sender's identity [16].

-Layers targeted: Data Link, Network, Transport, Application Layers

-Solution: A solution is presented which uses the cache of station (RSU or vehicles), and consists in comparing the recently received messages with new incoming messages to reject the received duplicate messages. Hence, it protects the node from replaying an attack, and makes this threat inefficient. In addition, another solution is presented which is "time stamping" for each transmitted packet to prevent the replay attacks [16].

Message Tampering-Suppression-Fabrication-Alteration: The attacker here aims to break the integrity of the exchanged messages which is done by altering, removing, or creating other messages [183]. Availability and non-repudiation services are also affected. This happens when the attacker manipulates the received messages for his/her own goals. Therefore, this will lead drivers to change their decisions and for example to take a different road than the one they intended to use in the first place.

-Layers targeted: Network Layer

-Solution: One of these security methods is using vehicular PKI (VPKI) or a zero-knowledge to authenticate the vehicles and to sign warning messages [116], [176], [177]. Furthermore, a group of communication can be established which is also considered an efficient method as indicated in [175]. The keys can be conducted by a Group Key Management system (GKM) [178]. In other words, if an intruder tries to attack, he/she will not be able to communicate through this closed group.

Incorrect Data Injecting Attack: This kind of attack is generated from a legitimate node. Thus, this can cause hazardous effects in the network and may lead to fatal accidents [16], by creating a false message and broadcasting it or removing the traffic warning. The strategy of this attack is to hide the real safety messages from allowed users and then inject false security messages in the network.

-Layers targeted: Network Layer

-Solution: To defend this attack, the broadcast message should be signed and included in the transferred message. However, a non-repudiation method is necessary to reveal the attacker's identity that should be appended in the RLCs [16].

Man in the middle attack: The Man in the middle Attack (MiMA) is a common attack on the communication that takes place among users. In this attack type, the attacker is placed between the two communicating legitimate node/vehicles, and eavesdrop their communication and inject the fake information or even modify the messages between them [184]. The attacker is usually situated between a minimum of two persons. The attacker here is a vehicle inserted between two communicating nodes (vehicles). The man in the middle, attacker, has the ability to control the communication between these legitimated nodes [140], so that they assume that they are directly communicating with each other. In this case, the attacker breaches the authentication, integrity and non-repudiation mechanisms.

-Layers targeted: Network Layer

-Solution: Using digital certificates, secure communication and good cryptography will be a good solution [179]. In addition, using an efficient authentication scheme as proposed in [170] can be another solution. It is proposed that a decentralized lightweight authentication scheme called trust-extended authentication mechanism (TEAM) can be used for vehicle-to-vehicle communication networks. Authors in [180] have modified the existing Anonymous Location-Based Efficient Routing Protocol (ALERT) to prevent the man-in-the-middle attacks by applying a hash function with the SHA-1 algorithm as well as location-based pseudonyms of nodes. Proposed scheme uses the concept of ACK for the successful delivery of packets so malicious nodes are detected by calculating the hash values at both source and destination. If the malicious node is detected, then it will send a negative acknowledgment to send packets again as well as using alternative path for routing. This proposal is cheap and efficient for reliable communication. While the disadvantage is taking so much time in a simulation for sending data.

All integrity attacks and their solutions are summarized in Table 10.

tools.

4.6.4. Confidentiality attacks:

Confidentiality is the ability to conceal messages from a passive attacker so that any message exchanged through the network remains confidential. This is the most important point in security, that is to say to protect the data from being collected by unauthorized users. The message confidentiality in ITS can be employed for specific applications that require sharing sensitive information such as those used for toll payments using a V2I connection. For example, here the confidentiality becomes essential to provide a secure Internet connection by encrypting the message transmitted between vehicles and RSUs [17]. However, if there is no sensitive information in the transferred messages, then the confidentiality is not mandatory [19]. Encryption process can be deployed in symmetric or asymmetric ciphers [185]. The asymmetric class requires heavy computation complexity and resources compared to symmetric ones. Encrypting messages needs a session key, which is generated initially after mutual authentication between the RSU and the vehicle. For each encrypted message, the MAC (Message Authentication Code) or a message authentication is attached to the encrypted message to add robustness against attacks. Several attacks can affect the network in the absence of confidential protection mechanism. Improper collection of clear information [16] affects the individuals' privacy, since the attacker is capable of gathering several information such as the location of the vehicle and its routes, etc. Unfortunately, the victim is not able to detect it since this kind of attack consists in listening to the media, which is easy to carry out. A list of passive confidential attacks is presented in the following and each one is briefly described:

Eavesdropping attack (EA): Eavesdropping attack only influences the network confidentiality and will not have any impact on the network itself [17]. The aim of this attack is to illegally obtain access to confidential data. By spying on the data, the adversary could easily discover communication contents. It detects useful information, such as data location, which can be employed for tracking vehicles.

-Layers targeted: Physical Layer

-Solution: To provide resistance against this attack, the sensitive data that risks the driver's privacy (positioning and vehicle identification data) should be securely encrypted [186].

Traffic Analysis Attack (TAA): TAA affects the user's privacy in addition to his/her confidentiality. This attack is extremely dangerous and consists in listening to the network for a communication pattern, then trying to analyze the collected data to extract as many useful information as possible. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm the network.

-Layers targeted: Physical Layer

-Solution: The same proposition that enables one to provide resistance against eavesdropping can be used to resist the TAA [186], in addition to using VIPER (Vehicle to Infrastructure communication Privacy Enforcement Protocol Algorithm) for V2I communications [183]. It is resilient to traffic analysis

attacks. In this solution, vehicle will send their messages directly to RSU and will not have vehicles acting as mix nodes.

Brute force attack: It is a trial and error method used to obtain information such as a user password or personal identification number or to crack encrypted data or even to test network security. The attacker can use the brute force technique to break the used cryptographic key [187]. In a transportation environment where connection times are relatively short, a brute force attack is not easy to perpetrate, since it is time consuming and resource exhausting.

-Layers targeted: Network, Transport Layer

-Solution: This attack can be made inefficient by using a strong encryption and key generation algorithms which are unbreakable within a reasonable running time [16]. Another Brute force attack solution is proposed by Langley et al. [188]. In this context, a secure authentication method requires the use of some unique identification for vehicles concatenated with some large random value and then hashed using some hash algorithm.

All confidentiality attacks and their solutions are summarized in Table 11.

Table 11: Different types of confidentiality attacks with their corresponding solutions.

Name of Attack	Communication Types	Proposed Solutions	Possible Reason
Eavesdropping attack (EA)	V2V/V2I	[186]	Broadcast nature of messages via wireless channels, un-encrypted communication channel
Traffic Analysis Attack (TAA)	V2V/V2I	[186] [183]	Vulnerable wireless communication channel, Data leakage on communication channel
Brute force attach	V2V/V2I	[16] [188]	Short cryptographic keys, and weak cryptographic methods.

4.6.5. Attacks on privacy:

Ensuring user's privacy is one of the most important challenges in ITS. Preserving users' privacy is mainly related to preventing the disclosure of their real identities and location information. Drivers need to keep their private information protected such as their identity, their driving behavior, the past and present location of their vehicle [189, 190]. In order to preserve the privacy of drivers, each vehicle is loaded with a pool of certified pseudonyms obtained from a certificate authority [191]. One of the most popular attacks here is the Sybil attack since this granted pool of pseudonyms can be used to pretend that they are for different

vehicles and send false messages to other vehicles (false traffic jams, or false alerts forcing others to modify their itinerary). The main goal of the authorities here is to ensure that the identities and their corresponding sensitive data are protected during communication. On the other hand, when an issue arises, the system operators and car manufacturers should interfere and this requires knowing the identity of the user. This indicates that a trade-off between privacy and security exists. Several privacy attacks are presented in [175] and [17] and are described below, then, common solutions are proposed.

Tracking: It allows to chase a vehicle during its journey and then discover the identity of the driver (relating the vehicle to place of work, home..) Therefore, even though the keys used usually do not use public relations to the true identity, MAC and IP addresses must change over time to avoid any possible identity disclosure [19]. MAC, IP addresses allocation, and used keys must be managed by new algorithms to avoid facing a large memory space dilemma.

Identity/Location Tracking: In this type of attack, an attacker may get a trace of the vehicle movements, and from the study of this trace, he/she can reveal the true identity of the vehicle and its personal information. An example of that is an employer in an organization who overhears a communication coming from the parking lot. Since he/she knows the identities of all the cars in the parking lot, he/she can simply know its arrival and departure dates. Another example is about a criminal organization that gains access to stationary communication boxes, then it extracts information to track law enforcement vehicles. Rental Car companies are using this ID and track the location of their own vehicles.

-Layers targeted: Privacy attacks usually target the Application Layer or Data link layer where identities are usually stored. Also, this can affect the physical layer when the credentials are stored in hardware modules (Trusted Platform Module - TPM) [192].

-Solutions: The existing privacy solutions are based on the architecture presented in [193] that defines the use of the pseudonyms to ensure an anonymous network. The responsibility to manage the vehicle identities (generation, distribution and revocation) is held by the certification authorities, which can be classified, based on a region. Therefore, a dense number of certification authorities (CAs) is required. In fact, vehicles need pseudonyms to preserve their privacy, but it is illogical to load each vehicle with a large number of pseudonyms and keys since this requires a large storage area. In addition, using the pseudonym more than once time will degrade the vehicle's privacy. Additionally, each station, vehicle or RSU, possesses a pair of private and public cryptographic keys and a unique identity. To obtain the real identity of the Vehicle, a judgment should be required. The limitations of this protocol is that it requires vehicles to store a large number of pseudonyms and certifications, where a revocation scheme for abolishing malicious vehicles is difficult to implement. It is preferable to preserve the location privacy of a vehicle by breaking the linkability between

two locations, for which the vehicle can update its pseudonym after each transmission. Taking into account that a powerful adversary may still link the new and old pseudonyms by monitoring the temporal and spatial relations between new and old locations, the techniques of mix zone [194] and silent period [195] have been proposed to enhance the pseudonym scheme. Each vehicle in a mix zone will stay silent during transmission, and randomly update its pseudonym when it travels out of the mix zone and becomes re-activated.

In [159], they proposed to use a set of anonymous keys that can be preloaded in the vehicle's TPD (Tamper Proof Device). Each key is certified by the CA and is used for a short time, which means that it must be changed frequently.

Lu et al. [196] proposes a privacy preservation protocol (ECPP) for anonymous authentication. The protocol uses short time anonymous keys between On-Board Units (OBUs) and Roadside Units (RSUs). The anonymous key needs a minimum of storage to avoid losing the security level. The network architecture is composed of the trusted authority (TA), the immobile RSUs on the roadside and the mobile OBUs equipped on the moving vehicles.

Zhang et al. [197] introduced a novel decentralized group-authentication protocol rather than by a centralized authority, where each RSU is used to maintain and manage an on-the-fly group within its communication range. Vehicles entering the group can anonymously broadcast vehicle-to-vehicle (V2V) messages, which can be instantly verified by the vehicles in the same group (and neighboring groups). Later, if the message is found to be false, a third party can be invoked to disclose the identity of the message originator. This protocol efficiently exploits the specific features of vehicular mobility, physical road limitations, and properly distributed RSUs. If some RSUs unexpectedly collapse, only the vehicles that are driving in those collapsed areas will be affected. Due to the numerous RSUs sharing the load to maintain the system, performance does not significantly degrade when more vehicles join the VANET; hence, the system is scalable.

