Electronics **2015**, *4*, 380-423; doi:10.3390/electronics4030380

OPEN ACCESS

electronics

ISSN 2079-9292

www.mdpi.com/journal/electronics

Article

Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures

Elyes Ben Hamida *, Hassan Noura and Wassim Znaidi

Qatar Mobility Innovations Center (QMIC), Qatar Science and Technology Park (QSTP), Doha, P.O. Box 210531, Qatar; E-Mails: hnouran@gmail.com (H.N.); wassimz@qmic.com (W.Z.)

* Author to whom correspondence should be addressed; E-Mail: elyesb@qmic.com; Tel.: +974-4459-5082.

Academic Editor: Felipe Jimenez

Received: 31 May 2015 / Accepted: 24 June 2015 / Published: 6 July 2015

Abstract: Due to the growing number of vehicles on the roads worldwide, road traffic accidents are currently recognized as a major public safety problem. In this context, connected vehicles are considered as the key enabling technology to improve road safety and to foster the emergence of next generation cooperative intelligent transport systems (ITS). Through the use of wireless communication technologies, the deployment of ITS will enable vehicles to autonomously communicate with other nearby vehicles and roadside infrastructures and will open the door for a wide range of novel road safety and driver assistive applications. However, connecting wireless-enabled vehicles to external entities can make ITS applications vulnerable to various security threats, thus impacting the safety of drivers. This article reviews the current research challenges and opportunities related to the development of secure and safe ITS applications. It first explores the architecture and main characteristics of ITS systems and surveys the key enabling standards and projects. Then, various ITS security threats are analyzed and classified, along with their corresponding cryptographic countermeasures. Finally, a detailed ITS safety application case study is analyzed and evaluated in light of the European ETSI TC ITS standard. An experimental test-bed is presented, and several elliptic curve digital signature algorithms (ECDSA) are benchmarked for signing and verifying ITS safety messages. To conclude, lessons learned, open research challenges and opportunities are discussed.

Keywords: cooperative intelligent transport systems (ITS); V2X communications; threats analysis; cryptographic countermeasures; ETSI TC ITS standard; elliptic curve digital signature algorithm (ECDSA); test-bed; experimental performance evaluation

1. Introduction

Due to the growing number of vehicles on the roads worldwide (more than two billion by 2050 [1]), road traffic accidents are currently recognized as a major societal and public health problem. According to the World Health Organization (WHO) [2], the total number of road traffic deaths due to accidents remains unacceptably high at around 1.24 million per year, in addition to twenty to fifty million who are injured and/or disabled. Projected trends suggest that road traffic injuries will become the fifth main cause of deaths by 2030. Road accidents and crashes have a major impact on national economies. For instance, the Automobile Association of America (AAA) estimated that the total cost of traffic crashes is around 166.7 billion USD [3]. This includes the costs of medical, emergency and police services, property damage and quality of life. Similar estimates from the WHO show that traffic injuries cost middle-income countries around 2% of their gross national product (over 100 billion USD per year). The above projected trends will have a tremendous impact on our society and our quality of life and will ask for specific actions to be put in place to deal with these in the next coming years. More specifically, traffic accidents can be partly mitigated through the launch of specific awareness campaigns and national strategic programs to promote a culture of safe road behavior (e.g., reducing speed, systemic usage of seat belts, *etc.*), to enforce traffic laws (e.g., warning, reporting, summonsing, *etc.*) and to plan for the design of safer roads and transportation systems.

In this context, cooperative intelligent transport systems (ITS) are considered as the key enabling technology to improve road safety, traffic efficiency and driving experience. There is currently a trend to deploy this new technology in vehicles to enable them to communicate not only with hotspots, but also with other nearby entities through direct short-range communications (DSRC), such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P) and vehicle-to-anything (V2X). Indeed, new market forecasts [4] clearly indicate that the connected vehicle market will be worth 39 billion USD in 2018, up from 13 billion USD in 2012, and that more than 50% of the vehicles sold worldwide in 2015 will have communication capabilities. It is envisioned that every new vehicle will be connected in multiple ways by 2025. This new reality of intelligent transport systems will leverage different types of vehicular communications (VC) and telematics services to enable the emergence of innovative active road safety applications, driver assistive services, smart mobility and traffic management services.

Research and standardization activities on intelligent transport systems had significantly started, worldwide, more than a decade ago [5,6] and encompasses various multidisciplinary areas, including radio channel modeling, data link protocols, wireless communications, networking protocols, security and localization. Standardization of ITS is also important to ensure interoperable V2X communications between different equipments and systems, regardless of their brands and models. In the United States,

IEEE proposed a novel Wireless Access in Vehicular Environments (WAVE) V2X protocol stack [7] for enabling future ITS applications. It relies on the IEEE 802.11p standard [8], which extended the PHY and MAC layers of the IEEE 802.11-2007 standard [9] to cover vehicular environments and the IEEE 1609 family of standards [7] to provide high level features (above the MAC layer), such as routing, addressing, security and resources management. In Europe, the European Telecommunications Standards Institute (ETSI) TC ITS working group [10] is working on a global standard for cooperative ITS systems, which adapts and optimizes ongoing ITS proposals at IEEE and ISO [11]. The ETSI TC ITS defines a reference architecture [10] for cooperative V2X communications, including the support for the IEEE 802.11p standard [8]. However, there is still a lack of experimental deployment and comprehensive performance evaluation of these standards under realistic environments, traffic load and application use cases, especially regarding the security of vehicular communications and the safety of ITS applications.

Even though ITS will have a great potential in the near future, there are many open research challenges and issues that need to be tackled in order to foster the emergence of safe ITS applications. Indeed, since this technology heavily relies on wireless communications, several threats and attacks can affect its functioning [12–15] and, thus, compromise the safety of the involved ITS entities and users. Typical attacks on ITS include denial of service (DoS) attacks [13], Sybil attacks [16], man-in-the-middle attacks [17], eavesdropping [18] and many others. For example, several external attacks were successfully demonstrated [19] on a sedan vehicle that has an e-call application and that is widely used in the U.S. More recently, it was demonstrated that long-range attacks were also possible on real vehicles using malicious smartphones [20]. Consequently, several security requirements should be ensured to resist these attacks, including authenticity, confidentiality, integrity, non-repudiation and data trust, and, thus, to enable the emergence of future autonomous (or driverless) vehicles [21].

This paper aims to review the current research challenges and opportunities related to the development of secure and safe ITS applications and to provide a comprehensive study about existing security threats and their corresponding cryptographic countermeasures. In this context, it is important to highlight the main differences of this paper in comparison to other surveys on ITS security, such as [12–14]. In contrast to existing works, this paper evaluates all recent cryptographic-based solutions that have been proposed separately for each ITS threat. To the best of our knowledge, most research works on the ITS security domain were either papers that address specific problems or general surveys. There is no previous work that focuses on linking ITS security issues with related cryptographic techniques, which can entirely solve or reduce problems and their impact. Moreover, an ITS safety application case study is analyzed in detail and evaluated in light of the European ETSI TC ITS standard. An experimental test-bed and implementation of this ITS standard is presented, and various elliptic curve digital signature algorithms (ECDSA) are evaluated for signing and verifying ITS safety messages. To the best knowledge of the authors, there have been very few works [22,23] that have attempted to evaluate the ETSI ITS security architecture. The first implementation was described in [22], and some weaknesses in the early version of the standard were identified and discussed; whereas some preliminary cryptographic performance indicators were presented in [23]. Finally, lessons learned, open research challenges and opportunities are discussed.

The remainder of this paper is structured as follows. Section 2 explores the architecture model, the main characteristics and challenges, as well as the target applications of intelligent transport systems. Section 3 surveys the main ITS standardization activities in Europe and the U.S. and briefly surveys the most important ITS projects that have been developed in the past and that are currently active. Section 4 discusses the main ITS security requirements and threats and classifies them based on their respective cryptographic countermeasures. Section 5 analyzes in detail an example of an ITS safety application use case (*i.e.*, the collision risk warning application) in light of the European ETSI TC ITS standard. An implementation of the ETSI TS 103 097 [24] security standard is described, and several elliptic curve digital signature algorithms (ECDSA) are evaluated for signing and verifying ITS safety messages. Section 6 provides a discussion of lessons learned, open research challenges and opportunities. Finally, Section 7 concludes the paper and provides future research directions.

2. ITS Architecture and Applications

With the technological advancements in the areas of mobile computing, wireless communications and remote sensing, intelligent transport systems (ITS) have recently emerged as a promising technology that will enable the deployment of diverse applications related to road safety, traffic efficiency and infotainment. This section provides a high level overview of the ITS architecture, characteristics, challenges and target applications.

2.1. ITS Architecture

The high level architecture of ITS comprises three main communication domains, *i.e.*, the in-vehicle domain, the V2X domain and the infrastructure domain, as shown in Figure 1.

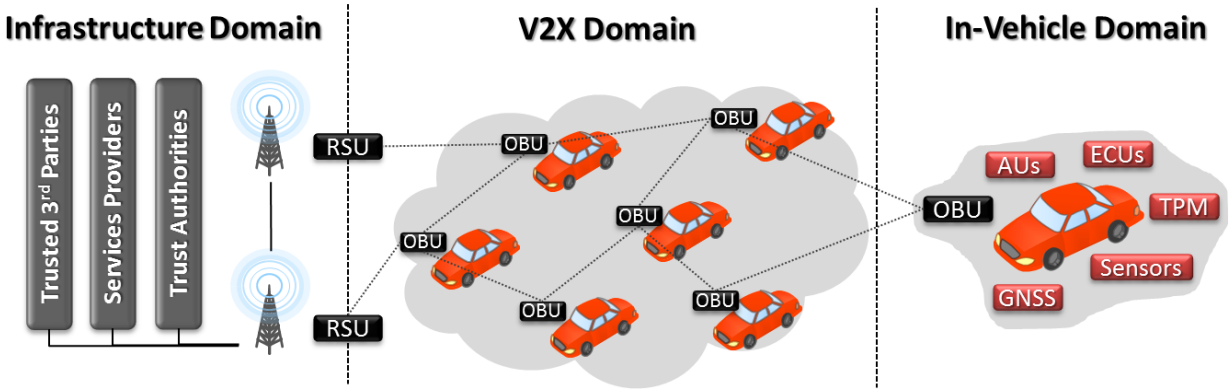


Figure 1. ITS high level architecture. RSU, road side unit; OBU, on-board unit; AU, application unit; ECU, electronic control unit; TPM, trusted platform module.

The in-vehicle domain consists of a connected vehicle equipped with electronic control units (ECUs), wireless-enabled on-board units (OBUs), a trusted platform module (TPM) and an application unit (AU). ECUs collect data about the vehicle's dynamics (e.g., location, speed, heading, vehicle size, *etc.*), the context of its immediate environment (e.g., the number of neighboring vehicles, local road

traffic conditions, *etc.*) and control its functionality. These ECUs collaborate by exchanging messages with the OBU and AU, and form an in-vehicle network (also known as the on-board network). The AU is responsible for running one or multiple applications, which are offered by remote service providers (SPs), and communicates with other nearby ITS entities using the communication capabilities of the OBU. Each connected vehicle is also equipped with a TPM to enable secure and efficient communications and to manage the different keys and certificates. Finally, a Global Navigation Satellite System (GNSS) unit is used to obtain accurate location information.

The V2X domain (or *ad hoc* domain) consists of vehicle OBUs and road-side units (RSUs) deployed along the roads. As shown in Figure 2, the information collected at the vehicles' OBUs, are exchanged in real time with nearby ITS entities (e.g., OBUs, RSUs, *etc.*) using various vehicular communication technologies (V2X), including: (i) vehicle-to-vehicle (V2V) communications between neighboring vehicles (or OBUs) using a dedicated short-range communications (DSRC) technology; (ii) vehicle-to-infrastructure (V2I) communications between the surrounding OBUs and RSUs, and *vice versa*; and (iii) vehicle-to-pedestrian (V2P) communications between the OBUs/RSUs and the surrounding pedestrian.

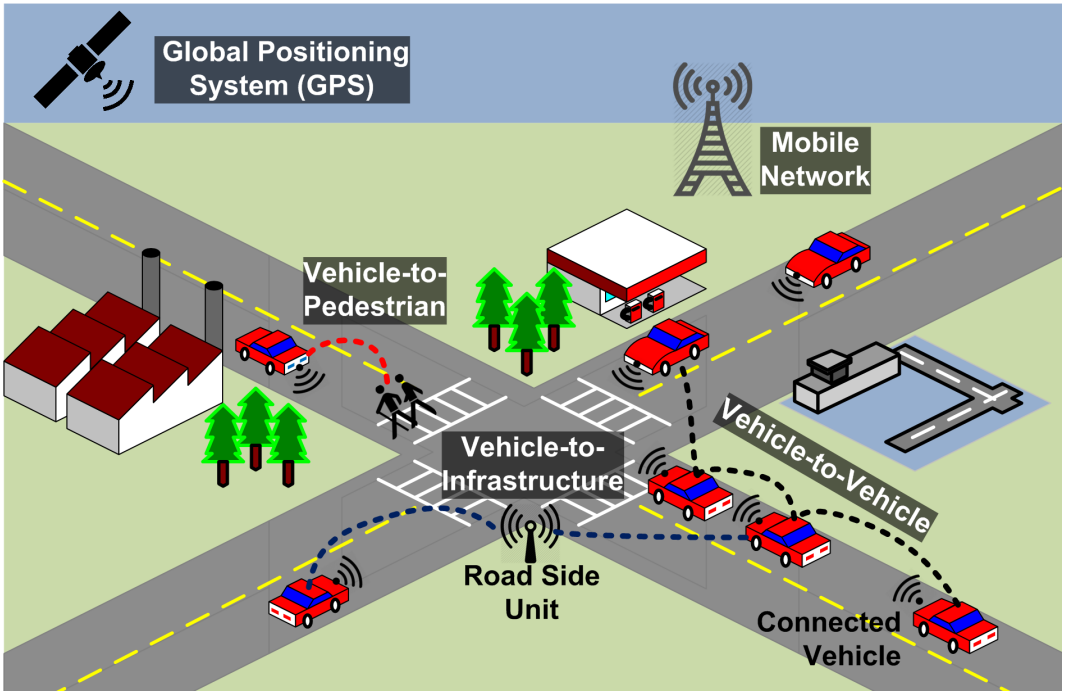


Figure 2. ITS V2X communications.

The infrastructure domain includes the trusted third parties (TTP), such as vehicles manufacturers, the service providers (SPs) and the trust authorities (TA). The fixed RSUs are generally not fully trusted and subordinated by the TA and can be considered as a bridge between the V2X and infrastructure domains. The registration and authentication of these RSUs and OBUs are realized by the TA. The SPs provide applications to the vehicles AUs and are responsible for managing software updates, billing and deliver added-value services. Several applications, such as intersection collision warning, wrong way driving warning and remote diagnostic of vehicles, will exploit the integration of the above network technologies to constitute a connected vehicle. We call these applications: intelligent transport system applications.

2.2. ITS Characteristics and Challenges

Even though ITS will have great potential in the near future, there are many open research challenges and issues that need to be addressed in order to deploy effective and safe ITS applications. In particular, the design of ITS applications requires special attention and is characterized by the following main features:

- Powerful capacity: ITS stations (*i.e.*, RSUs, OBUs) are powerful in terms of energy, localization, computation, storage and data rate capabilities;
- High mobility: ITS involves a huge number of nodes that move from one location to another, with different speeds and directions, thus making the prediction of node position very difficult and necessitating node protection [25];
- Dynamic network topology: depending on their locations and speeds, ITS stations can join and/or leave the network very quickly; the resulting network topology is thus highly dynamic;
- Time sensitivity: safety information must be delivered to nodes in a short period of time (e.g., 100-ms delay for safety-related messages), thus making latency one of the most important quality of service (QoS) limitations for these kinds of networks;
- Sufficient energy: unlike wireless sensor networks (WSN), where nodes have limited resources and a small battery lifetime, ITS entities are considered as resource-rich devices (*i.e.*, energy, storage and computation); this allows the implementation of complex algorithms to achieve a higher throughput in vehicular environments [26];
- Good physical protection: inside each ITS entity, physical protection can be ensured, giving the network immunity against physical attacks [26];
- Unbounded network size: ITS can be implemented in a small geographical area, or in cities, or even across several countries; this means that the size of the ITS network is not limited to a specific geographical area [27];
- Wireless communications: ITS entities communicate with each other and exchange information via a wireless connection; hence, some security measures and protocols must be used to ensure safe and protected communication;
- Heterogeneous V2X communication technologies: vehicles exploit different types of communication modes, such as multi-hop V2V, point-to-point V2I, short/long range V2I, *etc.*; in addition, connected vehicles support a wide range of communication technologies, such as IEEE 802.11p, Wi-Fi, Bluetooth, 3G/LTE, *etc.*;
- Heterogeneous environments: vehicles operate in various environments, such as indoor, outdoor, low and high network density, *etc.*;
- Security and privacy: security and privacy are of paramount importance in ITS; in most scenarios, attackers aim to affect the authentication, integrity and even the availability of the network; in this context, security protocols must be implemented with low communication overhead due to time constraint and low computation complexity to exchange quick and safe information.

