Cybersecurity in Smart Cities
Technology and Data Security in Intelligent Transport Systems

Nuno Fragoso Falcão

Instituto Superior Técnico (October 2019)

Abstract

With the use of technologies, 'cities' are able to control everything from traffic lights to the distribution of water in the city, traffic, environment, social actions, health, education, urban planning, security and public administration, are some of the main areas of activity.

The implementation of technology also brings other concerns such as data security and vulnerability and the privacy of individuals.

The evolution of Intelligent Transport Systems (ITS) has been accelerated, multifaceted and often based on the technological advances considered revolutionary for the Urban Mobility sector. Recently, the widespread use of ITS in the operation and management of urban mobility is part of everyday life. Numerous tools are now available for a variety of contexts and scales, with applications that directly impact both locally and globally.

This dissertation seeks to analyse the security risk within smart cities. It addresses the theme of what are intelligent transport systems and what are the main solutions to ensure the safety of these systems.

To this end, is performed an analysis and classification of ITS threats. With the help of the NS-3 network simulator to model the ITS communications architecture and the SUMO (Simulation of Urban Mobility) traffic simulator an urban road area scenario was generated. Finally, lessons learned and future research challenges to improve the security of ITS systems are presented.

Keywords:

Smart City; Safety; Privacy; Energy; Transportation; Data; Infrastructures; Mobility; Internet of Things (IoT), Traffic Control; E-Governance, Cybersecurity, Hackers, Intelligent Transportation Systems, SUMO.

1 - Introduction

Smart Cities are cities where digital infrastructure is widely available and provide access to value-added services as well as data analysis tools that will enable greater decision-making, problem anticipation and action. Proactive in managing public resources that have a direct impact on people's lives such as: traffic, environment, social actions, health, education, urban planning, security and public administration. The dangers of cities that have their systems pirated, have increased over the last few years. The aim of this dissertation is to investigate and understand threats, and to help to model and analyse cyber threat attacks in a smart city and in particular, intelligent transport systems (ITS).

Characteristics of a smart city

The key points in a smart city are energy, transport, data, infrastructure, mobility, health, agriculture, home, education, government, mobility, commerce and IoT devices. They have common features that go beyond their political and financial value. They are intelligent spaces characterized by process optimization and efficiency in the use of available resources. Intelligent Transport Systems (ITS) have brought new challenges. Each technology has distinctly available services and tools, not all extending to all cities, although there are a number of sectors on which they are based.

Work organization

This document is organized as follows: Chapter 2 provides an overview of security-related work. Chapter 3 looks at the hierarchy and layers that make up an ITS system, as well as its infrastructure, architecture, applications, and threats. Chapter 4 provides a safety assessment of the technology involved and the data that is part of the intelligent transport system. Chapter 5 explores the main threats and attacks that affect ITS systems by first analysing the ITS entities involved and the profiles of attackers. Chapter 6 will look at the difficulties and opportunities that surround the entire security process of a smart city and presents the main conclusions.

2 - Context and related works

Technology is one of the main aspects in the development of Smart Cities project, acting as an integral part of the various dimensions that encompass this process, facilitating innovation and also the generation, integration and/or modification of new dynamics within cities. Many smart cities are implementing new technologies to generate integrated information systems. These technologies include telecommunications (Wi-Fi, 3/4G, Digital TV), E-Government, E-Health, Creative Economy, Smartgrids, Big Data, IoT and Artificial Intelligence.

Consequences

Nowadays, in Portugal, cities are taking their first steps in smart transport within the concept of smart city. The key points are: city planning and the organization of mobility and transport are changing, with more and more sustainable mobility becoming increasingly favoured. The population living in cities is increasing, with the prospect of a larger population imbalance in the territory. The current public transport offer does not meet the needs of the population, either in terms of range, frequency and quality. The management of urban mobility is not yet done in an integrated method, which is reflected in an increase in the ownership and use of the individual motor vehicle, generating several negative impacts on the environment and on the citizens' quality of life. The transport sector is still excessively dependent on road transport and accounts for 24% of national CO^2 emissions.

Security risk within smart cities

There are some key areas of concern from a cyber-security perspective when it comes to smart cities. Recent DDoS attacks demonstrate the challenge that unprotected IoT devices can create. Smart cities will depend on IoT devices, sensors and a range of smart devices and are likely to have some of the highest and fastest growing IOT device concentrations. The best possible protection against hacking attacks is a security solution built into the IoT application.

The problem of traffic, one of the biggest problems facing large cities, is the concern of traffic congestion, which brings other problems, including ecological and the efficiency of public transport. Also, in this area, technology used in safety, such as cameras, is also used for traffic surveillance and thus can be more effectively monitored, improving the conditions of assistance. Synchronized traffic light timers are also a great help in traffic regulation, adjusting public transport schedules to reduce the amount of congestion. Ecological problems in cities have as their main source traffic congestion on public roads, generating unnecessary and easily avoidable CO^2 emissions and noise pollution. Safety is a very important factor in our daily lives.

Cybersecurity challenges on IoT devices

Homes, cars, public places and other social systems are on the road to full connectivity through the IoT. To benefit from them, the city's infrastructure and services are changing with the new interconnected monitoring, control and automation systems. Intelligent transport accesses a network of interconnected GPS location data for weather and traffic updates. Its implementation is essential for a smart city.

3 - Intelligent Transport Systems (ITS)

ITS are considered as the key technology to improve road safety, traffic efficiency and driving experience. Currently, there is a tendency to implement this new technology in vehicles so that they can communicate not only with hotspots, but also with other nearby entities through direct short-range communications (DSRC), such as vehicle-to-vehicles (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), and vehicle-to-anything (V2X). This new reality of transport systems will leverage different types of vehicular communications (VC) and telematics services to enable the emergence of innovative active road safety applications, driver assistance, mobility and traffic management services.

ITS Definition, objectives and importance

ITS applied to road networks, traffic and transit systems, is used to manage traffic and reduce congestion to enable users to make informed decisions, integrate technologies and knowledge to create and deliver innovative services, improve safety and mobility. and increase the efficiency of existing transport infrastructure.