In [198], they propose using group signature, where one group public key is associated with multiple group private keys. In the AMOEBA [199], vehicles form groups. The messages of all group members are forwarded by the group leader, which implies that the privacy of group members is protected by jeopardizing the privacy of the group leader. In case a malicious vehicle is selected as a group leader, then, all group members' privacy may be leaked by the malicious leader.

Zhang et al. [200] proposes a vehicular authentication protocol called "APPA" to trust the vehicular communications and privacy of vehicles. This protocol is identity-based cryptography, aggregate signature and one time signature. If a vehicle obtained a secret key from a trusted authority (the secret key is associated with the vehicle's identity), it could sign messages. The signature on a message uses the vehicles identity which is a one-time pseudonym.

Although privacy has been recognized as a serious problem, robust technologies and architectures still have to be developed in order to ensure the users' privacy. Discussed privacy threats and solutions are all summarized

in Table 12.

Table 12: Different types of privacy attacks with their corresponding solutions.

Name of Attack	Communication Types	Proposed Solutions	Possible Reason
Identity revealing	V2V	[159] [193] [201] [194] [195] [196] [197] [198]	OBU vulnerabilities, reusing pseudonyms,
Tracking	V2V		
Identity/Location Tracking	V2V		

4.6.6. Attacks on non-repudiation

It is the security mechanism in which the sender/receiver can prove that a transaction occurred while preventing the receiver/sender from denying that. This prevents false denials involved in the communication. The main aim of non-repudiation consists in collecting, maintaining, making available and validating undeniable evidence about a claimed event or an action in order to resolve disputes about the occurrence or non-occurrence of that event/action. Non-repudiation depends on authentication, but it generates an evidence in the system that can identify the attackers who will not be able to deny their crimes [202]. Any car information will be saved in a Tamper Proof Device (TPD) and any authorized official will be able to retrieve these data.

-Layers targeted: Application Layer

-Solutions: Three different solutions exist for non-repudiation: (1) Public Key Infrastructure [87] (2) ID-Based crypto-system [203] [204] and (3) Situation Modeling-Based mechanism. In PKI solution data authentication and non-repudiation can be performed using the digital signature, which is implemented using asymmetric cryptography where each entity has two keys: a public key and a private key. The ID-Based crypto-system uses any known information which represents the identity of the user for the purpose of verifying the digital signature. This public information could be an email address, network address, user name or any combination of these identities. The third solution, situation Modeling-Based mechanisms, is based on generating ITS models for vehicle driving trends and routines to enhance the security by nodes management [205, 206]. The challenges in these non-repudiation solutions are presented in Table 13.

Finally, at the top level, all the aforementioned attacks can be classified according to the layer(s) they affect, in the network protocol stacks as shown in Figure 6. Each layer is presented as a specific color, and the attacks having the same color means that they occur upon this specific layer. Moreover, attacks like Gray-Hole, Black-Hole, wormhole,Brute force, Replay, Sybil and DoS are represented with different colors since they affect more than one layer. Finally, as seen at the application layer some attacks can occur on data link as well.

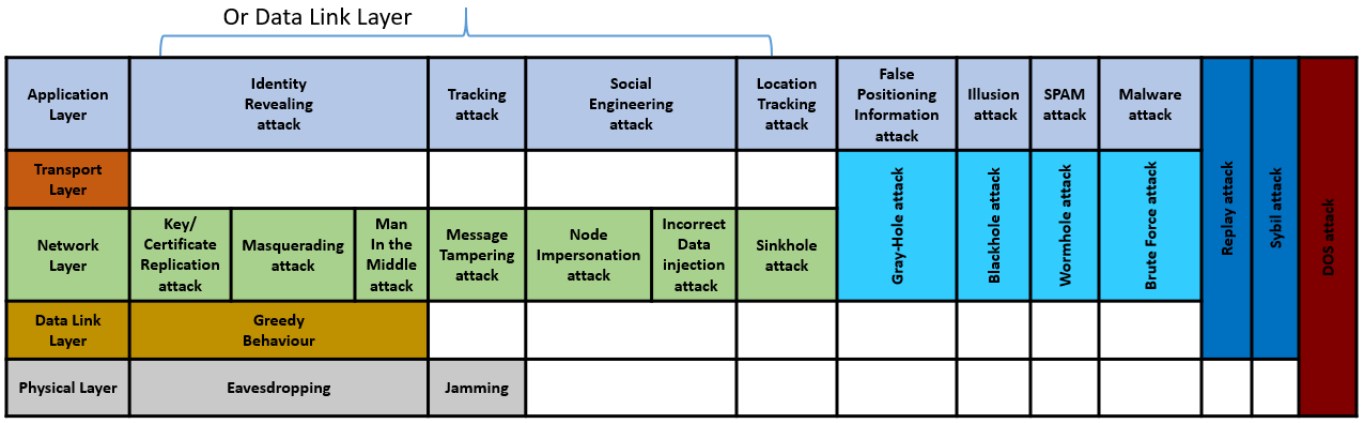

Figure 6: Attacks with their corresponding Internet Protocol Stack layers

Table 13: Non-repudation challenges in different architectures.

VANET ARCHITECURE	Challenge
PKI	Need communication resources and large communication overhead.
Identity based	Risking the ID- privacy of the Vanet users.
Situation Modeling	Complexity in different proposals.

4.7. Social Engineering Attacks (SE)

Social Engineering: Referred to as Advanced Persistent Threats (APT). These attacks have two main phases: Reconnaissance and Attack. It is a kind of emotional attack in which the attacker sends unscrupulous messages in the network with the aim to infuriate the legitimate users. Exploiting the emotional side of the drivers is the easiest attack a person can make. Due to this, the driving behavior of the vehicle gets affected and creates a problem in the network [104]. As described by Kevin Mitnick in [207], social engineering is as an "act of psychological manipulation which was popularized by hacker-turned-consultant". The attacker aims at pre-texting, phishing, and diversion theft, mainly. Due to the dynamic behavior of vehicles, social engineering attackers do not use these methods. Instead, there are three different scenarios in which a social attack can happen. (1) An attacker finds the busiest road in the area that usually has traffic and where it will be perfect to launch an attack. (2) An attacker chooses a traffic peak time (like lunch breaks, busy hours) to take advantage of the traffic. (3) An attacker starts collecting the personal data (user ID, location, passwords, private information, medical data). One type of such kind of attacks is the **Reverse Engineering attack** which is also known as a person-to-person attack. This allows the attacker to hide himself as a legitimate use. For example, he/she takes the role of a technician that wants to fix an issue in the network. This act can give him/her physical access to facilities, which in turn will allow for malware

or virus to spread into the whole system. Another example is just asking questions for different users to gain more knowledge about the network. Phishing attacks is the preferred method to obtain information or access into a network. A victim will open a harmless email, either click a link that leads to a malicious site or download an attachment which contains malicious code, and compromise his/her data. Phishing has been increasingly successful because the attackers are creating more legitimate looking emails and the attacks are becoming more sophisticated. Moreover, thanks to the prevalence of social media, an attacker can search up everything they need to know about a person and his/her interests, generate an email specially tailored to that person, and send it directly to them, which increases the chances of that person clicking. "Vishing" is essentially phishing over the phone. An attacker will simply call someone, such as an IT help desk, and with a little bit of information about a person (such as a name and date of birth from social media accounts), either he/she can get login credentials or more information about the individual, such as a social security number, credit card number, plate number etc..

This attack affects the privacy of users directly. Obtaining the ID and the location of certain vehicles is considered as a threat for the privacy of users. Usually, the attacker studies different areas and chooses the best one to launch an attack on the network. For example, the attacker can know that a specific ID has this location and can then link the different locations to it, which is basically what privacy tends to protect. Moreover, in December 2006, United States Congress approved a senate sponsored bill making the pre-texting of telephone records a federal felony with fines of up to $\$250{,}000$ and ten years in prison for individuals (or fines of up to $\$500{,}000$ for companies).

Solutions: There is no direct solution for this attack other than spreading knowledge and warning people of such kinds of attacks. Security awareness training programs are very helpful to reduce the risk of getting compromised and increase the level of awareness addressing the importance of the human factor. In fact, major data breaches and hacking of major companies such as Target, Sony, or even the State Department generally have one thing in common, and that is that despite the sophistication of the malware used to gather information, that malware has to be downloaded into the computers of the targeted company/platform. This is most probably done through social engineering methods that trick employees into clicking on links or downloading attachments that unwittingly download the malware.

4.8. An ITS risk analysis study

ITS are cooperative systems based on vehicular communications and are considered as a compromising approach to enhance road safety, efficiency and convenience. VANET and IoV pose several research challenges, especially on the aspect of security, since various elements are used such as communication architecture, applications, and protocols. Moreover, the existing literature focuses on preventive attack techniques to achieve security protection. In this section, a simple risk assessment is presented, while less work in this field is presented. However, a new risk assessment method is required to quantify the security risk of ITS

attacks, which is a complicated task. Addressing threats in ITS and analyzing their associated risks is an initial step to define new security solutions adapted to ITS applications and communications. Previously, some challenges and threats have been described, which will help to quantify the strength of attacks when necessary. The proposed risk analysis based on ETSI Threat, Risk, Vulnerability Analysis (TVRA) methodology [208] is based on the product of the likelihood of an attack and the impact of the attack on the system. The system assets and its associated threats in addition to the threat agent that tries to break the system should be identified by the TVRA method. Therefore, the outputs of TVRA are a measure of the risk of identified threats and can be determined based on their estimated value of likelihood and impact upon the system. In the following, several countermeasures and security frameworks are specified taking into account both ITS application constraints and the developed risk analysis. Three levels of risk are defined: Minor, Major, and Critical. Threats ranking as Critical mean that an urgent and priority countermeasure should be defined, while Major risk should also be treated with a lot of attention. On the other hand, threats that possess minor risk get less attention in the study. The existing threats that can be ranked as critical and major are represented in Table 14 risk analysis.

Table 14: Qualitative risk analysis according to [208]

Kind	Threat	Needed Attacker capabilities	Motivation of the attacker	Likelihood	Impact	Risk
Availability	Flooding/ Spamming	No rating	Moderate	Possible	Medium	Major
	Black hole	Moderate	High	Likely	High	Critical
	Malware	Basic	High	Likely	High	Critical
	Jamming	Basic	Moderate	Possible	Medium	Major
	RF Fingerprinting	Extensive	Low	Unlikely	Low	Minor
Authentication	Masquerade	Moderate	Moderate	Possible	High	Critical
	Sybil attack	Extensive	High	Possible	High	Critical
	Illusion attack	Extensive	High	Possible	High	Critical
	GPS Spoofing	Moderate	Moderate	Possible	High	Critical
	Sensor spoofing	Extensive	Moderate	Unlikely	High	Major
	Replay	No rating	Low	Possible	Medium	Major
Integrity	Manipulation of messages	Moderate	Moderate	Possible	Medium	Major
	Injection of false message	Moderate	Moderate	Possible	Medium	Major
Privacy &Confidentiality	Eavesdropping +data analysis	Extensive	High	Possible	Medium	Major
Privacy	Location tracking	Basic	High	Likely	Medium	Critical

4.9. Modern security layers

The security layer in ITS in Figure 7 is composed of 4 sub-layers:

Material layer: Several physical resources are used to reach the objectives of ITS such as OBU, GPS, radars, Event Data Recorder (EDR), antennas, etc. They should be protected in order to resist physical attacks. For that reason, these devices could be secured and should be built according to the Trusted Platform Module (TPM) specifications [209]. Furthermore, TPM is a hardware piece that can protect and store data in shielded locations [192] by employing a software infrastructure.