A careful analysis of the above characteristics reveals that the ITS design challenges are sometimes contradictory. On the one hand, vehicular communications should be efficient and provide real-time performance, but on the other hand, extra processing and message overheads are required to ensure the security and privacy of these communications. Hence, it is necessary to achieve optimal trade-offs between these two issues in order to meet the QoS requirements in terms of the safety and practicality of ITS applications.

2.3. ITS Applications

ITS applications exploit data collected from vehicles to improve the use of vehicles, the safety and comfort of drivers and to rationalize the use of public infrastructures. As shown in Figure 3, ITS applications can be categorized into four main classes: (i) infotainment and comfort; (ii) traffic management; (iii) road safety; and (iv) autonomous driving applications. The remainder of this section provides a high level overview of these four classes of ITS applications. We refer the readers to [28–31] for a more detailed description of emerging ITS applications.

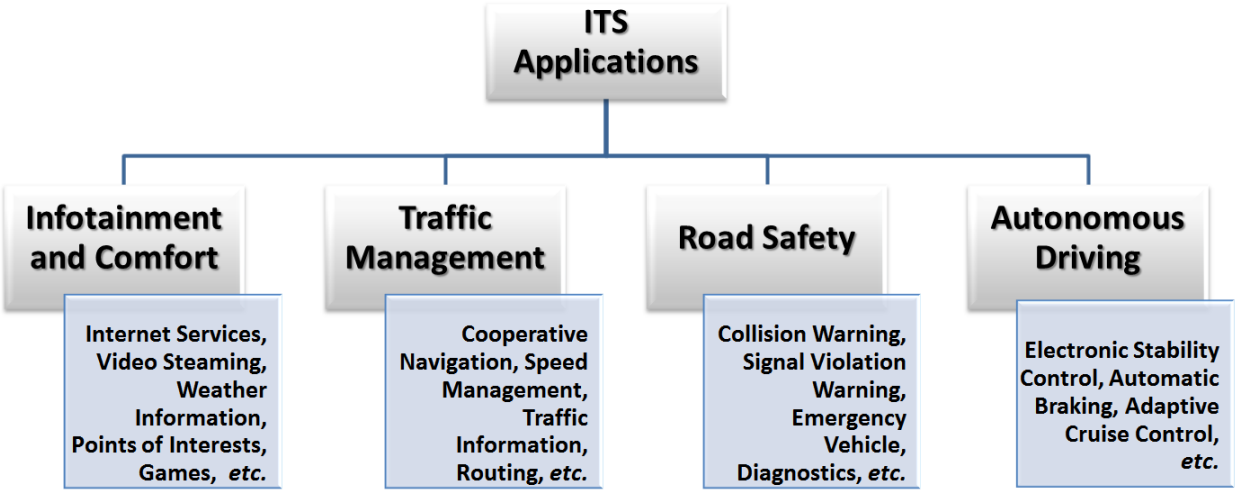


Figure 3. Classification of ITS applications.

2.3.1. Road Safety Applications

Road safety applications exploit wireless V2X communications between surrounding ITS entities (e.g., vehicles, road infrastructures, *etc.*) to reduce traffic accidents and to protect the drivers and pedestrian from various road hazards. To that end, each ITS entity periodically broadcasts safety messages to notify its neighborhood about its context and location information. Furthermore, depending on specific events (e.g., accidents, detected road hazards), each ITS entity may also trigger the transmission of notification messages to nearby vehicles and/or emergency services using multi-hop communications. As shown in Table 1, the critical latency (or end-to-end communication delay) represents one of the most important system requirement for road safety applications, which typically should not exceed one hundred milliseconds.

Table 1. Typical ITS Applications vs. Performance and System Requirements

Applications	Use Cases	Communication Modes	Radio Coverage	TX Frequency	Critical Latency
Active road safety	Intersection collision warning, Lane change assistance, etc.	Broadcasting , Cooperative messaging, etc.	From 300m to 20Km	10Hz	$\leq$ 100ms
Traffic Efficiency and Management	Regulatory speed limit notification	Periodic / permanent message broadcast	From 300m to 5Km	1-10Hz	-
	Green light optimal speed advisory			10Hz	$\leq$ 100ms
Cooperative Navigation	Electronic toll collection	Internet vehicle and unicast full duplex session	From 0m to 1Km	1Hz	$\leq 200ms$
	Adaptive cruise control, Vehicle highway automatic system	Cooperation awareness		2Hz	$\leq 100ms$
Global Internet Services	Insurance and financial services, Fleet management, etc.	Access to Internet	From 0m to full range	1Hz	$\leq 500ms$
Cooperative Local Services	Point of interest notifications	Periodic / permanent message broadcast	From 0m to full range	1Hz	$\leq 500ms$
	Electronic commerce	Full duplex communications			
	Media downloading	Access to Internet			

Three typical examples of emerging ITS road safety applications are shown in Figure 4. The first example consists in the pedestrian crossing warning application in which drivers are notified in case pedestrians are crossing the road (*cf.* Figure 4a). To that end, sensors are deployed along the sidewalks to detect the presence of people, and the corresponding sensory events are collected at the road side units. These RSUs can thus detect and/or predict the occurrence of potential accidents and notify the incoming vehicles. The second example consists in the left turn driver assistance application, as shown in Figure 4b. In this scenario, two vehicles might approach an intersection without seeing each other due to visual obstructions (e.g., trees, building, *etc.*). The objective of such an application is thus to assist the driver in making a safer left turn at the intersection. To that end, RSUs collect information about the in-vehicles OBUs and/or from the deployed road sensors to detect the occurrence of such an event and, thus, to provide timely recommendations and notifications to the involved drivers. Finally, the third application is related to the approaching emergency vehicle warning application, as shown in Figure 4c, in which an approaching emergency vehicle (e.g., ambulance, police or fire fighter) requests the surrounding vehicles to form a corridor and to provide a clear path. Eventually, the emergency vehicle could communicate with the surrounding road infrastructures to set the traffic lights to green, hence minimizing the emergency response time. Other examples of road safety applications include: emergency electronic brake lights warning, stationary vehicle indication, roadwork warning, intersection collision avoidance, lane change warning and many others [28–30]. A case study related to the collision risk warning (CRW) road safety application will be analyzed in more detail in Section 5.

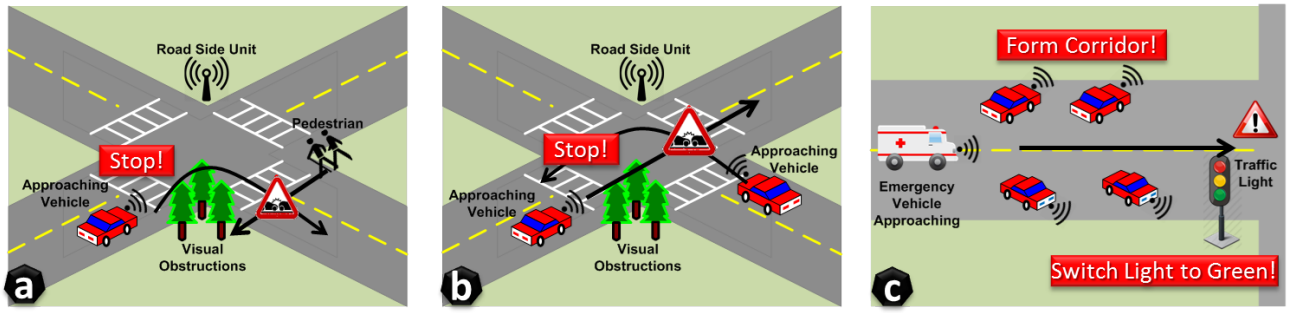


Figure 4. Examples of road safety applications: (a) pedestrian crossing warning; (b) left turn driver assistance; and (c) approaching emergency vehicle warning.

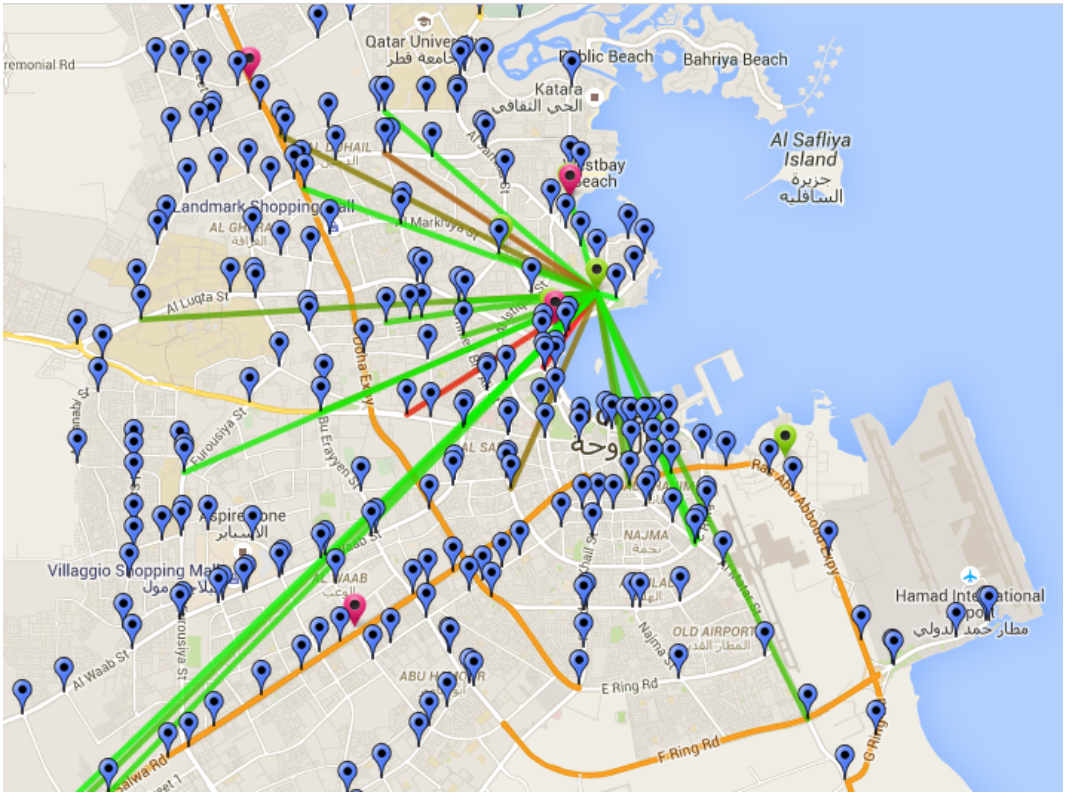


Figure 5. Origin-destination (OD) trip matrix.

2.3.2. Traffic Management Applications

Traffic management applications represent a second major class of ITS applications, whose main objective is to enhance the management and coordination of traffic flows and to provide various cooperative navigation services to the drivers. These applications rely on the collection and analysis of the exchanged ITS messages (*i.e.*, between ITS entities) in order to build and maintain global traffic map databases. The traffic data are generally collected by the deployed road side units and/or from road sensors and are transmitted wirelessly to remote trusted data centers for further data analysis and processing. The collected data include contextual and location-based information related to vehicles, drivers and road events.

Once the collected data are processed and translated into meaningful information, these are delivered to the drivers through services providers to notify them of current and/or future congested areas, recommended itineraries, navigation instructions, speed limit notifications, *etc.* Moreover, these traffic management applications can enable authorities to perform advanced spatio-temporal traffic data analysis, such as an origin-destination (OD) trip matrix. As shown in Figure 5, the OD-matrix aims at estimating the traffic volumes between different origins and destinations (e.g., zones, streets, cities, *etc.*) in order to better optimize the use and/or planning of future road infrastructures and buildings.

As shown in Table 1, these applications rely on the periodic broadcast of safety messages and/or unicast V2X communications, whose critical latency should typically not exceed two hundred milliseconds. Other examples of traffic management applications include: regulatory speed limit notification, green light optimal speed advisory, electronic toll collection, vehicle highway management and may others [28–30].

2.3.3. Infotainment and Comfort Applications

Infotainment and comfort applications aim at enhancing the driving experience by providing the drivers with various added-value services. These services are generally offered by trusted service providers, where the corresponding applications and services are downloaded and installed on the vehicles application units (AUs). AUs communicate with the remote SPs data centers through their OBUs, using different V2I communication technologies (e.g., 4G/LTE, 5G). A typical example of such an application consists in the remote vehicle diagnostic and maintenance application in which the SPs collect information from the in-vehicles sensors and send notifications to the drivers regarding detected safety defects and/or to remind them about planned car maintenance.

Another application consists of providing global Internet access to the vehicle's passengers to enable a wide range of comfort services, including online gaming, video streaming, weather information and many others [28–30]. As shown in Table 1, these applications rely mainly on V2I communications (vehicle-to-infrastructure/back office), whose latency should typically not exceed five hundred milliseconds.

2.3.4. Autonomous Driving Applications

Autonomous driving, also known as automated driving, applications represent the next big leap in human transport technologies, which is expected to be deployed by 2020 and fully functional by 2030 [31].

This new technology will rely on the automation of the vehicle sensing and driving functions, based on six levels of automation [31], where the human driver becomes a passenger and is no longer required (*i.e.*, full automation level). As shown in Figure 6, future autonomous cars will integrate different technologies, including: (i) ultrasonic sensors to detect the presence of obstacles; (ii) LiDAR and/or radar to create a 360-degree field of view to prevent accidents; (iii) high definition cameras to spot road hazards in real time, such as pedestrians and animals; (iv) Global Navigation Satellite System receivers to provide a highly accurate position for the car; and (v) V2X communication technologies to enable the car to communicate with the surrounding vehicles, road infrastructures, remote services providers and

trusted third parties. In addition to the previously described applications, autonomous driving technology will bring a wide range of new benefits, in terms of the increase of the roadway and parking capacity and the reduction of traffic congestion, car theft, accidents and collisions.

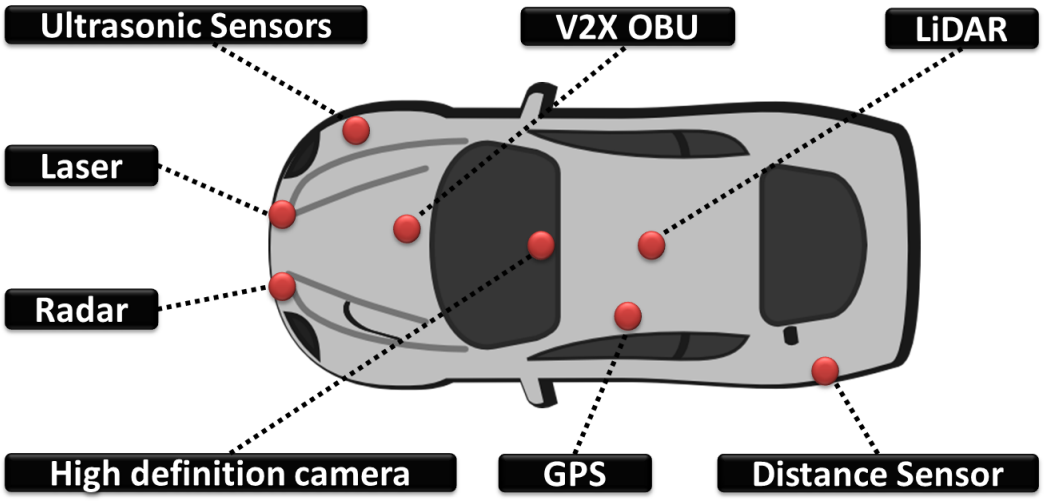


Figure 6. Key technologies enabling autonomous cars.