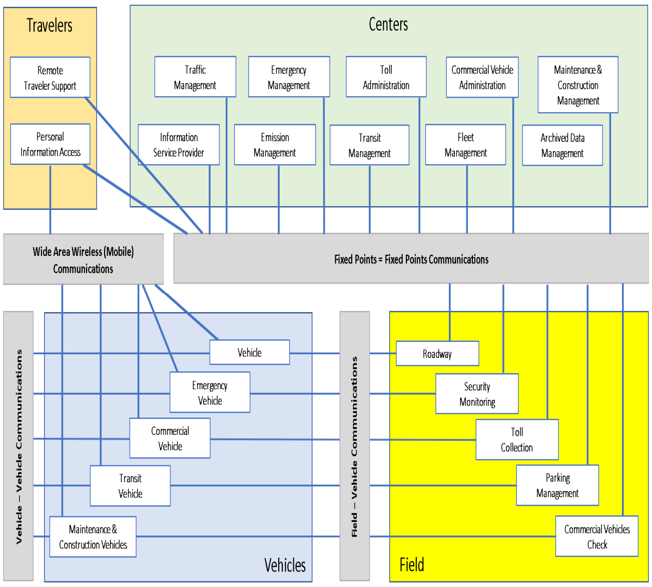

Travelers
Remote Traveler Support
Personal Information Access
Centers
Traffic Management
Emergency Management
Toll Administration
Commercial Vehicle Administration
Maintenance & Construction Management
Information Service Provider
Emission Management
Transit Management
Fleet Management
Archived Data Management
Wide Area Wireless (Mobile) Communications
Fixed Points = Fixed Points Communications
Vehicle – Vehicle Communications
Vehicle
Emergency Vehicle
Commercial Vehicle
Transit Vehicle
Maintenance & Construction Vehicles
Vehicles
Field – Vehicle Communications
Roadway
Security Monitoring
Toll Collection
Parking Management
Commercial Vehicles Check
Field

Figure 1 - USA National ITS Architecture of Transport

Hierarchy and Layers

The ITS architecture provides a framework to guide the planning and implementation of ITS technologies, to continue the evolution of architecture to incorporate technology developments and growing user needs, with a particular focus on connected vehicle requirements and support implementation to assist in the development, maintenance and enhancement of ITS architectures. The architecture framework consists of two technical layers, a transport layer and a communication layer, which must operate in the context of an institutional layer. The transport layer is where transport solutions are defined in terms of subsystems and interfaces and the underlying functionality and data definitions required for each transport service, this layer is the heart of the ITS architecture. This is where the objectives and requirements for ITS are set, traffic signal control system, area-wide signal coordination, arterial network traffic conditions, and rail level crossing system are some of the examples.

ITS Applications

ITS are emerging as a technology that enables the implementation of various applications related to traffic safety, traffic efficiency, information and entertainment. The

ITS high-level architecture comprises three main communication domains, namely vehicle related, V2X domain and infrastructure domain, as shown in the Figure 2.

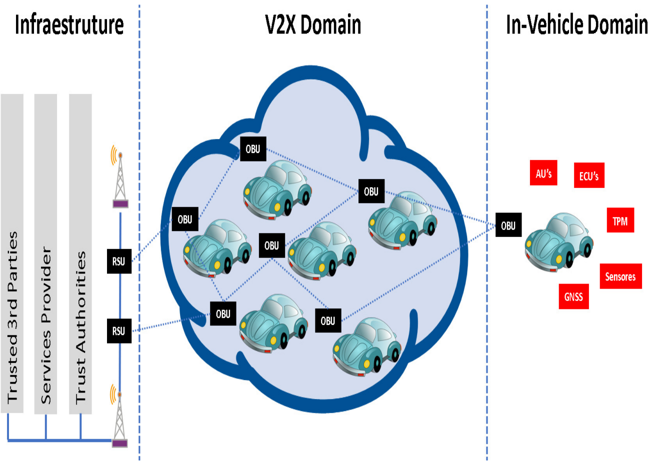


Figure 2 - High level architecture ITS. RSU; OBU, AU; ECU; TPM

The vehicle domain consists of a vehicle equipped with electronic control units (ECU's), wireless enabled onboard units (OBU's), a reliable platform module (TPM) and an application unit (AU). ECU's gather data on vehicle dynamics. ECU's collaborate with the message exchange with OBU and AU and form an on-board network. The AU is responsible for running one or more applications offered by the remote service (SP's) and communicating with other nearby ITS entities using OBU communication features. Each connected vehicle is also equipped with a TPM to enable secure and efficient communications and to manage different keys and certificates.

Finally, a global navigation satellite (GNSS) is used to obtain accurate location information. The V2X domain (or ad hoc domain) consists of an OBU of vehicles and road units (RSU's) available along the road. Information gathered from vehicle OBU's is exchanged in real time with nearby ITS entities (egg OBU's, RSU's, etc.) using various communication technology (V2X) vehicles, including: (a) vehicle-to-vehicle (V2V) communications between neighbouring vehicles (or OBU's) using dedicated short-range communications (DSRC) technology; (b) vehicle-to-infrastructure (V2I) communications between the surrounding OBU's and RSU's, and vice versa; and (c) vehicle-pedestrian (V2P) communications between OBU's/RSU's and surrounding pedestrians. The infrastructure domain includes trusted partners (TTP) such as vehicle manufacturers, service provider (SP's) and trusted authorities (TA). Heterogeneous V2X communication technologies, vehicles operate different types of communication modes such as multi-hop V2V, point-to-point V2I, short/long range V2I, etc.

ITS applications exploit the data gathered to improve vehicle use, driver safety and comfort, and rationalize the use of public infrastructure. They can be categorized into four main classes: (i) entertainment and comfort, (ii) traffic management, (iii) road safety and (iv) autonomous driving applications. As shown in Table 1, critical latency (or end-to-end communication delay) represents one of the most important system requirements for road safety applications, which typically should not exceed one hundred milliseconds.

Table 1 - Typical ITS Applications versus 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	Regulatory speed limit notification	Periodic / permanent message broadcast	From 300m to 5Km	1-10Hz	-
and Management	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			

Traffic data is gathered by the implemented road units and/or road sensors and transmitted to trusted data centers for analysis and processing. The data gathered includes contextual and location-based information related to vehicles, drivers and road events. As shown in the Table 1, these applications rely on periodic transmission of security messages, V2X communications, and/or unicast. Autonomous driving applications represent the next big leap in human transport technologies, which should be fully functional by 2030 [1]. As the Figure 3 shows, future autonomous cars will integrate different technologies.