Authentication layer: The authentication layer should ensure all kinds of authentications which are users, source and location authentication. The users' authentication prevents unauthorized users to access the system. Moreover, source authentication permits receivers to verify the source entities and ensure data integrity [210]. For that reason, the digital signature is used and requires the existence of the vehicular PKI. In the context of transportation systems, the location authentication is necessary and permits the receiver to verify the sender's position. These authentications are conducted progressively and not simultaneously.

Trust layer: The implementation of the trust layer consists of two parts, where the first one is a trust system [152], and the second one can be a reputation [211] or a Plausibility Check System(PCS) [212]. The importance of the trust layer is the validation of communication and it can provide the non-repudiation requirement. Indeed, the trust system consists in implementing the TPM mechanisms. The reputation system builds an opinion concerning a node that wishes to communicate. This opinion is obtained by analyzing several collected local information such as speed, position, acceleration, etc., as well as information from other internal users. On the other hand, if a PCS is used, a verification process is required to ensure that this information corresponds to this specific event. As a conclusion, the main goal of the trust layer is to discover which nodes are trustworthy. An important requirement that can help the trust layer is to collect sufficient information about the sender's node, which permits to register these traces in order to support their corresponding consequences. Let us say that the trust layer should provide resistance against availability attacks.

Privacy & Data confidentiality layer: The main goal of this layer is to preserve the privacy of users and their sensitive information in the network. Several solutions have been described previously to reach this objective. For that reason, sensitive information should be encrypted before being sent to avoid attacks on this layer.

It can be noted that the cryptographic primitives are implemented at both Authentication Layer and at the Privacy and Confidentiality Layer.
This approach could be illustrated to ensure three major objectives:

Prevention: Resembled by Security Material Level and the Authentication Layer.

Detection: Resembled by the Trust level.

Privacy: Resembled the Privacy and Confidentiality Layer where cryptographic primitives are mainly implemented.

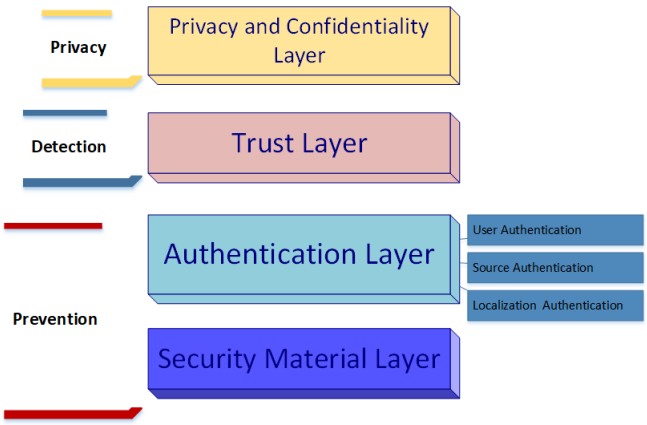

Figure 7: Security modern layers and their corresponding objectives.

4.10. Security services for communication types in ITS

Table 15: Required security services for VOB, IOB and IUV

Security Service	VOB	IOB	IUV	Mechanism
Confidentiality	%	%	!	Encrypting only sensitive messages; Randomizing Traffic Patterns
Authenticity	!	!	!	Message signature Trusted Hardware Module; Active Detection Systems
Integrity	!	!	!	Message signature and other integrity metrics for content delivery
Non-repudiation of source	!	!	!	Message signature
Authorization and privilege classes	!	!	!	Certificate accompanying message signature
Non-repudiation of receipt	%	%	%	Not mandatory
Anti-replay	!	!	!	Message signature containing verifiable time variant data
Plausibility verification	!	!	!	Check mechanisms ensured by IEEE P1609.2.
Availability	!	!	!	Pseudo-random Frequency Hopping Access Control and signature-based authentication
Privacy protection measures	!	!	!	Pseudonymity, Unlinkability ID-based/PKI based System for User Privacy

According to [213], three kinds of communication are presented, which are Vehicle-Originating Broadcast (VOB), Infrastructure-Originating Broadcast (IOB), Infrastructure-Vehicle Unicast (IVU). In Table 15 the required security services are described for each communication type. The application scenario defines the security services required to ensure a safe implementation. The three kinds of communication are described briefly in the following:

Vehicle-Originating Broadcast (VOB): The vehicle is the origin of the broadcast exchanged message that contains information about the behavior of the source such as its movements and safety (in ETSI CAM message is employed). This will inform the neighboring vehicles and will reduce dangerous hazardous situations. VOB is essential for road safety applications.

Infrastructure-Originating Broadcast (IOB): IOB communication is used by all vehicles under the communication range of a specific RSU. It will inform the vehicles, which are in the vicinity of a specific road infrastructure location, by safety and mobility information. This will ensure a better safety for data which is relevant to all vehicles. Indeed, the security service requirements for IOB are similar to that of VOB with few differences [214].

Infrastructure-Vehicle Unicast (IVU): IVU communication is employed for unicast transactions between a vehicle and RSU or vice versa. In fact, IVU can be used for commercial and comfort applications. The required security services for the different communications VOB, IOB, IUV are shown in Table 15. From a security viewpoint, the non-broadcast nature of IVU requires ensuring confidentiality in addition to the security service requirements of VOB and IOB.

5. Existing Cryptographic Solutions for ITS

In the previous section, lists and classification of attacks according to security services were introduced. Certain attacks can be prevented by using cryptographic solutions (algorithms and/or protocols). For this reason, section 5 is introduced to explain the different possible cryptographic solutions that can also secure ITS. Current security-system/architecture-based researches can be classified into the following three categories with reference to different technology vantage points. Current researches classify the security system architecture into four different cryptographic categories: (1) **Public Key Infrastructure (PKI) based** schemes (PKI based approaches, pseudonym-based approaches and group signature-based approaches), (2) **Crypto-Based security based** schemes (3) **Non-fully PKI based** schemes (identity based cryptography and hybrid approaches etc.), and (4) **Situation modelling-based** security system architecture which will be discussed briefly in the following.

5.1. PKI-based security system architecture

PKI is used for the asymmetrical algorithm based security applications. In addition, PKI provides several security services such as certificate generation, renewal, and cancellation, signing and issuing, check, maintenance, audit, etc. The certificate is provided by the PKI link public key in the public/private key array with the owner's identification and encryption technology. PKI requires using CRL (Certificate Revocation List) in order to ensure a safe and secure management in real network implementation. This requirement can be considered as a critical problem and introduces high communication overhead. Currently, a list of

recent security schemes that are based on PKI and a comparison of the communication overhead is presented in [215]. In [216], a TPM-based security architecture is proposed which can form trusted grouping through PKI security mechanism. Its robustness is proven in [217]. In [218] the problem of identification in such a heterogeneous environment is addressed by using the blockchain technology. The authors show that the blockchain technology is an example of that successfully solves this kind of challenge. The proposed solution is a combination of reliable system entity naming (public keys, digital certificates) and reliable system event logs and system histories.

5.2. Cryptographic Algorithms-Based Security

In [219], the authors provide a new security scheme for ITS that can provide privacy, data confidentiality and integrity, and non-repudiation by using a symmetric block cipher algorithm and a certificate-based public key cryptography scheme. The privacy and data confidentiality is ensured by employing the robust block cipher AES [220]. On the other hand, using digital signature to provide data integrity, source authentication, and non-repudiation, the exchanged message is signed by using the sender's private key. This scheme is based on certificate-based public key cryptography so an overhead of such a scheme can create a delay in transmission. The asymmetric cryptographic algorithms suffers from the latency limitations and a lot of recent optimization are presented towards making them suitable for time-critical applications such as in ITS. In the field of asymmetric cryptography, the security of all practical crypto-systems rely on hard computational problems strongly dependant on the choice of parameters. For example, authors in [221] have presented a way to exploit the GPUs to favor the asymmetric cryptography. It is clear that asymmetric solutions need a lot of enhancements and optimization in order to meet the requirements desired. Moreover, comparative studies have been proposed between cryptographic algorithms. For example, in [222], authors presented an overall comparison by using a real-time software named as cryptool to examine the real-time results depending on the file size. Processing times of each cryptographic algorithm has been compared on a different set of parameters. In addition, in [223] the authors proposed a combination of both symmetric and symmetric cryptography that reduces encryption time in preference to simply using an asymmetric cryptographic algorithm. The use of random keys for symmetric encryption each time solves the issue of session-key distribution and strengthens the symmetric encryption approach.

5.2.1. Anonymous Authentication Protocol

An anonymous authentication protocol is proposed in [224] for V2I communication and is based on Certificate-based Cryptography (CBC). This proposition can ensure conditional privacy and non-repudiation.

5.2.2. Message Linkable Group Signature (MLGS)

Qianhong Wu et al. [225] proposed a new privacy-preserving technique called Message Linkable Group Signature (MLGS). This technique provides anonymous authentication. In this technique, it is assumed that

most of the vehicles in the network are honest. In this system, a threshold mechanism is used as a priori countermeasure. A message is considered as trustworthy if at least n vehicles endorse this message. This n is a threshold which is adaptive. The sender can change the threshold. If a node produces two signatures on one message then a trusted authority will identify it as an attacker. A Sybil attack can be avoided by using this technique. If a vehicle receives a message with multiple signatures, it can check whether these multiple signatures are from a single vehicle or from multiple honest vehicles.

5.2.3. Direct Anonymous Attestation (DAA):

It was first proposed by [226]. This promising technique that provides both anonymity and accountability is an anonymous group signature scheme that is mainly used to attest to the state of a device based on a secure hardware root of trust. In DAA each user platform is upgraded with a Trusted Platform Module (TPM) which isolates a cryptographic key that will provide with the host platform a remote authentication in a privacy-preserving way. DAA allows using pseudonyms, which means that for each signature, the user (previously agreed with the recipient of the signature) can decide whether or not the signature should be linkable to another signature. DAA allows for detection of "known" keys; if the DAA secret keys are extracted from a TPM (Trusted platform Module) and published, a verifier can detect that a signature was produced using these secret keys [226]. It has been since then standardised by the Trusted Computing Group (TCG) which includes it in its TPM specification. The latest TPM 2.0 standard uses ECDAA (Elliptic-Curve based DAA) which is developed by authors in [227]. However, in [228] authors have addressed some security issues and applied some changes to the latter. One of the drawbacks is that the current schemes suffer from inefficiency in the revocation procedures which increases as the size of the revocation list increases [229]. The method usually used in DAA operates uniquely with the assumption that the long-term TPM secret is compromised and discovered by the verifier. In [230] authors proposed a decentralized DAA approach with the ability of shifting trust from the infrastructure to vehicles. Another solution is presented in [231], which is the REWIRE V2X revocation protocol. It uses trusted computing to allow revocation without pseudonym resolution and the OTOKEN protocol [232] enhances REWIRE using the results of symbolic protocol analysis. These schemes depend on having vehicle hosts which will properly forward revocation messages to the trusted platform. To solve this problem, Chen et al [233] proposed a DAA-based V2X scheme, while retaining centralised revocation, it provides a mechanism to detect vehicles that abuse their anonymity to send multiple messages relating to the same event. Then, an enhancement to this proposal is proposed as a Vehicular DAA Scheme (VDDA) [234]. It uses efficient standards-compliant ECDSA signatures on broadcast messages, tolerate communication overheads and prevents Sybil attacks. VDAA maintains vehicle privacy even under the much weaker assumption that the certificate authorities collaborate and that the TPM is compromised. Finally, the most recent solution was proposed in [218] where authors discussed that a solution based on Blockchain technology, which solves these problems in an inherent way.