In order to unlock the tremendous potential of the aforementioned emerging ITS applications, the ITS communication stack should provide efficient, secure and low-latency V2X communications. Indeed, safety applications require the periodic broadcasting of safety messages (or beacons) to detect and/or prevent the risk of collision between two or more vehicles or to locate hazards along the road. However, since this message exchange relies heavily on wireless communications, several threats and attacks can affect its functioning and, thus, lead to accidents. In the next sections, we will review the key enabling ITS standards, technologies and projects, followed by a detailed analysis on the existing ITS threats and their main cryptographic countermeasures.

3. ITS Standards and Projects

Research and standardization activities on intelligent transport systems had significantly started, worldwide, more than a decade ago and encompass various multidisciplinary areas, including radio channel modeling, data link protocols, wireless communications, networking protocols, security, data privacy and localization. This section briefly surveys the most relevant ITS standardization activities, technologies and research projects. We refer the readers to [5,6] for a more comprehensive description of existing ITS standards.

3.1. ITS Key Enabling Standards

In order to address the increasing demand for intelligent transport system applications, the IEEE 802.11p task group [8] was formed in 2004 to provide amendments and enhancements to the IEEE 802.11 standard for the support of Wireless Access in Vehicular Environments (WAVE). The resulting IEEE 802.11p standard was published in 2010 (Draft v11) [8] and allows the use of the licensed ITS band

of 5.9 GHz to enable V2V communications between highly mobile vehicles and V2I communications between vehicles and RSUs. It should be noted that the IEEE 802.11p standard defines only the specifications for the basic physical (PHY) and medium access control (MAC) layers, as shown in Table 2.

Table 2. Key enabling vehicular communication technologies (MAC/PHY). WAVE, Wireless Access in Vehicular Environments; V2V, vehicle-to-vehicle; V2I, vehicle-to-infrastructure.

Characteristics	Vehicular Communication Technologies		
	802.11p (WAVE)	802.11 a/b/g/n (Wi-Fi)	Cellular (3G, LTE)
Mode of operation	*Ad hoc*, Infrastructure	*Ad hoc*, Infrastructure	Infrastructure
Communication type	V2V, V2I	V2I	V2I
Bit rate	Up to 27 Mbps	Up to 54 Mbps	Up to 2 Mbps
Communication range	Up to 1000 m	Up to 100 m	Up to 15,000 m
Support for mobility	High	Low	High
Frequency bands	5, 86 to 5.92 GHz	[2.4, 5.2] GHz	[800, 900, 1800, 1900] MHz
Channel bandwidth	[10, 20] MHz	1 to 40 MHz	25 MHz (GSM), 60 MHz (UMTS[1])
Related standards	IEEE, ISO, ETSI	IEEE	ETSI, 3GPP[2]

[1] UMTS: Universal Mobile Telecommunications System

[2] 3GPP: 3rd Generation Partnership Project

The IEEE 802.11p PHY layer is based on the orthogonal frequency division multiplexing (OFDM) schema with a channel bandwidth of 10 MHz, the support for various data rates (from 3 to 27 Mbps) and a maximal communication range of 1 km. The IEEE 802.11p MAC layer is based on an enhanced distributed coordination function (DCF) algorithm that is already in use in the existing IEEE 802.11 family of standards [32]. The enhanced algorithm is known as enhanced distributed channel access (EDCA) and introduces the concept of quality of service (QoS) to ensure a high priority for latency-sensitive messages, such as ITS safety messages. QoS is achieved through the definition of various access category (AC) levels based on the required traffic priority, e.g., best effort traffic, safety/emergency notifications or video/audio traffic.

More recently, the IEEE working group 1609 [33] was formed to define additional higher layers (above the IEEE 802.11p PHY/MAC layers) and to complement the features of the IEEE 802.11p standard. As shown in Figure 7, the resulting IEEE 1609 family of standards include [7]: (i) IEEE 1609.1 for enhancing resource management; (ii) IEEE 1609.2 for enabling security services; (iii) IEEE 1609.3 for providing routing and addressing services; (iv) IEEE 1609.4 for supporting multi-channel operations; (v) IEEE 1609.5 for layers management; and (vi) IEEE 1609.6 for the application facilities management. The combination of the IEEE 802.11p and IEEE 1609 standards is generally known as Wireless Access in Vehicular Environments (WAVE).

Similar ongoing standardization activities are also being pursued in Europe within the European Telecommunications Standards Institute (ETSI) TC ITS working group [10]. The ETSI ITS standard defines a reference architecture for cooperative vehicular communications, including six main layers [10]: (i) the application layer for the general management of ITS applications (e.g., prioritization, classification, *etc.*); (ii) the facilities layer for the support of sessions and data presentation; (iii) the networking and transport layer, including the support of GeoNetworking, IPv6 networking, TCP/UDP transport protocol, *etc.*; (iv) the medium access layer with the support of various communication technologies (e.g., IEEE 802.11p, Wi-Fi, 2/3G, LTE, *etc.*), as shown in Table 2; (v) the management entity for managing the features of the whole ITS architecture layers; and (vi) the security entity which provides security services.

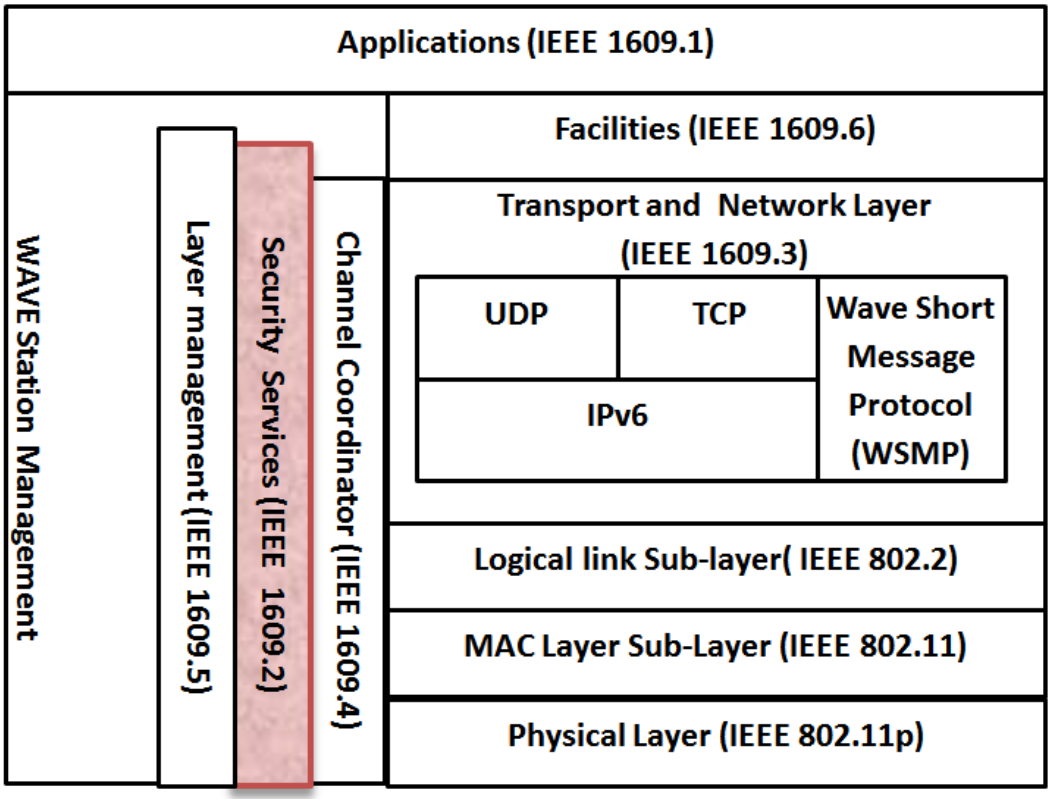


Figure 7. WAVE standards for the ITS communications layered architecture (U.S.).

A detailed overview of the ETSI TC ITS standard [10], including its security layer [24], will be provided in Section 5 and analyzed in the context of an ITS safety application use case.

3.2. ITS Research Projects

As described above, ITS is a multidisciplinary and cross-sectoral research area, which can only be achieved through the convergence and synergy of research on many different research topics. For this reason, research on ITS is typically conducted through large research projects. This section surveys the most important research projects that have been developed in the past and that are currently active.

Many ambitious projects have been completed. Some notable examples are: (i) Open vehicular secure platform project (OVERSEE - EU/FP7) [34], which realized an open and standard-compliant in-vehicle platform to enable the development of secure ITS applications and to ensure a high level of isolation between independent applications; (ii) E-safety vehicle intrusion protected applications project (EVITA - EU/FP7) [35], which proposed and developed a secure in-vehicle communication architecture that is robust to thwart tempering and to protect sensitive data inside the vehicle; (iii) Privacy enabled capability in co-operative systems and safety applications project (PRECIOSA - EU/FP7) [36], which analyzed and evaluated privacy-related issues in cooperative vehicular and road safety systems and proposed a privacy aware architecture for V2V and V2I communications; (iv) Intellidrive for safety, mobility, and user fee project (Intellidrive - U.S.) [37], which designed and evaluated new security mechanisms for V2V and V2I communications, which were experimentally evaluated through real deployments; (v) SafeSpot project (EU/FP6) [38], which designed dynamic and cooperative *ad hoc* networking and localization mechanisms for V2V and V2I communications; (vi) Secure vehicle communication project (SEVECOM - EU/FP6) [39], which proposed security architecture, protocols and mechanisms for vehicular communications systems, including identity management, data consistency and privacy and performance evaluation; and (vii) Cooperative cars and roads for safer and intelligent transportation systems project (CopITS - Qatar National Research Fund) [40], whose objective was to develop advanced communication protocols and networking services to enhance the data transfer over V2V and V2I links and to evaluate them using an ETSI ITS standard-compliant [10] platform and real deployment scenarios.

More recently, new research projects have been launched or are ongoing. Some notable examples are as follows: (i) COMeSafety2 project (EU/FP7) [41], whose objective is to facilitate the development and deployment of cooperative ITS safety applications and to promote their benefits towards industrial stakeholders and authorities; (ii) Preparing secure v2x communication systems project (PRESERVE - EU/FP7) [42], whose main goal is to design, develop and evaluate secure and scalable V2V and V2I communication systems in realistic deployment scenarios; (iii) Advanced cellular technologies for connected cars project (CellCar - Qatar National Research Fund) [43], whose goal is to propose new strategies to combine the IEEE 802.11p standard with LTE to improve the network performance and enable delay-tolerant services; (iv) Cooperative systems for smart mobility services and solutions project (CosMob - Qatar National Research Fund) [44], whose objective is to enhance road traffic efficiency by proposing new cooperative and real-time traffic data collection and dissemination concepts, as well as their analysis and delivery to the vehicles' drivers; (v) Security and safety modelling project (SESAMO - EU/FP7) [45], whose main goal is to better investigate, understand and model the relations between functional safety and security mechanisms in embedded systems in multiple domains; and (vi) Engineering security and performance aware vehicular applications for safer and smarter roads (SafeITS - Qatar National Research Fund) [46], whose main objective is to design an adaptive and context-aware ITS applications framework enabling the dynamic adaptation of the quality of service and security features to ensure the safety of the ITS users and entities.

4. ITS Threats Analysis and Classification

Research on ITS security has attracted a lot of attention from the research community in the last decade [12–15], since the challenges were observed as a social barrier to the common adoption of ITS systems. ITS technology was primarily designed to improve road safety, passenger safety and traffic efficiency. However, since it heavily relies on wireless communications, several threats can affect its functioning and, thus, lead to accidents. As shown in Figure 8, the main ITS threats and attacks are related to the following main security services: availability, identification and authenticity, confidentiality and privacy, integrity and data trust and non-repudiation and accountability. This section explores in detail the main threats and attacks that affect ITS systems. First, the involved ITS entities and the attackers profiles are identified. Then, the main ITS security requirements are discussed in detail. Finally, the existing ITS attacks are analyzed and classified, along with their main cryptographic countermeasures.

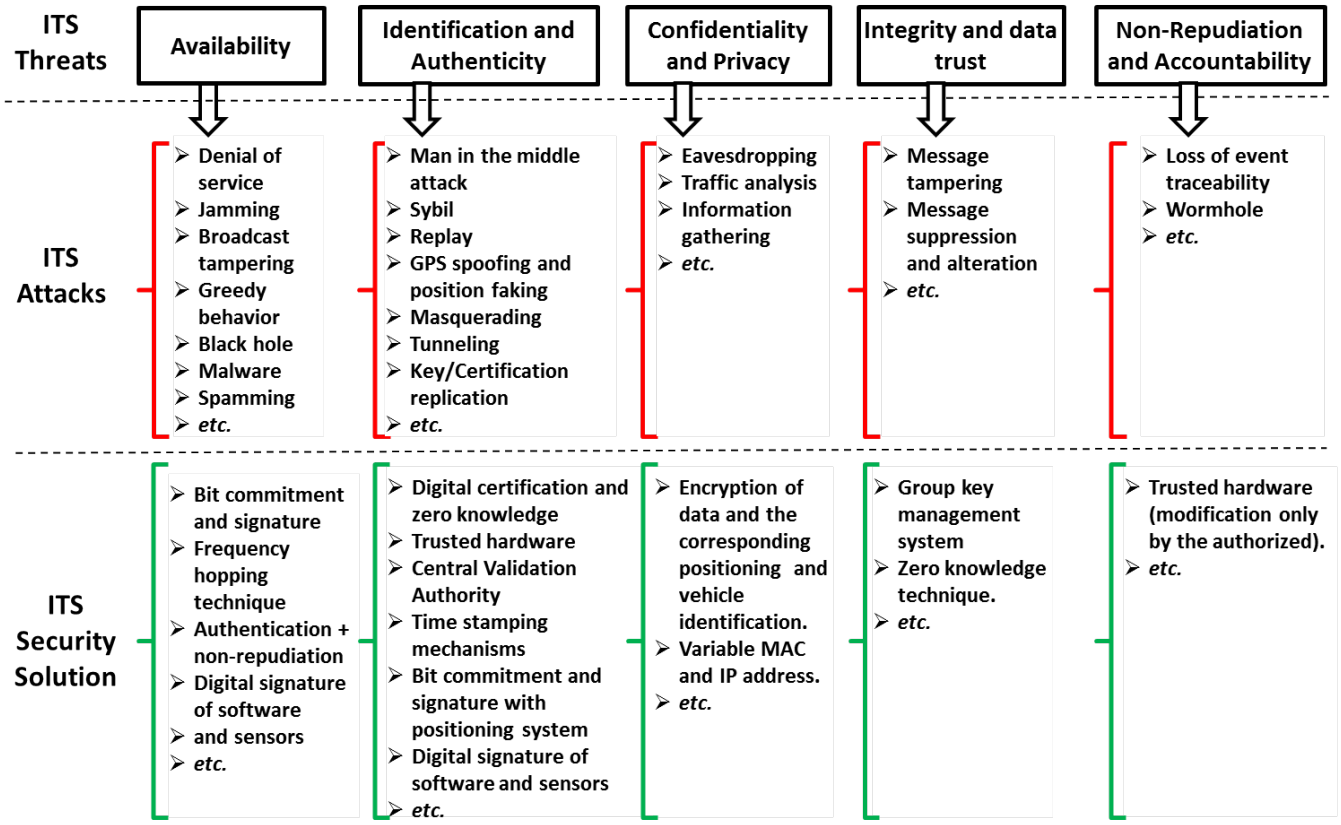


Figure 8. Examples of ITS threats, attacks and countermeasures.