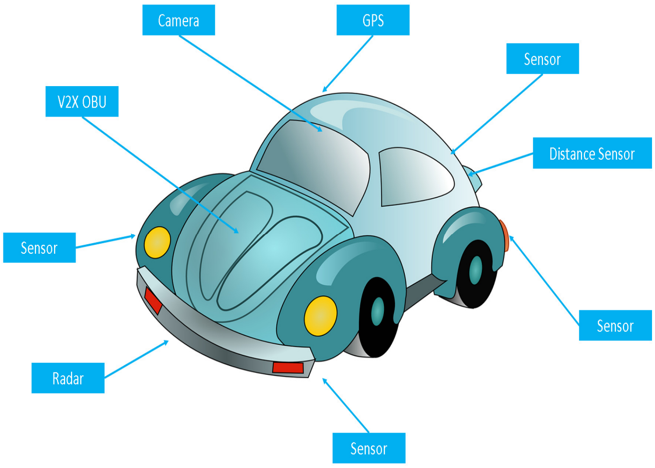


Figure 3 - Key technologies that allow autonomous cars

ITS Infrastructure

The physical components of an ITS infrastructure can be divided into 3 types: field equipment such as inductive loop detectors, magnetic detectors, infrared detectors, acoustic detectors, and video imaging. Wired (fibre optic, twisted pair) and wireless (microwave, radio, mobile technology) communication, Traffic management centre with basic signal control (hardware, software), traffic surveillance, traffic control road, regional control integration, incident detection, incident response, information dissemination, electronic tools and crossing monitor. Connectivity unleashes the potential of automated vehicles.

ITS Security architecture

To efficiently manage ITS security features, WAVE and ETSI standards defined the security architecture. IEEE 1609.2 in WAVE and ETSI TS 103 097 in ETSI specifies key security components, including security headers, certificate format, and security profiles. Security specifications in both standards are similar and suggest the use of Elliptic Curve Cryptography (ECC). ETSI TC ITS defines security as a vertical layer, adjacent to the access, network, and installation layers.

Corresponding security services are provided on a layer by layer basis through specific service access points (SAP). In this context, ETSI TS 103 097 specifies key security components, including security headers, certificate format and security profiles, as well as the existing IEEE 1609.2 security standard.

Security Profiles

The security algorithm analysed in this document is **ECDSA** for signing and verifying exchanged messages whose purpose is to ensure the integrity, authenticity and non-repudiation of exchanged data. In this context, the ETSI TC ITS standard recommends using the ecdsa_nistp256_with_sha256 public key algorithm, even though the standard is flexible enough to support other algorithms. Depending on the ETSI ITS security profile, Secured Message content can also be checked against security profile rules.

ITS Security threats

The use of elliptic curve cryptography (ECC) based algorithms has been proposed for digital signatures and ITS message encryption in these standards. Specifically, for digital signature, the Elliptic Curve Digital Signature (ECDSA) algorithm is an advanced elliptic curve encryption scheme (ECIES) with Advanced Encryption Standard (AES), it is the standard encryption algorithm. Higher packet size increases security packet end-to-end delay and wireless channel occupancy. This can cause congestion, particularly in high density traffic scenarios.

Key standards, vehicles form the core component of ITS along with TCC. Using Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications, important traffic and mobility information is shared between the different components of ITS.

There are currently two main ITS standards known as Wireless Access for Vehicle Environments (WAVE) and European Telecommunications Standards Institute (ETSI) in the United States and Europe, respectively. Both standards define the complete network architecture of MAC/PHY layer functions, network layer transport and mechanism, data traffic and application layer, and security and management procedures for ITS applications.

Vehicles periodically transmit mobility and traffic data between them, these being designated basic safety messages (BSM's) in standard WAVE consent messages and Cooperative Awareness Messages (CAM's) in the standard ETSI. In addition, the ETSI standard defines a special message for warning notification dissemination called decentralized environmental notifications (DENM's).

Using information received in CAM's, each ITS station develops a local dynamic map (LDM), which is a traffic database. With the help of LDM, vehicles can make driving decisions, RSU's can broadcast geographic alert notifications, and CBT can manage city-level traffic. LDM accuracy holds the key to vehicle traffic awareness accuracy.

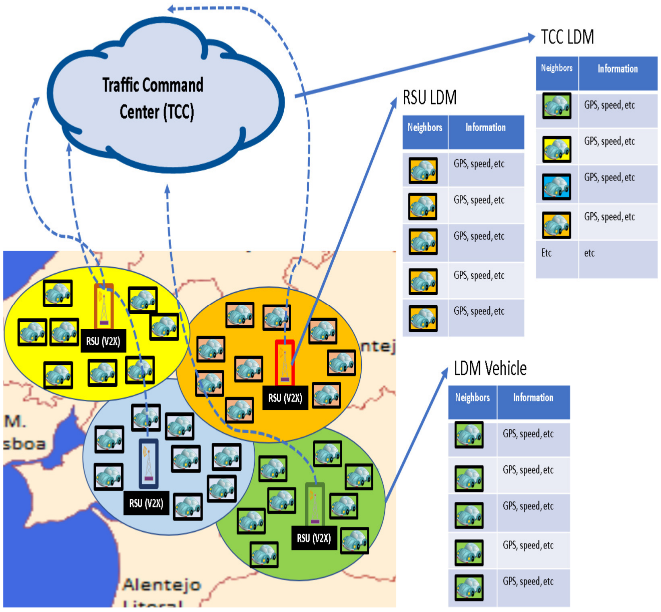


Figure 4 - Local dynamic map based on ITS.

The key requirements for a secure system for secure data transmission are provided through lightweight overload cryptographic algorithms. The list of security attacks, security requirements that mean a threat, and possible countermeasures are shown in Table 2.

Table 2 - Security Attacks, Compromised Security Requirements, and Countermeasures.

Security Attack	Compromised Security Requirement	Countermeasure
Denial of Service (DoS)	Availability	Digital Signature
Jamming, Flooding	Availability	Digital Signature
Sybil	Availability, Authentication	Digital Signature
Malware, Spamming, Black hole, Grey hole, Sink hole, Warm hole	Availability, Authentication	Digital Signature
Eavesdropping	Confidentiality	Encryption
Data Interception	Confidentiality	Encryption
Falsified Entities	Authentication, Authorization	Digital Signature and Encryption
Cryptographic Replication	Authentication, Authorization	Digital Signature and Encryption
GNSS Spoofing	Authentication, Authorization	Digital Signature and Encryption
Timing	Authentication, Authorization	Digital Signature and Encryption
Masquerading	Data Integrity	Digital Signature with Certificate
Data Playback	Data Integrity	Digital Signature with Certificate
Data Alteration	Data Integrity	Digital Signature with Certificate

To overcome these attacks, encryption is required for critical messages with sensitive information.

