Internet of Things (IoT) Technologies for Smart Cities

Article · September 2017

DOI: 10.1049/iet-net.2017.0163

5 authors, including:

Badis Hammi
Télécom ParisTech
16 PUBLICATIONS **83** CITATIONS
SEE PROFILE

Rida Khatoun
Télécom ParisTech
62 PUBLICATIONS **331** CITATIONS
SEE PROFILE

Achraf Fayad
Télécom ParisTech
4 PUBLICATIONS **19** CITATIONS
SEE PROFILE

Lyes Khoukhi
Université de Technologie de Troyes
113 PUBLICATIONS **577** CITATIONS
SEE PROFILE

IET Journals
The Institution of Engineering and Technology

Internet of Things (IoT) Technologies for Smart Cities

ISSN 1751-8644
doi: 0000000000
www.ietdl.org

Badis HAMMI[1] *Rida KHATOUN*[1] *Sherali ZEADALLY*[2] *Achraf FAYAD*[1] *Lyes KHOUKHI*[3]

[1] *Telecom ParisTech, 46 Rue Barrault, 75013 Paris, France*
[2] *University of Kentucky, Lexington, KY 40506-0224, USA*
[3] *Troyes University of Technology, 12 rue Marie Curie, 10004 Troyes, France*
* *E-mail: badis.hammi@telecom-paristech.fr*

Abstract: The large deployment of Internet of Things (IoT) is actually enabling Smart City projects and initiatives all over the world. Objects used in daily life are being equipped with electronic devices and protocol suites in order to make them interconnected and connected to the Internet. According to a recent Gartner study, 50 billion connected objects will be deployed in smart cities by 2020. These connected objects will make our cities smart. However, they will also open up risks and privacy issues. As various smart city initiatives and projects have been launched in recent years, we have witnessed not only the expected benefits but the risks introduced. We describe the current and future trends of smart city and IoT. We also discuss the interaction between smart cities and IoT and explain some of the drivers behind the evolution and development of IoT and smart city. Finally, we discuss some of the IoT weaknesses and how they can be addressed when used for smart cities.

1 Introduction

As cities grow and expand, smart and innovative solutions are crucial for improving productivity, increasing operational efficiencies, and reducing management costs [1]. Citizens are gradually equipping their homes with IoT devices such as TV and Internet box. In the real estate sector, connected objects include thermostats, smart alarms, smart door locks, and other systems and appliances. At the United Nations conference on climate change (Cop21) held in Paris in 2016, connected objects were extensively addressed and gave to many local communities the opportunity to rethink their environmental objectives in order to reduce their CO2 emissions through the use of IoT*†. The latter can play a vital role in the context of smart cities. For example, intelligent waste containers can bring real benefits to citizens; they will be able to indicate that they are soon going to be full and must be emptied. Citizens can check through a smart phone application if the waste containers in the street are full or not. Also, after waste containers reports their status, companies can offer route optimization solution to the teams responsible for garbage collection. Places can be equipped with sensors and monitor environmental conditions, cyclists or athletes can find the most "healthy" trips and the city can respond by adjusting the traffic or by planting more trees in some areas. The data will be accessible to all citizens to promote the creation of applications using real-time information for residents. Cities have become hubs for knowledge-sharing. The technologies and solutions needed for creating smart cities are just beginning to emerge. Figure 1 describes an example of a smart city.

Gartner has reported [2] that the investment in IoT will be crucial to build smart cities, services as data using will generate most of the revenues. Safety and security of smart homes will be the second largest market in terms of service revenues. As for services related to health and well-being, they should represent a market of $ 38 billion in 2020 [2]. A practical solution must find the trade-offs between effectiveness and privacy risks. A sophisticated attacker could, for example, take control of various intelligent devices such as lights, cameras, traffic lights, connected cars and many other smart devices in cities. With over 50 billion devices connected by 2020, municipalities will be very much concerned for the safety of their intelligent cities [2] [3]. However, solutions to address safety, security, and privacy concerns of smart cities relying on diverse intelligent objects fall not only into the technology realm but also in other areas including sociology, legal, and policy management.

In this chapter, we present an overview of IoT in the context of smart cities, and we discuss how IoT can enhance a city's smartness. We also identify the weaknesses and risks associated with IoT deployment and adoption in the smart city environment. In the next section, we present some background information on IoT and smart city. Section 3 discusses the main architectures used within IoT. Section 4 describes how IoT can be considered as an enabling technology for smart city. In Section 5, we describe the weaknesses that need to be addressed when IoT is used for smart cities. Finally, in the last section, we make some concluding remarks.

2 Internet of Things and Smart City

In the recent literature, several authors have provided definitions for the term Internet of Things [4] [5] [6]. IoT may be defined as "Objects having identities and virtual personalities in smart spaces using intelligent interfaces to connect and communicate within social, medical, environmental and users context [7]". Huge investments are currently being made in the IoT area to support the delivery of a wide range services. Various aspects of social and economic life are currently being studied for IoT. Trust in IoT implies that investors do not hesitate to commit to it financially; 100 million euros were invested by large corporations such as Telefónica, SK Telecom, NTT Docomo Ventures, Elliott Management Corporation and industry groups GDF SUEZ, Air Liquide for research and development of IoT.

The deployment of IoT needs communication standards that seamlessly operate among the various objects. Several worldwide organizations are involved in standardizing such communications. These include the International Telecommunication Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), Global Standard1 (GS1), the Organization for the Advancement of Structured Information

* *http://www.gartner.com/smarterwithgartner/cop21-can-the-internet-of-things-improve-organizations-sustainability-performance/*
† *http://www.cloud-experience.fr/cop21-le-role-des-tic/*
‡ *CISCO Copyright 2014*

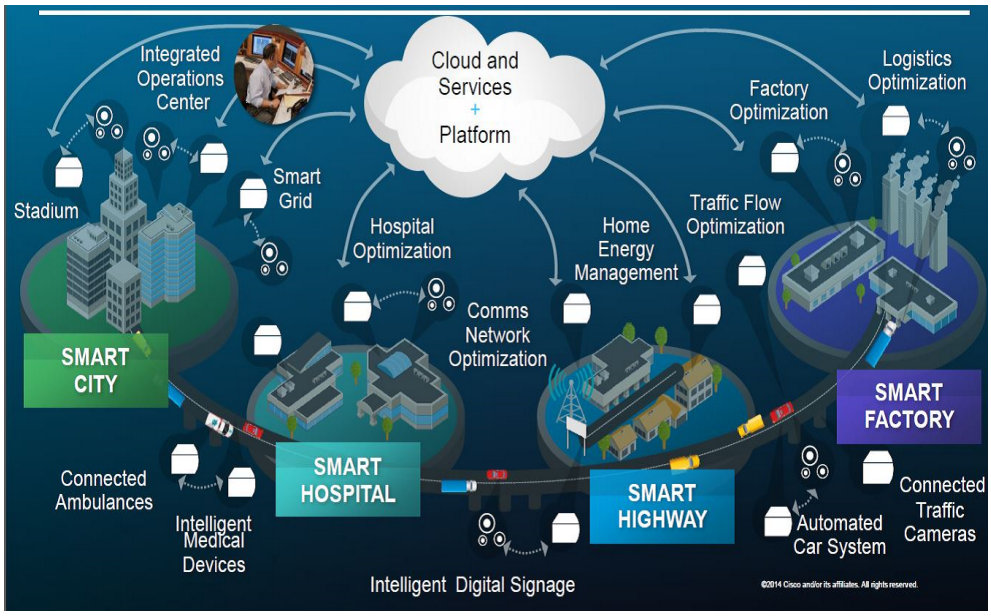

Fig. 1: Development of smart cities[‡]

Standards (OASIS), the Industrial Internet Consortium (IIC), and several others. We briefly present some of these IoT standards and initiatives in Table 1. For example, the Internet of Things Standard Global Initiative (IoT-GSI) supported by ITU made two recommendations: the ITU-T Y.2060 [8], which provides an overview of the concept of IoT and ITU-T Y.2061 [8], which describes the conditions for the machine interface oriented towards applications. Various standards were proposed by IEEE and IETF at different levels for sensor networks based on the Internet Protocol (IP). For example, at the link layer, the IEEE 802.15.4 standard is more suitable than Ethernet in industrial environments. At the network level, the IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) standard can adapt the IPv6 protocol for wireless communications [9]. In 2011, the IETF published the IPv6 Routing Protocol (RPL) standard for Low-power Networks.

IETF has also launched a Working Group to standardize an application layer-oriented protocol for connected objects. The reference protocol is called the Constrained Application Protocol (CoAP). CoAP (see RFC 7252 of June 2014) provides methods and commands (such as, HTTP Get) to query an object and change its status. CoAP relies on UDP and can optionally use Datagram Transport Layer Security (DTLS), to provide communication security. Operating systems [10] used in IoT include: TinyOS, Contiki OS, MantisOS, Nano-RK, Android, Brillo (Google), Windows 10 IoT Core, LiteOS (Huawei), Mbed OS (ARM). In addition, several platforms [10] have been developed for IoT: Arrayent, Californium CoAP Java framework, Erbium, CoAP framework for Contiki, and XMesh networking stack. At the application layer, a large number of applications have been developed [10]: Iobridge Thingspeak, Nimbits, Evrythng, Open.Sen.se, NanoService, exosite One, HP supposed, Isidorey, SensorCloud, Manybots, and so on. Figure 2 compares the 6lowPAN communication stack with other popular communication stacks.