4.1. ITS Involved Entities

From a security point of view, different entities might be involved in ITS systems [13], including:

- The drivers: Drivers are the most important element of ITS, since they have to make vital decisions and can interact with the driving assistance systems to ensure their safety;

- The on-board unit (OBU): OBU refers to both the driver and the vehicle in the literature. OBUs can be classified into: (i) normal OBUs, which operate in a normal way; and (ii) malicious OBUs, which try to mislead the system;
- The road side unit (RSU): Similarly to OBU, RSUs can be classified into: (i) normal RSU terminals; and (ii) malicious RSU terminals, which try to mislead the system;
- Third party entities: Third party entities can be trusted or semi-trusted, and are responsible for managing the security certificates, as well as the diverse secrets/public key pairs. Examples of such entities include the transportation regulatory agencies and the vehicle manufacturers;
- The attackers: Attackers try to violate the security of ITS systems by using several techniques. These attackers can be classified into different categories, as discussed in the following subsection.

4.2. ITS Attackers Profiles

Attacker profiles are generally categorized into three bipolar criteria [47], *i.e.*, active *vs.* passive, external *vs.* internal and malicious *vs.* rational, as discussed below:

- Active *vs.* passive: Active attackers transmit malicious packets to harm other nodes or a part of the network. Generally, this attacker has the authorization to operate within the network. Moreover, active nodes that have insider status could perpetrate almost any kind of attack. In contrast, passive attackers eavesdrop on the communications between the other nodes in the network, in order to extract useful information. Although it cannot cause any direct damage to the network, the gathered information could be used for future attacks. In general, passive nodes are also outsiders;
- External *vs.* internal: External attackers are generally not authenticated and authorized to operate within the ITS network. External attacks target generally the confidentiality and availability of the system. In contrast, internal attackers are generally part of the ITS network and can perpetrate almost any kind of attack;
- Malicious *vs.* rational: Malicious attackers have no specific targets, and their main goal is to destroy the network, for example by transmitting false information to vehicles in a specific geographic area [48]. In contrast, rational attackers have a specific target and can be very dangerous [49] due to their unpredictable nature.

4.3. ITS Security Requirements

To ensure a practical deployment of ITS systems, diverse security requirements must be attained to ensure secure V2X communications and ultimately safe driving. In particular, the design of ITS applications requires special attention and is characterized by specific challenges and requirements, as listed in Table 3 and discussed below in more detail:

- Authentication: This is one of the most important ITS security requirement, which can be classified into three sub-requirements: (i) user authentication to prevent Sybil attacks and dismiss malicious entities; (ii) source authentication to ensure that messages were generated by legitimate ITS stations; and (iii) location authentication to ensure the integrity and relevance of the received information;

- Data integrity: ITS entities (e.g., OBUs, RSUs, *etc.*) should be able to verify and validate the integrity of the received messages in order to prevent any unauthorized or malicious modification, manipulation or deletion during transmission;
- Privacy and anonymity: The identities of drivers and vehicles should not be easily identifiable from the exchanged messages, and the right of the driver to control the access and use of her/his personal data should be enforced;
- Availability: Exchanged information should be processed and made available in real time, requiring thus the implementation of low-overhead and lightweight cryptographic algorithms;
- Traceability and revocation: ITS authorities should be able to track malicious ITS entities that are misusing the ITS system, in order to revoke them in a timely manner. The trust authority (TA) should be able to trace the vehicle and reveal its true identity. Furthermore, in case of a dispute or when a malicious vehicle is detected, the TA must revoke it and add its identity to the revocation list;
- Authorization: It is necessary to define the access control and authorization for the different entities. Specific rules should be enforced for accessing or denying specific ITS entities access and/or use of certain functions or data;
- Non-repudiation: Each ITS entity should be uniquely associated with its information and actions in order to achieve data authenticity and origination;
- Robustness against external attacks: ITS entities should be robust against external attacks, such as availability attacks, and ITS software should be almost free of vulnerabilities (e.g., buffer overflow) and logic flaws.
- Data confidentiality: Exchanged messages should be properly encrypted and protected in order to prevent the disclosure of sensitive information to malicious nodes or unauthorized parties;

Table 3. Security requirements *versus* V2X communication types.

Security Requirement	Broadcast	Unicast	Security Mechanisms
Confidentiality	✗	✓	Encryption on sensitive messages; randomizing traffic patterns
Authenticity	✓	✓	Message signature Trusted hardware module; active detection systems
Integrity	✓	✓	Message signature and other integrity metrics for content delivery
Authorization	✓	✓	Certificate accompanying message signature
Non-repudiation of origin	✓	✓	Message signature
Non-repudiation of receipt	✗	✗	Not necessary
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	✓	✓	Pseudonymity, unlinkability ID-based system for user privacy

As shown in Table 3, the above ITS security requirements depend on the considered V2X communications types. For instance, vehicle-originating broadcast (VOB) and infrastructure-originating broadcast (IOB) involve the broadcast of cooperative awareness messages to enable road safety applications. In this context, ensuring the confidentiality of the broadcast messages is not required, since all of the neighboring vehicles should be able to receive and decode these safety messages. In contrast, infrastructure-vehicle unicast (IVU) and vehicle-vehicle unicast (VVU) employ unicast communications between OBUs and/or RSUs to enable commercial and comfort applications. In this context, it is necessary to ensure the confidentiality of the communications, in addition to the other security requirements that are listed in Table 3.

Table 4. Impact of attacks *versus* compromised security services.

Compromised Security Services / Attacks	Availability	Authentication	Non-Repudiation	Integrity	Privacy	Confidentiality
Denial of service attacks (DoS)	✓					
Jamming attack	✓					
Sybil attack	✓	✓				
Variants of DoS (greedy, Black hole, gray hole, sink hole Wormhole, malware, masquerading Spamming, tunneling)	✓	✓	✓	✓	✓	
Loss of event traceability			✓			
Illusion		✓		✓		
Replay		✓		✓		
Key and/or certificate replication		✓				✓
GPS spoofing/position faking		✓			✓	
Message tampering/ suppression/fabrication/alteration	✓		✓	✓		
Broadcast tampering				✓		
Node impersonation		✓	✓	✓		
Brute force						✓
Eavesdropping						✓
Traffic analysis					✓	✓
Tracking/social engineering					✓	
Timing attack	✓					
Man in the middle attack		✓	✓	✓		

4.4. Classification of ITS Attacks and Cryptographic Countermeasures

ITS applications are susceptible to several kinds of threats and attacks, as shown in Figure 8, such as passive and active attacks. While the passive attacks seriously impair the confidentiality and privacy of the network, the active attacks can damage the network resources and functioning, by inserting, deleting or modifying the exchanged packets. Several classifications of these attacks have been proposed in

the literature [18,50]. As in [13], this section adopts a cryptography-based classification to classify all of the major ITS attacks and to analyze the existing cryptographic countermeasures. Indeed, modern cryptography offers a variety of security methods that can be used to ensure the aforementioned ITS security requirements, such as encryption and decryption algorithms, key generation and exchange protocols, hash functions, digital signatures and many others. In the following, we analyze in detail the attacks and countermeasures on the availability, authenticity and identification, integrity and data trust, confidentiality, privacy and non-repudiation security requirements, as listed in Table 4.

4.4.1. Attacks on Availability and Countermeasures

The availability of ITS systems is mandatory to ensure the safety of the involved drivers and vehicles. In this context, denial of service (DoS) attacks are currently recognized as the most dangerous threat to the availability of ITS systems, due to their major impact on the network resources. Indeed, the main objective of these attacks is to prevent legitimate users from using the network services and resources [18]. This kind of attack can be realized in the network by internal or external malicious nodes [51]. Moreover, an important variant of DoS attacks is the distributed denial of service (DDoS) attack [52], which is a distributed attack ordered by an attack manager with other agents who may be also victims unknowingly. In the following, several examples of intentional DoS and DDoS attacks are described, along with their corresponding countermeasures.

- Jamming attacks: This kind of attack is realized at the physical layer, and its goal is to disrupt the communication channel [53] by transmitting noisy signals with high frequency, so as to increase the interference level. This leads to attaining a lower signal-to-noise ratio (SNR) and makes the vehicles unable to communicate with other vehicles and RSU stations [54]. The effects of jamming can be detected using specific techniques [53,55] and can be mitigated, for example, by randomizing the frequency hopping spread spectrum (FHSS) mechanism of the orthogonal frequency-division multiplexing (OFDM) standard [56], using efficient pseudo-random generator algorithms;
- Flooding attacks: This type of attack consists of flooding the network with a huge volume of dummy messages that are intentionally generated by malicious nodes [57], making thus the OBUs and RSUs unable to communicate over the wireless channel. This can lead, for example, to accidents if the basic safety messages are not received in time by the legitimate vehicles;
- Sybil attacks: The main goal of Sybil attacks is to jam the network by employing false nodes identities [16,58]. Therefore, legitimate vehicles conclude that the malicious messages are coming from legitimate vehicles and cannot detect the real identities of the attackers. To overcome this attack, a central validation authority (CVA) can be deployed to validate the entities in real time. The process of validation can be direct or indirect: for the direct one, any incoming node should authenticate itself with the CVA by establishing a direct connection. On the other hand, indirect validation enables an already authenticated entity to accept an incoming entity. The certificates that are used by the CVA are generally temporary [17]. Moreover, the authentication process should be further strengthened by using distance bounding protocols, such as the bit commitment and

zero-knowledge methods [59]. Furthermore, other solutions to Sybil attacks consist of validating unknown nodes with the method of secure location verification [60];

- Malware attacks: Malware attacks consist of virus, worms and Trojan horses that can affect the vehicular network [51], as well as the software components of the OBU and RSUs [17,18]. Such attacks can lead to dangerous consequences for ITS systems and can be mitigated by using anti-virus and anti-malware software. However, modern polymorphic and/or metamorphic malware can transform their structures and properties during the replication phase, thus making their detection much more difficult [61]. The typical cryptographic countermeasure consists of signing software updates and to verify them prior to their installation by the ECUs and OBUs;
- Spamming attacks: The main goal of spamming attacks is to consume the network bandwidth and to introduce a high latency in the network, by sending spamming messages (e.g., advertisement messages) to a group of users. The control of this type of message is more difficult [18,51], due to the lack of centralized infrastructure [62];
- Black hole attacks: The black hole attack exists in any kind of *ad hoc* network, including ITS, and is considered as a conventional attack against availability. In fact, a black hole is formed within the network when malicious nodes fail or refuse to propagate messages. The black hole attack means that the malicious node indicates that it is part of the network and is able to participate, while this is not the practical case [17,51]. This kind of attack is very dangerous for several ITS applications, especially for latency-sensitive road safety applications;
- Gray hole attacks: The gray hole attack is considered a variant of the black hole attack and consists of dropping the data packets related to specific ITS applications [63] during the routing process;
- Sink hole attacks: The sink hole attack can be used to prepare other attacks, such as gray hole and black hole attacks. In this attack, the packets of neighboring nodes are transmitted through malicious nodes, which can lead to eliminating or modifying the received packets before re-transmitting them eventually;
- Worm hole attacks: The worm hole attack is a DoS attack that requires the participation of at least two nodes, where an attacker 'A' sends a message to an attacker 'B', who is geographically far from him. This message suggests to neighboring nodes of 'B' that 'A' is their neighbor [64]. This attack allows two or more legitimate nodes and non-neighbors to exchange control packets between them [65] and to create non-existent routes;
- Tunneling attacks: The tunneling attack is similar to the worm hole attack [51] with the minor difference that it uses the same network to establish a private connection (or tunnel). It aims at connecting two distant parts of the vehicular network by using an additional communication channel, such as a hidden tunnel [66]. Thus, the victims of two distant parts of the network can communicate as neighbors.

Cryptographic solutions are generally not efficient to circumvent the attacks on availability (*i.e.*, greedy, black hole, gray hole, sink hole, worm hole, malware, masquerading, spamming and tunneling). However, as shown in Figure 8, some cryptographic methods, such as digital signature algorithms and bit-commitment schemes, can limit their impact.

4.4.2. Attacks on Authenticity/Identification and Countermeasures

Authenticity is a key requirement in ITS systems to ensure the protection of the legitimate nodes against several attacks, including black holes, spoofing and replay attacks. The digital signature represents the most commonly-used cryptographic countermeasure for ensuring the authentication of the ITS entities. It allows the receivers to verify the origin of the data. Only the authenticated nodes can access the ITS resources and services. Any weakness in the process of identification and/or authentication can expose the entire network to serious consequences. Indeed, external or internal attacks can be achieved using falsified identities [51]. In the following, several examples of attacks on authentication are described along with their corresponding cryptographic countermeasures.

- Falsified entities attacks: In the falsified entities attack, the attacker obtains a valid identifier and passes for another legitimate node. This constitutes a violation of the authentication process. Every ITS entity has a network identifier, which allows distinguishing it from the other nodes of the ITS system [17]. For example, rogue access points (AP) can be deployed along the roads to mimic legitimate RSUs and to launch attacks on the associated users and vehicles [67]. This attack can be prevented by implementing proper authentication mechanisms, for example by using a public key infrastructure, where each ITS entity is associated with a valid certificate, which is signed by the ITS authority;
- Cryptographic replication attacks: In this kind of attack, keys and/or certificates are duplicated to create ambiguity. This can prevent the authorities from identifying a vehicle, especially in the case of a dispute. The first countermeasure consists of the use of certified and disposable keys to resist these attacks. Another solution is the real-time verification of the certificate validity through a certificate revocation list (CRL) [47,68]. However, this solution is challenging in the context of ITS, since it requires cross-certification trusts between the different certification authorities involved in the ITS security scheme [68];
- GNSS spoofing and injection attacks: In ITS, position information is of crucial importance and must be accurate and authentic [18]. Such information is generally obtained from Global Navigation Satellite Systems (GNSS). In this context, the GNSS spoofing and injection attack is considered as the most dangerous threat on cooperative ITS [15]. It consists of providing the neighboring vehicles with false location information. The exact location information is generally obtained from a GPS system. Each vehicle is equipped with a GPS receiver, then the attack can be achieved using a transmitter generating localization signals stronger than those generated by the real GPS satellites [17,69]. The successful GPS spoofing attack can facilitate other attacks, such as attacks against location-based identification methods. This attack can be prevented by using bit commitment and signature schemes with positioning systems that accept only authentic location data [59,70];
- Timing attacks: In ITS safety applications, the timely delivery/reception of safety messages is of prime importance to ensure the safety of drivers and passengers. In this context, the timing attack consists of delaying the transmission of latency-sensitive messages so that the safety requirements are not achieved [71]. This attack can be enabled by forcing legitimate ITS entities to transmit their messages through a malicious node or tunnel, which will delay the reception of these messages

by the other legitimate entities. The most common countermeasure consists of time-stamping the delay-sensitive packets at the cost, however, of more complex time synchronization mechanisms.

4.4.3. Attacks on Integrity/Data Trust and Countermeasures

The main goal of integrity protection is to ensure that the exchanged messages are not altered during their transmission by malicious users. Moreover, it gives the ability to resist destruction, unauthorized creation and alteration of data. Several methods can be used to violate the integrity property, and consequently, the protocol would be deemed flawed [72]. The main cryptographic solution consists of appending a signature to each exchanged message. However, this kind of protection cannot be applied when a data aggregation process is applied. A legitimate node within a network can be vulnerable to both external and internal attacks. The effect of external attacks remains small in comparison with the effect of internal ones (*i.e.*, authenticated attacker). Cryptographic hash functions form the essential solution for integrity problems. In the following, several examples of integrity attacks are described briefly with their countermeasures.