ITS Security and technology

Current security solutions directly affect quality of service (QoS) and security awareness in vehicle applications, in terms of packet delays, packet loss, cryptographic loss, and reduced security applications. The concept of this system is a vehicle connectivity that forms a Vehicle-Internet (VoI), providing a clear view of road traffic. Together with vehicle-to-vehicle connection, data is gathered from road infrastructure units (MSW) and various other roadside sensors, buildings and humans that constitute a smart city paradigm.

There are many applications in ITS-based smart cities, including cooperative awareness, safe lane shifting, safe intersection, traffic light control, emergency warning notifications, smart parking, and multimedia download from the internet. The participating vehicle is equipped with an on-board computer system, communication interfaces, sensors and user interfaces.

A roadside network infrastructure, called the Road Side Unit (RSU), is also part of Vehicular Ad-Hoc Network (VANET's) and facilitates communication of network nodes and access to the Internet. Additionally, passenger handheld devices and the vehicle system can be connected to the internet via the RSU infrastructure. A management system can be used to control and authenticate the entry of vehicles into the network, especially in the area of computer security, such as cryptographic key distribution and authentication servers. Thus, vehicular networks can be considered as a type of MANET's (mobile ad-hoc network).

The types of communication in vehicular networks can be divided into the following characteristics, Vehicle-Vehicle (V2V), allows direct communication of vehicles without relying on fixed infrastructure support. In this type of communication vehicles can exchange road condition data, detect the presence of other vehicles and even information about vehicles in unsafe movement.

Infrastructure Vehicle (V2I) allows a vehicle to communicate with road infrastructure, so the vehicle can receive information on obstacles and pedestrians, road condition data, announcements and also safety information that will assist in safe driving. Hybrid architecture, combines V2V and V2I solutions. In this case, a vehicle can communicate with the road infrastructure in a single jump or multiple hops according to its location relative to the infrastructure connection point for different purposes. Security is a key challenge in deploying ITS applications.

Vehicle Communication Standards

The WAVE standard is divided into two parts: i) RoadSide Unit (RSU) that can be installed on streetlights, traffic lights and so on; and ii) Onboard Unit (OBU) which are installed on vehicles (car, motorcycle, truck, bus). Parts of the pattern operate independently and vehicles can be organized into small networks called WAVE Basic Service Set (WBSS). The WBSS may consist only of OBU's or a mixture of OBU's and RSU's, as illustrated in Figure 5. Members of a particular WBSS exchange information through some service (SCH) and control (CCH) channels. However, Internet Protocol (IP) packets are allowed only on the SCH channel and vehicles must be members of the same WBSS.

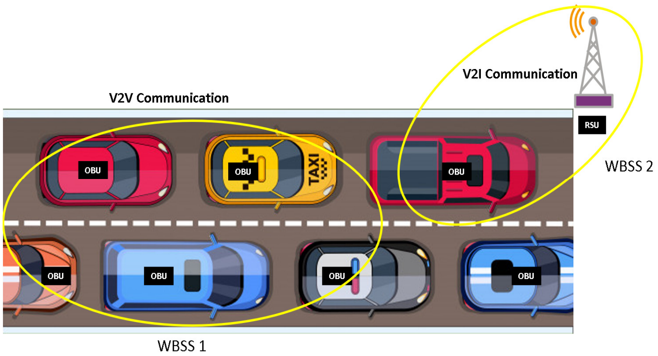
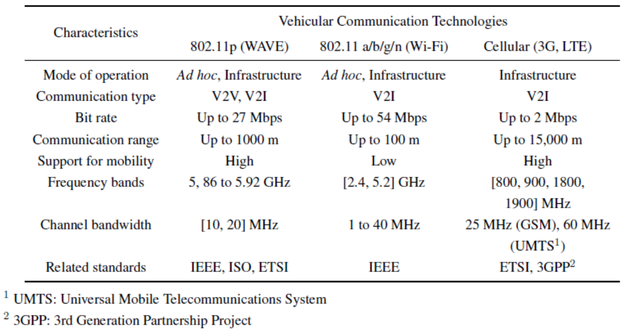


Figure 5 – Standard Communications

Standards and projects

The IEEE 802.11p standard was published in 2010 [2], enabling the use of the 5.9 GHz ITS band to enable V2V communications between highly mobile vehicles and V2I communications between vehicles and RSU's. The IEEE 802.11p standard defines only specifications for basic physical layers (PHY) and Media access control (MAC), as shown in the Table 3.

Table 3 - Major vehicular communication technologies (MAC / PHY).



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

Wireless access in vehicular environments; V2V, vehicle to vehicle; V2I, vehicle for infrastructure

4 – ITS Technology and data security

Intelligent transport has access to a network of interconnected data including features, GPS, vehicle status, weather and traffic updates. Vehicles are data sources from a variety of subsystems that produce different types of information. This data is collected locally, but can also be transmitted and collected in central repositories for analysis and use.

Sources and data types of transport systems

Vehicles and their systems can be an important source of various types of data. Within a car, the various systems represent different data sources with different types of data. Global positioning satellite (GPS) systems for location and navigation and telephone devices and messaging services have become commonplace in vehicles. Some of the sources and types of data these systems collect and store on local instrumentation are OBD/EDR (on-board devices, event data recorders) speed, acceleration, braking, seat belt use, vehicle condition, airbag deployment; telephone and hands-free messaging; GPS navigation systems (trip data, start and end location, backtrack data).

Vulnerabilities and security risks

There are two main security vulnerabilities in smart cities. The first is related to the security of newly installed smart technologies. The second is the security of data generated, stored and shared by these technologies and infrastructures. It is related to the first, because incorrect access to data is usually caused by security deficiencies in the components, architecture and operation of the systems. There are three distinct forms of attacks: availability seeking to close a system or denying service, confidentiality seeking to extract information and tracking activities, and integrity seeking to enter a system to change information and settings (so that components outperform) erasing critical software through malware and viruses).