The Electronic Product Code Global (EPC Global) initiative of the organization Global Standard 1(GS1)[*] defines a unique individual identifier for identifying an electronic product and the overall EPC network architecture that defines the organization of information systems designed to ensure the exchange of information in an EPC network [12] [13]. One of its main components is the Object Naming Service (ONS) which is based on the Domain Name System (DNS). In fact, in 1970 the European Article Numbering (EAN) standard emerged for product identification. However, this EAN barcode is actually used to identify a class of products, not individual instances within this class. Furthermore, in IoT, a unique IP address for each connection is required. This is why EPC was proposed by GS1 as a new standard. Meanwhile, OASIS[†] issued various recommendations on network technologies in IoT and messaging technologies such as Message Queue Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP) and the Data Distribution Service for Real-Time Systems (DDS). In 2014, a new Industrial Internet Consortium (ICC[‡])was launched in order to coordinate and establish the priorities and enabling technologies of the Industrial Internet. There are thousands of founding and contributing members of ICC and they include: Bosh, Intel, IBM, Schneider, Huawei, Cisco, and several others. There are currently 19 Working Groups and teams working on different areas: Business Strategy and Solution Lifecycle, Legal, Liaison, Security, Technology Testbeds, Marketing and Membership, and so on. Figure 3 summarizes some IoT's protocols and standards and Table 2 details the used acronyms.

A smart city is defined as a city connecting physical infrastructures, ICT infrastructures, social infrastructures and business infrastructures to leverage the collective intelligence of the city [15]. A city can be smart through a large deployment of IoT (especially through machine-to-machine and human-to-machine communications). Wireless Sensor Networks (WSNs), the sensing-actuation arm of the IoT, seamlessly integrate into urban infrastructure forming a "digital skin" around it. The information generated is shared across diverse platforms and applications to develop a Common Operating Picture (COP) of the city [16].

3 IoT Architecture

IoT technologies are expected to be part of large scale networks, with the number of devices in the thousands and areas spanning several kilometers. In the rest of this chapter, we focus primarily on the

[*] *http://www.gs1.org*

[†] *www.oasis-open.org*

[‡] *http://www.iiconsortium.org*

	802.11a	802.11b	802.11g	802.11n	802.11 ac	802.11 ad	802.15.1	802.15.3	802.15.4	802.15.6	NFC
Network Type	WLAN	WLAN	WLAN	WLAN	WLAN	WLAN	WPAN	WPAN	WPAN	WBAN	Point-to-Point
Date	1999	1999	2003	2009	2014	2012	2002/2005	2003	2007	2011	2011
Network Size	30	30	30	30			7	245	65535	250	-
Bit Rate	54 Mbps	11Mbps	54 Mbps	248 Mbps	3.2 Gbps	$\geq$ 7Gbps	3 Mbps	55 Mbps	250 Kbps	10 Mbps	424 Kbps
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5/60GHz	2.4 GHz	2.4 GHz	868-915 MHz 2.4 GHz	402-405 MHz	13.56 Mhz
Range	120 m	140 m	140 m	50 m indoor 250 m outdoor	30 m	5 m	100 m	100 m	75 m	2-5 m	0.2 m
Modulation	BPSK, QPSK 16-QAM 64-QAM OFDM	DBPSK DQPSK CCK DSSS	DBPSK DQPSK 16-QAM 64-QAM OFDM	OFDM	OFDM	QAM-256	8DPSK DQPSK PIDQPSK GFSK AFM	QPSK DQPSK 16-QAM 32-QAM 64-QAM	ASK DSSS PSSS		Manschester and Modified Miller
Application	WiFi	WiFi	WiFi	WiFi			Bluetooth		ZigBee		

Table 1 Main communication standards within IoT

Acronym	Description	Acronym	Description
HBase	Hadoop Database	RapidMQ	Rapid Message Queuing
MQTT	Message Queuing Telemetry Transport	DDS	Data Distribution Service
XMPP	Extensible Messaging and Presence Protocol	AMQP	Advanced Message Queuing Protocol
HTTP	HyperText Transfer Protocol	FTP	File Transfer Protocol
Telnet	Telecommunication Network	SSH	Secure SHell
IPv4	Internet Protocol Version 4	IPv6	Internet Protocol version 6
6LowPan	IPv6 over Low power Wireless Personal Area Networks	RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks
BLE	Bluetooth Low Energy	RFID	radio frequency identification
GSM	Global System for Mobile Communications	CDMA	Code division multiple access
OBD2	On-board diagnostics 2	PLC	Power-line communication
RS-232	Recommended Standard 232	Modbus	Modicon Communication Bus
USB	Universal Serial Bus	SPI	Serial Peripheral Interface
AES	Advanced Encryption Standard	SSL	Secure Sockets Layer

Table 2 Acronym table

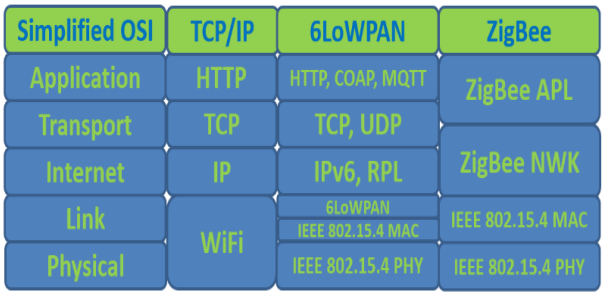

Fig. 2: Comparison of 6LowPAN's stack with other stacks [11]

LoRa Ultra-Narrow Band (UNB) technology which was developed by Semtech and SigFox's .

3.1 LoRa

LoRa is a wireless technology designed to provide the low-power within wide-area networks (LPWANs) required for Internet of Things services [17]. The technology offers a mix of long range, low power consumption and secure data transmission. The LoRa standard has been developed for IoT-type devices in regional or global networks. This technology provides seamless interoperability among devices without requiring any complex installations. The services targeted include home energy monitoring, alarm systems, remote health monitoring, transportation, environment protection, and so on. This specification defines the communication protocol and system architecture for the underlying network. It supports frequencies in the 433, 868 or 915 MHz ISM bands, depending on the area where it is deployed. In Europe, it uses either Gaussian Frequency Shift Keying (GFSK) or the proprietary LoRa modulation system, which works with a version of Chirp Spread Spectrum using 125 KHz channel bandwidth [18]. LoRa architecture is describes in Figure 4

The hierarchical star-based topology is used by LoRa networks. IoT devices in such networks can be servers, end-points, or gateways. Data rates can range, in Europe, from 0.3 Kbps up to 50 Kbps when channel aggregation is employed. In North America, the minimum data rate is 0.9 Kbps because of Federal Communications Commission (FCC) requirements. The payload for this technology can range from 2 to 255 bytes [19]. This standard is optimized for low cost and battery operated sensors. The devices are asynchronous and communicate only when they have data ready to send whether event-driven or scheduled. Power consumption is proportional to the time devices spent while in the listening mode.

LoRa is gaining significant attention in IoT networks that are being deployed by wireless network operators. It can be deployed with minimum upfront infrastructure investments and operating costs. When increased network capacity is required, further Gateways can be added. It has been estimated that the deployment cost of this technology in unlicensed bands needs much less capital than even a 3G software upgrade [19]. Major Telecom operators (e.g., Swisscom, NKE Electronics, and others) are deploying this technology for nationwide networks because of its benefits over competing technologies. These benefits include bi-directional communications, mobility for asset tracking, security, and accurate localization [20].

3.2 SigFox

SigFox created an ultra-narrowband IoT communications system designed to support IoT deployments over long ranges, e.g. in excess of 20 km between a client device and a base station*. SigFox uses license-exempt spectrum for its product, namely the 868 MHz band in Europe and 915 MHz band in the US, to transmit data over a narrow spectrum to and from connected objects. The ultra-narrow band operation is achieved using bandwidth channels lower than 1 KHz transmitting data payloads of 12 bytes uplink and 8 bytes downlink with a protocol overhead of 26 bytes [19].

One of the advantages of SigFox devices is their resource efficiency. The power demand is negligible because devices are only "on" when they are transmitting; this means that the power demand is a fraction of that for a device operating on cellular networks. SigFox

*http://www.sigfox.com

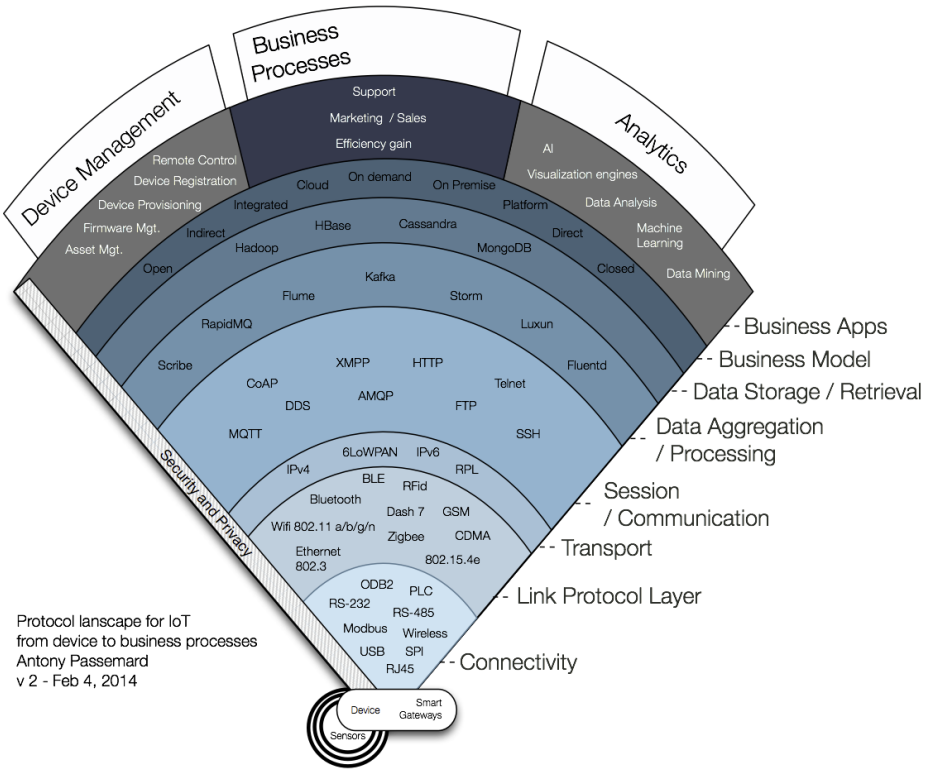

Fig. 3: Internet of Things protocol stack [14]