- Masquerading attacks: This kind of attack is hidden, uses a valid identity (known as a mask) to ensure that it has the appearance of an authentic node, tries to produce false messages and broadcasts them to neighbor vehicles in order to attain specific objectives, for example to slow down the speed of a vehicle. A malicious node attempts to act as an emergency vehicle and, thus, cheats the other vehicles. To overcome this attack, a certificate revocation list (CRL) is used to maintain the identities of the detected malicious vehicles, which is furthermore distributed to the overall nodes within the ITS network. Even though this solution can reduce the effects of the masquerading attack [47], it requires the implementation of an efficient malicious nodes detection technique;
- Data playback attacks: This attack consists of replaying (broadcasting) a previously transmitted message [73], for example to manipulate the vehicle location and/or the nodes' routing tables [51]. To provide robustness against this kind of attack, a cache can be implemented at the OBUs and RSUs stations to compare the recently received messages with the oldest ones in order to reject the duplicated messages (e.g., based on sequence numbers or timestamping information). Moreover, secure session tokens can be generated to uniquely identify a communication session between two legitimate entities, and nonces (*i.e.*, a random number used only once in cryptographic systems) can be exploited to ensure that each message is processed only once;
- Data alteration attacks: This kind of attack consists of breaking the integrity of the exchanged messages by modifying, deleting, constructing or altering their content [66]. Additionally, it can affect the availability and the non-repudiation services. The attacker falsifies received messages to achieve its own benefits by leading the driver to change the decision, such as by indicating that a given route is congested or not. Another dangerous threat consists of the injection of false safety messages, thus impacting the safety of the drivers and vehicles [15]. Several techniques can be employed to overcome this threat, such as vehicular public key infrastructure (VPKI) or zero-knowledge to ensure the authentication between vehicles and for signing ITS messages [74,75]. Another efficient method consists of establishing group communications,

as discussed in [75,76], where the keys can be managed by a group key management (GKM) system [77]. This means that an intruder should not be able to communicate with the group members;

- Map database poisoning attacks: Based on the exchanged messages (e.g., broadcast safety messages), each OBU builds and maintains a local map database to keep track of all surrounding vehicles, events and points of interest. This attack consists of sending malicious messages to impact the accuracy of the local map databases of ITS entities and, thus, to impact the safety of ITS applications and users. The main countermeasure consists of verifying the signatures of the received messages and detecting and blacklisting the misbehaving nodes;
- Data tampering attacks: This attack can be realized by a legitimate node, can destroy the network and causes dangerous consequences, such as accidents [51], by fabricating and broadcasting false messages. Its mechanism consists of hiding the true safety messages to legitimate users and tries to generate and inject fake security alert messages in the network. The main countermeasure is to sign and verify the transmitted messages. A non-repudiation mechanism is also required to detect the attacker identity, which should be added to the CRLs [51];
- Man-in-the-middle attacks: The man-in-the-middle attack can be achieved in several contexts. As its name indicates, the attacker is inserted between the transmitter and the receiver. In the case of ITS, the attacker can be an OBU or RSU, which is inserted between two vehicles that communicate. The attacker controls the communication between the two victims [17], while they believe that they are in direct communication with each other. In the literature, the man-in-the-middle attack is used to violate the authentication, integrity and non-repudiation mechanisms. A typical cryptographic countermeasure consists of using digital certification to properly authenticate the legitimate users [78].

4.4.4. Attacks on Confidentiality and Countermeasures

The confidentiality of ITS messages can be required by some specific applications, for example to provide secure toll payments and Internet services by encrypting the messages transmitted between vehicles and RSUs [18]. However, if the exchanged messages do not contain any sensitive information (e.g., ITS safety messages), the confidentiality is not necessary [47,79]. Several attacks can affect the network during the absence of confidentiality protection mechanisms [51]. In the following, several examples of these attacks are described briefly with their countermeasures.

- Eavesdropping attacks: An eavesdropping attack affects only the network confidentiality and does not impact the network resources and availability [18]. This kind of attack enables the attacker to extract sensitive information from the transmitted packets, such as the location information of the vehicles. To provide resistance against this kind of attack, all sensitive data that have crucial importance should be encrypted so as to ensure the privacy of the involved ITS entities and their communications;
- Data interception attacks: This attack affects the user privacy in addition to confidentiality. This attack is dangerous and consists of listening to the network for a certain duration and then tries to analyze the collected traffic data to extract the maximum amount of useful information. The same

countermeasure that permits providing resistance to eavesdropping can be adopted to resist traffic analysis attacks;

- Brute force attacks: The brute force attack can be performed against the confidentiality of exchanged messages or the authentication process. For example, this attack can reveal the network identifier of the vehicle by using an extensive dictionary search approach. However, due to the dynamic nature of the ITS network, connection times are relatively short, and hence, a brute force attack is not easy to conduct, since it is time consuming and resource intensive. Furthermore, this attack can become harder when using stronger encryption and key generation algorithms [51].

4.4.5. Attacks on Privacy and Countermeasures

The privacy of ITS entities and their messages is a key requirement, and all sensitive data should be protected, including the identities of the drivers, their driving behaviors and the historical vehicle locations [80]. However, some ITS road safety applications require the transmission of vehicle-centric data (e.g., location, speed, heading, *etc.*) to notify the surrounding vehicles and infrastructures about potential road hazards. Moreover, when an issue arises (e.g., accidents, road traffic offense, malicious users), the ITS system operators should be able to identify the identities of the involved drivers and vehicles. There is thus a clear trade-off between the privacy and security requirements.

Several attacks on privacy exist [18,76]. One typical attack on privacy consists of the tracking of the vehicles and/or users during their journeys. Indeed, ITS entities are generally equipped with Wi-Fi- or Bluetooth-enabled devices, which broadcast various information in clear text (e.g., identifiers, MAC addresses, devices types, *etc.*). This information can be collected by third party entities to triangulate the positions of users and track their movement within an urban environment. The main countermeasure consists of using randomized and/or temporary identifiers (e.g., MAC and IP addresses) to unlink them from the vehicles and drivers. Another approach consists of the usage of pseudonyms in order to ensure anonymous communications [26,81].

4.4.6. Attacks on Non-Repudiation/Accountability and Countermeasures

Non-repudiation is defined as the impossibility for one of the ITS users involved in a communication to deny having participated in all or part of a communication event. This protects against false denials involved in the communication. Non-repudiation provides the receiver with proof that the sender is accountable for the messages it generated [82]. The main goal of non-repudiation consists of collecting, maintaining, making available and validating undeniable evidence about a claimed event or an action. Non-repudiation depends on authentication, but it generates solid proof, as the system can identify the attackers who cannot deny their crimes [83]. Violators or misbehaving users cannot deny their actions. Any car information (e.g., speed, trip route and violation) will be stored in a tamper-proof device (TPD), and any authorized official will be able to retrieve these data.

4.5. ITS Security Architectures

In the previous sections, the ITS security requirements, attacks and countermeasures were analyzed, and in the following, we will focus on describing global security architectures for ITS.

The current research works classify the ITS security system architectures into three main different cryptography-based categories: (1) public key infrastructure (PKI)-based architectures; (2) crypto-based architectures; and (3) ID-based security architectures; as briefly described below.

- PKI-based security architectures: Public key infrastructure-based architectures rely on asymmetric encryption/decryption algorithms to provide several security services, such as certificates generation, renewal and revocation, signing and issuing, checking and auditing. A certificate provided by a PKI aims to link a public key with the owner's identification and encryption technology. PKI requires the use of a certificate revocation list (CRL) in order to ensure safe and secure management in real network environments. This requirement can be considered as a critical problem and introduces high communication overhead. A detailed list of recent PKI-based security schemes and their evaluation in terms of communication overheads are presented in [84];
- Crypto-based security architectures: Crypto-based approaches are generally based on symmetric and asymmetric security algorithms to provide several security services. For instance, [85] provides a novel ITS security scheme that can provide privacy, data confidentiality and integrity and non-repudiation by using 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 Advanced Encryption Standard (AES) [86];
- ID-based security architectures: In order to cancel the overhead of CRL- and PKI-based approaches, ID-based security architectures can be adopted, in which an encryption algorithm is employed for the generation of pseudonyms. ID-based security method aims to guarantee ID privacy, a precondition for the protection of user safety and privacy. The key point lies in generating irreversible algorithm for pseudonyms based on an ID with firm confirmation that only one pseudonym is available within the same entity to prevent Sybil attacks. Indeed, [87] employs ID-based encryption for pseudonym generation and conducts control of signature and identify authentication through a threshold scheme to satisfy security and privacy requirements. ID-based encryption is also used by [88] to ensure robust and secure V2I, V2V and I2V authentication processes. Finally, ID-based encryption can also be employed to generate the public keys from the entities identifiers [89], reducing thus the overhead of PKI-based solutions.

5. Securing ITS Applications: A Practical Case Study

A careful analysis of the ITS performance and security requirements reveals that these two categories of design challenges are sometimes contradictory. On the one hand, vehicular communications should be efficient and provide real-time performance (*cf.* critical latency in Table 1), but on the other hand, extra processing and messages overheads are required to ensure the security of these communications (as discussed in Section 4). Furthermore, there is still a lack of experimental deployment and performance evaluation of existing standards under realistic conditions, especially regarding the security of V2X communications. In order to elaborate more on this issue, this section analyzes a detailed application case study related to the collision risk warning (CRW) safety application, where vehicles periodically exchange ITS safety messages (or beacons) to detect and prevent the risk of collision between two or more vehicles. In this context, existing standards (*i.e.*, IEEE 1609 [7] and ETSI TS ITS [10]) recommend

the usage of digital signature algorithms (DSA) to ensure the authenticity, integrity and non-repudiation of the exchanged messages.

Without loss of generality, the case study is analyzed in light of the European ETSI ITS reference architecture [10], even though a similar analysis can be made using the IEEE 1609 ITS standard [7,33]. To the best knowledge of the authors, there have been very few works [22,23] that have attempted to evaluate the ETSI ITS security layer. The first implementation was described in [22], where some weaknesses in the early version of the standard were identified and discussed; whereas some preliminary cryptographic performance indicators were presented in [23]. In the following, we extend these works by describing a new implementation of the ETSI TS 103 097 [24] security layer and its integration into an existing standard-compliant V2X platform [90]. Various elliptic curve digital signature algorithms (ECDSA) are then experimentally evaluated for signing and verifying ITS safety messages. Finally, lessons learned are provided to enhance the future versions of the standard and to highlight future interesting research directions.

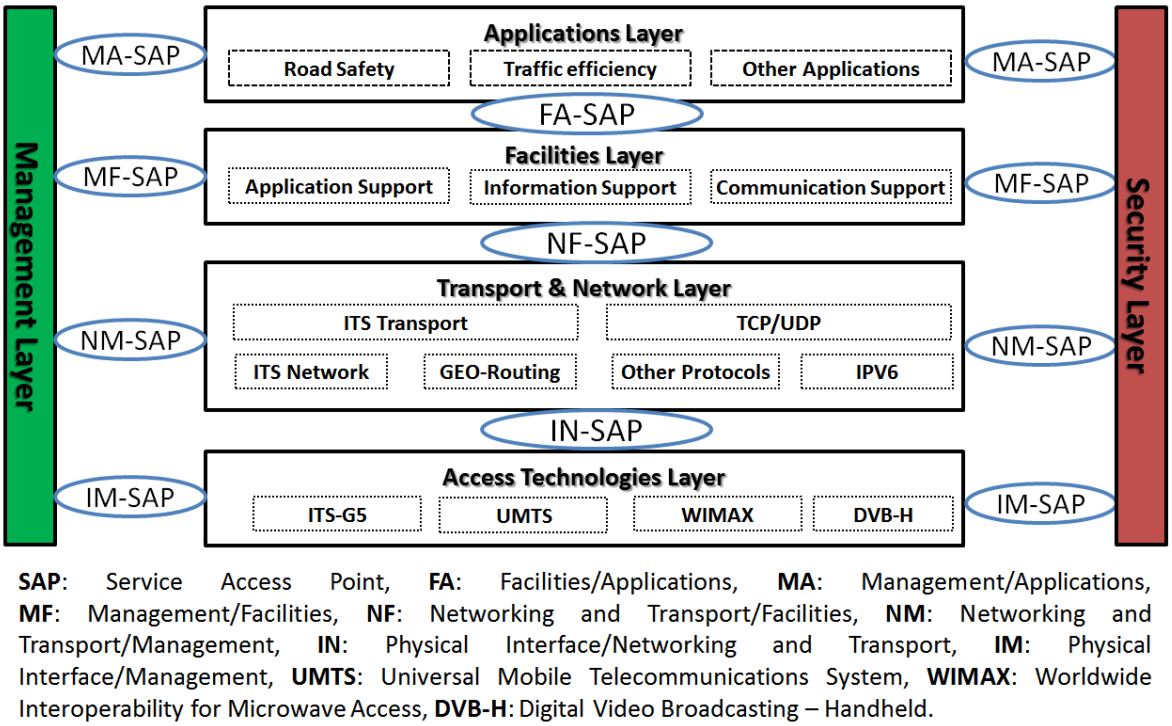


Figure 9. ETSI TC ITS reference architecture.

5.1. ETSI TC ITS V2X Reference Architecture

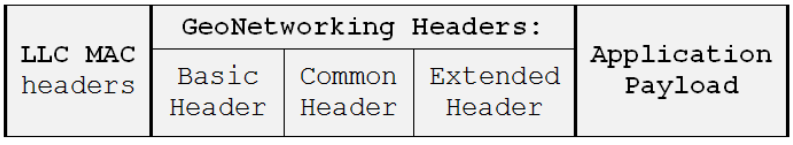
ETSI TC ITS has defined a reference architecture as shown in Figure 9, which is similar to the U.S. Architecture [7,91]. It is based on a slightly modified IEEE 802.11p at the access layer, and enables new networking functionalities based on geographical addressing at the network layer, and new facilities layer on top that enables a set of rich messages that support different types of applications. Compared to the U.S. ITS Architecture, the ETSI TC ITS architecture includes more features at the network layer to support further communication scenarios, such as multi-hop forwarding. The facilities layer

functionalities are very similar in both architectures as most of them have been initially defined by the U.S. standard, then adopted and slightly adapted by the EU standard (ETSI).

V2X is intended to enable critical safety applications first, where vehicles and road infrastructure cooperate by exchanging real-time information to be used for the prediction and the avoidance of accidents and, thus, to improve road safety. This type of application requires fast communication. Once the technology is deployed, it will also open the door to enable new traffic efficiency applications, as well as useful infotainment and added-value applications. The technology will support also the autonomous driving application, as it is important for an autonomous vehicle to communicate with other autonomous vehicles around it to negotiate the sharing of the road resources.

The above applications require well-defined messages that could provide all of the required information in an efficient and reliable meaner. ETSI TC ITS has been working on defining key messages at the facilities layer, such as cooperative awareness messages (CAM) and decentralized environmental notification messages (DENM) [10]. The CAM is intended to be sent by each vehicle at least once every second and at most 10 per second, based on the vehicle dynamics [11]. Each CAM message includes a list of information about the location and status of the vehicle. The CAM exchange enables each vehicle to build a local map about all vehicles in the surrounding. While CAM is a proactive message, the DENM is a reactive message and triggered by an event, e.g., when an accident is detected, a DENM generation mechanism is triggered to initiate a related DENM to inform all vehicles within the relevant geographical area about the accident. As mentioned above, some messages like DENM need to be disseminated within a limited geographical area and to support that there was a need to enable new dissemination algorithms at the transport and network layers. The GeoNetworking functionalities at the network layer of the ETSI TC ITS have been introduced to support geographical-based routing mechanisms where a packet is forwarded based on geographical addressing schemes that use geospatial coordinates.

Figure 10 shows the structure of a standard GeoNetworking packet, where the GeoNetworking header is divided into three mandatory sub-headers, *i.e.*, basic, common and extended sub-headers. One of the motivations for splitting the common header into two sub-headers (*i.e.*, basic and common) is to facilitate the application of security, as explained in the following subsection.



LLC: Logical Link Control, MAC: Medium Access Control.

Figure 10. GeoNetworking packet structure as defined in ETSI TC ITS.