In general, they seek to exploit one of the top five vulnerabilities of digital technologies that are critical to smart city systems. (1) Poor software security and data encryption (2) Using insecure and poorly maintained legacy systems. (3) Intelligent city systems are generally large, complex and diverse, with many large and complex interdependencies and attack surfaces. (4) The interdependencies between smart city technologies and systems have the potential to create cascading effects where interconnected entities quickly transmit adverse consequences to each other. (5) There are multiple vulnerabilities arising from human error or intentional error. The typical approach to securing smart city systems has been to use a set of well-known technical solutions and software security approaches to try to prevent access and enable recovery. Using these techniques, the goal is to reduce the possibility of attack as much as possible and make the system robust and resilient as possible, as well as quickly recoverable in the event of a failure. Phishing, for example, is a common social engineering technique by which a hacker goes through a reputable person or organization.

Threat modelling

To achieve a goal, an organization must identify the various actors who will ensure that the goal is met or not. The model in Figure 6, shows the concepts and the relationships between them. The threat agent may intend to attack the system and exploit vulnerable points using TTP methods to manipulate it. Requirements are used to ensure the security goal and restrictions are met to meet the organizational goal.

The attacking entity is linked to the threat agent, TTP, risks, and threats because properties determine the nature of the likely attacks and threats. The requirements, risks, controls and reporting of cyber incident can affect the organizational purpose as well as the input and output data. This interrelationship provides evidence of the degree of threat or cascading effect of how a specific risk could impact data. The likelihood of an attack being a likely threat is determined by the threat intelligence gathered.

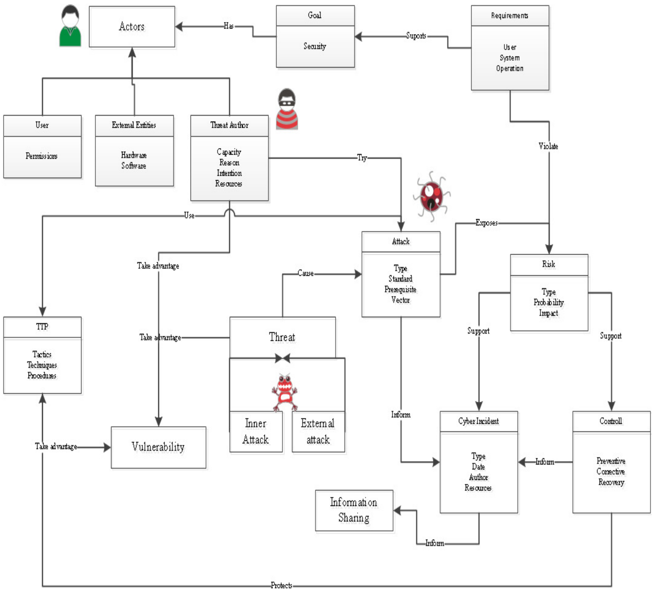


Figure 6 - Meta Model

The underlying process involves a systematic approach to identify the organization's data system, internal infrastructure, business processes, attack context, and relevant controls. The process consists of five main phases, as shown in the Figure 7.

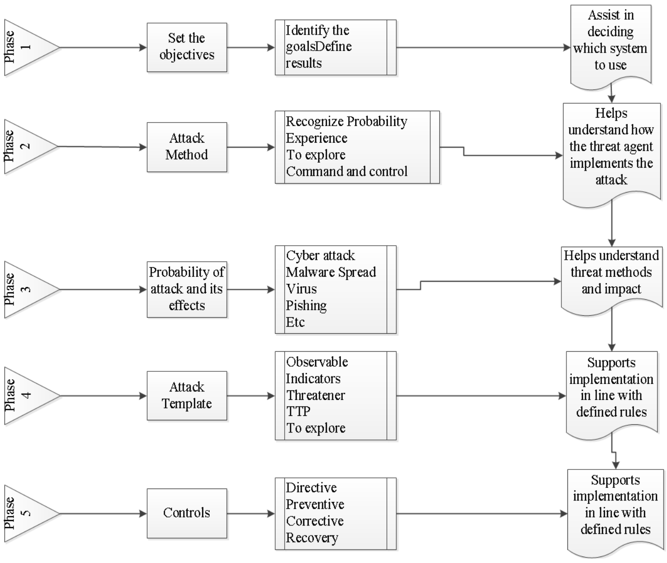

Phase 1
Set the objectives
Identify the goalsDefine results
Assist in deciding which system to use
Phase 2
Attack Method
Recognize Probability
Experience
To explore
Command and control
Helps understand how the threat agent implements the attack
Phase 3
Probability of attack and its effects
Cyber attack
Malware Spread
Virus
Pishing
Etc
Helps understand threat methods and impact
Phase 4
Attack Template
Observable Indicators
Threatener
TTP
To explore
Supports implementation in line with defined rules
Phase 5
Controls
Directive
Preventive
Corrective
Recovery
Supports implementation in line with defined rules

Figure 7 - Threat Model Process

Phase 1, the purpose of this phase is to identify the overall organizational environment, including goals and requirements. It includes two activities, the first consists in identifying organizational objectives. The second is the definition of the results. **Phase 2**, identifies the threat agent's activities and the TTP used to implement the attack. The threat agent explores the organizational system and the information input and output chains, as shown in the Figure 8.

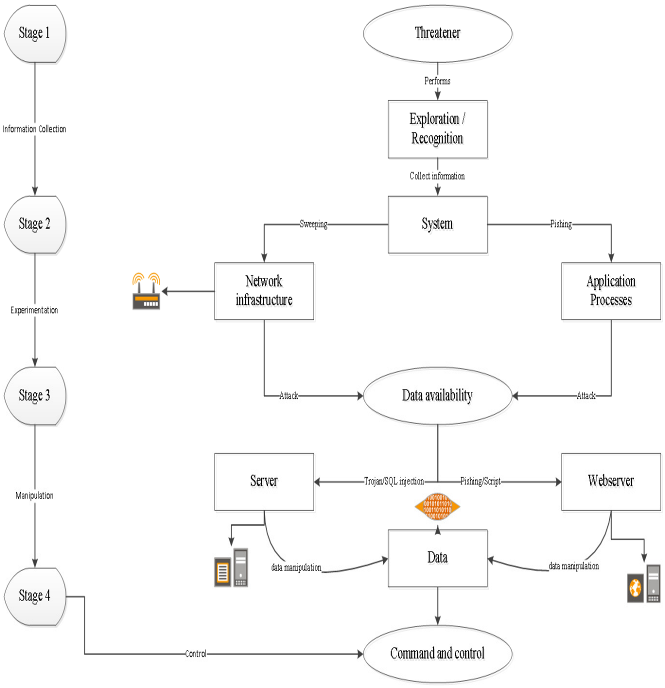


Figure 8 – Attack steps

The attack steps are as follows: reconnaissance, trial, exploit and command and control.