5.3. ID-based security system architecture

To cancel the overhead of CRL and to avoid the use of PKI, the architecture of ID-based security system is presented. Moreover, an ID-based Encryption algorithm is used for the generation of a pseudonym, which is renewed as required. It is feasible for an entity to possess assemble groups made of several pseudonyms for privacy defense when the authentication and the signature are approved. ID-based security method must guarantee ID privacy, a precondition for protection of user's safety and privacy. The key point lies in generating an irreversible algorithm for pseudonyms based on ID with the firm confirmation that only one pseudonym is available within the same entity to prevent a Sybil attack. Indeed, in [54], they employ ID-based encryption for pseudonym generation and conduct the control of signatures and identify authentications through a threshold scheme to satisfy security and privacy requirements. In addition, a method for trust domain division pursuant to common domain in use is presented. Additionally, in [235], they combine the ID-based signature (IBS) scheme with the ID-based online/offline signature (IBOOS) scheme apart from ECC based short digital signature for time-validity improvement.

5.3.1. ID-Based Authentication Scheme

Table 16: Security Solutions for different features

Taxonomy	Entity-base Rep.(VARS) [211]	Data-Centric Trust-Model [236]	Event-base Reputation [237]	ID-based Auth [238]	MLGS [225]	RaBTM [239]	ID-Based Security [54]	D. Sig. &Pwd [235]	Cert. based Auth [224]	EDR [240]
Authentication				!	!		!	!	!	
Non-Repudiation				!			!		!	
Integrity		!						!		
Privacy				!	!	!	!		!	!
Confidentiality							!			
Privacy (pseudonymity)				!	!	!		!	!	
Reputation	!	!	!			!				
Revocation										!

An authentication framework for RSUs and Vehicles is presented in [238] and it uses ID-based encryption. The process of authentication consists of three kinds of authentication, which are V2I authentication, V2V authentication, and I2V authentication. The authentication between the RSU and the vehicle is ensured by using an ID-Based Signature (IBS) scheme, while the authentication between vehicles is guaranteed by employing ID-Based Online/Offline Signature (IBOOS) scheme. The registration of vehicles at Regional Trusted Authority (RTA) is an initial and important process which enables a vehicle to drive on a road. After that, RTA generates corresponding certified domain parameters in response to an authentication request, and publishes it. Then, this certification is hashed and stores its corresponding hash values in a database instead of its real ID. In addition, the vehicle privacy is ensured by using the pseudonyms, which are self-generated identifiers. A vehicle changing its pseudonym should unicast its new generated one to RSU. After that, RSU

verifies the received pseudonym by checking the signature and accepts if its authenticated. However, this scheme suffers from latency limitations and can be considered as unsuitable for safety critical applications, since safety application cannot support a delay of even milliseconds, especially when the pseudonym of a new vehicle is not known by the other vehicles.

5.3.2. Identity-Based Encryption Scheme

A secure identity based cryptography scheme is presented in [241] that generates the public key from a public unique identity of station. As a consequence, the overhead that is added when a certificate scheme (CRL) is used is reduced. The traceability and privacy are provided by using a pseudonym, which can be generated by RSU or the vehicles. The privacy preservation and non-frame ability against misbehaving nodes are achieved by using threshold signature and authentications. An important issue of this scheme is the revocation of a user's public key, since when a user's public key is revoked, that means that the corresponding identity is changed, which is inconvenient.

5.3.3. Pairing-Based Decentralized Revocation

A revocation protocol is proposed based on pairing Efficient Decentralized Revocation (EDR) [240]. This protocol is based on probabilistic random key distribution and its nature is decentralized and permits to build a group of legitimate neighboring vehicles, which can revoke a nearby malicious vehicle by applying a vote and the result will exceed the threshold.

5.4. Situation modelling-based security system architecture

According to [19], an architecture of flexible secret key management and trust information was presented and called SAT (situation-aware trust). According to specified situations, SAT is able to build up compatible trust mechanisms. SAT also discusses a rapid establishment of trust mechanism by means of popular social websites. In [159], the authors assume that the vehicles on the road of location act as intelligent agents, based on which trust models are built. Several reputation systems are presented such as Vehicle ad-hoc Reputation System (VARS) [211], Data-Centric Trust Based Security [236], Event-Based Reputation System [237], and Trust Management System - RaBTM [239]. Finally, the solutions for the security features are all presented in Table 16.

6. Limitations and Open Issues

Limitations:

After introducing all the aforementioned information, it is clear that we need to shed the light on some limitations that need to be addresses. For example, defeating attacks still need to be more studied and lots

of tests should be done. Below, we list some of the limitations in detecting/defeating some of the attacks previously mentioned.

Sybil attack: Various studies have been proposed in this work, however, there is still some enhancements that should be done. Almost all the proposed methods depends on nodes and very few that are dependent on RSUs.

DoS attack: One of the most dangerous attacks, still there are some proposed methods that rely on manual setting of parameters. This is not a feasible option and in some proposed solutions malicious nodes are not discovered if the network is flooded with valid signatures and bogus information. Therefore, despite these solutions, there is a scope for more improvements due to the mentioned flaws.

DDoS: Although there are several works addressing DDoS, no comparison is being made with different existing solutions and few of them are able to detect a single attacker. More work can be done to deal with DDoS more effectively.

Black-hole attack: In spite of numerous existing security solutions for blackhole attacks, some have major drawbacks. Some of the proposed solutions assume the presence of only single malicious node; which is not realistic. Also, some of them are computationally heavy and need a large memory requirements which is a limitation when dealing with IoV.

Grey-hole: The first drawback in the proposed solutions is that few proposed methods accept inputs as numerical values, few of them rely on conventional routing which results in decreasing the efficiency.

Wormhole attack: The proposed solutions have a high consumption of power due to number of nodes. In addition, the results of the proposed methods are not compared with other proposals.

Node impersonation attack: Proposed solutions are not that much efficient/famous in securing the network, besides, they have a high overhead and delay.

GPS spoofing: The amount of work done in this domain is really very low compared to other attacks. More work should be done and more proposals should be published.

Other attacks: Let us take for example, Bogus Information Attack, Replay Attack, Timing Attack, Spamming Attack, Illusion Attack, Social Attack, Message Tampering, Brute Force Attack, Repudiation Attack, and Key and/or Certificate Replication Attack. All of these attacks are not addressed separately in a real simulation to find a real security solution that can defeat them. The research community has to focus on providing more solutions for such attacks.

Open Issues:

Some of the open issues that are not addressed yet or are not well managed today are stated below.

Truly Connected Vehicle: This states that the vehicle is always connected to the network starting from the day it is manufactured. This will provide the manufacturers with better insight and know the performance of the vehicles with time as well as providing a platform to manage the vehicle. The online connectivity can run regular checks and record vehicle status, then it can be used to detect and troubleshoot issues remotely, keep a record of vehicle service and repairs, and also can help in reducing insurance costs for conscientious drivers.

Vehicular Payments: Another open issue is the trends of the integration of automatic payment methods into the ITS network. That is the user can avoid the unwanted stops to pay for gas, fuel, parking, or road tax. This is a challenge that needs a lot of studying.

Data Processing: As the ITs grows, it is of major importance to keep upgrading the resources in the network. Processing large amounts of data, or collecting them can be achieved by two methods: increase the processing power, and more efficient algorithms to process the data.

Network model and service model of human-vehicle: Efficient network model of human-vehicle in IoV is considered as an open issue and it needs to be addressed. However, we have to keep in mind the maximization of resource usage, stability, and robustness of the network. Building a cognitive learning model, studying the service characteristics during the process of coordination are fundamental issues. This would improve the ability to cope with complex space-time change of service requirements in the IoV but there is no research on this issue.

Localization Accuracy: Since in IoV we are using the GPS which have less accuracy, accurate localization of vehicles is an open issue and a challenge. For example, in crowded areas, or in some countries, GPS signals are often week, and the speed of the vehicle is not considered. The speed in IoV is an important parameter in IoV. No solution have been presented to solve this open issue until now.

Virtual vehicles with drivers: When going for IoV, a collaborative platform containing different in-car operating systems (like Carplay, QNX Car..) is formed. Therefore, a connection is initiated between the virtual vehicles and the connected drivers. Thus, sharing information by using cooperation technologies. This cooperation is made of two phases: (1) sensing and gathering crucial information and (2) the interaction and evaluation of virtual vehicles with drivers. More designs and suggestions should be carefully suggested since the cooperation between drivers and virtual vehicles is an important and challenging issue and can impact the entire network performance in IoV.

Lack of standards for robust V2V communication: To improve the user experiences and services in the IoV ecosystem, open standards are needed to accomplish an efficient communication and information dissemination. This should be transparent and seamlessly integrated with current closed standards, which is not the case until the date of writing this survey.

Security: The importance of using lightweight cryptography has been agreed on from all parties. When going for IoT, different requirements are needed. That is why NIST is now in its way to standardize a lightweight encryption standard for such systems. However, to this moment, IoV is not taken into consideration and almost, all cryptography solutions do not work efficiently in this platform. There must be a lightweight security solution that respects the large amount data, minimum delay, low memory/CPU requirements, mobility, loss of connection sometimes etc..

6.1. Suggestions & Recommendations

VANETs and IoV have revolutionized the transportation systems due to the advanced information and communication technology that will result in ITS. Both systems depend on real-time information, thus delay cannot be tolerated. Security is major requirement here because the vehicle itself can be controlled by hacker/attacker resulting in a full control of the vehicle in his hands which may lead to hazardous situations. In the following we propose some recommendations to enhance ITS security:

Define New Lightweight Host/Network IDS/IPS: An efficient IDS is required in such systems. In fact, using IDS have gained lots of interest in these days, after introducing the technologies that can aid in this kind of systems. ITS can be seriously impaired and cryptographic solutions alone are not efficient. Therefore, introducing a lightweight IDS that uses hybrid detection techniques (i.e. signature-based, specification-based and anomaly-based detection methods) is highly recommended to make the right decisions in an ITS real-time applications.

Lightweight Multi-factor Authentication Scheme: One cryptographic factor is not sufficient to reach the highest level of security. Any vulnerability in the identification/authentication schemes would threaten the vehicles and could then be used for malicious purposes. This would eventually lead to drastic outcomes. To solve such issues, a combination between lightweight cryptographic and non-cryptographic-based solutions should be used to avoid any potential illegal access into ITS [242, 243].

Lightweight Dynamic cryptographic Algorithms: Most of the recently proposed lightweight cryptographic schemes does not meet the requirements in ITS. Either they have high processing computation, high memory requirement, does not meet the NIST requirements or even are prone to different kinds of attacks. Designing a new lightweight cryptographic solution is a necessity in such systems. For example, authors in [244, 245, 246] use single round functions to reach the security level desired. More research work should focus on this requirement especially that we need a balance between performance, security and real implementations.