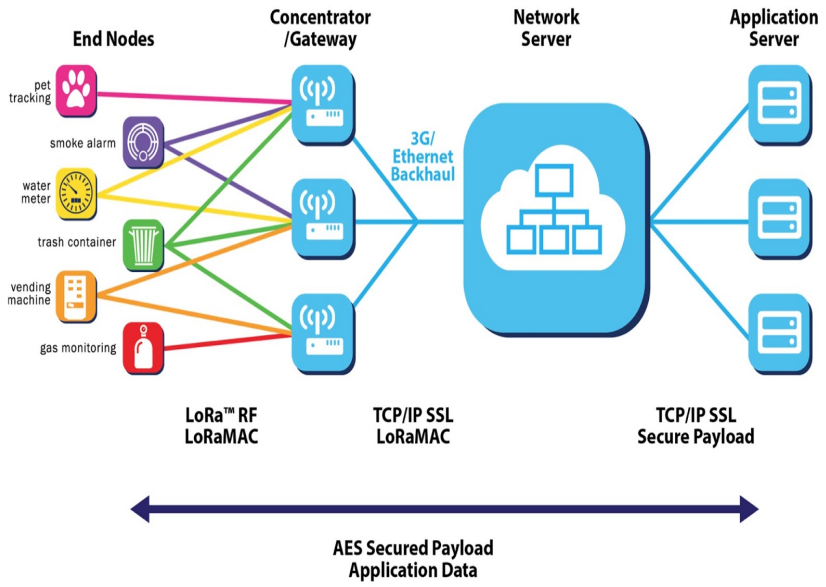

Fig. 4: LoRa architecture [20]

Standard	SIGFOX	LoRaWAN	LTE-M	IEEE P802.11ah (low power WiFi)	Dash7 Alliance Protocol 1.0	Ingenu RPMA	nWave
Frequency Band	868 MHz/902 MHz ISM	868 MHz/902 MHz ISM	Cellular	License-exempt bands below 1 GHz, excluding the TV White Spaces	433, 868, 915 MHz	2.4 GHz ISM	Sub-GHz ISM
Range	30-50km (rural), 3-10km (urban), 1000km LoS	2-5k (urban), 15k (rural)	2.5-5km	Up to 1Km (outdoor)	0.5 km	>500 km LoS	10km (urban), 20-30km (rural)

Table 3 Comparison of low power WAN technologies [21]

technology allows deploying very efficient, low throughput communications by limiting the number of antennas (base stations). For the same level of coverage, SigFox requires around 1,000 times less antennas and base stations, compared with some cellular networks*. This technology offers access to a service management interface, which can enable the control of main communication parameters such as battery and temperature settings, signal quality, volume of exchanged data, and others †. Networks based on SigFox technology have already connected thousands of devices in several international cities. They are currently operational in 14 countries, covering an area of more than 1.2 million km2 and reach 223 million people‡.

In general, IoT can be divided into three layers: the perception layer, the network layer and the application layer. The perception layer is mainly used to capture and gather, distinguish and identify the information of objects in the physical world [5]. This layer includes RFID tags, cameras, GPS, sensors, laser scanners, and so on. The network layer is used to forward packets over a reliable communication medium. The application layer processes the data, aggregates various sources and displays it. Table 3 compares different low power WAN technologies used in IoT use case scenarios.

4 IoT as an enabling technology for Smart City

The IoT concept leverages several ubiquitous services to enable Smart City deployments all over the world. IoT introduces new opportunities such as the capability to monitor and manage devices remotely, analyze and take actions based on the information received from various real-time traffic data streams. As a result, IoT products are changing cities by enhancing infrastructures, creating more effective and cost-efficient municipal services, improving transportation services by decreasing road traffic congestion, and improving citizens' safety. To achieve the full potential of IoT, smart city architects and providers recognize that cities must not offer a separate smart city feature, but rather deliver scalable and secure IoT solutions that include efficient IoT systems.

4.1 IoT for Smart Cities: requirements and real examples

An efficient smart city solution should design and incorporate IoT platforms that meet the requirements of today's IoT, and allows the management of millions of connected devices, systems and people. In particular, an IoT platform should:

- Reduce the cost and risk required to create and evolve IoT services.
- Connect multiple heterogeneous systems in a city.
- Decrease the time required to implement and deploy IoT services which are part of smart city initiatives.
- Deliver secure and scalable service access and open up new opportunities for the city.
- Create value (e.g., better services) from smart connected data and devices.

IoT objects with various capabilities (e.g., temperature, light, humidity, pressure) have appeared today and many of them allow us to anticipate rather than simply react. Indeed, there are many sectors (health, manufacturing, transportation, and others) where connected objects are being deployed.

According to IDC [22], the Chinese IoT market is expected to reach $ 361 billion by 2020 with an increase of 13.3% over the next five years. Well-known Chinese firms such as Alibaba, Baidu, Huawei, Lenovo and Xiaomi are making heavy investments in the IoT sector. Moreover, in the city of Zhonggnauchun, also called the "Chinese Silicon Valley", located in the northeast of Beijing, has also attracted IoT entrepreneurs from around the world.

In 2015, the White House launched the Smart City Initiative which aims to facilitate technological collaboration between cities, federal agencies, universities and the private sector *†. In the US, Kansas City has signed an agreement with Sprint and Cisco to create the biggest smart city in North America with the intention of improving municipal services. Through a wide area sensor network and Wi-Fi, the project (worth over $15 million) will provide different types of information to citizens by gathering data on their behavior in the city.

Fujisawa‡, a city located in the south of Tokyo, is under construction by Panasonic and 3000 people are expected to be there by 2018.

Songdo§ in South Korea is being built by Gale, a powerful US real estate group. Songdo hopes to welcome about 300 000 workers and 65,000 residents by 2020. The UAE is also looking into the future beyond the post-oil era and had led to investments worth $18 billion to build Masdar¶, a city in the desert powered entirely (100%) by renewable energy. In Masdar, for example, wastewater is used to irrigate green spaces.

The Malmo Green Digital City project‖ in Sweden aims to make Malmo a carbon neutral city by 2020. The project also aims to make the city run entirely on renewable energy by 2030. Malmo officials foresee that this city project will be able to house 10,000 people and they expect an additional 20,000 to work or study there.

In Fujisawa, street light illuminates only when sensors detect the presence of an individual. Recycling is also a major concern. In Songdo, rainwater is collected, filtered and used to irrigate parks.

In France, the Ministry of Transport has launched (in 2016) a project called scoop@F to develop an infrastructure for smart vehicles. In this project, 3,000 intelligent vehicles will be tested in 6 locations including Ile-de-France, on the Bordeaux ring road and the Isère department. The budget of scoop@F is estimated at 20 million euros funded between the state, communities, industrial and the EU. In this project, adapted vehicles driven by individuals and professionals, will be connected to the smart route and interconnected

*http://www.atmel.com/images/atmel-9372-smart-rf-ata8520datasheet.pdf
†http://www.sigfox.com
‡http://www.iotglobalnetwork.com

*http://smartcitiescouncil.com/article/white-house-announces-160-million-smart-cities-initiative
†https://obamawhitehouse.archives.gov/the-press-office/2016/09/26/fact-sheet-announcing-over-80-million-new-federal-investment-and
‡http://fujisawasst.com/EN/
§http://songdoibd.com/
¶http://www.masdar.ae/
‖http://malmo.se/gronit

via WiFi, 4G or 5G technologies to share information among them about traffic, accident, presence of debris or an animal on the road. A connected car is therefore a solution that improves the driving conditions by collecting and disseminating real-time traffic information and traffic conditions among the vehicles which will improve the traffic security [23] [24].

To summarize, smart cities are connected cities that use telecommunication technologies and information systems to improve the lives of citizen. we think that a smart city can be made smart by achieving two principal objectives:

- Providing an advanced urban infrastructure with the ability to collect and process data using emerging technologies such as smart grid, smart meters, smart buildings, connected objects and big data in order to anticipate any anomalies.
- Allowing users to interact with the environment through smart applications in order to reduce CO2 emissions. Reduced pollution levels will improve the environment and ultimately the quality of life (e.g., improved health, safer, faster, cheaper commute) of the citizens.

4.2 *IoT Applications for Smart Cities*

It is interesting to consider the application of the IoT paradigm to an urban context. Indeed, many national governments extensively are currently studying and planning how to adopt Information Communication Technology (ICT) solutions in the management of public services in order to realize Smart City concept [25].

4.2.1 Health of Buildings: To properly maintain the historical buildings of a city we need to: (1) continuously monitor the actual conditions of each building and (2) to identify the most affected areas due to various external agents [26]. The city contains multiple structures, which have different sizes and different ages. It is different from one city to another, but, generally, most of the structures are very old (such as buildings, dams, or bridges [27]). To assess the conditions of a building, passive WSNs can be embedded within a concrete structure, and periodically send a radio signal of suitable amplitude and phase characteristic to inform about the structure's state [16].