Phase 3, the likelihood of attack and its cascading effects on a cyber-attack. **Phase 4**, threat model, in this phase, can be observed, among others, the following characteristics: observables, indicators, threat agent, exploitation and TTP, to describe the interrelationships and actions that an attack can perform to penetrate and manipulate the system. **Phase 5**, to ensure adequate security controls, a strategic team should be formed to identify, investigate, review and evaluate system processes and applications.

Discussions and conclusions

There are several threats and vulnerabilities that the threat agent can exploit. These attacks include malware, redirection script, or SQL injection. The root causes of these types of attacks may be the motivation and intent of the threat actor, it is possible to use the attacker's implemented TTP to determine the reason and intent. Attacking cyber physical components, opponents can breach source code by using malware or spyware on the system and remotely manipulate software. Threat modelling and analysis examines the various instances of how threat agents pursue and exploit an intent (reasons, opportunities, and methods). The intelligence gathered provides an understanding of the capabilities, actions and intentions of opponents.

This chapter tried to analyse systems security at a general level by considering an attack model using concepts such as objective, agent, attack, and TTP, along with their interdependencies. The objective of the opponent is to penetrate and manipulate data. The motives and methods of the threat actors, as well as the cascading effects of the attacks, were observed. The findings showed that attack modelling and analysis of observed behaviour patterns help to understand security risks.

5 - ITS Threat analysis and classification

This chapter seeks to explore the main threats and attacks that affect ITS systems by first analysing the ITS entities involved and attacker profiles. Then the key ITS security requirements are discussed in more detail and finally, existing ITS attacks are analysed and ranked along with their main countermeasures. There are many threats that can affect its operation and lead to incidents. Figure 9 shows the typical ITS communication scenario. Radio communication can carry telemetry data, audio, video and control information. In addition to what the radio communication link carries, the satellite link allows to carry GPS and weather information. Information routing on the network should be performed by wireless sensors that meet high availability as well as indispensable security requirements [3].

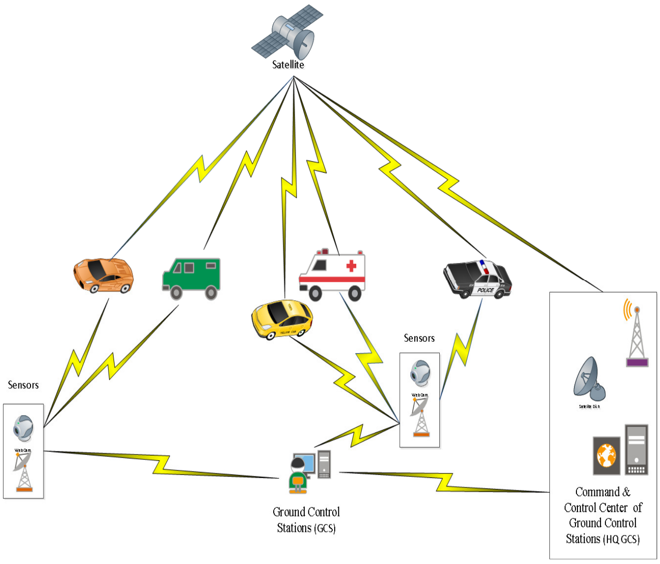

Satellite
Sensors
Sensors
POLICE
Ground Control Stations (GCS)
Command & Control Center of Ground Control Stations (HQ GCS)

Figure 9 - Typical ITS Communication Scenario

Entities involved

The on-board unit (OBU) refers to the driver and the vehicle, the road side unit (RSU), third party entities and attackers. Building ITS applications requires special attention and is characterized by specific challenges and requirements, such as confidentiality, authenticity, integrity, authorization, non-repudiation of origin/receipt, anti-replay, availability and privacy.

Technical approach and modelling

The model can be used as a test for the possibility of system penetration, validating as the system evolves [4].Figure 10 shows a simple model of a vehicle showing some of the various systems involved. The basic ITS model can be defined as a combination of six separate but dependent systems: data acquisition module, reference and location system, NAV (navigation) system, control module, data logging module and module. telemetry [5]. In designing the ITS system architecture, an attempt was made to include all communication channels for the system that are important for safety.

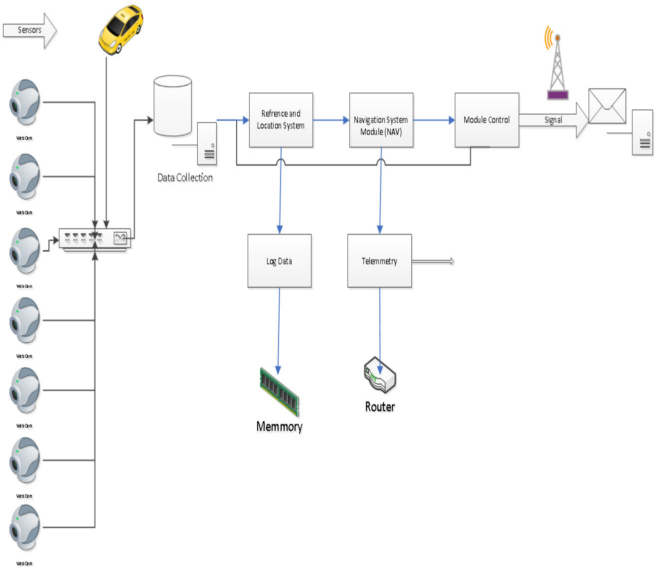


Figure 10 – ITS system Architecture

As can be seen in Figure 11, the different system components rely on wireless communication channels to communicate with each other. Ground control stations (GCS) can be of two types, local or at a station control centre (HQ). HQ GCS may be located in a command and control centre of the relevant agency/department. Portable GCS is a subclass of local GCS that can be Portable Control Stations (smartphones, computers, etc). The link between a satellite and a vehicle is Line of Sight (LOS) radio communication while vehicle-vehicle, PDA-vehicle, and GCS (local) -Vehicle communicate via radio or GPRS/EDGE-based communication using the existing communication infrastructure. Components such as Satellite and HQ GCS may be subject to certain threats, but are not very vulnerable due to security measures in these systems [6].