7. Conclusion

VANET/IoV which are considered as ITS are both interesting fields of modern emerging networks and their importance comes from their practical benefits related to the safety of human lives, especially for ITS applications such as road safety and traffic management. Therefore, securing ITS applications is a great challenge since these applications suffer from several limitations. In this survey, ITS applications, characteristics, recent standardization works, threats and their impact on the system were all discussed. Also, the evolution of VANET to IoV and their differences are stated. The main difference however is the heterogeneity introduced in IoV which adds more challenges for researchers. This survey identifies all existing security issues and challenges and then classifies them from a security viewpoint. The attacks were classified according to their impact they cause on the security service they target and also they are classified according to the network layer they affect. The solutions for every attack that were proposed in the research works are also stated. Then, we also list some of the existing security architectures that are used in Intelligent Transportation Systems. Finally, challenges and open issues in our point of view ware stated. To sum up, this survey will help researchers get a clear and a detailed look at every aspect of security issues in Intelligent Transportation Systems and will pave the way for them to innovate and find new practical solutions.

References

[1] T. Kosch, I. Kulp, M. Bechler, M. Strassberger, B. Weyl, R. Lasowski, Communication architecture for cooperative systems in europe, Communications Magazine, IEEE 47 (5) (2009) 116–125.

[2] M. Saini, A. Alelaiwi, A. E. Saddik, How close are we to realizing a pragmatic vanet solution? a meta-survey, ACM Computing Surveys (CSUR) 48 (2) (2015) 29.

[3] R. Millman, Connected cars report: 125 million vehicles by 2022, 5g coming, [Online; 2018] (2018).
URL https://internetofbusiness.com/worldwide-connected-car-market-to-top-125-million-by-2022/

[4] B. Aslam, P. Wang, C. C. Zou, Extension of internet access to vanet via satellite receive–only terminals, International Journal of Ad Hoc and Ubiquitous Computing 14 (3) (2013) 172–190.

[5] S. Bitam, A. Mellouk, S. Zeadally, Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks, IEEE Wireless Communications 22 (1) (2015) 96–102.

[6] J. Toutouh, E. Alba, Light commodity devices for building vehicular ad hoc networks: An experimental study, Ad Hoc Networks 37 (2016) 499–511.

[7] J. Contreras-Castillo, S. Zeadally, J. A. Guerrero-Ibañez, Internet of vehicles: Architecture, protocols, and security, IEEE internet of things Journal 5 (5) (2017) 3701–3709.

[8] J. A. Guerrero-Ibanez, S. Zeadally, J. Contreras-Castillo, Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies, IEEE Wireless Communications 22 (6) (2015) 122–128.

[9] R. D. Pietro, S. Guarino, N. Verde, J. Domingo-Ferrer, Security in wireless ad-hoc networks – a survey, Computer Communications 51 (0) (2014) 1 – 20.

[10] G. Yan, S. Olariu, M. C. Weigle, Providing fVANETg security through active position detection, Computer Communications 31 (12) (2008) 2883 – 2897, mobility Protocols for ITS/VANET.

[11] R. G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, fVANETg security surveys, Computer Communications 44 (0) (2014) 1 – 13.

[12] M. N. Mejri, J. Ben-Othman, M. Hamdi, Survey on fVANETg security challenges and possible cryptographic solutions, Vehicular Communications 1 (2) (2014) 53 – 66.

[13] N. Kumar, R. Iqbal, S. Misra, J. J. Rodrigues, An intelligent approach for building a secure decentralized public key infrastructure in fVANETg, Journal of Computer and System Sciences (0) (2014) –.

[14] A. Daeinabi, A. G. Rahbar, An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks, Computers & Electrical Engineering 40 (2) (2014) 517 – 529.

[15] B. Mishra, P. Nayak, S. Behera, D. Jena, Security in vehicular adhoc networks: A survey, in: Proceedings of the 2011 International Conference on Communication, Computing & Security, ICCCS '11, ACM, New York, NY, USA, 2011, pp. 590–595.

[16] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (vanets): status, results, and challenges, Telecommunication Systems 50 (4) (2012) 217–241.

[17] A. Dhamgaye, N. Chavhan, Survey on security challenges in vanet.

[18] S. Gillani, F. Shahzad, A. Qayyum, R. Mehmood, A survey on security in vehicular ad hoc networks, in: M. Berbineau, M. Jonsson, J.-M. Bonnin, S. Cherkaoui, M. Aguado, C. Rico-Garcia, H. Ghannoum, R. Mehmood, A. Vinel (Eds.), Communication Technologies for Vehicles, Vol. 7865 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2013, pp. 59–74.

[19] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, Journal of Computer Security 15 (1) (2007) 39–68.

[20] Y. Wang, F. Li, Vehicular ad hoc networks, in: Guide to wireless ad hoc networks, Springer, 2009, pp. 503–525.

[21] D. Jiang, L. Delgrossi, Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments, in: Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, IEEE, 2008, pp. 2036–2040.

[22] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, P. Mudalige, Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 ghz dedicated short range communication (dsrc) frequency band, Selected Areas in Communications, IEEE Journal on 25 (8) (2007) 1501–1516.

[23] A. N. Hassan, O. Kaiwartya, A. H. Abdullah, D. K. Sheet, R. S. Raw, Inter vehicle distance based connectivity aware routing in vehicular adhoc networks, Wireless Personal Communications 98 (1) (2018) 33–54.

[24] H. El-Sayed, S. Sankar, M. Prasad, D. Puthal, A. Gupta, M. Mohanty, C.-T. Lin, Edge of things: The big picture on the integration of edge, iot and the cloud in a distributed computing environment, IEEE Access 6 (2017) 1706–1717.

[25] W. H. Organization, Global status report on road safety 2018, [Online; 2018] (2018).
URL https://www.who.int/violence_injury_prevention/road_safety_status/2018/en/

[26] K. Abhimanyu, How connected cars are turning into revenue-generating machines, [Online; 2016] (2016).
URL https://techcrunch.com/2016/08/28/how-connected-cars-are-turning-into-revenue-generating-mach
?

[27] B. O'Brien, https://www.ariasystems.com/blog/will-profit-connected-cars/, [Online; 2018] (2018).
URL https://www.ariasystems.com/blog/will-profit-connected-cars/

[28] M. Zhang, C. Chen, T. Wo, T. Xie, M. Z. A. Bhuiyan, X. Lin, Safedrive: online driving anomaly detection from large-scale vehicle data, IEEE Transactions on Industrial Informatics 13 (4) (2017) 2087–2096.

[29] J. Dai, J. Teng, X. Bai, Z. Shen, D. Xuan, Mobile phone based drunk driving detection, in: 2010 4th International Conference on Pervasive Computing Technologies for Healthcare, IEEE, 2010, pp. 1–8.

[30] G. Tripathi, M. A. Ahad, M. Sathiyanarayanan, The role of blockchain in internet of vehicles (iov): Issues, challenges and opportunities, in: 2019 International Conference on contemporary Computing and Informatics (IC3I), IEEE, 2019, pp. 26–31.

[31] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, J. Zhao, Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory, IEEE Transactions on Vehicular Technology 68 (3) (2019) 2906–2920.

[32] V. Puri, R. Kumar, C. Van Le, R. Sharma, I. Priyadarshini, A vital role of blockchain technology toward internet of vehicles, in: Handbook of Research on Blockchain Technology, Elsevier, 2020, pp. 407–416.

[33] L. Mendiboure, M. A. Chalouf, F. Krief, Survey on blockchain-based applications in internet of vehicles, Computers & Electrical Engineering 84 (2020) 106646.

[34] Z. Ning, J. Huang, X. Wang, J. J. Rodrigues, L. Guo, Mobile edge computing-enabled internet of vehicles: Toward energy-efficient scheduling, IEEE Network 33 (5) (2019) 198–205.

[35] G. Wang, F. Xu, Regional intelligent resource allocation in mobile edge computing based vehicular network, IEEE Access 8 (2020) 7173–7182.

[36] F. Liang, W. Yu, X. Liu, D. Griffith, N. Golmie, Towards edge-based deep learning in industrial internet of things, IEEE Internet of Things Journal.

[37] H. Ji, O. Alfarraj, A. Tolba, Artificial intelligence-empowered edge of vehicles: Architecture, enabling technologies, and applications, IEEE Access 8 (2020) 61020–61034.

[38] A. Hammoud, H. Sami, A. Mourad, H. Otrok, R. Mizouni, J. Bentahar, Ai, blockchain and vehicular edge computing for smart and secure iov: Challenges and directions.

[39] Z. Mahmood, Connected Vehicles in the IoV: Concepts, Technologies and Architectures, Springer International Publishing, Cham, 2020, pp. 3–18. doi:10.1007/978-3-030-36167-9_1.
URL https://doi.org/10.1007/978-3-030-36167-9_1

[40] H. Fouchal, E. Bourdy, G. Wilhelm, M. Ayaida, Secured communications on vehicular networks over cellular networks, in: International Conference on Distributed Computing and Internet Technology, Springer, 2019, pp. 31–41.

[41] C. R. Storck, F. Duarte-Figueiredo, A 5g v2x ecosystem providing internet of vehicles, Sensors 19 (3) (2019) 550.

[42] G. Leen, D. Heffernan, Expanding automotive electronic systems, Computer 35 (1) (2002) 88–93.

[43] Z. Chang, Z. Zhou, S. Zhou, T. Chen, T. Ristaniemi, Towards service-oriented 5g: Virtualizing the networks for everything-as-a-service, IEEE Access 6 (2017) 1480–1489.

[44] H. Moustafa, Y. Zhang, Vehicular networks: techniques, standards, and applications, Auerbach publications, 2009.

[45] R. S. Raw, M. Kumar, N. Singh, Security challenges, issues and their solutions for vanet.

[46] R. Meulen, Gartner says by 2020, a quarter billion connected vehicles will enable new in-vehicle services and automated driving capabilities, Gartner, STAMFORD, Conn.

[47] E. Schoch, F. Kargl, M. Weber, T. Leinmuller, Communication patterns in vanets, Communications Magazine, IEEE 46 (11) (2008) 119–125.

[48] X. Li, M. Li, W. Shu, M. Wu, A practical map-matching algorithm for gps-based vehicular networks in shanghai urban area, in: Wireless, Mobile and Sensor Networks, 2007.(CCWMSN07). IET Conference on, IET, 2007, pp. 454–457.

[49] R. Panayappan, J. M. Trivedi, A. Studer, A. Perrig, Vanet-based approach for parking space availability, in: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, ACM, 2007, pp. 75–76.

[50] A. Boukerche, H. A. Oliveira, E. F. Nakamura, A. A. Loureiro, Vehicular ad hoc networks: A new challenge for localization-based systems, Computer communications 31 (12) (2008) 2838–2849.

[51] Intelligent transport systems (ITS); v2v application; part 1: Cooperative awareness application (caa) specification. (2011).

[52] ETSI TS 101 539-3, Intelligent transport system (its); v2v application; part 3: Longitudinal collision risk warning (lcrw) application specification.

[53] ETSI TS 101 539-2, Intelligent transport system (its); v2v application; part 2: Intersection collision risk warning (icrw) application specification.

[54] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions, Communications Surveys & Tutorials, IEEE 13 (4) 584–616.

[55] A. E. Sallab, M. Abdou, E. Perot, S. Yogamani, Deep reinforcement learning framework for autonomous driving, Electronic Imaging 2017 (19) (2017) 70–76.

[56] L. Abdi, A. Meddeb, In-vehicle augmented reality tsr to improve driving safety and enhance the driver's experience, Signal, Image and Video Processing 12 (1) (2018) 75–82.

[57] X. Gao, B. Firner, S. Sugrim, V. Kaiser-Pendergrast, Y. Yang, J. Lindqvist, Elastic pathing: Your speed is enough to track you, in: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2014, pp. 975–986.

