A SURVEY ON IOT APPLICATIONS FOR INTELLIGENT TRANSPORT SYSTEMS

[1]Anitha Chepuru , [2]Dr.K.Venugopal Rao
[1]Associate Professor IT Dept , [2]Professor CSE Dept
G.Narayanamma Institute of Technology and Science (for women),
Shaikpet, Hyderabad, Andhra Pradesh, India.
Email:[1]anithachepuru@rediffmail.com,[2]Kvgrao1234@gmail.com

Abstract

Information technology (IT) has transformed many industries, from education to health care to government, and is now in the early stages of transforming transportation systems. While many think improving a country's transportation system solely means building new roads or repairing aging infrastructures, the future of transportation lies not only in concrete and steel, but also increasingly in using IT. IT enables elements within the transportation system vehicles, roads, traffic lights, message signs, etc. to become intelligent by embedding them with microchips and sensors and empowering them to communicate with each other through wireless technologies. In the leading nations in the world, intelligent transport system (ITS) bring significant improvement in transportation system performance, including reduced congestion and increased safety and traveler convenience. The Internet of Things (IoT) makes smart objects the ultimate building blocks in the development of cyber-physical smart pervasive frameworks. The IoT has a variety of application domains, including health care. This paper surveys advances in IoT based ITS technologies and reviews the state-of-the-art network architectures, applications, and industrial trends in IoT based ITS. In addition, this paper analyzes distinct IoT security and privacy features, including security requirements, threat models, and attack taxonomies from the transportation perspective. Further, this paper proposes some avenues for future research on IoT-based intelligent transport based on a set of open issues and challenges.

Key words —intelligent traffic monitoring, Internet of Things, services, applications, networks, architectures, platforms, security, technologies, challenges, security.

Introduction :

Many think improving a country's transportation system solely means building new roads or repairing aging infrastructure. But the future of transportation lies not only in concrete and steel, but also in the implementation of technology, specifically a network of sensors, microchips, and communication devices that collect and disseminate information about the functioning of the transportation system. Transportation systems are really about networks, and much of the value of a network is contained in its information: For example, whether a traffic signal "knows" there is traffic waiting to pass through an intersection; whether a vehicle is drifting out of its lane; whether two vehicles are likely to collide at an intersection; whether a roadway is congested with traffic; what the true cost of operating a roadway is, etc. What intelligent transportation systems do is empower actors in the transportation system from commuters, to highway and transit network operators, even down to the actual traffic lights themselves with actionable information (or, intelligence) to make better-informed decisions, whether it's choosing which route to take; when to travel; whether to

mode-shift (take mass transit instead of driving); how to optimize traffic signals; where to build new roadways; what the true cost of roadways are and how best to price their use; or how to hold providers of transportation services accountable for results. The big opportunity at hand is to bring information to bear on transportation networks, transforming them into truly intelligent transportation systems. Internet of Things (IoT) has emerged as one of the most powerful communication paradigms of the 21st century. In the IoT environment, all objects in our daily life become part of the Internet because of their communication and computing capabilities that allow them to communicate with other objects. IoT extends the concept of the Internet and makes it more pervasive. In the IoT environment, the seamless interactions among different types of devices, such as vehicles, medical sensors, monitoring cameras, home appliances, etc., have led to the emergence of many applications such as smart city, home automation, smart grid, traffic management, etc.

ITS Architecture

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. 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 2.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.

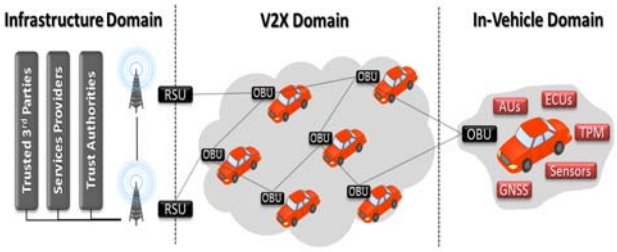

Figure 1. ITS high level architecture. RSU, road side unit; OBU, on-board unit; AU, application unit; ECU, electronic control unit; TPM, trusted platform module.
Finally, a Global Navigation Satellite System (GNSS) unit is used to obtain accurate location information. The V2X domain (or ad hoc domain) consists of vehicle OBUs and road-side units (RSUs) deployed along the roads. As shown in Figure 1.