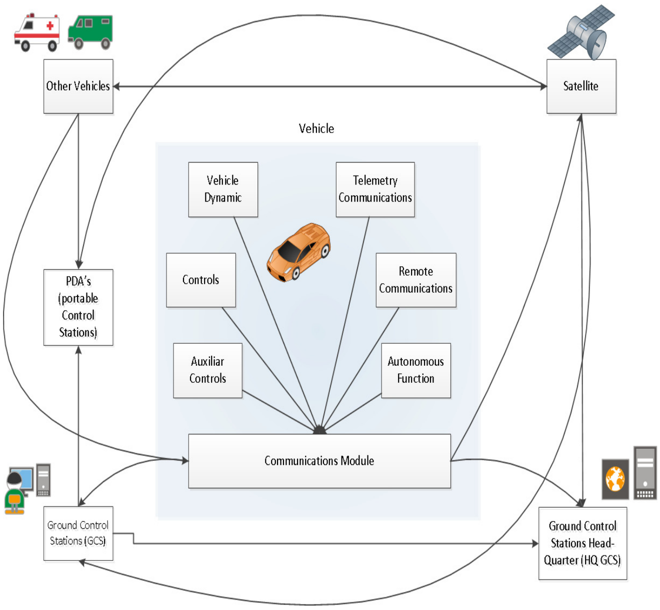


Figure 11 – ITS communication Model

Classification of ITS attacks

Availability attacks, denial of service (DoS) attacks are currently recognized as the most dangerous threat to the availability of ITS systems due to their large impact on network resources. The main purpose of these attacks is to prevent legitimate users from using network services and resources. In addition, an important variant of DoS attacks is Distributed Denial of Service (DDoS) [7], which is a distributed attack ordered by an attacker with other agents who may also be unknowingly victims.

Attacks on authenticity/identification - The digital signature represents the most commonly used cryptographic countermeasure to ensure authentication of ITS entities, allowing recipients to verify the source of data. The integrity of a system can be compromised by using two basic operations, modifying existing information and building new information. The main purpose of integrity protection is to ensure that exchanged messages are not altered during transmission by malicious users. In addition, it gives the ability to resist data destruction, unauthorized creation and alteration. mechanisms. A typical cryptographic countermeasure is to use digital certification to properly authenticate legitimate users [8].

Confidentiality Attacks - ITS messaging confidentiality may be required by some specific applications to provide secure internet payments and services by encrypting messages transmitted between vehicles and RSU's. However, if messages exchanged do not contain confidential information, confidentiality is not required. Privacy Attacks **-** A typical attack consists of tracking vehicles and/or users while traveling. In fact, ITS entities are generally equipped with Wi-Fi or Bluetooth enabled devices, which transmit various information in clear text (egg identifiers, MAC addresses, device types, etc.). The main purpose of non-repudiation is to gather, maintain, make available and validate undeniable evidence about a claimed event or action. Non-repudiation depends on authentication, but it provides solid evidence because the system can identify attackers who cannot deny their actions in this way [9].

Collision Hazard Warning

One vehicle (or unit on the road) detects the risk of collision between two or more vehicles and transmits a DENM message to all neighbouring vehicles. The general detection and notification process can go through fourteen main steps, Figure 12.

At time T0, a vehicle (on the left side) performs sudden braking due to a threat of danger. At time T1, information related to this sudden braking event is available on the vehicle's ECUs. At time T2, this information is received by the vehicle's OBU. At time T3, a DENM message is created at the installation layer, including all information requirements (for example, timestamp, location, speed, event type, etc.). At time T4, the DENM message is received and processed by the network and transport layer. At time T5, the DENM message is signed by the security layer using an elliptical digital curve signing algorithm (ECDSA) [10] and encapsulated (Encap) into a secure message, which includes the ITS station certificate. At time T6, the signed DENM message is received again by the network layer. At time T7, the packet is transmitted by the IEEE 802.11p MAC and PHY layers. Eventually, the packet may be retransmitted multiple times due to collisions and / or severe propagation conditions in the PHY layer.

At time T8, the packet is finally received by the OBU from a neighbouring vehicle (vehicle on the right side of Figure 12). From time T9 to T13, the message is decapsulated and verified (using ECDSA) by the security layer and is made available to the ITS, T13 application layer. At T14, a warning message is displayed to the vehicle driver to immediately take action or an automatic action is triggered by the vehicle's ECUs (egg emergency brake, speed reduction, etc.).

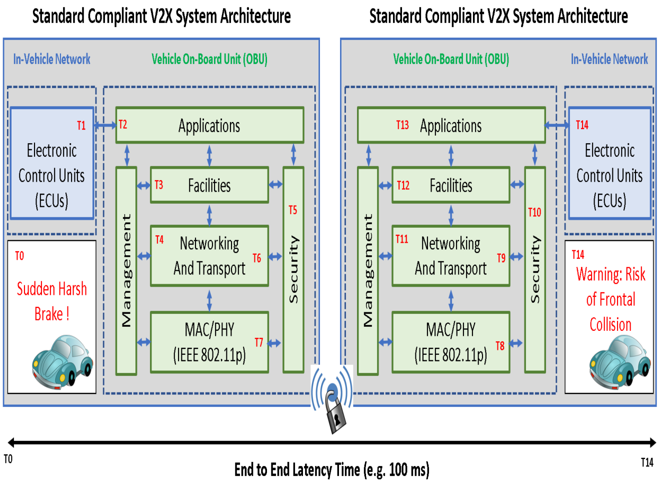

Standard Compliant V2X System Architecture
Standard Compliant V2X System Architecture
In-Vehicle Network
Vehicle On-Board Unit (OBU)
Vehicle On-Board Unit (OBU)
In-Vehicle Network
T1
Electronic Control Units (ECUs)
T2
Applications
T3
Facilities
T4
Networking And Transport
T6
MAC/PHY (IEEE 802.11p)
T7
T5
Management
Security
T0
Sudden Harsh Brake !
T13
Applications
T12
Facilities
T11
Networking And Transport
T9
MAC/PHY (IEEE 802.11p)
T8
T10
Management
Security
T14
Electronic Control Units (ECUs)
T14
Warning: Risk of Frontal Collision
T0
End to End Latency Time (e.g. 100 ms)
T14

Figure 12 - Collision Hazard Warning.