4.2.2 Environmental Monitoring: WSNs process, analyze, and disseminate information collected from multiple environments [27]. The various parameters measured by sensors [28] are:

- Water level for lakes, streams, sewages.
- Gas concentration in the air for cities, laboratories, and deposits.
- Soil humidity and other characteristics.
- Inclination for static structures (e.g., bridges, dams).
- Position changes (e.g., for landslides).
- Lighting conditions either as part of combined sensing or standalone (e.g., to detect intrusions in dark places).
- Infrared radiation for heat (fire) or animal detection.

4.2.3 Waste Management: Waste management becomes an increasing problem in urban living. It is related to many aspects including socioeconomic and environmental ones. One important feature in waste management is environmental sustainability [29]. A major benefit of global IoT infrastructures is that they provide us with the ability to collect data and, further help in improving effective management for various issues. Nowadays, the garbage-truck needs to pick-up all garbage cans even when they are empty [30]. By using IoT devices inside the garbage can, these devices will be connected to the computing server using one of LPWAN technologies. The computing server can collect the information and optimize the way to garbage-collection is performed by the garbage trucks.

4.2.4 Smart Parking: In this use case, there is a wireless sensor (or connected object) at each parking spot. If a vehicle parks, or if a parked vehicle leaves a parking spot, the sensor at the parking spot sends a notification to a management server. By collecting information regarding the parking bay occupancy, the server can provide parking vacancy information to drivers through a visualization platforms such as smart-phones, vehicles' Human Machine Interfaces (HMIs) or advertisement boards. These information will also enable the city council to apply fines in case of parking infringements [16]. Radio Frequency IDentification (RFID) technology is automated and can be very useful to vehicle identification systems. Vehicles are identified and parking-lot fees are collected automatically via this system [31]. As for the hardware requirements, by utilizing RFID readers, barriers, parking-lot check-in and check-out controls can be achieved. In this way, in contrast to personnel-controlled traditional parking-lot operations, an unmanned, automated vehicle control and identification system can be developed as described in [31]. The development of Vehicle Ad Hoc Networks (VANETs) [32] along with the advances and wide deployments of wireless communication technologies, many major car manufactories and telecommunication industries are increasingly fitting their cars with On Board Unit (OBU) communication device. This allows different cars to communicate with each other as well as with the roadside infrastructure. Thus, applications that provide information on parking space occupancy or guide drivers to empty parking spaces, are made possible through vehicular communications [33].

4.2.5 Smart Health: A Wireless Body Area Network (WBAN) which is based on a low-cost wireless sensor network technology could greatly benefit patient monitoring systems in hospitals, residential and work environments [34]. The miniature sensors can be embedded inside the body or mounted on the surface of the body. The sensors communicate with a medical devices using different technologies of WPAN (ZigBee, 6LowPAN, CoAP, etc.). The sensors are also capable of measuring various physiological parameters information (e.g., blood flow, respiratory rate, blood pressure, blood PH, body temperature, and so on), which are collected and analyzed by remote servers (see Figure 5). The wearability requirement poses physical limitations on the design of these sensors. The sensors must be light, small, and should not hinder a patient's movements and mobility. Moreover, because the sensors need to operate on small batteries included in the wearable package, they need to be highly energy-efficient [35].

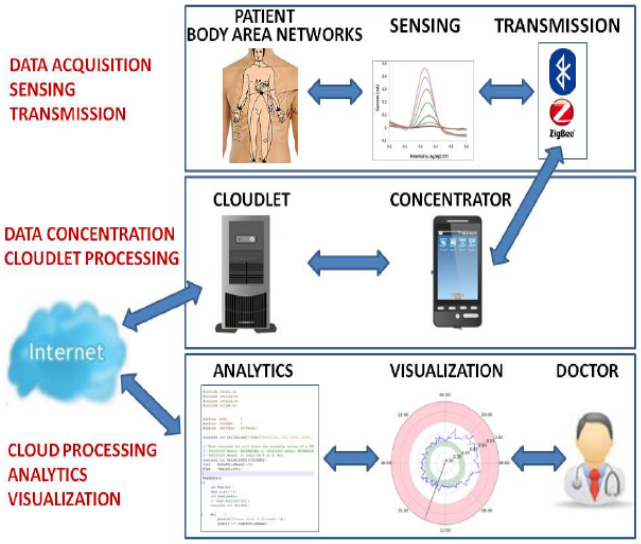

Fig. 5: Components of a remote patient monitoring system that is based on an IoT-Cloud architecture [35]

4.2.6 Navigation System for Urban Bus Riders: UBN is based on an IoT architecture which uses a set of distributed software and hardware components that are tightly integrated with the

bus system. The UBN system deployed in Madrid, Spain is composed of three key components: 1) the network-enabled urban bus system with WiFi equipped buses, 2) the UBN navigation application for bus riders, and 3) the bus crowd information server which collects real-time occupancy information from buses operating on different routes in Madrid [36].

4.2.7 Smart Grid: The smart grid uses new technologies such as intelligent and autonomous controllers, advanced software for data management, and two-way communications between power utilities and consumers, to create an automated and distributed advanced energy delivery network (see Figure 6) [37]. Deployed as an infrastructure for sensing and transmitting information for the smart grid, the IoT technology, when applied to the power network, will play a significant role in cost-effective power generation, distribution, transmission and consumption [38].

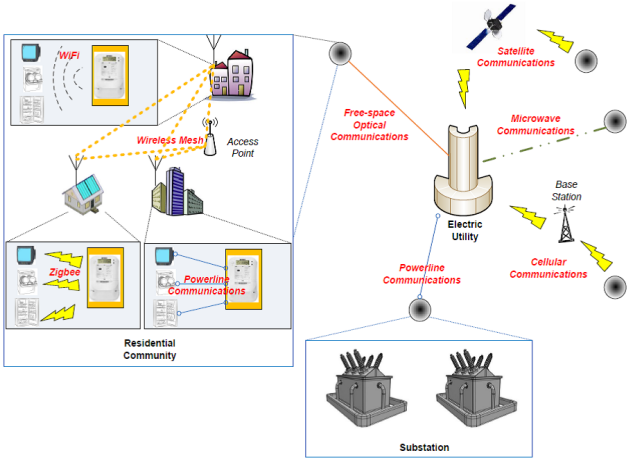

Fig. 6: Smart Grid architecture [37]

4.2.8 Autonomous driving: In a smart city, autonomous driving technologies will be synonymous with saving time for the user. This technology would help speed up the flow of traffic in a city and save almost 60% [39] of parking space by parking the cars closer to each other. According to Nissan-Renault, autonomous vehicles will likely to be marketed in 2020. These "automatic cars" will circulate autonomously at around 30 to 50 km/h as the Renault Next Two-autonomous model of the French manufacturer [40]. In 2017, Volvo will experiment with a hundred autonomous cars driving in real traffic conditions on roads in Gothenburg, London and several Chinese cities. Through a combination of radar, cameras and ultrasonic sensors located around the car, an autonomous car can detect anomalies all around and trigger an alert that automatically activates the emergency brakes to prevent accidents or collisions. The Intelligent Transport System could enable us to calculate the best route in real-time by connecting different transport modes to save time and reduce carbon emissions.

4.3 IoT platforms

The significant growth in IoT deployment have led to the emergence of IoT platforms which support:

- Easy integration of new devices and services.
- Communication between devices (objects and servers).
- The management of different devices and communication protocols.
- The transmission of data flows and the creation of new applications.
- Interoperability among components, objects, gateway, cloud data, and software applications.
- Scalability of the IoT infrastructure.

According to the level of services provided, IoT platforms can be divided into:

1. Infrastructure-as-a-service backends: they provide hosting space and processing power for applications and services, e.g. IBM Bluemix*.
2. M2M connectivity platforms: they focus only on the connectivity of IoT objects through telecommunication networks and protocols, e.g. Comarch† and AirVantage‡
3. Hardware-specific software platforms: numerous companies sell their proprietary technology which includes the hardware and the software backend, e.g Google Nest§
4. Enterprise software extensions: some software and operating system companies such as Windows and Apple are increasingly allowing the integration of IoT devices such as smartphones, connected watches and home devices.

According to [41] [42] the main features that an IoT platform must achieve are:

- Device integration.
- Networking.
- Device management.
- Security.
- Protocols for data collection.
- Analytics.
- Support for visualizations.

Based on these features, the authors in [43] have proposed a stack for the IoT platform architecture as shown in Figure 7.

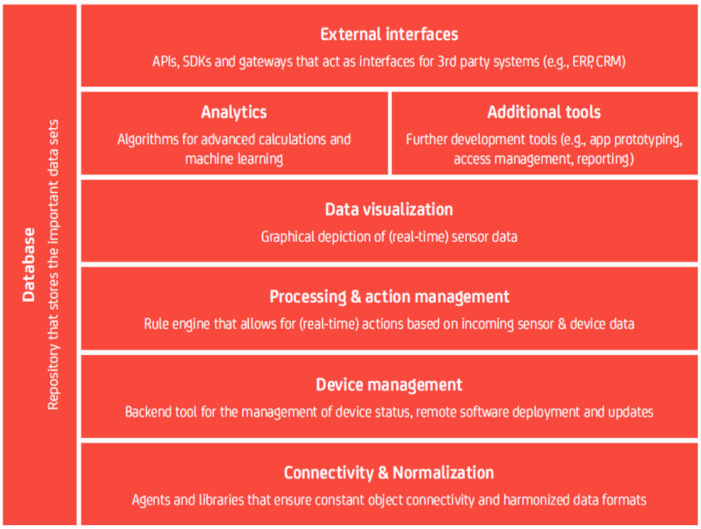

Fig. 7: Main components of an IoT Application Enablement Platform [43]

As we mentioned earlier, the number of IoT platforms is growing at a fast pace. According to [44] this market will reach $1 billion in 2019. In Table 4 we provide a comparison of different platforms where we describe their offered services, advantages and limitations.