5.2. The Collision Risk Warning Application Case Study

As shown in Figure 11, the case study consists of the collision risk warning (CRW) road safety application, in which a vehicle (or roadside unit) detects the risk of collision between two or more vehicles and broadcasts a DENM message to all of its neighboring vehicles. The overall detection and notification process undergoes fourteen main steps, as described below:

- At time T0, a vehicle (on the left side) performs a sudden and harsh braking due to a detected hazard;
- At time T1, the information related to this harsh braking event is available at the in-vehicle's ECUs;
- At time T2, this information is received by the vehicle's OBU by the corresponding ITS application;
- At time T3, a DENM message is built at the facilities layer, including all of the required information (e.g., timestamp, location, speed, event-type, *etc.*);
- At time T4, the DENM message is received and processed by the networking and transport layer;
- At time T5, the DENM message is signed by the security layer using an elliptic curve digital signature algorithm (ECDSA) [12] and is encapsulated (Encap) into a secured message, which includes the certificate of the ITS station;
- At time T6, the signed DENM message is received again by the networking layer and is queued;
- At time T7, the packet is transmitted over the air by the IEEE 802.11p MAC and PHY layers. Eventually, the packet might be re-transmitted multiple times due to collisions and/or harsh propagation conditions at the PHY layer;
- At time T8, the packet is finally received by a neighbor vehicle's OBU (vehicle on the right side of Figure 2);
- From time T9 to T13, the message undergoes the reverse flow, *i.e.*, the message is decapsulated (Decap) and verified (using ECDSA) by the security layer and is made available to the ITS application layer at time T13;
- At time T14, a warning message is displayed to the vehicle's driver for taking immediate action or an automatic action is triggered by the vehicle's ECUs (e.g., emergency brake, speed reduction, *etc.*).

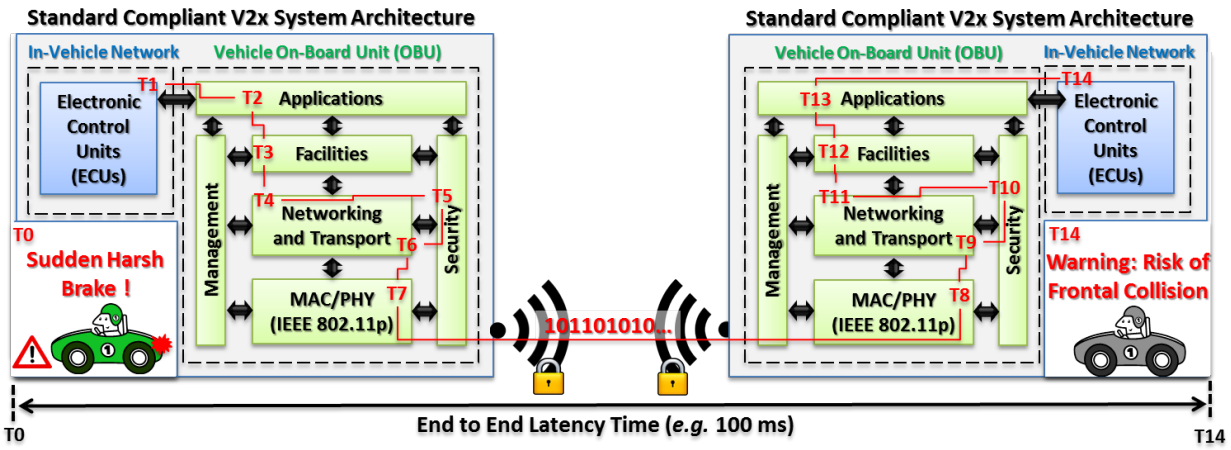


Figure 11. The collision risk warning road safety ITS application case study.

As shown in the above communication flow, the real-time availability and processing of the information is a key requirement, especially in life-threatening scenarios, such as road safety applications. If we assume that the second vehicle (on the right) is driving at 120 km/h (around 33 m/s), while keeping a minimal safe distance of 66 meters with the first vehicle (on the left), the

time-to-collision (TTC) will be around 2 s. This time period corresponds to the minimal time required to perceive a given hazard (*i.e.*, either by humans or machine/ITS-based systems) and to react accordingly in order to avoid the collision. The end-to-end system critical-latency (*i.e.*, $T14 - T0$ in Figure 11) is thus one of the most critical requirements for ITS safety applications.

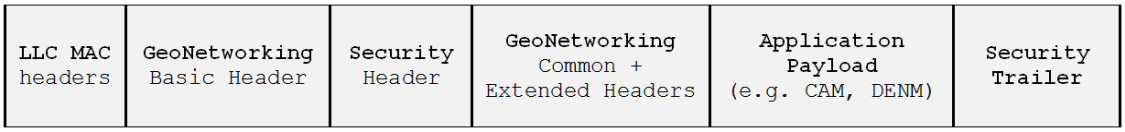
The typical values of such critical-latencies depend mainly on the target ITS use cases, as listed in Table 1, and are mostly impacted by three main factors: (i) the message queuing and QoS management strategy; (ii) the performance limitations of the underlying wireless channel; and (iii) the overhead of the cryptographic operations. For instance, the ETSI standard recommends the usage of the ecdsa_nistp256_with_sha256digital signature schema for signing and verifying safety messages [24] (*i.e.*, DENM and CAM); whereas the IEEE 1609 standard supports the ecdsa_nistp224_with_sha224 schema [92] in addition to the previous one.

5.3. ETSI Security Layer: TS 103 097

ETSI TC ITS defines security as a vertical layer adjacent to the access, networking and facilities layers, as shown in Figure 9. The corresponding security services are provided on a layer-by-layer basis through specific service access points (SAP). In this context, ETSI TS 103 097 [24] specifies the main security components, including the security headers, certificate format and security profiles, and reuses as much as possible the existing IEEE 1609.2 security standard [92]. The remainder of this section provides a high level overview of these security components as defined by the latest specifications of ETSI TS 103 097, which was recently released to the public under Version 1.2.1 [24].

5.3.1. Security Headers

ETSI TS 103 097 [24] defines different security headers and formats to ensure the interoperability of the different elements and security information that are being exchanged between the ITS stations for security purposes. The main security header is the SecuredMessagestructure, which specifies how to encode a generic security message, which is itself encapsulated inside a GeoNetworking packet, as shown in Figure 12.



LLC: Logical Link Control, MAC: Medium Access Control.

Figure 12. Secured GeoNetworking packet structure as defined in ETSI TC ITS. CAM, cooperative awareness message; DENM, decentralized environmental notification message.

As shown in Listing 1, a SecuredMessage starts with a one-octet protocol_version field that should be incremented each time the security standard is updated. The current protocol version is two, as defined by the latest ETSI TS 103 097 [24] specifications. Then, a variable-length vector header_fields is defined, which shall contain the different information required by the security layer [24], such as generation_time (0), expiration (2), generation_location (3), its_aid (5), signer_info (128), encryption_parameters (129),

recipient_info (130), *etc.* Depending on the considered security profile, the sequence of these header fields should be encoded in ascending numerical order of their type values. Next, a message payload is included, which consist of a payload type (*i.e.*, unsecured, signed, encrypted, signed_external or signed_and_encrypted) followed by a variable-length vector containing the actual message payload (e.g., CAM, DENM, *etc.*).

Listing 1: ETSI ITS SecuredMessage structure.

```
Struct {
        uint8  protocol_version;
        HeaderField header_fields<var>;
        Payload  payload_field;
        TrailerField trailer_fields<var>;
} SecuredMessage;
```

According to the latest standard specifications, only one payload can be included in a SecuredMessage. Finally, a variable-length vector trailer_fields is encoded just after the payload. These trailer fields contain security information that is necessary to verify the messages integrity and authenticity using a signature. Depending on the considered security profile, the sequence of these trailer fields should be encoded in ascending numerical order of their type values. It should be noted that the exact content of a SecuredMessage is determined by the corresponding security profile (*cf.* Subsection 5.3.3), which will check its validity, prior to applying any security operations.

5.3.2. Certificate Format

ETSI TS 103 097 [24] proposes a new certificate format that specifies how to encode the different information required by each type of certificate, *i.e.*, root certificate, Authority Authorization (AA) certificate, *etc.*, as described in the ETSI ITS authority hierarchy [93].

Listing 2: ETSI ITS certificate structure.

```
Struct {
        uint8     version;
        SignerInfo   signer_info;
        SubjectInfo   subject_info;
        SubjectAttribute subject_attributes<var>;
        ValidityRestriction validity_restrictions<var>;
        Signature   signature;
} Certificate;
```

As shown in Listing 2, an ETSI ITS certificate starts with a one-octet certificate version field that shall be set to two for conformance with the latest standard specifications [24]. The information of the certificate's signer is then given by the signer_info field, which can be of type self (0), certificate_digest_with_sha256 (1), certificate (2), certificate_chain (3) or certificate_digest_with_other _algorithm (4). Next, the certificate's subject name and type (e.g., root_ca, crl_signer, enrollment_credential, authorization_ticket, *etc.*) are given by the subject_info field; whereas

the certificate's subject attributes are given by the variable-length vector subject_attributes, such as verification_key (0), encryption_key (1), assurance_level (2), its_aid_list (32), *etc.*

The certificate's validity information is then encoded by the variable-length vector validity_restrictions, whose elements can include the time_end (0), time_start_and_end (1), time_start_and_duration (2) and region (3). It should be noted that the elements of the subject_attributes and validity_restrictions fields should be encoded in ascending numerical order of their respective types. Finally, the signature field holds the certificate's signature, which is signed by the certificate authority (CA). This signature is calculated based of the preceding certificate fields.

5.3.3. Security Profiles

ETSI TS 103 097 [24] defines four main security profiles for CAMs, DENMs, generic messages and certificates. In this context, the standard recommends the usage of the ecdsa_nistp256_with_sha256 algorithm, *i.e.*, elliptic curve digital signature algorithm [94] (ECDSA), for signing and verifying these messages and certificates, even though the standard is flexible enough to support other algorithms; however, no further details are given [24]. Each of the above security profiles defines the elements that should be part (or not) of a SecuredMessage, as well as their order and number of occurrences. One of the main difference between the CAM and DENM security profiles consists of the content of the signer_info field. For DENM messages, signer_info should always include one element of type certificate; whereas an element of type certificate_digest_with_sha256 should be included in the normal case for CAM messages. The element of type certificate is typically included in CAMs periodically (every 1 s) or in case a request_unrecognized_certificate is received from a nearby ITS station.

The signature process works according to three main steps:

(1) A message digest is computed using a Secure Hash Algorithm (SHA) with a 256 bits block size (*i.e.*, SHA-256) over the protocol_version, header_fields, payload_field, the length of the trailer_fields and the type of the signature trailer field;
(2) The message digest is then signed using ecdsa_nistp256_with_sha256 and the private key of the ITS station certificate;
(3) The signer information and the generated signature are stored inside the signer_info and signature structures, respectively.

Once a signed message is received by an ITS station, the verification process undergoes three main steps:

(1) The content of the SecuredMessage is checked against the rules of the corresponding security profile;
(2) The certificate is validated against timing, location and security considerations; in case the signer's certificate is unknown, a request_unrecognized_certificate is generated;
(3) The signature of the message is checked using the same steps as in the signature process.

5.4. Test-Bed Platform

In order to evaluate the performance of the ETSI TC ITS security layer under realistic conditions, we have implemented and experimentally benchmarked the aforementioned security headers, certificate and security profiles. We also analyzed the security weaknesses in the existing standard. To the best knowledge of the authors, there have been very few works [95,96] that have attempted to evaluate the ETSI ITS security architecture, especially in terms of achieved cryptographic performances.

The ETSI ITS security layer was implemented in conformance with the latest version of ETSI TS 103 097 [24] and was integrated into an existing standard compliant V2X platform [90]. This platform implements the latest ETSI TC ITS suite of standards, as shown in Figure 9. Our implementation was tested and validated during the fourth ETSI ITS Plugtest event (March 2015) and against the online Fraunhofer FOKUS ETSI TS 103 097 web validator [97]. ETSI TS 103 097 [24] was implemented as a standalone software module and was integrated with the GeoNetworking and facilities layers through standard compliant service access points [98]. In particular, the SN-ENCAP and SN-DECAP service primitives [98] were implemented to enable the above security profiles (*cf.* Section 5.3.3). An SN-ENCAP request is sent from the networking and transport layer to the security entity to request the encapsulation of an outbound message (e.g., CAM, DENM, *etc.*) into a SecuredMessage envelope according to a security profile. The outbound message is secured (signed) and encapsulated into a SecuredMessage (as already described in Section 5.3) and is sent back to the requesting layer. The secured message is then encapsulated into a GeoNetworking packet, which is transmitted over the wireless channel by the MAC layer (e.g., IEEE 802.11p). An SN-DECAP request is sent from the networking and transport layer to the security entity to decapsulate an inbound message from the SecuredMessage envelope. The message payload is extracted, verified and made available to the networking and transport layer.

The elliptic curve digital signature algorithm was implemented using the Bouncy Castle Crypto APIs [99]. For the sake of the completeness of this study, different ECDSA schemas were implemented for signing and verifying CAM and DENM messages: (1) ecdsa_nistp256_with_sha256 in conformance with ETSI TS 103 097 [24]; (2) ecdsa_nistp224_with_sha224 as recommended by the IEEE 1609.2 standard [92]; and (3) three NIST-recommended schemes [94], *i.e.*, ecdsa_nistp192_with_sha256, ecdsa_nistp224_with_sha256 and ecdsa_nistp384_with_ sha384. The SN-ENCAP and SN-DECAP service primitives were benchmarked on two different CPU architectures in terms of achieved operations per second (OPS) for signing and verifying CAM messages (a payload of 100 bytes) in conformance with all of the rules of the CAM security profile [24]. The results were averaged over 1000 iterations within the 95% confidence interval.

5.5. Experimental Results

Figures 13 and 14 provide an overview of the achieved average number of operations per second for the SN-ENCAP and SN-DECAP service primitives [98]. The results suggest clearly that generic automotive processors (around 1 GHz) are able to achieve up to 162 signature generations (SN-ENCAP) per second (around 6.17 ms per operation) and up to 23 signature verifications (SN-DECAP) per second (around 44.03 ms per operation) using the ETSI's recommended signature

schema (ecdsa_nistp256_with_sha256); whereas the IEEE 1609.2 recommended signature schema (ecdsa_nistp224_with_sha224) is able to achieve a slightly higher SN-DECAP operations rate. The best cryptographic performances were obtained using the ecdsa_nistp192_with_sha256 NIST-recommended schema with 41 SN-DECAP and 281 SN-ENCAP operations per second. However, in ITS safety applications, each vehicle is expected to broadcast at most 10 CAM safety messages per second. Depending on the vehicular network density, each ITS station might thus receive several hundred (or thousand) CAMs per second from surrounding vehicles, whose signatures should be verified prior to their exploitation by the higher layers or ITS applications.

In order to achieve an important speedup in handling secure V2X communications, all of the cryptographic operations can be delegated to more powerful CPU architectures or dedicated hardware security modules (HSM). For instance, performance gains of up to 50× can be achieved using a general-purpose 3-GHz Intel CPU, as shown in Figure 14 and Table 5. In this context, ETSI TS 103 097 was found to be achieving 3831 SN-ENCAP operations per second (around 0.26 ms per operation) and 817 SN-DECAP operations per second (around 1.22 ms per operation). Theoretically, this might enable a vehicle to process the CAM messages received from several tens of neighboring vehicles without a major impact on the end-to-end system's critical-latency (around 100 ms for road safety applications). However, when assuming denser urban environments (e.g., 200/400 vehicles per km^2 [100]) combined with more heterogeneous data traffic loads, new lightweight and adaptive security solutions will need to be designed in order to not exceed the maximum allowable critical latencies of ITS safety-critical applications.