As shown in Figure 12, the availability and real-time processing of information is an essential requirement, especially in life-threatening scenarios. If we assume that the second vehicle (on the right) has a speed of 120 km/h (about 33 m/s), maintaining a safe minimum distance of 66 meters with the first vehicle (on the left), the collision time (TTC) will be about 2 s. This period is the minimum time required to perceive a particular hazard (i.e. by humans or machine-based / ITS systems) and react accordingly to avoid collision.

6 – Assessment and conclusion

With the evolution of technologies, vehicular networks and also the communication of metropolitan networks, it becomes possible to create environments in which vehicles interact with each other and also be influenced by their surroundings. In this context, it is possible to monitor the entire trajectory of vehicles, the density in each region of the city and also the evolution of traffic throughout the day, reacting according to the demand and events of the city.

Smart cities may include services to coordinate traffic lights, parking, location services, weather services, tourist services and emergency services. All services should be integrated to improve the accuracy of information delivered to the end user. To this end, it is important to standardize vehicle-to-vehicle-to-infrastructure communication protocols to ensure connectivity between. In addition, cooperation between vehicular networks, other networks, and computing devices in the task of collecting environmental data and improving services to citizens is essential. Smart cities can also work to provide streets with sensors that track and alert the driver of hazards on the route. In addition, autonomous vehicles can make use of these sensors to guide passengers to their destination.

Difficulties and opportunities

It is not possible to consider all the advantages and disadvantages of such a complex proposal; however, it is possible to identify as major **difficulties -**the fact that not all technologies are mature and their prices are not yet competitive; issues such as data security and data protection must be scrupulously followed by Smart initiatives while being internalized by the population; The major **opportunities –** are the potential economic and infrastructure savings; the possibility of automatic management of certain infrastructures and services opens with the consequent savings associated with efficiency. reduction of infrastructure operating expenses.

Results

The best cryptographic performances were obtained using the NIST recommended ecdsa_nistp192_with_sha256 method with 41 SN-DECAP and 281 SN-ENCAP operations per second. However, in application security, each vehicle is expected to transmit a maximum of 10 CAM safety messages per second. Depending on the density of the vehicular network, each ITS station can receive several hundred (or thousands) CAM’s per second from neighbouring vehicles, whose signatures must be verified before scanning by upper layers or ITS applications. The recipient should always send their own certificate (or certificate chain) if they find their own hashId8 certificate in an unrecognized certificate message. Malicious users may thus continue to send spoofed packets to force the recipient to send their certificate continuously, which may deplete local resources and allocated network bandwidth.

Conclusion

Vehicle networks enable a number of applications that can make the driving experience safer as they avoid collisions, are more efficient as they reduce travel time, avoid traffic jams and increase road capacity, and make travel safer enjoyable as they provide new entertainment applications. However, the characteristics of these networks bring challenges to their development. In addition to the problems inherent to the wireless transmission in vehicular networks, there is also the high mobility of the nodes.

This latter feature can make vehicular networks highly unstable as the number of link breaks tends to be higher. This scenario demonstrates the need for new protocols and mechanisms that take into attention at first the limitations of these networks. Otherwise, the performance obtained may be lower than required by the new applications. However, the success of wireless networks and the rapid enhancement that related technologies are achieving indicate that this path is viable.

Throughout this dissertation, some concepts related to intelligent transport systems were presented. Existing architectures, vehicle network communication patterns and systems integration with different types of communication were analysed, showing the need for standardization and integration of these systems.

In addition, some types of existing applications in ITS were seen, in order to show the works found in the literature that already employ these concepts in order to leave some directions of new work. Decisions relevant to the application of new tools and procedures should be preceded by evaluations of existing experiences and results. A security assessment of the technology involved and the data that is part of the ITS was made. Namely data sources and types, vulnerabilities, and security solutions.

Today, ITS systems are considered the key technologies for improving road safety, traffic efficiency and driving experience. Detailed system threat analysis has helped to identify various vulnerabilities so that appropriate mitigation and recovery measures can be taken. Over the coming decades, smart cities will be defined primarily as those that are capable of acting within national and global constraints; those who work well with others serve the elderly and the poor, and those who try to provide a local environment for all. Doing this is smart.

References

[1] D. Jadranka, B. M. e G. M., “European Roadmap Smart Systems for Automated Driving,” 2015.

[2] A. V. Felipe Cunha, “Extrac¸ao de Propriedades Sociais em Redes Veiculares,” [Online]. Available: http://sbrc2014.ufsc.br/anais/files/wp2p/ST2-1.pdf. [Acedido em 15 Nov 2018].

[3] “Engineering Security and Performance Aware Vehicular Applications for Safer and Smarter Roads (SafeITS)”.

[4] M. Mejri, J. Ben-Othman e M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” Veh. Commun. , 2014, p. 53–66.

[5] M. Raya e J. Hubaux, “Securing vehicular ad hoc networks,” *J. Comput. Secur.,* p. 39–68, 2007.

[6] A. A. R. M. B. a. W. H. T. Theodore S. Rappaport, “Wireless Communications: Past Events and a Future Perspective,” IEEE Communications Magazine 50th Anniversary Commemorative Issue, 2002. [Online]. Available: https://ieeexplore.ieee.org/document/1006984. [Acedido em 15 Nov 2018].

[7] J. G. a. S. D. T. Reed, “SkyNET: a 3G-enabled mobile attack drone and stealth botmaster,” 2011. [Online]. Available: https://www.usenix.org/legacy/events/woot11/tech/final_files/Reed.pdf. [Acedido em 19 Ago 2019].

[8] J. Warner e R. Johnston, “GPS spoofing countermeasures,” pp. 1-8, 2003.

[9] S. Sharma e C. Krishna, “An Efficient Distributed Group Key Management Using Hierarchical Approach with Elliptic Curve Cryptography,” *2015 IEEE International Conference on Computational Intelligence Communication Technology (CICT),* p. 687–693, 2015.

[10] N. Nowdehi e T. Olovsson, “Experiences from implementing the ETSI ITS SecuredMessage service.,” em *IEEE Intelligent Vehicles Symposium Proceedings*, 2014, p. 1055–1060.