[58] R. Wang, F. Xie, B. Zhang, W. Liu, W. Qian, W. Xian, Detecting abnormal driving behaviors by smartphone sensors based on multi-feature convolutional neural network, in: 2019 Chinese Control Conference (CCC), IEEE, 2019, pp. 6639–6644.

[59] G. Castignani, T. Derrmann, R. Frank, T. Engel, Smartphone-based adaptive driving maneuver detection: A large-scale evaluation study, IEEE Transactions on Intelligent Transportation Systems 18 (9) (2017) 2330–2339.

[60] C. Chen, D. Zhang, P. S. Castro, N. Li, L. Sun, S. Li, Z. Wang, iboat: Isolation-based online anomalous trajectory detection, IEEE Transactions on Intelligent Transportation Systems 14 (2) (2013) 806–818.

[61] C. Chen, Y. Ding, X. Xie, S. Zhang, Z. Wang, L. Feng, Trajcompressor: an online map-matching-based trajectory compression framework leveraging vehicle heading direction and change, IEEE Transactions on Intelligent Transportation Systems.

[62] E. M. Carboni, V. Bogorny, Inferring drivers behavior through trajectory analysis, in: Intelligent Systems' 2014, Springer, 2015, pp. 837–848.

[63] S. Liu, L. M. Ni, R. Krishnan, Fraud detection from taxis' driving behaviors, IEEE Transactions on Vehicular Technology 63 (1) (2013) 464–472.

[64] X. Kong, X. Song, F. Xia, H. Guo, J. Wang, A. Tolba, Lotad: Long-term traffic anomaly detection based on crowdsourced bus trajectory data, World Wide Web 21 (3) (2018) 825–847.

[65] Z. Li, X. Jin, X. Zhao, Drunk driving detection based on classification of multivariate time series, Journal of safety research 54 (2015) 61–e29.

[66] Committee SCC32, IEEE P1609.4 standard for wireless access in vehicular environments (WAVE) - multi-channel operation.

[67] ETSI TS 102 636-5-1, Intelligent transport systems (ITS); vehicular communications; geonetworking; part 5: Transport protocols; sub-part 1: Basic transport protocol, Version 1.1.1 (Feb. 2011).

[68] S. Grafling, P. Mahonen, J. Riihijarvi, Performance evaluation of ieee 1609 wave and ieee 802.11 p for vehicular communications, in: Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on, IEEE, 2010, pp. 344–348.

[69] J. B. Kenney, Dedicated short-range communications (dsrc) standards in the united states, Proceedings of the IEEE 99 (7) (2011) 1162–1182.

[70] M. Lusheng, D. Karim, J. v. W. Barend, H. Yskandar, Evaluation and enhancement of ieee 802.11p standard: A survey, Vol. 1, 2012.

[71] Intelligent transport systems — communications access for land mobiles (CALM) — architecture, ISO 21217:2010, ISO TC204, Geneva, Switzerland (Apr. 2010).

[72] S. Zeadally, M. A. Javed, E. B. Hamida, Vehicular communications for its: Standardization and challenges, IEEE Communications Standards Magazine 4 (1) (2020) 11–17.

[73] European Telecommunications Standards Institute, Intelligent Transport Systems (ITS); Communications Architecture, EN 302 665 V1.1.1, ETSI (September 2010).

[74] I. T. U. (ITU), International Telecommunication Union (ITU), [Online; 2019] (2019).
URL https://www.itu.int

[75] T. M. B. Standard, The mobile broadband standard, [Online; 2018] (2018).
URL http://www.3gpp.org

[76] ETSI–5G, The mobile broadband standard, [Online; 2019] (2019).
URL http://www.etsi.org/technologies-clusters/technologies/5g

[77] N. G. W. Paper, Ngmn 5g white paper, [Online; 2019] (2019).
URL https://www.ngmn.org

[78] T. A. for Telecommunications Industry Solutions, The alliance for telecommunications industry solutions, [Online; 2019] (2019).
URL https://www.atis.org

[79] T. G. I. P. P. Partnership, The 5g infrastructure public private partnership, [Online; 2019] (2019).
URL https://5g-ppp.eu

[80] I. F. N. E. 5G, Beyond, Ieee future networks enabling 5g and beyond, [Online; 2019] (2019).
URL futurenetworks.ieee.org

[81] 5G-Americas, 5g americas white papers, [Online; 2019] (2019).
URL http://www.5gamericas.org

[82] F. G. M. C. P. Forum, Fifth generation mobile communication promotion forum, [Online; 2019] (2019).
URL http://5gmf.jp

[83] V. G. T. Forum, Verizon 5g technical forum, [Online; 2019] (2019).
URL http://www.5gtf.net

[84] 5TONIC, 5tonic, [Online; 2019] (2019).
URL https://www.5tonic.org

[85] G. A. Association, 5g automotive association, [Online; 2019] (2019).
URL http://5gaa.org

[86] H. Hasbullah, I. A. Soomro, J.-l. Ab Manan, Denial of Service (DOS) Attack and Its Possible Solutions in VANET 41.

[87] K. Plößl, H. Federrath, A privacy aware and efficient security infrastructure for vehicular ad hoc networks, Computer Standards & Interfaces 30 (6) (2008) 390–397.

[88] H. N. Noura, O. Salman, A. Chehab, R. Couturier, Distlog: A distributed logging scheme for iot forensics, Ad Hoc Networks 98 (2020) 102061.

[89] H. Noura, O. Salman, A. Chehab, R. Couturier, Preserving data security in distributed fog computing, Ad Hoc Networks 94 (2019) 101937.

[90] H. Qiu, H. Noura, M. Qiu, Z. Ming, G. Memmi, A user-centric data protection method for cloud storage based on invertible dwt, IEEE Transactions on Cloud Computing.

[91] A. Nanda, D. Puthal, J. J. Rodrigues, S. A. Kozlov, Internet of autonomous vehicles communications security: overview, issues, and directions, IEEE Wireless Communications 26 (4) (2019) 60–65.

[92] K. Papapanagiotou, G. F. Marias, P. Georgiadis, A certificate validation protocol for vanets, in: Globecom Workshops, 2007 IEEE, IEEE, 2007, pp. 1–9.

[93] N. Vighnesh, N. Kavita, S. R. Urs, S. Sampalli, A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks, in: Wireless Technology and Applications (ISWTA), 2011 IEEE Symposium on, IEEE, 2011, pp. 96–101.

[94] F. Sabahi, The security of vehicular adhoc networks, in: Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on, IEEE, 2011, pp. 338–342.

[95] Intelligent transport systems (its), security, threat, vulnerability and risk analysis (tvra), Tech. Rep. ETSI TR 102 893 V1.1.1 (03 2010).

[96] H. Hasbullah, I. Ahmed Soomro, J.-l. Ab Manan, Denial of service (dos) attack and its possible solutions in vanet, World Academy of Science, Engineering and Technology (WASET) 65 (2010) 411–415.

[97] K. Verma, H. Hasbullah, A. Kumar, Prevention of dos attacks in vanet, Wireless personal communications 73 (1) (2013) 95–126.

[98] L. He, W. T. Zhu, Mitigating dos attacks against signature-based authentication in vanets, in: Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on, Vol. 3, IEEE, 2012, pp. 261–265.

[99] S. Sharma, A. Kaul, Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized ids for vanet, Vehicular Communications 12 (2018) 23–38.

[100] H. H. R. Sherazi, R. Iqbal, F. Ahmad, Z. A. Khan, M. H. Chaudary, Ddos attack detection: A key enabler for sustainable communication in internet of vehicles, Sustainable Computing: Informatics and Systems 23 (2019) 13–20.

[101] U. D. Gandhi, R. Keerthana, Request response detection algorithm for detecting dos attack in vanet, in: 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), IEEE, 2014, pp. 192–194.

[102] R. Minhas, M. Tilal, Effects of jamming on ieee 802.11 p systems.

[103] A. Hamieh, J. Ben-Othman, L. Mokdad, Detection of radio interference attacks in vanet, in: Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, IEEE, 2009, pp. 1–5.

[104] A. M. Malla, R. K. Sahu, Security attacks with an effective solution for dos attacks in vanet, International Journal of Computer Applications 66 (22) (2013) 45–49.

[105] K. Rabieh, M. M. Mahmoud, T. N. Guo, M. Younis, Cross-layer scheme for detecting large-scale colluding sybil attack in vanets, in: 2015 IEEE International Conference on Communications (ICC), IEEE, 2015, pp. 7298–7303.

[106] M. Kaur, M. Mahajan, Movement abnormality evaluation model in the partially centralized vanets for prevention against sybil attack, International Journal of Modern Education and Computer Science 7 (11) (2015) 20.

[107] J. Grover, M. S. Gaur, V. Laxmi, Multivariate verification for sybil attack detection in vanet, Open Computer Science 1 (open-issue).

[108] A. K. Sharma, S. K. Saroj, S. K. Chauhan, S. K. Saini, Sybil attack prevention and detection in vehicular ad hoc network, in: 2016 International Conference on Computing, Communication and Automation (ICCCA), IEEE, 2016, pp. 594–599.

[109] S. Han, D. Ban, W. Park, M. Gerla, Localization of sybil nodes with electro-acoustic positioning in vanets, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–6.

[110] C. Sowattana, W. Viriyasitavat, A. Khurat, Distributed consensus-based sybil nodes detection in vanets, in: 2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE), IEEE, 2017, pp. 1–6.

[111] M. Khalil, M. A. Azer, Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks, in: 2018 Wireless Days (WD), IEEE, 2018, pp. 184–186.

[112] Y. Yao, B. Xiao, G. Yang, Y. Hu, L. Wang, X. Zhou, Power control identification: A novel sybil attack detection scheme in vanets using rssi, IEEE Journal on Selected Areas in Communications 37 (11) (2019) 2588–2602.

[113] K. Lim, T. Islam, H. Kim, J. Joung, A sybil attack detection scheme based on adas sensors for vehicular networks, in: 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2020, pp. 1–5.

[114] I. A. Saeed, A. Selamat, A. M. Abuagoub, A survey on malware and malware detection systems, International Journal of Computer Applications 67 (16).

[115] M. Wazid, A. K. Das, J. J. Rodrigues, S. Shetty, Y. Park, Iomt malware detection approaches: Analysis and research challenges, IEEE Access.

[116] D. Singelee, B. Preneel, Location verification using secure distance bounding protocols, in: Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on, IEEE, 2005, pp. 7–pp.

[117] A. Gupta, R. Kaushal, Improving spam detection in online social networks, in: 2015 International conference on cognitive computing and information processing (CCIP), IEEE, 2015, pp. 1–6.

[118] K. M. A. Alheeti, A. Gruebler, K. D. McDonald-Maier, An intrusion detection system against black hole attacks on the communication network of self-driving cars, in: 2015 sixth international conference on emerging security technologies (EST), IEEE, 2015, pp. 86–91.

[119] R. Baiad, O. Alhussein, H. Otrok, S. Muhaidat, Novel cross layer detection schemes to detect blackhole attack against qos-olsr protocol in vanet, Vehicular Communications 5 (2016) 9–17.

[120] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, Z. A. Zukarnain, Li-aodv: lifetime improving aodv routing for detecting and removing black-hole attack from vanet, Journal of Theoretical and Applied Information Technology 95 (1) (2017) 196.

[121] K. Kumar, P. Yadav, S. Sharma, Robust analysis for aodv protocol in vehicular adhoc network under black hole attack in ns 2, International Journal on Recent and Innovation Trends in Computing and Communication.(Jun. 2018).