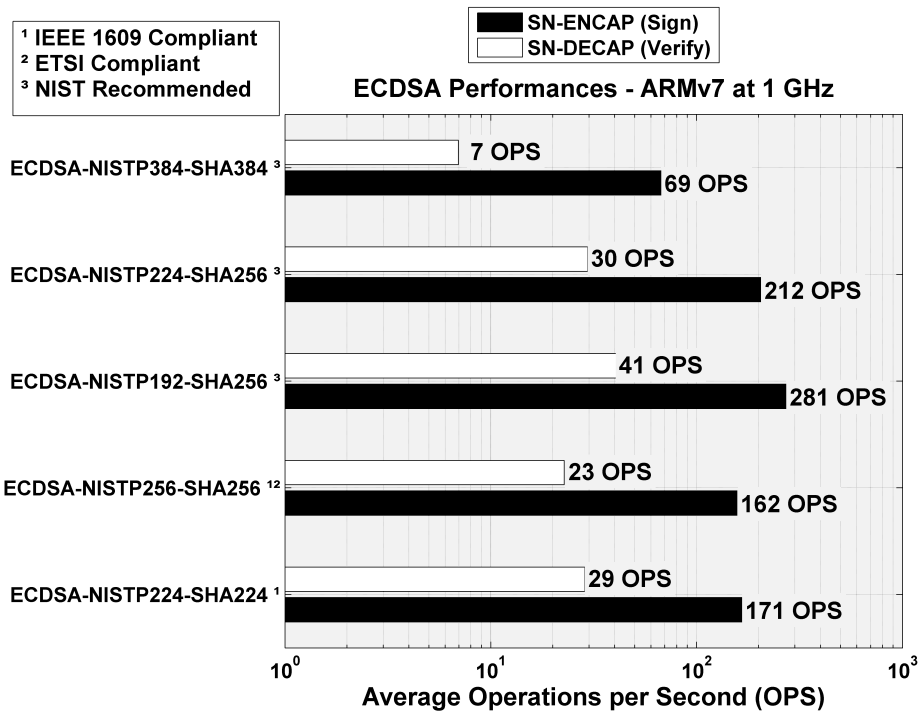


Figure 13. Cryptographic performances of an ETSI ITS security software implementation (ECDSA) running on an ARMv7 CPU at 1 GHz.

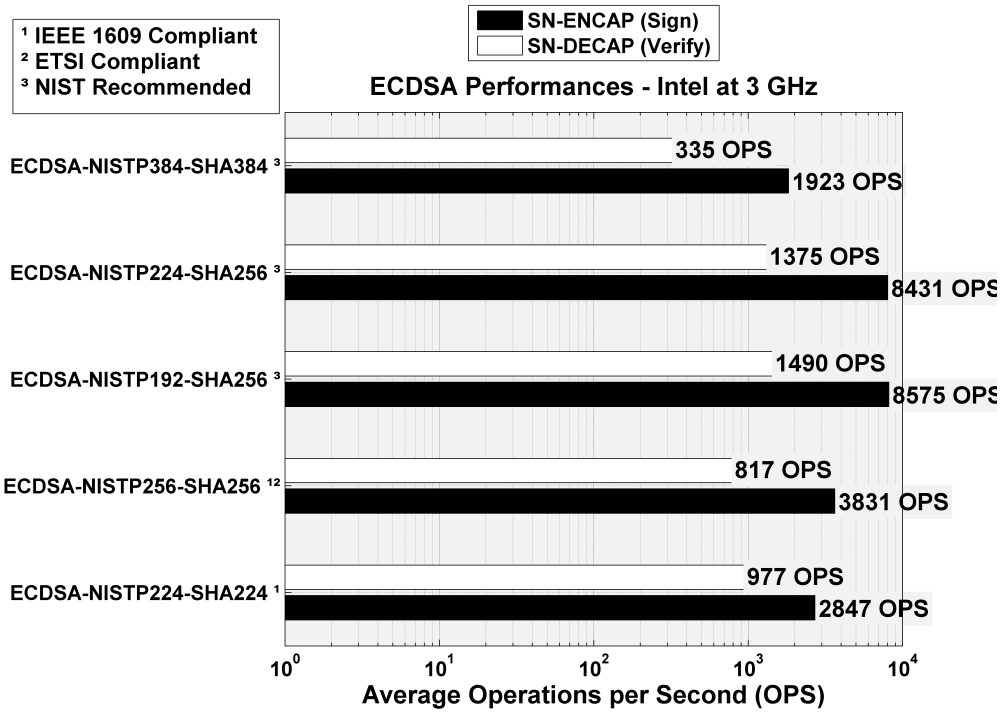


Figure 14. Cryptographic performances of an ETSI ITS security software implementation (ECDSA) running on an Intel CPU at 3 GHz.

Table 5. ETSI TS 103 097 average cryptographic operation delay (milliseconds; 95% confidence interval).

Cryptographic Algorithms	Intel CPU at 1 GHz		Intel CPU at 3 GHz	
	SN-ENCAP	SN-DECAP	SN-ENCAP	SN-DECAP
ecdsa_nistp192_with_sha256	3.56 ± 0.10	24.43 ± 0.23	0.12 ± 0.006	0.67 ± 0.014
ecdsa_nistp224_with_sha224	5.84 ± 0.28	34.91 ± 0.46	0.35 ± 0.022	1.02 ± 0.048
ecdsa_nistp224_with_sha256	4.73 ± 0.17	33.82 ± 0.33	0.12 ± 0.003	0.73 ± 0.013
ecdsa_nistp256_with_sha256	6.17 ± 0.16	44.03 ± 0.31	0.26 ± 0.012	1.22 ± 0.047
ecdsa_nistp384_with_sha384	14.55 ± 0.20	143.63 ± 0.5	0.52 ± 0.019	2.98 ± 0.036

[a] NIST-recommended ECDSA schema. [b] ETSI ITS-compliant ECDSA schema. [c] IEEE 1609.2 compliant ECDSA schema.

5.6. Lessons Learned

During our implementation of the latest version of TS 103 097 [24], we have noticed that the previously identified flaws [95], such as the unbounded limit of the integer variable length structure or the multiple payload support, were already fixed. During the last fourth ETSI Plugtest event, we had not experienced any major flaws with our current implementation, but we will underline below some possible issues or misunderstandings in the current draft document [24]. First, the geographical validation of certificates is not yet very clear; especially the one related to the identified region where no information is

yet available for such structures and for how the received locations will be checked. Second, the signature verification step cannot be achieved until the received packet is parsed. This is due to the fact that the signature structure is dynamic and extendable, so the user should know the trailer field structure before being able to compute the message digest. This may lead to malicious code injection-based attacks, as many of the data structures are of variable lengths.The last point we have encountered is that the ETSI TC ITS security architecture seems to be vulnerable to denial of service (DoS) attacks. As described in the ETSI draft document, the receiver should always send its own certificate (or certificate chain) if it encounters its own certificate hashId8 inside a request_unrecognized_certificate message. Malicious users can thus keep sending forged packets to force the receiver to send its certificate continuously, which could exhaust the local resources and the allocated network bandwidth.

6. Research Challenges and Opportunities

Intelligent transport systems have been an active research area in recent years with great focus. However, there are still a few challenges to be overcome before mass market penetration and deployment of the V2X communications technology.

First, existing ITS systems and standards still have a static selection of the security features. For instance, the ETSI TC ITS standard [24] recommends the usage of the ecdsa_nistp256_with_sha256 digital signature schema for signing and verifying safety messages (*i.e.*, DENM and CAM), and the ecies_nistp_256 (*i.e.*, Elliptic Curve Integrated Encryption Scheme with NIST P-256 curve) public key algorithm and the aes_128_ccm (*i.e.*, Advanced Encryption Standard counter with Cipher Block Chaining Message Authentication Code and a block length of 128 bits) symmetric algorithm for the encryption and decryption of sensitive data. However, as already highlighted in our previous case study (*cf.* Section 5), existing security schema are based on expensive cryptographic overheads and are not able to efficiently handle a large amount of secure messages, without impacting the system's critical latency and, thus, the safety of ITS applications. There is therefore a need for novel ITS security frameworks that can dynamically adapt the security features at runtime, based on context changes [101] (e.g., local network density, wireless channel conditions, available resources, *etc.*) and/or based on required quality of services (e.g., maximal end-to-end latency, packet delivery rates, *etc.*). Such security frameworks could improve the scalability and safety of ITS systems at the cost of lower security overheads.

Another way to achieve an important speedup in handling secure V2X communications is to delegate all of the cryptographic operations to dedicated hardware security modules (HSM) or trusted platform modules (TPM). It is expected that vehicles' OBUs will be equipped with such hardware modules, as security co-processors. As highlighted in our previous case study, the usage of higher CPU frequencies can enable the handling of a higher number of cryptographic operations, such as ECDSA signature verifications. However, the security gain of such an approach is still unclear, and more experimental investigations are needed to better quantify the benefits of such solutions.

Second, the optimal broadcasting of secure ITS safety messages (or cooperative awareness messages) still continues to represent an important research challenge. Indeed, most of the road safety applications rely on these periodic beacons to construct local maps about the surrounding vehicles in order to enable the timely detection of collisions and/or road accidents. However, the underlying IEEE 802.11p layer

is not efficient enough to handle a huge amount of transmissions due to collisions and interference, especially in high density networks. These collisions can lead to multiple packet re-transmissions, thus increasing the system's end-to-end latency. Moreover, the extra security overheads, in terms of packets sizes and security processing times, can also negatively impact the achieved quality of service. In this context, novel message broadcasting techniques are needed [102–104], such as the verify-on-demand (VoD) approach [103], which was proposed for IEEE 1609-based ITS systems and where signed messages are only verified on demand (e.g., based on their impact on the driver's safety). However, the integration of such techniques in ETSI TC ITS-based systems requires further research to better quantify their benefits in terms of achieved safety *versus* security and QoS.

Finally, the safety, security and QoS issues are generally considered as separate aspects of ITS systems and are evaluated independently of each other. In contrast, we believe that there is still a lack of research addressing the development of ITS applications by jointly considering the interplay between safety, security and QoS to limit potential threats to connected vehicles. This motivates the need for the research and development of new ITS applications frameworks, which are able to dynamically adapt these features so as to ensure the safety of the involved vehicles and users. In this context, self-adaptive software solutions can be considered and extended to take into account the specific requirements and challenges of connected vehicles. Self-adaptive software solutions are capable of adjusting their behavior at runtime to achieve certain functional service goals (e.g., quality of service level, safety, *etc.*). A common approach to achieve self-adaptation is the architecture-based approach, which was recently proposed in [105] for self-protecting software that is ale to detect security threats and to mitigate them using runtime adaptation techniques.

7. Conclusions

Cooperative intelligent transport systems (ITS) are currently considered as the key emerging technology to improve road safety, traffic efficiency and driving experience. Even though research on ITS had significantly started more than a decade ago, there are still open research challenges that need to be addressed in order to reach mass market penetration and deployment of such technology. In this context, this article reviewed the current research challenges and opportunities related to the development of secure and safe ITS applications. After a detailed overview of the key ITS architecture, requirements and standards, existing ITS threats and attacks were analyzed and classified, along with their main cryptographic countermeasures. These security algorithms are generally known for their high complexity and communication overhead. In order to better investigate this latter issue, this article analyzed a detailed ITS safety application case study in light of the European ETSI TC ITS standard. Various elliptic curve digital signature algorithms were implemented and benchmarked on different hardware architectures. The results show that existing security standards are still unable to handle secure V2X communications in dense urban environments, without impacting the critical latency of ITS applications. Finally, open research challenges and opportunities were discussed, especially regarding the dynamic adaptation of the security features, the optimal broadcasting of ITS safety messages and the interplay between safety, security and QoS.

Acknowledgments

This article was made possible by NPRP grant No. 7-1113-1-199 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

Author Contributions

This article was prepared through the collective efforts of all of the authors. Wassim Znaidi has made contributions towards the implementation of the ETSI TC ITS security standard and the setup of the experimental test-bed platform. Hassan Noura has made contributions to the sections on ITS architecture, applications, threats analysis and classification. Finally, Elyes Ben Hamida has made substantial contributions towards overall writing, organization and presentation of the paper. In particular, he has contributed to the Introduction, standards, projects, case study, research challenges and opportunities. He also contributed significantly to the implementation of the ETSI TC ITS security standard, the setup of the test-bed platform and the experimental evaluation of the various cryptographic algorithms.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. International Energy Agency—How Many Cars Will Be on the Planet in the Future? Available online: http://www.iea.org/aboutus/faqs/transport/ (accessed on 21 May 2015).
2. World Health Organization (WHO). *Global Status Report on Road Safety 2013*; Technical Report; World Health Organization (WHO): Geneva, Switzerland, 2013.
3. Automobile Association of America—Cost of Auto Crashes and Statistics. Available online: http://www.rmiia.org/auto/traffic_safety/Cost_of_crashes.asp (accessed on 21 May 2015).
4. GSM Association (GSMA). *Connected Car Forecast: Global Connected Car Market to Grow Threefold within Five Years*; Technical Report; GSM Association (GSMA): London, UK, 2013.
5. Sharef, B.T.; Alsaqour, R.A.; Ismail, M. Vehicular communication ad hoc routing protocols: A survey. *J. Netw. Comput. Appl.* **2014**, *40*, 363–396.
6. Da Cunha, F.D.; Boukerche, A.; Villas, L.; Viana, A.C.; Loureiro, A.A.F. *Data Communication in VANETs: A Survey, Challenges and Applications*; Technical Report RR-8498; INRIA Saclay: Palaiseau, France, 2014.
7. IEEE Guide for Wireless Access in Vehicular Environments (WAVE)—Architecture. *IEEE Std. 1609.0-2013* **2014**, 1–78. doi:10.1109/IEEESTD.2014.6755433.
8. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. *IEEE 802.11p Publ. Stand.* **2010**, 1–51. doi:10.1109/IEEESTD.2010.5514475.

9. IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2012* **1997**,1–2793, doi:10.1109/IEEESTD.2012.6178212.
10. ETSI—Intelligent Transport Systems. Available online: http://www.etsi.org/technologies-clusters/technologies/intelligent-transport (accessed on 21 May 2015).
11. Festag, A. Cooperative intelligent transport systems standards in europe. *IEEE Commun. Mag.* **2014**, *52*, 166–172.
12. Pietro, R.D.; Guarino, S.; Verde, N.; Domingo-Ferrer, J. Security in wireless ad-hoc networks—A survey. *Comput. Commun.* **2014**, *51*, 1–20.
13. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66.
14. Engoulou, R.G.; Bellaiche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13.
15. Petit, J.; Shladover, S. Potential Cyberattacks on Automated Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 546–556.
16. Vinoth Kumar, P.; Maheshwari, M. Prevention of Sybil attack and priority batch verification in VANETs. In Proceedings of the 2014 International Conference on Information Communication and Embedded Systems (ICICES), Chennal, India, 27–28 February 2014; pp. 1–5.
17. Al-kahtani, M. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In Proceedings of the 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, Australia, 12–14 December 2012; pp. 1–9.
18. Dhamgaye, A.; Chavhan, N. Survey on security challenges in VANET. *Int. J. Comput. Sci. Netw.* **2013**, *2*, 88–96.
19. Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. *Comprehensive Experimental Analyses of Automotive Attack Surfaces*; USENIX Security: San Francisco, CA, USA, 2011.
20. Woo, S.; Jo, H.J.; Lee, D.H. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 993–1006.
21. Amoozadeh, M.; Raghuramu, A.; Chuah, C.N.; Ghosal, D.; Zhang, H.; Rowe, J.; Levitt, K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132.
22. Nowdehi, N.; Olovsson, T. Experiences from implementing the ETSI ITS SecuredMessage service. In Proceedigns of the 2014 IEEE Intelligent Vehicles Symposium Proceedings, Dearborn, Michigan, USA, 8–11 June 2014; pp. 1055–1060.
23. Moalla, R.; Lonc, B.; Segarra, G.; Laguna, M.; Papadimitratos, P.; Petit, J.; Labiod, H. Experimentation with the PRESERVE VSS and the Score@F System. In Proceedings of the 5th Conference on Transport Research Arena (TRA), Paris, France, 14–17 April 2014.
24. ETSI TS 103 097 V1.2.1 (2015-06)—Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats. Available online: http://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.02.01_60/ts_103097v010201p.pdf (accessed on 14 June 2015).