*https://www.ibm.com/cloud-computing/bluemix/fr
†http://www.comarch.com/telecommunications/solutions/m2m-platform/
‡https://airvantage.net
§https://nest.com/

Platform	Services	Advantages	Disadvantages
AWS IoT [45]	visualization, monitoring, and analyzing data received from wired or wireless sensors	data transactions security	private platform
Oracle IoT cloud [46]	real-time data capture, M2M platform	support millions of device endpoints, heterogeneous connectivity	no support for open source based devices
Microsoft research Lab of Things [47]	smart home services	HomeOS source code (platform, drivers, apps) is available for academic research	available only for Microsoft based products
Open remote [48]	buildings, home automation, healthcare and smart cities services	variety of supported protocols. Cloud services	high cost
KAA [49]	multi-domain open source platform : agriculture, healthcare, industrial IoT, applications for consumer electronics and smart home	open IoT cloud platform. Big data support	limited hardware modules supported
ThingsBoard [50]	open-source IoT platform: data collection, processing, visualization, and device management. Support IoT protocols : MQTT, CoAP and HTTP	data confidentiality and device authentication	relatively new platform and not tested in large scale use
Plotly [51]	data visualization, Interactive charts and dashboards	excellent visualization tools	offers only visualization services
IBM IoT [52]	cognitive IoT	Single Sign-On (SSO) authentication, IDentity as a Service	network latency
Kii [53]	mobile back-end as a service (MBaaS) : user management, data management and push notification functionality, numerous services in multiple areas	API specification is open to the public. Load balancing and security	communication latency between the mobile app and devices
Echelon [54]	industrial platform for different use cases: area and street lighting, building automation, transportation systems	autonomous control and security. Integration of multivendor devices in extensible architecture	high cost, proprietary technology
Axeda [55]	cloud-based software for managing IoT	highly secure communications, M2M learning	integration of third party systems

Table 4 Comparison of the main IoT platforms

5 IoT Challenges for achieving smart cities

As explained previously, IoT relies on multiple technologies. Thus, weaknesses and security issues of IoT could be divided into two categories: (1) issues related to the technologies on which IoT is based on, and (2) new issues that emerge with IoT deployments. Figure 8 illustrates the main IoT characteristics to achieve smart cities and the challenges that must be overcome to achieve such a goal. The main issues are those related to scalability, networking and transport, heterogeneity, privacy and authentication. In this section we discuss these issues. Table 5 summarizes the most common IoT issues that arise from the the three-layered IoT architecture as proposed by ITU-T [56].

5.1 Networking and transport issues

IoT will include a huge number of objects that should be reachable. Besides, each object will produce content that can be retrieved by any authorized user regardless of his/her location. To achieve this goal, effective addressing policies should be implemented. Currently, IPv4 is the most predominant protocol. However, it is well-known that the number of available IPv4 addresses is decreasing rapidly and IPv4 will soon become inadequate in providing new addresses. Therefore, we need to use other addressing policies.

IPv6 addressing represents the best alternative to IPv4. Many works that aim to integrate IPv6 with IoT have been undertaken recently. For example, 6LowPAN [57] describes how to implement IPv6 protocol in a WSN context. However, since RFID tags use identifiers rather than MAC addresses (as standardized by EPC global [58]), it is necessary to propose new solutions in order to enable the addressing of RFID tags in IPv6-based networks. Recently,

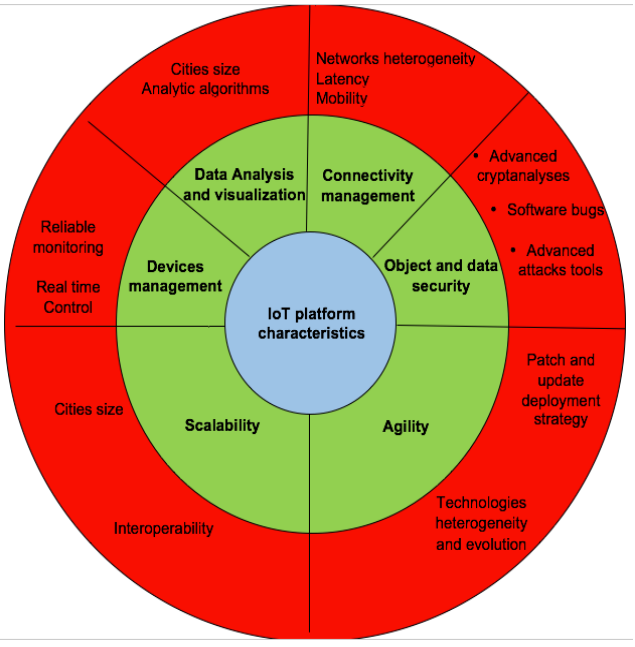

Fig. 8: IoT characteristics to achieve smart city and their limitations

multiple studies that intend to integrate RFID tags into IPv6 networks have been investigated and multiple approaches aimed at integrating RFID identifiers and IPv6 addresses have been proposed

	Issues	*Confidentiality*	*Integrity*	*Authentication*	*Authorization*	*Unlinkability*	*Anonymity*	*Traceability*	*Non-Repudiation*
Application Layer	Applications' issues	x	x	x	x	x	x	x	x
	Storage issues	x	x	x	x		x		
	Key management issues	x	x	x			x	x	x
	Trust management issues		x	x	x				x
	Middleware issues	x	x	x	x	x	x	x	x
	Data integrity issues		x	x					
	Data confidentiality issues	x	x						x
	Data authentication issues		x	x					x
Transportation Layer	WIFI issues	x	x	x	x	x	x	x	x
	ZigBee issues	x	x	x	x	x	x	x	x
	3G issues	x	x	x	x	x	x	x	x
	GPRS issues	x	x	x	x	x	x	x	x
	Network access issues		x	x	x	x	x	x	
	Routing protocols issues		x	x			x		
	Encoding issues		x						
	Heterogeneity issues		x	x			x	x	x
Perception Layer	RFID issues	x	x	x	x	x	x	x	x
	WSN issues	x	x	x	x	x	x	x	x
	RSN issues	x	x	x	x	x	x	x	x
	GPS issues	x	x	x	x	x	x	x	x
	Platform issues	x	x	x	x	x	x	x	x

Table 5 Overview on main IoT issues

[59][60][61]. However, results in this area are not completely mature and in particular there are no standards that currently describe how this integration should be done. It is also important to note that RFID mobility is not supported and still represents an open research issue.

In traditional networks, IP addresses are resolved through the Domain Name System (DNS). In IoT, communications occur between objects. Thus, the concept of Object Name Service (ONS) must be introduced and supported [62] [63] [5]. The difficulty of ONS arises especially in the case where the object is an RFID tag. In this case, the tag identifier (or IP address) is mapped onto an Internet Uniform Reference Locator (URL), which points to the relevant information of the object. In other cases, the ONS must have the capacity to associate the object's description with a given RFID tag identifier (or IP address). However, the design and standardization of such a system is still being investigated by researchers and designers of such systems [5].

The main goals of the transport layer resides in guaranteeing end-to-end reliability and to perform congestion control. In traditional networks, the Transmission Control Protocol (TCP) supports these goals. However, it is known that TCP is not adapted to IoT environments [5] [64] because of many reasons:

1. Connection setup: in TCP, each session begins with a connection phase procedure called the three-way handshake. Within the IoT ecosystem, a small amount of data will be exchanged. Therefore, the setup phase would last for a large part of the session time. This may lead to additional consumption of resources and energy.
2. Congestion control: TCP ensures end-to-end congestion control. In the IoT context, it can generate performance problems as most of the communications are wireless. Indeed, such an environment is not well optimized for TCP [65]. Besides, the exchanged data amount within a single session, is in general, very small. Finally, TCP congestion control is not very adapted to the IoT environment because the whole TCP session includes just the transmission of the first segment and the reception of subsequent acknowledgements [5] [9].
3. Data buffering: TCP stores data in a memory buffer at both source and destination. (1) at the source for retransmission needs and (2) at the destination for ordered delivery purposes. The management and allocation of such buffers may be too costly for objects.

As a result, TCP cannot be used efficiently for the end-to-end transmission control in IoT and new transport layer protocol solutions are required [9]. The transport layer plays an essential role in IoT. Indeed, attacks towards this layer and its underlying routing protocol will seriously affect the network's operation. Therefore, the design of secure and effective routing protocols is an important research area in the IoT context. Due to typical characteristics of IoT objects, existing solutions that have been previously applied to ad hoc and sensor networks do not completely address the needs of IoT. For example, Denial of Service (DoS) attacks could be more easily achieved on multiple IoT systems. The consequences of such attacks would be disastrous to the systems and their end-users. The best way to detect and stop DoS and DDoS attacks is by using Intrusion Detection Systems (IDSs). However, the implementation of such systems in an IoT infrastructure appears to be a very challenging task because of the specific characteristics of the objects and their capabilities.

Another important issue is traffic characterization. Indeed, in IoT, highly heterogeneous objects lead to different scenarios. The characteristics of the related traffic flows generated by these scenarios

have not really been studied extensively [5]. The traffic's characterization represents a is very important step, because it helps network providers to plan the expansion of their infrastructures when it is needed, and to develop appropriate solutions for Quality of Service (QoS) support when needed.