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 in Figure 3.

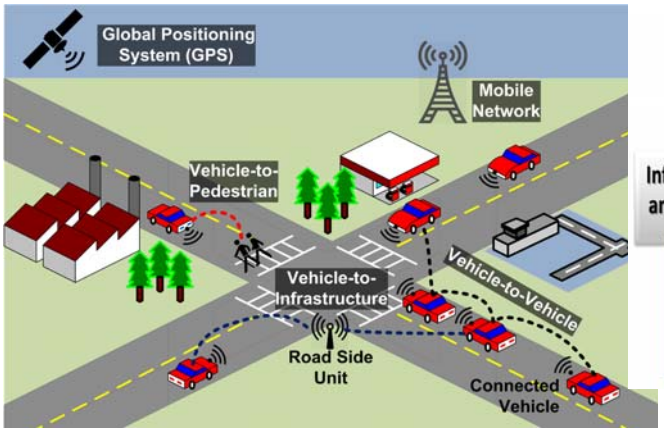

Figure 2. ITS V2X communications.

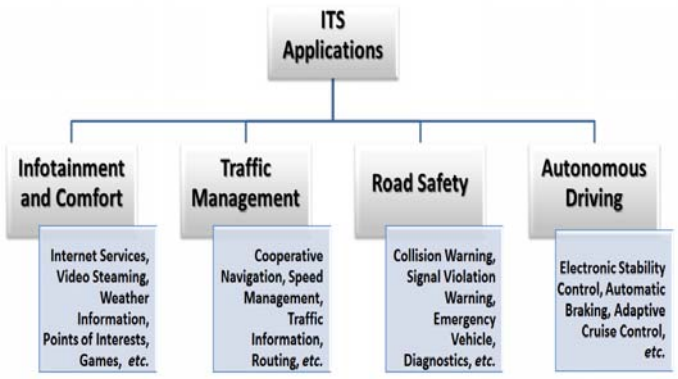

Figure 3. Classification of ITS applications

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.

Applications of ITS

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 4,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 for a more detailed description of emerging ITS applications in Figure 3.

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., 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.

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 . The applications rely mainly on V2I communications (vehicle-to-infrastructure/back office), whose latency should typically not exceed five hundred milliseconds.

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.

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.This new technology will rely on the automation of the vehicle sensing and driving functions, based on six levels of automation ,where the human driver becomes a passenger and is no longer required (i.e., full automation level). 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 5.

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.

Key underlying technologies

Wireless communications

Various forms of wireless communications technologies have been proposed for intelligent transportation systems. Radio modem communication on UHF and VHF frequencies are widely used for short and long range communication within ITS figure 4.

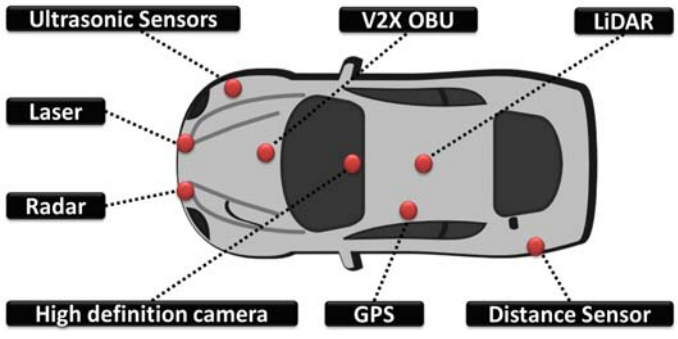

Figure 4. Key technologies enabling autonomous cars.

Short-range communications of 350 m can be accomplished using IEEE 802.11 protocols,

specifically WAVE or the Dedicated Short Range Communications standard being promoted by the Intelligent Transportation Society of America and the United States Department of Transportation. Theoretically, the range of these protocols can be extended using Mobile ad hoc networks or Mesh networking. Longer range communications have been proposed using infrastructure networks such as WiMAX (IEEE 802.16), Global System for Mobile Communications (GSM), or 3G. Long-range communications using these methods are well established, but, unlike the short-range protocols, these methods require extensive and very expensive infrastructure deployment. There is lack of consensus as to what business model should support this infrastructure. Auto Insurance companies have utilized ad hoc solutions to support e-Call and behavioral tracking functionalities in the form of Telematics 2.0. baseline data. Some of these technologies are described in the following sections.