[122] B. Cherkaoui, A. Beni-hssane, M. Erritali, Variable control chart for detecting black hole attack in vehicular ad-hoc networks, Journal of Ambient Intelligence and Humanized Computing (2020) 1–10.

[123] S. Marti, T. J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the 6th annual international conference on Mobile computing and networking, ACM, 2000, pp. 255–265.

[124] N. Schweitzer, A. Stulman, R. D. Margalit, A. Shabtai, Contradiction based gray-hole attack minimization for ad-hoc networks, IEEE Transactions on Mobile Computing 16 (8) (2016) 2174–2183.

[125] M. Bendjima, M. Feham, Wormhole attack detection in wireless sensor networks, in: 2016 SAI Computing Conference (SAI), IEEE, 2016, pp. 1319–1326.

[126] R. Abdulhammed, M. Faezipour, K. Elleithy, Intrusion detection system in self-organizing networks: A survey.

[127] A. S. Nikam, A. Sarawagi, Security over wormhole attack in vanet network system, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 7 (8).

[128] E. C. Ngai, J. Liu, M. R. Lyu, On the intruder detection for sinkhole attack in wireless sensor networks, in: 2006 IEEE International Conference on Communications, Vol. 8, IEEE, 2006, pp. 3383–3389.

[129] Z. Zhang, S. Liu, Y. Bai, Y. Zheng, M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks, Cluster Computing 22 (3) (2019) 7677–7685.

[130] S. Vidhya, T. Sasilatha, Sinkhole attack detection in wsn using pure md5 algorithm, Indian Journal of Science and Technology 10 (2017) 24.

[131] K. Devibala, S. BalaMurali, S. Venkateselu, Decentralized detection and mitigation of sinkhole attacks in wireless sensor networks based on network density estimation technique, Journal of Control Theory and Applications 9 (1).

[132] G. Jahandoust, F. Ghassemi, An adaptive sinkhole aware algorithm in wireless sensor networks, Ad Hoc Networks 59 (2017) 24–34.

[133] M. N. Mejri, J. Ben-Othman, Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks, in: 2014 IEEE Global Communications Conference, IEEE, 2014, pp. 5032–5037.

[134] M. N. Mejri, J. Ben-Othman, Gdvan: a new greedy behavior attack detection algorithm for vanets, IEEE Transactions on Mobile Computing 16 (3) (2016) 759–771.

[135] J. A. Onieva, D. Sauveron, S. Chaumette, D. Gollmann, K. Markantonakis, Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks: Second IFIP WG 11.2 International Workshop, WISTP 2008, Seville, Spain, May 13-16, 2008, Vol. 5019, Springer, 2008.

[136] M. S. Al-Kahtani, Survey on security attacks in vehicular ad hoc networks (vanets), in: 2012 6th International Conference on Signal Processing and Communication Systems, IEEE, 2012, pp. 1–9.

[137] I. A. Sumra, I. Ahmad, H. Hasbullah, J.-L. bin Ab Manan, Classes of attacks in vanet, in: Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, IEEE, 2011, pp. 1–5.

[138] I. A. Sumra, H. Hasbullah, I. Ahmad, et al., New card based scheme to ensure security and trust in vehicular communications, in: 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC), IEEE, 2011, pp. 1–6.

[139] J. R. Douceur, The sybil attack, in: Peer-to-peer Systems, Springer, 2002, pp. 251–260.

[140] M. Al-kahtani, Survey on security attacks in vehicular ad hoc networks (vanets), in: Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on, 2012, pp. 1–9.

[141] I. A. Sumra, H. Hasbullah, I. Ahmad, J.-L. bin Ab Manan, Forming vehicular web of trust in vanet, in: Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, IEEE, 2011, pp. 1–6.

[142] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, Z. A. Zukarnain, Vehicular ad hoc networks and security issues: survey, Modern Applied Science 11 (5) (2017) 30.

[143] B. Cherkaoui, A. Beni-Hssane, M. Erritali, Quality control chart for detecting the black hole attack in vehicular ad-hoc networks, Procedia computer science 113 (2017) 170–177.

[144] H. Hasrouny, A. E. Samhat, C. Bassil, A. Laouiti, Vanet security challenges and solutions: A survey, Vehicular Communications 7 (2017) 7–20.

[145] W. R. Pires Jr, T. H. de Paula Figueiredo, H. C. Wong, A. A. F. Loureiro, Malicious node detection in wireless sensor networks, in: Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International, IEEE, 2004, p. 24.

[146] S. M. Safi, A. Movaghar, M. Mohammadizadeh, A novel approach for avoiding wormhole attacks in vanet, in: Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on, IEEE, 2009, pp. 1–6.

[147] F. Nait-Abdesselam, B. Bensaou, T. Taleb, Detecting and avoiding wormhole attacks in wireless ad hoc networks, IEEE Communications Magazine 46 (4) (2008) 127–133.

[148] A. Burg, Ad hoc network specific attacks, in: Seminar Ad hoc networking: Concepts, Applications, and Security. Technische Universitat Munchen,‘03, 2003.

[149] L. Chen, K. A. Almoubayed, J. Leneutre, Detection and prevention of greedy behavior in ad hoc networks, in: International Conference on Risks and Security of Internet and Systems (CRISIS 2007), 2007.

[150] Y. Boufenneche, N. Gharbi, R. Zitouni, L. George, Formal modeling of greedy behavior in secure internet of things networks, in: 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, 2019, pp. 188–193.

[151] M. Raya, P. Papadimitratos, J.-P. Hubaux, Securing vehicular communications, IEEE wireless communications 13 (5) (2006) 8–15.

[152] I. A. Sumra, H. Hasbullah, Trust and trusted computing in vanet.

[153] M. G. Zapata, Secure ad hoc on-demand distance vector routing, ACM SIGMOBILE Mobile Computing and Communications Review 6 (3) (2002) 106–107.

[154] L. Tamilselvan, D. V. Sankaranarayanan, Prevention of impersonation attack in wireless mobile ad hoc networks, International Journal of Computer Science and Network Security (IJCSNS) 7 (3) (2007) 118–123.

[155] D. Huang, A. Sinha, D. Medhi, A double authentication scheme to detect impersonation attack in link state routing protocols, in: IEEE International Conference on Communications, 2003. ICC'03., Vol. 3, IEEE, 2003, pp. 1723–1727.

[156] T. W. Chim, S.-M. Yiu, L. C. Hui, V. O. Li, Specs: Secure and privacy enhancing communications schemes for vanets, Ad Hoc Networks 9 (2) (2011) 189–203.

[157] N. Gour, A. Kumar, Efficient detection and prevention of impersonation attack in manet.

[158] B. Lakshmi, B. S. Lakshmi, R. Karthikeyan, Detection and prevention of impersonation attack in wireless networks, Int. J. Adv. Res. Comput. Sci. Technol 2 (1) (2014) 267–270.

[159] M. Raya, P. Papadimitratos, J.-P. Hubaux, Securing vehicular communications, Wireless Communications, IEEE 13 (5) (2006) 8–15. doi:10.1109/WC-M.2006.250352.

[160] M. Elsa Mathew, A. R. Kumar, Threat analysis and defence mechanisms in vanet, International Journal of Advanced Research in Computer Science and Software Engineering 3 (1) (2013) 47–53.

[161] N.-W. Lo, H.-C. Tsai, Illusion attack on vanet applications-a message plausibility problem, in: 2007 IEEE Globecom Workshops, IEEE, 2007, pp. 1–8.

[162] R. Engoulou, Sécurisation des vanets par la méthode de réputation des noeuds, Ph.D. thesis, École Polytechnique de Montréal (2013).

[163] J. S. Warner, R. G. Johnston, Gps spoofing countermeasures, Homeland Security Journal.

[164] J.-P. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles, IEEE Security & Privacy Magazine 2 (LCA-ARTICLE-2004-007) (2004) 49–55.

[165] M. Wolf, Vehicular security mechanisms, in: Security Engineering for Vehicular IT Systems, Springer, 2009, pp. 121–165.

[166] S. Tayeb, M. Pirouz, G. Esguerra, K. Ghobadi, J. Huang, R. Hill, D. Lawson, S. Li, T. Zhan, J. Zhan, et al., Securing the positioning signals of autonomous vehicles, in: 2017 IEEE International Conference on Big Data (Big Data), IEEE, 2017, pp. 4522–4528.

[167] M. N. Mejri, J. Ben-Othman, M. Hamdi, Survey on vanet security challenges and possible cryptographic solutions, Vehicular Communications 1 (2) (2014) 53–66.

[168] I. A. Sumra, J.-L. Ab Manan, H. Hasbullah, Timing attack in vehicular network, in: Proceedings of the 15th WSEAS International Conference on Computers, World Scientific and Engineering Academy and Society (WSEAS), 2011, pp. 151–155.

[169] S. Sharma, A. Kaul, A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud, Vehicular Communications 12 (2018) 138–164.

[170] M.-C. Chuang, J.-F. Lee, Team: Trust-extended authentication mechanism for vehicular ad hoc networks, IEEE systems journal 8 (3) (2013) 749–758.

[171] J. M. d. Fuentes, A. I. González-Tablas, A. Ribagorda, Overview of security issues in vehicular ad-hoc networks.

[172] B. Sridevi, M. Gopika, Masquerade attack detection and prevention using enhanced key management techniques.

[173] S. Abbas, M. Faisal, H. U. Rahman, M. Z. Khan, M. Merabti, et al., Masquerading attacks detection in mobile ad hoc networks, IEEE Access 6 (2018) 55013–55025.

[174] A. K. Malhi, S. Batra, Genetic-based framework for prevention of masquerade and ddos attacks in vehicular ad-hocnetworks, Security and Communication Networks 9 (15) (2016) 2612–2626.

[175] S. S. Kaushik, Review of different approaches for privacy scheme in vanets, Int. J 5 (2) (2012) 2231–1963.

[176] J. Blum, A. Eskandarian, The threat of intelligent collisions, IT Professional 6 (1) (2004) 24–29.

[177] J. Domingo-Ferrer, Q. Wu, Safety and privacy in vehicular communications, in: Privacy in Location-Based Applications, Springer, 2009, pp. 173–189.

[178] S. Rafaeli, D. Hutchison, A survey of key management for secure group communication, ACM Computing Surveys (CSUR) 35 (3) (2003) 309–329.

[179] V. H. La, A. R. Cavalli, Security attacks and solutions in vehicular ad hoc networks: a survey.

[180] P. Patil, N. Marathe, V. Jethani, Improved alert protocol in manet with strategies to prevent dos & mitm attacks, in: 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), IEEE, 2016, pp. 372–377.

[181] L. Bariah, D. Shehada, E. Salahat, C. Y. Yeun, Recent advances in vanet security: a survey, in: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), IEEE, 2015, pp. 1–7.

[182] B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Workshop on hot topics in networks (HotNets-IV), 2005, pp. 1–6.

[183] A. Rawat, S. Sharma, R. Sushil, Vanet: security attacks and its possible solutions, Journal of Information and Operations Management 3 (1) (2012) 301–304.

[184] A. Kumar, M. Sinha, Overview on vehicular ad hoc network and its security issues, in: 2014 International conference on computing for sustainable global development (INDIACom), IEEE, 2014, pp. 792–797.

[185] A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET, CRC press, 2010.