5.2 Security issues

The security of IoT is a major challenge for the sustainability and competitiveness of companies and administrations. The US Federal Trade Commission (FTC) pointed out in a report [66] that the planned deployment of IoT technology will open up various security and privacy issues for IoT users and they need to be well addressed or resolved. For many of these critical IoT applications, the use of incorrect or maliciously corrupted data can have serious consequences. Conventional security solutions such as authentication, confidentiality, and data integrity are critical to IoT objects, networks, and applications. If IoT objects have enough memory and processing power, existing security protocols and algorithms may be applicable, but because of the resource constraints of IoT objects, these existing security solutions are too costly for the objects in IoT.

Security issues remain major obstacles to the worldwide adoption and deployment of IoT. In other words, users will not fully adopt IoT if there is no guarantee that it will protect their privacy. Indeed, IoT is highly vulnerable to attacks for numerous reasons: (1) usually, objects spend most of their time unattended, which makes physical attacks on them relatively easy, (2) most of the communications are wireless, which makes Man-in-the-Middle attack, one of the most common attacks on such a system. Consequently, exchanged messages may be subject to eavesdropping, malicious routing, message tampering and other security issues which can affect the security of the entire IoT, and (3) multiple types of objects such as RFID tags have limited resources in terms of energy and computation power, which prevent them from implementing advanced security solutions.

Connected objects have their own vulnerabilities related to their specific features, in addition to existing vulnerabilities. These new vulnerabilities are caused by:

- Many different types of operating systems are used by the connected objects and are not always well known. The code of an operating system is usually in the order of tens of thousands or millions of lines code. Hence, the likelihood of having vulnerabilities is high.
- There are no known security standards.
- There are many proprietary protocols.
- The architectures are very heterogeneous, and the physical security is often compromised.
- The software integrity update of connected objects is not guaranteed.
- The security of the stored data is not guaranteed.
- The limited resources of a connected object prevent the use of classic cryptographic functions and security protocols.

Data security issues can be summarized into data confidentiality, data authenticity, data integrity, and data freshness. Cryptographic techniques are the best solutions to support these security needs [67].

5.2.1 Data confidentiality, integrity and authentication:

Many IoT application scenarios require high data security, including data confidentiality and data integrity. This requirement can be solved by data encryption. Data encryption algorithms are divided into two categories: (1) symmetric encryption algorithms, and (2) public-key encryption algorithms. The latter consume more resources which make them difficult to implement on objects with limited power and energy resources. In contrast, symmetric algorithms are suitable for such devices and are widely used in this context [67]. However they suffer from several drawbacks: (1) the symmetric key exchange protocols of such cryptosystems are too complex which limits infrastructure scalability [7], and (2) they suffer from the confidentiality problem of shared keys. Indeed, the higher the number of objects is, the bigger is the security risk. If one key is compromised, all system communications are compromised also. As a solution, the system can be divided into multiple groups and a different symmetric key is used within each group. However, the risk remains, since if one key is compromised, the communications with the group are also compromised. To address this problem, researchers have considered public-key encryption algorithms. In this solution, each object owns a pair of public and private keys. Each object keeps its private key, while the base station stores the public keys of all objects. Actually, the main proposals [68] [69] [70] of public key encryption algorithms suitable for IoT [67] include Rabin's Scheme [71], NtruEncrypt[72] and Elliptic Curve Cryptography (ECC) [73]. ECC offers good scalability, without complex key management protocol. However, the application of these algorithms to the IoT environment is still being investigated. In addition, they are not applicable to all types of objects especially RFID tags, where the problem of problem of limited resources remains a challenging issue. Furthermore, public key encryption solution suffers from trust issues. Indeed, a base station that owns public keys cannot prove that the objects are really what they pretend to be.

5.2.2 Key management:

Key management is another important issue in IoT. It is plays a vital role in the implementation of various security solutions. Key management includes multiple steps that include key generation, distribution, storage, update and the destruction. An important component of the key management cycle is key distribution which includes secure transmission and distribution to legitimate users of (1) public keys and shared secrets in the case of asymmetric cryptography, and (2) secret keys in the case of symmetric cryptography.

Numerous works [74] [75] [76] have proposed key management schemes adapted to technologies making up the IoT ecosystem, and more specifically for WSN in recent years. they use symmetric key management, public keys, abbreviated (a shortened certificate where some fields are removed) [77] or implicit certificates. However, these solutions were designed for WSNs primarily, and are not suited for all objects' types. Consequently the design of lightweight key management schemes adapted to the IoT environment and its application scenarios remains a key issue that needs to be solved in the future.

5.2.3 Trust management:

We need to develop and implement trust management mechanisms into IoT. Indeed, in numerous scenarios, the network relies on the cooperation of all nodes. The vulnerability of a single node can have serious consequences on the entire network. Indeed, if an attacker succeeds to compromise or add one or multiple objects in the network, the attacker can provide fake or erroneous information, which can subsequently affect the cooperation of nodes, data treatment and the result provided to the final user. Thus, the credibility of each single node is key to ensuring accurate and reliable network service delivery. Current trust management schemes like those proposed in [74] [78] only provide verification of data consistency and validity, but cannot guarantee objects' authentication. Furthermore, these previously proposed schemes are not completely adaptable to the IoT context. Consequently, more research is needed to develop lightweight trust management techniques and protocols that are specifically well suited for IoT scenarios in the future.

5.3 Heterogeneity issues

Often, in IoT scenarios, data is collected from large number of objects which are widely distributed. However, the data collected in different ways using different protocols typically have different formats. Thus, it is not possible to effectively analyze, process, store such data without some standard format. This lack of standard also makes the integration of data obtained from heterogeneous sources difficult. Thus, it is necessary to develop (1) standards regarding unified data encoding and (2) information exchange protocols that will enable efficient and seamless data collection among heterogeneous IoT objects.

5.4 Denial of service

The huge number of Internet devices in cities provides a real attack vector for malicious people [79] [80]. For example, in a big city, thousands or ten thousands of devices simultaneously communicate with both users and among themselves, the security implications are significant. Smart cities are the ideal target for hackers to create IoT bot networks. An IoT botnet consists of devices compromised and used to perform different tasks without the knowledge of their legitimate users. In 2016, Dyn firm* suffered from a denial of service attack caused by tens of thousands of connected objects (they were mostly connected cameras manufactured by the Chinese manufacturer XiongMai) to saturate its infrastructure†. The attack resulted in Dyn's inability to provide the DNS service. Some of connected objects involved in the attack was caused by Mirai malware [81]. This tool exploits vulnerabilities present in some connected objects such as the use of a default password that has not changed by users. Hence, IoT networks are increasingly being used as an attack platform by malicious attackers.

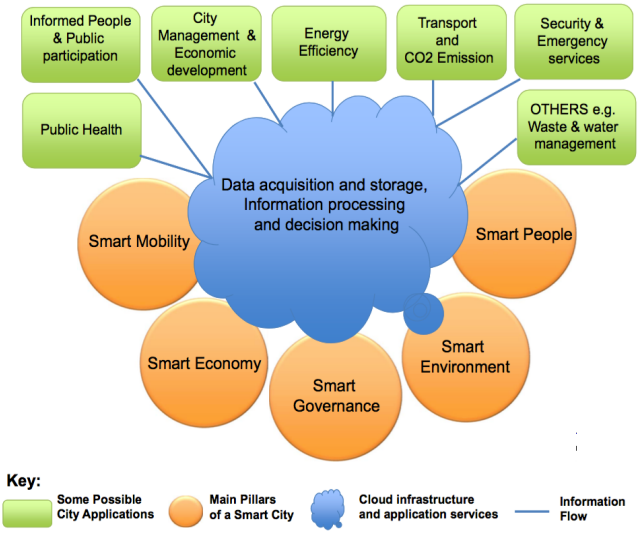

Fig. 9: Cross thematic data management and analysis for smart city applications in a cloud computing environment [82]

5.5 Big data management

As we mentioned previously, a smart city relies primarily on communication technologies. Thus, as the number of devices grows exponentially, a smart city becomes a source of huge amounts of data often referred to as big data [83] [84]. Indeed, according to the literature [85] [83] [86], big data is characterized by specific characteristics which when related to smart cities, we note that:

- ***Volume:*** the huge number of devices generates continuously generate large amounts of data.
- ***Velocity:*** for many applications data is created and used in real or near real-time. For example, traffic data must be used in real time to inform users and to guide them [87]. Another example is social media, where, sometimes messages, tweets, status updates, and so on which are only a few seconds old may no longer be of interest to users.
- ***Variety:*** there are multiple types of devices, parts of different applications that are communicating through various protocols that generate a lot of heterogeneous data.

An efficient use, mashing and correlation of these different types of data can enhance multiple applications and tasks such as:

- Facilitating decision making in order to enhance the quality of service offered to end-users.
- Visualization and simulation of events and use cases.
- Modeling new use case scenarios.
- Accidents and disaster management.

For example, if an accident occurs, it will be reported to the management infrastructure (center) through traffic information. Then, the management center sends the nearest police cars (having lower task priorities according to their transmitted information) and requests for ambulances. Besides, the center sends accident warnings to car drivers in the accident area through car's Human Machine Interfaces (HMI) and road advertisement boards, and recommends journey modifications to cars going through the accident area. It can also modify traffic flows and lights to facilitate ambulances' tasks. The same scenario is possible in case of fire where the management center will be informed through dedicated devices.