Global Positioning System (GPS).

Embedded GPS receivers in vehicles' on-board units (OBUs, a common term for telematics devices) receive signals from several different satellites to calculate the device's (and thus the vehicle's) position. This requires line of sight to satellites, which can inhibit use of GPS in downtown settings due to "urban canyon" effects. Location can usually be determined to within ten meters. GPS is the core technology behind many in-vehicle navigation and route guidance systems. Several countries, notably Holland and Germany, are using or will use OBUs equipped with satellite-based GPS devices to record miles traveled by automobiles and/or trucks in order to implement user fees based on vehicle miles traveled to finance their transportation systems.

Dedicated-Short Range Communications (DSRC).

DSRC is a short- to medium-range wireless communication channel, operating in the 5.8 or 5.9GHz wireless spectrum, specifically designed for automotive uses. Critically, DSRC enables two-way wireless communications between the vehicle (through embedded tags or sensors) and roadside equipment (RSE). DSRC is a key enabling technology for many intelligent transportation systems, including vehicle-to-infrastructure
integration, vehicle-to-vehicle communication, adaptive traffic signal timing, electronic toll collection, congestion charging, electronic road pricing, information provision, etc. DSRC is a subset of radio frequency identification (RFID) technology. The technology for ITS applications works on the 5.9GHz band (United States) or the 5.8GHz band (in Japan and Europe). At present, DSRC systems in Europe, Japan, and the United States are generally not compatible (although there are indications that Europe may be trying to migrate to 5.9GHz). In 2004, the U.S. Federal Communications Commission (FCC), atypically for a U.S. regulator, prescribed a common standard for the DSRC band both to promote interoperability and to discourage the limitation of competition through proprietary technologies.

Wireless Networks

Similar to technology commonly used for wireless Internet access, wireless networks allow rapid communications between vehicles and the roadside, but have a range of only a few hundred meters. However, this range can be extended by each successive vehicle or roadside node passing information onto the next vehicle or node. South Korea is increasingly using WiBro, based on WiMAX technology, as the wireless communications infrastructure to transmit traffic and public transit information throughout its transportation network.

Mobile Telephony

ITS applications can transmit information over standard third or fourth generation (3G or 4G)
mobile telephone networks. Advantages of mobile networks include wide availability in towns and along major roads. However,

additional network capacity may be required if vehicles are fitted with this technology, and network operators might need to cover these costs. Mobile telephony may not be suitable for some safety-critical ITS applications since it may be too slow.

Radio wave or Infrared Beacons

Japan's Vehicle Information Communications System (VICS) uses radio wave beacons on expressways and infrared beacons on trunk and arterial roadways to communicate real-time traffic information.

(Arterial roadways are moderate capacity roadways just below highways in level of service; a key distinction is that arterial roadways tend to use traffic signals. Arterial roadways carry large volumes of traffic between areas in urban centers.) VICS uses 5.8GHz DSRC wireless technology.

Roadside Camera Recognition.

Camera- or tag-based schemes can be used for zone-based congestion charging systems (as in London), or for charging on specific roads. Such systems use cameras placed on roadways where drivers enter and exit congestion zones. The cameras use Automatic License Plate Recognition (ALPR), based on Optical Character Recognition (OCR) technology, to identify vehicle license plates; this information is passed digitally to back-office servers, which assess and post charges to drivers for their use of roadways within the congestion zone.

Probe Vehicles or Devices

Several countries deploy so-called "probe vehicles" (often taxis or government-owned vehicles equipped with DSRC or other wireless technology) that report their speed and location to a central traffic operations management center, where probe data is aggregated to generate an area-wide picture of traffic flow and to identify congested locations. Extensive research has also been performed into using mobile phones that drivers often carry as a mechanism to generate real-time traffic information, using the GPS-derived location of the phone as it moves along with the vehicle. As a related example, in Beijing, more than 10,000 taxis and commercial vehicles have been outfitted with GPS chips that send travel speed information to a satellite, which then sends the information down to the Beijing Transportation Information Center, which then translates the data into average travel speeds on every road in the city.