[186] M. Naor, M. Yung, Public-key cryptosystems provably secure against chosen ciphertext attacks, in: Proceedings of the twenty-second annual ACM symposium on Theory of computing, Citeseer, 1990, pp. 427–437.

[187] J. T. Isaac, S. Zeadally, J. S. Camara, Security attacks and solutions for vehicular ad hoc networks, IET communications 4 (7) (2010) 894–903.

[188] C. Langley, R. Lucas, H. Fu, Key management in vehicular ad-hoc networks, in: 2008 IEEE International Conference on Electro/Information Technology, IEEE, 2008, pp. 223–226.

[189] F. K. Karnadi, Z. H. Mo, K.-c. Lan, Rapid generation of realistic mobility models for vanet, in: Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE, IEEE, 2007, pp. 2506–2511.

[190] G. Samara, W. A. Al-Salihy, R. Sures, Security analysis of vehicular ad hoc nerworks (vanet), in: Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on, IEEE, 2010, pp. 55–60.

[191] R. Lu, X. Lin, T. H. Luan, X. Liang, X. Shen, Pseudonym changing at social spots: An effective strategy for location privacy in vanets, IEEE transactions on vehicular technology 61 (1) (2011) 86–96.

[192] G. Guette, C. Bryce, Using tpms to secure vehicular ad-hoc networks (vanets), in: Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks, Springer, 2008, pp. 106–116.

[193] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, M. Raya, Architecture for secure and private vehicular communications, in: Telecommunications, 2007. ITST'07. 7th International Conference on ITS, IEEE, 2007, pp. 1–6.

[194] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, J.-P. Hubaux, Mix-zones for location privacy in vehicular networks, in: ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), no. CONF, 2007.

[195] J. Guo, J. P. Baugh, S. Wang, A group signature based secure and privacy-preserving vehicular communication framework, Mobile Networking for Vehicular Environments 2007 (2007) 103–108.

[196] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications, in: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, IEEE, 2008.

[197] L. Zhang, Q. Wu, A. Solanas, J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications, vehicular Technology, IEEE Transactions on 59 (4) (2010) 1606–1617.

[198] L.-Y. Yeh, Y.-C. Chen, J.-L. Huang, Paacp: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks, Computer Communications 34 (3) (2011) 447–456.

[199] K. Sampigethaya, M. Li, L. Huang, R. Poovendran, Amoeba: Robust location privacy scheme for vanet, IEEE Journal on Selected Areas in communications 25 (8) (2007) 1569–1589.

[200] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, Appa: aggregate privacy-preserving authentication in vehicular ad hoc networks, in: Information Security, Springer, 2011, pp. 293–308.

[201] K. Rabieh, M. M. Mahmoud, M. Azer, M. Allam, A secure and privacy-preserving event reporting scheme for vehicular ad hoc networks, Security and Communication Networks 8 (17) (2015) 3271–3281.

[202] Z. Li, C. Chigan, On joint privacy and reputation assurance for vehicular ad hoc networks, Mobile Computing, IEEE Transactions on 13 (10) (2014) 2334–2344.

[203] P. Kamat, A. Baliga, W. Trappe, An identity-based security framework for vanets, in: Proceedings of the 3rd international workshop on Vehicular ad hoc networks, ACM, 2006, pp. 94–95.

[204] C.-T. Li, M.-S. Hwang, Y.-P. Chu, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, Computer Communications 31 (12) (2008) 2803–2814.

[205] Q. Liu, Q. Wu, L. Yong, A hierarchical security architecture of vanet.

[206] J. Sun, C. Zhang, Y. Fang, An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks, in: MILCOM 2007-IEEE Military Communications Conference, IEEE, 2007, pp. 1–7.

[207] R. Anderson, Security engineering, John Wiley & Sons, 2008.

[208] R. Moalla, H. Labiod, B. Lonc, N. Simoni, Risk analysis study of its communication architecture, in: Network of the Future (NOF), 2012 Third International Conference on the, 2012, pp. 1–5. doi:10.1109/NOF.2012.6463997.

[209] X. Li, H. Kang, P. Harrington, J. Thomas, Autonomic and trusted computing paradigms, in: Autonomic and Trusted Computing, Springer, 2006, pp. 143–152.

[210] A. Studer, F. Bai, B. Bellur, A. Perrig, Flexible, extensible, and efficient vanet authentication, Communications and Networks, Journal of 11 (6) (2009) 574–588.

[211] F. Dotzer, L. Fischer, P. Magiera, Vars: A vehicle ad-hoc network reputation system, in: World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a, IEEE, 2005, pp. 454–456.

[212] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, A. Tyagi, Securing vehicular networks: a reputation and plausibility checks-based approach, in: GLOBECOM Workshops (GC Wkshps), 2010 IEEE, IEEE, 2010, pp. 1550–1554.

[213] EU-US ITS Task Force 1-1, Standards harmonization working group harmonization task group 1 , "current status of security standards".

[214] Status of its security standards, Tech. Rep. Document HTG1-1, EU-US ITS Task Force Standards Harmonization Working Group Harmonization Task Group 1 (Novembre 2012).

[215] Y. Kortesniemi, M. Särelä, Survey of certificate usage in distributed access control, Computers & Security 44 (2014) 16–32.

[216] A. Wagan, B. Mughal, H. Hasbullah, Vanet security framework for trusted grouping using tpm hardware, in: Communication Software and Networks, 2010. ICCSN '10. Second International Conference on, 2010, pp. 309–312.

[217] A. A. Wagan, B. M. Mughal, H. Hasbullah, Vanet security framework for trusted grouping using tpm hardware: Group formation and message dissemination, in: Information Technology (ITSim), 2010 International Symposium in, Vol. 2, IEEE, 2010, pp. 607–611.

[218] M. Simić, M. Vučetić, T. Unkašević, Z. Banjac, M. Stanković, Entity identification and security solutions in iot based on pki and blockchain technology, in: 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH), IEEE, 2020, pp. 1–6.

[219] N.-W. Wang, Y.-M. Huang, W.-M. Chen, A novel secure communication scheme in vehicular ad hoc networks, Computer communications 31 (12) (2008) 2827–2837.

[220] J. Daemen, V. Rijmen, Aes proposal: Rijndael.

[221] R. Szerwinski, T. Güneysu, Exploiting the power of gpus for asymmetric cryptography, in: International Workshop on Cryptographic hardware and embedded systems, Springer, 2008, pp. 79–99.

[222] K. Ali, F. Akhtar, S. A. Memon, A. Shakeel, A. Ali, A. Raheem, Performance of cryptographic algorithms based on time complexity, in: 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE, 2020, pp. 1–5.

[223] M. S. Henriques, N. K. Vernekar, Using symmetric and asymmetric cryptography to secure communication between devices in iot, in: 2017 International Conference on IoT and Application (ICIOT), IEEE, 2017, pp. 1–4.

[224] X. Wang, T. Liu, G. Xiao, Certificate-based anonymous authentication protocol for vehicular ad-hoc network, IETE Technical Review 29 (5) (2012) 388–393.

[225] Q. Wu, J. Domingo-Ferrer, U. González-Nicolás, Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications, Vehicular Technology, IEEE Transactions on 59 (2) (2010) 559–573.

[226] E. Brickell, J. Camenisch, L. Chen, Direct anonymous attestation, in: Proceedings of the 11th ACM conference on Computer and communications security, 2004, pp. 132–145.

[227] L. Chen, D. Page, N. P. Smart, On the design and implementation of an efficient daa scheme, in: International Conference on Smart Card Research and Advanced Applications, Springer, 2010, pp. 223–237.

[228] J. Camenisch, L. Chen, M. Drijvers, A. Lehmann, D. Novick, R. Urian, One tpm to bind them all: Fixing tpm 2.0 for provably secure anonymous attestation, in: 2017 IEEE Symposium on Security and Privacy (SP), IEEE, 2017, pp. 901–920.

[229] V. Kumar, H. Li, N. Luther, P. Asokan, J.-M. Park, K. Bian, M. B. Weiss, T. Znati, Direct anonymous attestation with efficient verifier-local revocation for subscription system, in: Proceedings of the 2018 on Asia Conference on Computer and Communications Security, 2018, pp. 567–574.

[230] J. Whitefield, L. Chen, T. Giannetsos, S. Schneider, H. Treharne, Privacy-enhanced capabilities for vanets using direct anonymous attestation, in: 2017 IEEE Vehicular Networking Conference (VNC), IEEE, 2017, pp. 123–130.

[231] D. Förster, H. Löhr, J. Zibuschka, F. Kargl, Rewire–revocation without resolution: A privacy-friendly revocation mechanism for vehicular ad-hoc networks, in: International Conference on Trust and Trustworthy Computing, Springer, 2015, pp. 193–208.

[232] J. Whitefield, L. Chen, F. Kargl, A. Paverd, S. Schneider, H. Treharne, S. Wesemeyer, Formal analysis of v2x revocation protocols, in: International Workshop on Security and Trust Management, Springer, 2017, pp. 147–163.

[233] L. Chen, S.-L. Ng, G. Wang, Threshold anonymous announcement in vanets, IEEE Journal on Selected Areas in Communications 29 (3) (2011) 605–615.

[234] C. Hicks, F. D. Garcia, A vehicular daa scheme for unlinkable ecdsa pseudonyms in v2x.

[235] Y. Toor, P. Muhlethaler, A. Laouiti, Vehicle ad hoc networks: Applications and related technical issues, Communications Surveys & Tutorials, IEEE 10 (3) 74–88.

[236] M. Raya, P. Papadimitratos, V. D. Gligor, J.-P. Hubaux, On data-centric trust establishment in ephemeral ad hoc networks, in: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, IEEE, 2008.

[237] N.-W. Lo, H.-C. Tsai, A reputation system for traffic safety event on vehicular ad hoc networks, EURASIP Journal on Wireless Communications and Networking 2009 (2009) 9.

[238] H. Lu, J. Li, M. Guizani, A novel id-based authentication framework with adaptive privacy preservation for vanets, in: Computing, Communications and Applications Conference (ComComAp), 2012, 2012, pp. 345–350.

[239] Y.-C. Wei, Y.-M. Chen, An efficient trust management system for balancing the safety and location privacy in vanets, in: Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012, pp. 393–400. doi:10.1109/TrustCom.2012.79.

[240] A. Wasef, X. Shen, Edr: Efficient decentralized revocation protocol for vehicular ad hoc networks, Vehicular Technology, IEEE Transactions on 58 (9) (2009) 5214–5224.

[241] J. Sun, C. Zhang, Y. Zhang, Y. Fang, An identity-based security system for user privacy in vehicular ad hoc networks, Parallel and Distributed Systems, IEEE Transactions on 21 (9) (2010) 1227–1239.

[242] R. Melki, H. N. Noura, A. Chehab, Lightweight multi-factor mutual authentication protocol for iot devices, International Journal of Information Security (2019) 1–16.

[243] H. N. Noura, R. Melki, A. Chehab, Secure and lightweight mutual multi-factor authentication for iot communication systems, in: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1–7.

[244] H. Noura, R. Couturier, C. Pham, A. Chehab, Lightweight stream cipher scheme for resource-constrained iot devices, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2019, pp. 1–8.

[245] H. N. Noura, A. Chehab, R. Couturier, Efficient & secure cipher scheme with dynamic key-dependent mode of operation, Signal Processing: Image Communication 78 (2019) 448–464.

[246] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, M. M. Mansour, One round cipher algorithm for multimedia iot devices, Multimedia tools and applications 77 (14) (2018) 18383–18413.