However, none of the aforementioned benefits can be achieved without an efficient way to manage and leverage such large quantities of data generated and large-scale infrastructures. Currently, the most popular technology is cloud computing [85] [88] [82] [89]. Indeed, cloud computing solutions help in the storage, visualization, and processing of the data collected in order to make timely inferences and decisions. [82]. Figure 9 depicts data management and analysis for smart city applications in a cloud based environment.

Fig. 10: Centro De Operacoes Prefeitura Do Rio*data analytics center

There are numerous examples of applications that manage and analyze city data, and provide helpful information to users. The authors in [85] discuss several interesting use cases. One example is the collaboration between IBM and the Brazilian government to build a city-wide instrumented system that collects, processes and analyzes data flows from 30 sources such as weather data, traffic state and public transport data, emergency services data, municipal and utility services data, and so on. The correlation and mashing of information investigate particular aspects of city life to continuously propose new solutions. This data analytics center, called "Centro De Operacoes Prefeitura Do Rio†" is located in Rio De Janeiro [85] (as shown in Figure 10).

Dyn is one of the companies providing DNS service

†*https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/*

http://ultimosegundo.ig.com.br/brasil/rj/2012-05-03/ig-visita-o-centro-de-operacoes-do-rio-de-janeiro.html

†*http://ultimosegundo.ig.com.br/brasil/rj/2012-05-03/ig-visita-o-centro-de-operacoes-do-rio-de-janeiro.html*

Fig. 11: Screenshots of SmartSantanderRA mobile application*†

Another example is SmartSantanderRA‡ which represents a reality augmented application that includes information from about 2700 places such as beaches, parks and gardens, monuments, Points Of Interest (POI), tourism offices, shops, art galleries, museums, libraries, culture events agenda, shops, public buses, taxis, bikes, parking places, and so on in the city of Santander (Spain) [85]. SmartSantanderRA allows real time access to traffic and beaches' cameras, weather reports and forecast, information about public buses and bike-rental service thereby generating a unique ecosystem for citizens and visitors when walking around the city. Figure 11 presents examples of the mobile application's screenshots.

Cloud-based solutions can meet the majority of smart city applications requirements. However, considering the current infrastructure scalability evolution, these types of solutions alone will become inadequate in meeting future requirements of smart city applications (especially those real-time ones) because of the: the physical distance between data collection and its processing and the central nature of cloud computing. To address these aforementioned challenges, Fog-based computing and Edge computing solutions have been proposed [90] [91] [92]. Fog computing is a computing infrastructure that extends the cloud computing solution by keeping the advantages and power of the cloud closer to where data is created and acted upon all by relying on a decentralized infrastructure. Data, processing, storage and applications are distributed in the most logical and efficient locations between the data source and the cloud. Similarly, Edge computing brings data processing at the periphery of the network, as close as possible to the data source [93] [94].

6 Conclusion

With the expansion and the growth of cities, making them smart becomes vital. Indeed, numerous governments such as US, Chinese or UAE launched smart city's projects e.g. Malmo, Fujisawa, Songdo and Masdar.

IoT represents the best way to make a city smart. Indeed, IoT can applied in multiple scenarios such as monitoring of building's status with passive WSNs, environmental monitoring e.g. Gas concentration, Water level for lakes or soil humidity, waste management, smart parking, reducing CO2 footprint, or autonomous driving. Achieving such goals needs a tremendous number of connected objects. Indeed, the number of connected objects is growing exponentially and it is estimated that 50 billion connected objects will be deployed in smart cities by 2020. However, this high number will open up numerous risks and privacy issues.

In this work, we presented an overview of IoT in the context of smart cities, and discussed how it can enhance a city's smartness. We also identified the weaknesses and risks associated to IoT deployment and adoption in the smart city environment.

As part of our future work, we plan to survey the different solutions and recommendations to address several of the challenges of IoT and smart cities we have discussed in this paper and in particular the security challenges and issues.

Acknowledgments.

We thank the anonymous reviewers for their comments which helped us improve the content and quality of this paper.

7 References

1 Rida Khatoun and Sherali Zeadally. Smart cities: concepts, architectures, research opportunities. *Communications of the ACM*, 59(8):46–57, 2016.

2 Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things. Technical report, Gartner, Inc, 2016.

3 Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645 – 1660, 2013.

4 Coordination And Support Action for Global RFID-related Activities and Standardisation: RFID and the Inclusive Model for the Internet of Things. Technical report, CASAGRAS, 2009.

5 Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

6 Debasis Bandyopadhyay and Jaydip Sen. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1):49–69, 2011.

7 Debiao He and Sherali Zeadally. An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE internet of things journal*, 2(1):72–83, 2015.

8 Next Generation Networks - Frameworks and functional architecture models. Recommendation ITU-T Y.2060. Overview of the Internet of things. Technical report, International Telecommunication Union, 2012.

9 Oladayo Bello, Sherali Zeadally, and Mohamad Badra. Network layer interoperation of device-to-device communication technologies in internet of things (iot). *Ad Hoc Networks*, 57:52 – 62, 2017. Special Issue on Internet of Things and Smart Cities: security, privacy and new technologies.

10 Hanna Okkonen, Oleksiy Mazhelis, Petri Ahokangas, Pasi Pussinen, Mervi Rajahonka, Riikka Siuruainen, Seppo Leminen, Alexey Shveykovskiy, Jenni Myllykoski, and Henna Warma. Internet-of-things market, value networks, and business models: state of the art report. *Computer science and information systems reports. TR, Technical reports 39.*, 2013.

11 Damian Christie. IoT Standards, Why so many? `https://www.linkedin.com/pulse/iot-standards-why-so-many-damian-christie`, 2016.

12 Xue Li, Jing Liu, Quan Z. Sheng, Sherali Zeadally, and Weicai Zhong. Tms-rfid: Temporal management of large-scale rfid applications. *Information Systems Frontiers*, 13(4):481–500, 2011.

13 Quan Z Sheng, Xue Li, and Sherali Zeadally. Enabling next-generation rfid applications: Solutions and challenges. *Computer*, 41(9):21–28, 2008.

‡*http://www.smartsantander.eu/index.php/blog/item/174-smartsantanderra-santander-augmented-reality-application*

†*http://www.mobogenie.com/download-smartsantanderra-941886.html*

†*http://www.apkmonk.com/app/es.unican.tlmat.smartsantanderra/*

14 Wordpress. The Internet of Things Protocol stack âĂŞ from sensors to business value. https://entrepreneurshiptalk.wordpress.com/2014/01/29/the-internet-of-thing-protocol-stack-from-sensors-to-business-value/, 2014.

15 Colin Harrison, Barbara Eckman, Rick Hamilton, Perry Hartswick, Jayant Kalagnanam, Jurij Paraszczak, and Peter Williams. Foundations for smarter cities. *IBM Journal of Research and Development*, 54(4):1–16, 2010.

16 Jiong Jin, Jayavardhana Gubbi, Slaven Marusic, and Marimuthu Palaniswami. An information framework for creating a smart city through internet of things. *IEEE Internet of Things Journal*, 1(2):112–121, 2014.

17 LoRa Alliance. Wide Area Networks For IoT. https://www.lora-alliance.org, 2017.

18 LoRa Alliance. LoRa Technology. https://www.lora-alliance.org/What-Is-LoRa/Technology, 2017.

19 Keith E Nolan, Wael Guibene, and Mark Y Kelly. An evaluation of low power wide area network technologies for the Internet of Things. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International*, pages 439–444. IEEE, 2016.

20 LoRaWAN, What is it. A Technical Overview of LoRa and LoRaWAN. Technical report, LoRa Alliance. Technical Marketing Workgroup 1.0, November 2015.

21 CNXSOFT. Comparison Table of Low Power WAN Standards for Industrial Applications. http://www.cnx-software.com/2015/09/21/comparison-table-of-low-power-wan-standards-for-industrial-applications/, 2015.

22 Worldwide Internet of Things Forecast Update, 2016âĂŞ2020. Technical report, IDC, 2016.

23 J. A. Guerrero-Ibáñez, C. Flores-Cortés, and Sherali Zeadally. *Vehicular Ad-hoc Networks (VANETs): Architecture, Protocols and Applications*, pages 49–70. Springer London, 2013.

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

25 Tomás Sánchez López, Damith C Ranasinghe, Mark Harrison, and Duncan McFarlane. Adding sense to the Internet of Things. *Personal and Ubiquitous Computing*, 16(3):291–308, 2012.

26 Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32, 2014.

27 Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12):2292–2330, 2008.

28 Mihai T Lazarescu. Design of a wsn platform for long-term environmental monitoring for iot applications. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 3(1):45–54, 2013.

29 Dijana Capeska Bogatinoska, Reza Malekian, Jasna Trengoska, and William Asiama Nyako. Advanced sensing and internet of things in smart cities. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention on*, pages 632–637. IEEE, 2016.

30 Radek Fujdiak, Pavel Masek, Petr Mlynek, Jiri Misurec, and Ekaterina Olshannikova. Using genetic algorithm for advanced municipal waste collection in smart city. In *Communication Systems, Networks and Digital Signal Processing (CSNDSP), 2016 10th International Symposium on*, pages 1–6. IEEE, 2016.

31 Zeydin Pala and Nihat Inanc. Smart parking applications using RFID technology. In *RFID Eurasia, 2007 1st Annual*, pages 1–3. IEEE, 2007.

32 Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. Vehicular ad hoc networks (vanets): status, results, and challenges. *Telecommunication Systems*, 50(4):217–241, 2012.

33 Rongxing Lu, Xiaodong Lin, Haojin Zhu, and Xuemin Shen. SPARK: A new VANET-based smart parking scheme for large parking lots. In *INFOCOM 2009, IEEE*, pages 1413–1421. IEEE, 2009.

34 Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73–81, 2006.