Sensing technologies

Technological advances in telecommunications and information technology, coupled with ultramodern/state-of-the-art microchip, RFID (Radio Frequency Identification), and inexpensive intelligent beacon sensing technologies, have enhanced the technical capabilities that will facilitate motorist safety benefits for intelligent transportation systems globally. Sensing systems for ITS are vehicle- and infrastructure-based networked systems, i.e., Intelligent vehicle technologies. Infrastructure sensors are indestructible (such as in-road reflectors) devices that are installed or embedded in the road or surrounding the road (e.g., on buildings, posts, and signs), as required, and may be manually disseminated during preventive road construction maintenance or by sensor injection machinery for rapid deployment. Vehicle-sensing systems include deployment of infrastructure-to-vehicle and vehicle-to-infrastructure electronic beacons for identification communications and may also employ video automatic number plate recognition or vehicle magnetic signature detection technologies at desired intervals to increase sustained monitoring of vehicles operating in critical zones.

Traffic control has been an issue since humans put the first wheels on the first cart. The modern world demands mobility. Cars represent the main method of mobility, but today's congested highways and city streets don't move fast, and sometimes they don't move at all. Intelligent traffic systems (ITS), sometimes called intelligent transportation systems, apply communications and information technology to provide solutions to this congestion as well as other traffic control issues. Intelligent Transportation Systems (ITS) represent a major transition in transportation on many dimensions. ITS is an international program intended to improve the effectiveness and efficiency of surface transportation systems

through advanced technologies in information systems, communications, and sensors. ITS (Intelligent Transport Systems) is a system which is designed to promote advance technology, to ensure that the Electronic Toll Collection System (ETC) is effective and to support safe driving. With this system, people, roads, and vehicles use the latest information communication technology.

The intelligent transport system (ITS) takes the first step towards meeting this challenge by providing effective, reliable and meaningful knowledge to motorists in time. Problems like high traffic congestion, low transportation efficiency, low safety and endangered environment can be solved through innovative and sophisticated ways of handling latest techniques that have emerged in recent years in integrating information technology, electronics and telecommunication with roads and traffic management. Intelligent transportation systems, or ITS, encompass a broad range of wireless and wireline communications-based information, control and electronics technologies.

When integrated into the transportation system infrastructure, and in vehicles themselves, these technologies help monitor and manage traffic flow, reduce congestion, provide alternate routes to travelers, enhance productivity, and save lives, time and money. Intelligent transportation systems provide the tools for skilled transportation professionals to collect, analyze, and archive data about the performance of the system during the hours of peak use. Having this data enhances traffic operators' ability to respond to incidents, adverse weather or other capacity constricting events

ITS Threats Analysis and Classification

Research on ITS security has attracted a lot of attention from the research community in the last decade, 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 5, 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.

ITS Involved Entities

From a security point of view, different entities might be involved in ITS systems, 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.

ITS Attackers Profiles

Attacker profiles are generally categorized into three bipolar criteria, 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.

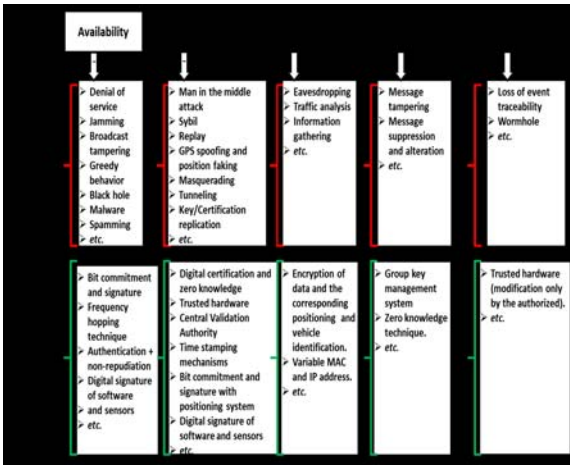

Figure 5. Examples of ITS threats, attacks and countermeasures.

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. In contrast, rational attackers have a specific target and can be very dangerous due to their unpredictable nature

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, 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 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.