25. Moustafa, H.; Zhang, Y. *Vehicular Networks: Techniques, Standards, and Applications*; Auerbach Publications: Boca Raton, FL, USA, 2009.
26. Cheng, H.T.; Shan, H.; Zhuang, W. Infotainment and road safety service support in vehicular networking: From a communication perspective. *Mech. Syst. Signal Process.* **2011**, *25*, 2020–2038.
27. Raw, R.S.; Kumar, M.; Singh, N. Security Challenges, Issues and Their Solutions for VANET. *Int. J. Netw. Secur. Its Appl.* **2013**, *5*, 95–105. doi:10.5121/ijnsa.2013.5508.
28. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular Ad Hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392.
29. Bhoi, S.; Khilar, P. Vehicular communication: A survey. *IET Netw.* **2014**, *3*, 204–217.
30. Lebre, M.A.; Mouel, F.L.; Menard, E.; Dillschneider, J.; Denis, R. *VANET Applications: Hot Use Cases*; Technical Report hal-01024271; 2014, 1–36. Available online: https://hal.inria.fr/hal-01024271 (access on 6 July 2015).
31. Jadranka, D.; Beate M.; Gereon M. *European Roadmap Smart Systems for Automated Driving*; Technical Report Version 1.2, European Technology Platform on Smart Systems Integration (EPoSS): Berlin, Germany; 2015.
32. Rezgui, J.; Cherkaoui, S.; Chakroun, O. Deterministic access for dsrc/802.11 p vehicular safety communication. In Proceedings of the 2011 7th International Wireless Communications and Mobile Computing Conference (IWCMC), Istanbul, Turkey, 4–8 July 2011; pp. 595–600.
33. 1609 WG—Dedicated Short Range Communication Working Group. IEEE Standards Development Working Group. Available online: http://standards.ieee.org/develop/wg/1609_WG.html (accessed on 21 May 2015).
34. Open Vehicular Secure Platform (OVERSEE). Available online: https://www.oversee-project.com/ (accessed on 21 May 2015).
35. E-Safety Vehicle Intrusion Protected Applications (EVITA). Available online: http://www.evita-project.org/ (accessed on 21 May 2015).
36. Privacy Enabled Capability in Co-operative Systems and Safety Applications (PRECIOSA). Available online: http://www.transport-research.info/web/projects/project_details.cfm?id=44532 (accessed on 21 May 2015).
37. Intellidrive for Safety, Mobility, and User Fee Project: Driver Performance and Distraction Evaluation. Available online: http://www.its.umn.edu/Research/ProjectDetail.html?id=2011091 (accessed on 21 May 2015).
38. Cooperative Systems for Road Safety—Smart Vehicles on Smart Roads (SAFESPOT). Available online: http://www.safespot-eu.org/ (accessed on 21 May 2015).
39. Secure Vehicular Communication EU Funded Project. Available online: http://cordis.europa.eu/project/rcn/80592_en.html (accessed on 21 May 2015).
40. Cooperative Cars and Roads for Safer and Intelligent Transportation Systems (CopITS). Available online: http://www.copits.org (accessed on 21 May 2015).
41. Communications for eSafety (COMeSafety2). Available online: http://www.comesafety.org (accessed on 21 May 2015).

42. Preparing Secure Vehicle-to-X Communication Systems (PRESERVE). Available online: http://www.preserve-project.eu (accessed on 21 May 2015).
43. Advanced Cellular Technologies for Connected Cars (CellCar). Available online: http://www.cellcar.org (accessed on 21 May 2015).
44. Cooperative Systems for Smart Mobility Services and Solutions (CosMob). Available online: http://www.cosmob.org (accessed on 21 May 2015).
45. Security and Safety Modelling (SESAMO). Available online: http://www.sesamo-project.eu (accessed on 21 May 2015).
46. Engineering Security and Performance Aware Vehicular Applications for Safer and Smarter Roads (SafeITS). Available online: http://www.safeits.org (accessed on 21 May 2015).
47. Raya, M.; Hubaux, J.P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68.
48. Vighnesh, N.; Kavita, N.; Urs, S.R.; Sampalli, S. A novel sender authentication scheme based on hash chain for Vehicular Ad-Hoc Networks. In Proceedings of the 2011 IEEE Symposium on Wireless Technology and Applications (ISWTA), Langkawi, Malaysia, 25–28 September 2011; pp. 96–101.
49. Sabahi, F. The Security of Vehicular Adhoc Networks. In Proceedings of the 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), Bali, Indonesia, 26–28 July 2011; pp. 338–342.
50. *Intelligent Transport Systems (Its), Security, Threat, Vulnerability and Risk Analysis (TVRA)*; Technical Report ETSI TR 102 893 V1.1.1; ETSI: Sophia Antipolis, France, 2010. Available online: http://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.01.01_60/tr_102893v010101p.pdf (accessed on 6 July 2015).
51. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241.
52. Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput. Commun. Rev.* **2004**, *34*, 39–53.
53. Tengstrand, S.; Fors, K.; Stenumgaard, P.; Wiklundh, K. Jamming and interference vulnerability of IEEE 802.11p. In Proceedings of the 2014 International Symposium on Electromagnetic Compatibility (EMC Europe), Gothenburg, Sweden, 1–4 September 2014; pp. 533–538.
54. Sumra, I.A.; Ahmad, I.; Hasbullah, H.; bin Ab Manan, J.L. Classes of attacks in VANET. In Proceedings of the 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC), Riyadh, Saudi Arabia, 24–26 April 2011; pp. 1–5.
55. Hamieh, A.; Ben-Othman, J.; Mokdad, L. Detection of radio interference attacks in VANET. In Proceedings of the Global Telecommunications Conference (GLOBECOM), Honolulu, Hawaii, USA, 2009; pp. 1–5.
56. Malla, A.M.; Sahu, R.K. Security attacks with an effective solution for DoS attacks in VANET. *Int. J. Comput. Appl.* **2013**, *66*, 45–49.

57. RoselinMary, S.; Maheshwari, M.; Thamaraiselvan, M. Early detection of DoS attacks in VANET using attacked packet detection algorithm (apda). In Proceedings of the 2013 International Conference on Information Communication and Embedded Systems (ICICES), Tamilnadu, India, 21–22 February 2013; pp. 237–240.
58. Shrivastava, D.; Pandey, A.; others. A Study of Sybil and Temporal Attacks in Vehicular Ad Hoc Networks: Types, Challenges, and Impacts. *Int. J. Comput. Appl. Technol. Res.* **2014**, *3*, 284–291.
59. Wolf, M. Vehicular security mechanisms. In *Security Engineering for Vehicular IT Systems*; Springer: Wiesbaden, Germany, 2009; pp. 121–165.
60. Xiao, B.; Yu, B.; Gao, C. Detection and localization of sybil nodes in VANETs. In Proceedings of the 2006 Workshop on Dependability Issues in Wireless ad Hoc Networks and Sensor Networks, Los Angeles, CA, USA, 29 September 2006; ACM: New York, NY, USA, 2006; pp. 1–8.
61. Zhang, T.; Antunes, H.; Aggarwal, S. Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. *IEEE Internet Things J.* **2014**, *1*, 10–21.
62. Sumra, I.A.; Hasbullah, H.; Ahmad, I.; bin Ab Manan, J.L. Forming vehicular web of trust in VANET. In Proceedings of the Saudi International Electronics, Communications and Photonics Conference (SIECPC), Riyadh, Saudi Arabia, 24–26 April 2011; pp. 1–6.
63. Nogueira, M.; Silva, H.; Santos, A.; Pujolle, G. A security management architecture for supporting routing services on WANETs. *IEEE Trans. Netw. Serv. Manag.* **2012**, *9*, 156–168.
64. Sedjelmaci, H.; Senouci, S. A new Intrusion Detection Framework for Vehicular Networks. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Clayton, Australia, 10–14 June 2014; pp. 538–543.
65. Safi, S.M.; Movaghar, A.; Mohammadizadeh, M. A novel approach for avoiding wormhole attacks in VANET. In Proceedings of the First Asian Himalayas International Conference on Internet (AH-ICI 2009), Kathmundu, Nepal, 3–5 November 2009; pp. 1–6.
66. Rawat, A.; Sharma, S.; Sushil, R. VANET: Security attacks and its possible solutions. *J. Inf. Oper. Manag.* **2012**, *3*, 301–304.
67. Han, H.; Xu, F.; Tan, C.; Zhang, Y.; Li, Q. VR-Defender: Self-Defense Against Vehicular Rogue APs for Drive-Thru Internet. *IEEE Trans. Veh. Technol.* **2014**, *63*, 3927–3934.
68. Raya, M.; Papadimitratos, P.; Hubaux, J.P. Securing Vehicular Communications. *IEEE Wirel. Commun.* **2006**, *13*, 8–15.
69. Warner, J.S.; Johnston, R.G. GPS spoofing countermeasures. *Homel. Secur. J.* **2003**, 1–8. Available online: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-6163 (accessed on 6 July 2015).
70. He, L.; Zhu, W.T. Mitigating DoS attacks against signature-based authentication in VANETs. In Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 25–27 May 2012; volume 3, pp. 261–265.
71. Sumra, I.A.; Ab Manan, J.L.; Hasbullah, H. Timing attack in vehicular network. In Proceedings of the 15th WSEAS International Conference on Computers, World Scientific and Engineering Academy and Society (WSEAS), Corfu Island, Greece, 2011; pp. 151–155.

72. Fuentes, J.M.d.; González-Tablas, A.I.; Ribagorda, A. Overview of security issues in Vehicular Ad-hoc Networks. In *Handbook of Research on Mobility and Computing*; IGI Global: Hershey, PA, USA, 2010.
73. Mikki, M.; Mansour, Y.; Yim, K. Privacy Preserving Secure Communication Protocol for Vehicular Ad Hoc Networks. In Proceedings of the 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Taichung, Taiwan, 3–5 July 2013; pp. 188–195.
74. Blum, J.; Eskandarian, A. The threat of intelligent collisions. *IT Prof.* **2004**, *6*, 24–29.
75. Domingo-Ferrer, J.; Wu, Q. Safety and privacy in vehicular communications. In *Privacy in Location-Based Applications*; Springer: Berlin, Germany, 2009; pp. 173–189.
76. Kaushik, S.S. Review of different approaches for privacy scheme in VANETs. *Int. J. Adv. Eng. Technol.* **2013**, *5*, 2231–1963.
77. Sharma, S.; Krishna, C. An Efficient Distributed Group Key Management Using Hierarchical Approach with Elliptic Curve Cryptography. In Proceedings of the 2015 IEEE International Conference on Computational Intelligence Communication Technology (CICT), Ghaziabad U.P., India, 13–14 February 2015; pp. 687–693.
78. Varshney, N.; Roy, T.; Chaudhary, N. Security protocol for VANET by using digital certification to provide security with low bandwidth. In Proceedings of the 2014 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, India, 3–5 April 2014; pp. 768–772.
79. Pathan, A.S.K. *Security of self-organizing networks: MANET, WSN, WMN, VANET*; CRC Press: Boca Raton, FL, USA, 2010.
80. Badra, M.; Hamida, E.B. A Novel Cryptography based Privacy Preserving Solution for Urban Mobility and Traffic Control. In Proceedings of the 7th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2015), New York, NY, USA, 27–29 July 2015.
81. Priya, K.; Karuppanan, K. Secure privacy and distributed group authentication for VANET. In Proceedings of the 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 3–5 July 2011; pp. 301–306.
82. Armknecht, F.; Festag, A.; Westhoff, D.; Zeng, K. Cross-layer privacy enhancement and non-repudiation in vehicular communication. In Proceedings of the 2007 ITG-GI Conference on Communication in Distributed Systems (KiVS), VDE, Bern, Switzerland, 26 February–2 March 2007; pp. 1–12.
83. Li, Z.; Chigan, C. On Joint Privacy and Reputation Assurance for Vehicular Ad Hoc Networks. *IEEE Trans. Mob. Comput.* **2014**, *13*, 2334–2344.
84. Kortesniemi, Y.; Särelä, M. Survey of certificate usage in distributed access control. *Comput. Secur.* **2014**, *44*, 16–32.
85. Wang, N.W.; Huang, Y.M.; Chen, W.M. A novel secure communication scheme in vehicular ad hoc networks. *Comput. Commun.* **2008**, *31*, 2827–2837.
86. Daemen, J.; Rijmen, V. *AES proposal: Rijndael*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2003.

87. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 584–616.
88. Lu, H.; Li, J.; Guizani, M. A novel ID-based authentication framework with adaptive privacy preservation for VANETs. In Proceedings of the Computing, Communications and Applications Conference (ComComAp), Hong Kong, China, 11–13 January 2012; pp. 345–350.
89. Sun, J.; Zhang, C.; Zhang, Y.; Fang, Y. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Trans. Parallel Distrib. Syst.* **2010**, *21*, 1227–1239.
90. Menouar, H.; Filali, F.; Abu-Dayya, A. Experimental evaluation of 5.9 GHz link asymmetry using standards-compliant implementation. In Proceedings of the 2013 21st IEEE International Conference on Network Protocols (ICNP), Goettingen, Germany, 7–10 October 2013; pp. 1–6.
91. IEEE Standard for Information technology—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)* **2010**, 1–51. doi:10.1109/IEEESTD.2010.5514475.
92. IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages. *IEEE Std. 1609.2-2013 (Revis. IEEE Std. 1609.2-2006)* **2013**, 1–289. doi:10.1109/IEEESTD.2013.6509896.
93. *ETSI TS 102 941 V1.1.1—Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*; Technical Report; ETSI: Sophia Antipolis, France, 2012.
94. Turner, S.; Brown, D.; Yiu, K.; Housley, R.; Polk, T. Elliptic Curve Cryptography Subject Public Key Information. *Internet Eng. Task Force (IETF)—RFC 5480* **2009**, 1–20. Available online: https://tools.ietf.org/html/rfc5480 (accessed on 6 July 2015).
95. Nowdehi, N.; Olovsson, T. Experiences from implementing the ETSI ITS SecuredMessage service. In Proceedings of the 2014 IEEE Intelligent Vehicles Symposium Proceedings, Dearborn, Michigan, USA, 8–11 June 2014; pp. 1055–1060.
96. Moalla, R.; Lonc, B.; Segarra, G.; Laguna, M.; Papadimitratos, P.; Petit, J.; Labiod, H. Experimentation with the PRESERVE VSS and the Score@F System. In Proceedings of the 5th Conference on Transport Research Arena (TRA), Paris, France, 14–17 April 2014.
97. Fraunhofer FOKUS WebValidator for TS 103 097. Available online: https://werkzeug.dcaiti.tu-berlin.de/etsi/ts103097/ (accessed on 21 May 2015).
98. Draft ETSI TS 102 723-8 V1.0.4—Intelligent Transport Systems (ITS). *OSI Cross-Layer Topis; Part 8: Interface between Security Entity and Network and Transport Layer*; Technical Report; ETSI: Sophia Antipolis, France, 2014.
99. Bouncy Castle Crypto APIs. Available online: http://www.bouncycastle.org (accessed on 21 May 2015).
100. Monteiro, R.; Sargento, S.; Viriyasitavat, W.; Tonguz, O. Improving VANET protocols via network science. In Proceedings of the 2012 IEEE Vehicular Networking Conference (VNC), Seoul, South Korea, 14–16 November 2012; pp. 17–24.

101. Rocha, B.P.S.; Costa, D.N.O.; Moreira, R.A.; Rezende, C.G.; Loureiro, A.A.F.; Boukerche, A. Adaptive Security Protocol Selection for Mobile Computing. *J. Netw. Comput. Appl.* **2010**, *33*, 569–587.
102. Yang, L.; Guo, J.; Wu, Y. Piggyback Cooperative Repetition for Reliable Broadcasting of Safety Messages in VANETs. In Proceedings of the 6th IEEE Consumer Communications and Networking Conference (CCNC 2009), Las Vegas, Nevada, USA, 10–13 January 2009; pp. 1–5.
103. Krishnan, H.; Weimerskirch, A. Verify-on-Demand—A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication. *SAE Int. J. Passeng. Cars—Mech. Syst.* **2011**, *4*, 536–546.
104. Anaya, J.J.; Talavera, E.; Jimenez, F.; Gomez, N.; Naranjo, J.E. A Novel Geo-Broadcast Algorithm for V2V Communications over WSN. *Electronics* **2014**, *3*, 521–537.
105. Yuan, E.; Malek, S.; Schmerl, B.; Garlan, D.; Gennari, J. Architecture-based Self-protecting Software Systems. In Proceedings of the 9th International ACM Sigsoft Conference on Quality of Software Architectures (QoSA '13), Vancouver, BC, Canada, 17–21 June 2013; pp. 33–42.