35 Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, and Silvana Andreescu. Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. In *Services Computing (SCC), 2015 IEEE International Conference on*, pages 285–292. IEEE, 2015.

36 Marcus Handte, Stefan Foell, Stephan Wagner, Gerd Kortuem, and Pedro José Marrón. An Internet-of-Things Enabled Connected Navigation System for Urban Bus Riders. *IEEE internet of things journal*, 3(5):735–744, 2016.

37 Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart gridâĂŤthe new and improved power grid: A survey. *IEEE communications surveys & tutorials*, 14(4):944–980, 2012.

38 Jianming Liu, Xiangzhen Li, Xi Chen, Yan Zhen, and Lingkang Zeng. Applications of internet of things on smart grid in china. In *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, pages 13–17. IEEE, 2011.

39 Urban Mobility System Upgrade How shared self-driving cars could change city traffic. Technical report, OECD/International Transport Forum, 2015.

40 Renault NEXT TWO et la vie Ãă bord hyper- connectÃľe pour tous. Technical report, Renault, 2014.

41 Vangelis Gazis, Manuel Görtz, Marco Huber, Alessandro Leonardi, Kostas Mathioudakis, Alexander Wiesmaier, Florian Zeiger, and Emmanouil Vasilomanolakis. A survey of technologies for the internet of things. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International*, pages 1090–1095. IEEE, 2015.

42 Miyuru Dayarathna. Comparing 11 IoT Development Platforms. https://dzone.com/articles/iot-software-platform-comparison, 2016.

43 Padraig Scully. 5 Things To Know About The IoT Platform Ecosystem. https://iot-analytics.com/5-things-know-about-iot-platform/, 2016.

44 IoT Platforms: Market Report 2015-2021. Technical report, IoT Analytics Insights for the Internet of Things, 2016.

45 Amazon Web Services. AWS IoT. https://aws.amazon.com/iot-platform/, 2017.

46 Oracle. Oracle Internet of Things Cloud Service. https://aws.amazon.com/iot-platform/, 2017.

47 Microsoft. Microsoft Research, Lab of Things. http://www.lab-of-things.com, 2013.

48 OpenRemote. OpenRemote is the Open Source Middleware for the Internet of Things. http://www.openremote.com, 2016.

49 KAA. KAA: The truly open-source Kaa IoT Platform. https://www.kaaproject.org, 2014.

50 ThingsBoard. ThingsBoard: Open-source IoT Platform. https://thingsboard.io, 2017.

51 Plotly. Plotly: Visualize Data, Together. https://plot.ly, 2017.

52 IBM. IBM Watson IoT Platform. https://internetofthings.ibmcloud.com/#/, 2017.

53 KII. KII Platform. https://en.kii.com, 2016.

54 Echelon. Echelon: Industrial Internet of Things. http://www.echelon.com/izot-platform, 2017.

55 Axeda. Axeda Machine Cloud. https://www.ptc.com/en/axeda, 2017.

56 Y ITU-T. Overview of ubiquitous networking and of its support in NGN. *ITU-T Recommendation*, 2009.

57 Zach Shelby and Carsten Bormann. *6LoWPAN: The wireless embedded Internet*, volume 43. John Wiley & Sons, 2011.

58 Ken Traub, Greg Allgair, Henri Barthel, Leo Burstein, John Garrett, Bernie Hogan, Bryan Rodrigues, Sanjay Sarma, Johannes Schmidt, Chuck Schramek, et al. The EPCglobal architecture framework. *EPCglobal Ratified specification*, 2005.

59 Sang-Do Lee, Myung-Ki Shin, and Hyoung-Jun Kim. EPC vs. IPv6 mapping mechanism. In *Advanced Communication Technology, The 9th International Conference on*, volume 2, pages 1243–1245. IEEE, 2007.

60 Dong Geun Yoon, Dong Hyeon Lee, Chang Ho Seo, and Seong Gon Choi. RFID networking mechanism using address management agent. In *Networked Computing and Advanced Information Management, 2008. NCM'08. Fourth International Conference on*, volume 1, pages 617–622. IEEE, 2008.

61 PC Jain and KP Vijaygopalan. RFID and wireless sensor networks. *Proceedings of ASCNT–2010, CDAC, Noida, India*, pages 1–11, 2010.

62 Ratified Standard Specification with Approved, Fixed Errata. EPCglobal Object Name Service (ONS) 1.0.1. Technical report, EPCglobal Inc, May 2008.

63 Ratified Standard. GS1 Object Name Service (ONS) Version 2.0.1. Technical report, GS1, January 2013.

64 Oladayo Bello and Sherali Zeadally. Intelligent device-to-device communication in the internet of things. *IEEE Systems Journal*, 10(3):1172–1182, 2016.

65 TV Lakshman and Upamanyu Madhow. The performance of tcp/ip for networks with high bandwidth-delay products and random loss. *IEEE/ACM Transactions on Networking (ToN)*, 5(3):336–350, 1997.

66 Internet of Things: Privacy and Security in a Connected World. Technical report, US Federal Trade Commission (FTC), 2015.

67 Qi Jing, Athanasios V Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. Security of the internet of things: Perspectives and challenges. *Wireless Networks*, 20(8):2481–2501, 2014.

68 Kai Han, Jun Luo, Yang Liu, and Athanasios V Vasilakos. Algorithm design for data communications in duty-cycled wireless sensor networks: A survey. *IEEE Communications Magazine*, 51(7):107–113, 2013.

69 David J Malan, Matt Welsh, and Michael D Smith. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*, pages 71–80. IEEE, 2004.

70 Mo Li, Zhenjiang Li, and Athanasios V Vasilakos. A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues. *Proceedings of the IEEE*, 101(12):2538–2557, 2013.

71 Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

72 J Hoffstein, N Howgrave-Graham, J Pipher, JH Silverman, and W Whyte. NTRUEncrypt and NTRUSign: efficient public key algorithms for a post-quantum world. In *Proceedings of the International Workshop on Post-Quantum Cryptography (PQCrypto 2006)*, pages 71–77, 2006.

73 Darrel Hankerson, Alfred J Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

74 Laurent Eschenauer and Virgil D Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 41–47. ACM, 2002.

75 Gunnar Gaubatz, J-P Kaps, Erdinc Ozturk, and Berk Sunar. State of the art in ultra-low power public key cryptography for wireless sensor networks. In *Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on*, pages 146–150. IEEE, 2005.

76 Adrian Perrig, Robert Szewczyk, Justin Douglas Tygar, Victor Wen, and David E Culler. SPINS: Security protocols for sensor networks. *Wireless networks*, 8(5):521–534, 2002.

77 Arvinderpal S Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz. Energy analysis of public-key cryptography for wireless sensor networks. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pages 324–328. IEEE, 2005.

78 TV LANDEGEM and H Viswanathan. Anywhere, anytime, immersive communications [j]. *Enriching Communications*, 2(1):1–6, 2008.
79 M Rmayti, Youcef Begriche, Rida Khatoun, Lyes Khoukhi, and Dominique Gaiti. Denial of service (dos) attacks detection in manets using bayesian classifiers. In *Communications and Vehicular Technology in the Benelux (SCVT), 2014 IEEE 21st Symposium on*, pages 7–12. IEEE, 2014.
80 Juliette Dromard, Rida Khatoun, and Lyes Khoukhi. A watchdog extension scheme considering packet loss for a reputation system in wireless mesh network. In *Telecommunications (ICT), 2013 20th International Conference on*, pages 1–5. IEEE, 2013.
81 John Biggs. Hackers release source code for a powerful DDoS app called Mirai. `https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-appcalled-mirai/`, October 2016.
82 Zaheer Khan, Ashiq Anjum, and Saad Liaquat Kiani. Cloud based big data analytics for smart future cities. In *Proceedings of the 2013 IEEE/ACM 6th international conference on utility and cloud computing*, pages 381–386. IEEE Computer Society, 2013.
83 James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela H Byers. Big data: The next frontier for innovation, competition, and productivity. Technical report, McKinsey Global Institute, 2011.
84 Saint John Walker. Big data a revolution that will transform how we live work and think, 2014.
85 Rob Kitchin. The real-time city? big data and smart urbanism. *GeoJournal*, 79(1):1–14, 2014.
86 Min Chen, Shiwen Mao, and Yunhao Liu. Big data: A survey. *Mobile Networks and Applications*, 19(2):171–209, 2014.
87 Juan Contreras-Castillo, Sherali Zeadally, and Juan Antonio Guerrero Ibañez. Solving vehicular ad hoc network challenges with big data solutions. *IET Networks*, 5(4):81–84, 2016.
88 Michael Batty. Big data, smart cities and city planning. *Dialogues in Human Geography*, 3(3):274–279, 2013.
89 Yogesh Simmhan, Saima Aman, Alok Kumbhare, Rongyang Liu, Sam Stevens, Qunzhi Zhou, and Viktor Prasanna. Cloud-based software platform for big data analytics in smart grids. *Computing in Science & Engineering*, 15(4):38–47, 2013.
90 Margaret Rouse. fog computing (fog networking, fogging). `http://searchdatacenter.techtarget.com/definition/edge-computing`, 2016.
91 Flavio Bonomi, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pages 13–16. ACM, 2012.
92 Flavio Bonomi, Rodolfo Milito, Preethi Natarajan, and Jiang Zhu. Fog computing: A platform for internet of things and analytics. In *Big Data and Internet of Things: A Roadmap for Smart Environments*, pages 169–186. Springer, 2014.
93 Margaret Rouse. edge computing. `http://searchdatacenter.techtarget.com/definition/edge-computing`, 2016.
94 Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5):637–646, 2016.