IoT transport system security

Internet of Things (IoT) semantically means "a worldwide network of interconnected objects uniquely addressable, based on standard communication protocols", which is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as (RFID) tags, sensors, actuators, mobile vehicles, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals .Potentialities offered by the IoT make possible the development of a huge number of applications, of which can be grouped into the following domains . Traffic transportation and logistics domain. Healthcare domain. Smart environment (home, office, plant) domain. Personal and social domain. According literature , the three-tier architecture of the Internet of Things is as shown in

Figure 6. The bottom layer is an object-object network, namely a network that takes use of a variety of sensors, RFID to form object identification and data reading and writing between objects. This layer is data acquisition layer whose supporting technologies are mainly EPC, RFID, etc. When data pools together, it needs transmission, where a second layer is forms, which is called data transport layer. The network formation of data transport layer contains wired network and wireless network, its supporting technology mainly includes GPS, GPRS, the Internet and so on. The top layer of the Internet of Things is data processing and data exchange layer, whose task is to complete data exchange and data processing, data calculation, data storage and other functions. Actualization of the IoT concept into the real world is possible through the integration of several enabling technologies, such as EPC, RFID, GPS, GPRS, Internet, WSN etc. The following is the further introductions for the principles of these key technologies.

RFID and EPC

Radio Frequency Identification (RFID) systems provide
direct object identity sensing. They use a small device
(RFID tag) to receive and send remote commands. RFID
systems contain tags, readers, hosts and antennae. There is a small low-cost tag in each RFID object that provides
every product a unique identity—the Electronic Product
Code (EPC). Once an RFID reader sends a request signal,
the RFID tag responds to the reader's reading and writing
request. RFID offers wireless communication between the tags and readers with non-line-of-sight readability, which eliminates manual data collection and introduces the potential for automated identification process.

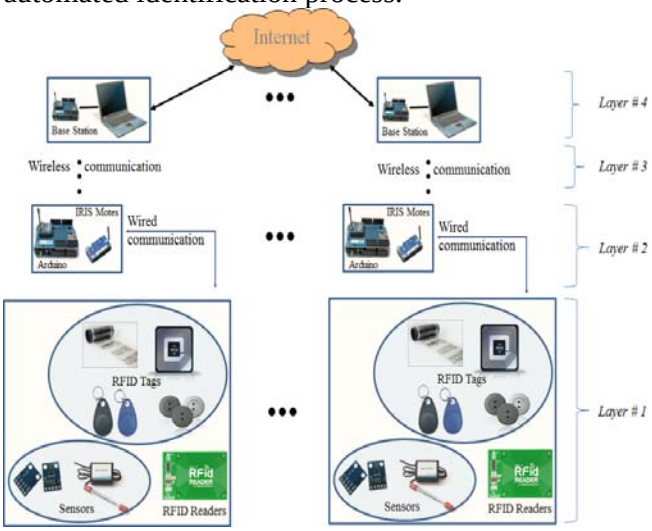

Fig 6.Three-tier architecture of the Internet of Things

The technology offers some unique advantages over the traditional barcode or smart card such as the flexible contactless identification range, multiple products identification, expressive read reliability and durability, massive data storage, and high level of data security. In general terms, a RFID tag contains a microchip with some computational and storage capabilities, and a coupling element, such as an

antenna coil for communication. Tags can be classified according to two main criteria: by type of memory or by source of power.

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. Digital signature schema for signing and verifying safety messages and the , Elliptic Curve Integrated Encryption Scheme curve public key algorithm and 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. .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 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.

Finally, the safety, security and QoS issues are generally considered as separate aspects of ITS systems.

Conclusion

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 ITS architecture, requirements and standards, existing ITS threats and attacks were analyzed and classified .These security algorithms are generally known for their high complexity and communication overhead. Various elliptic curve digital signature algorithms were implemented and benchmarked on different architectures. The paper offers a broad view on how recent and ongoing advances in sensors, devices, internet applications, and other technologies have motivated affordable healthcare gadgets and connected health services to limitlessly expand the potential of IoT-based ITS for further developments. To better understand IoT ITS security, the considers various security requirements and challenges and unveils different research problems in this area to propose a model that can mitigate associated security risks.

In sum results of this paper are expected to be use full for researchers ,engineers ,traffic monitoring working in this area of IoT Intelligent transport system.

References

1. J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, *From*

Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Amsterdam, The Netherlands: Elsevier, 2014.
2. "A wave of opportunity or a typhoon?" The 2009 Network National convention Seminars, ttp://www.networkhq.org/2009-convention/seminars-telematics.htm.
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).
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,
oi:10.1109/IEEESTD.2012.6178212.
10. ETSI—Intelligent Transport Systems. Available online: http://www.etsi.org/technologiesclusters/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