American Journal of Humanities and Social Sciences Research (AJHSSR)
e-ISSN : 2378-703X
Volume-07, Issue-02, pp-158-165
www.ajhssr.com
Research Paper Open Access

Implementation of IoTs in Smart Cities

[1]Nikolaos Raptis, [2]Charalampos Trasanidis , [3]Vasiliki Delitheou
[1]*MBA in entrepreneurship and innovation, Frederic University Cyprus*
[2]*University of Sheffield, Sheffield, Engla*
[3]*Panteion University of Social and Political Sciences, Athens, Greece*

ABSTRACT : The Internet of Things (IoT) describes a special network with many physical things which have embedded sensors, software, and other technologies. These devices, such as traffic lights, vehicles, home alarms and other objects are connected for the purpose of exchanging data with other devices and systems over the internet. The IoT technology is utilized by Smart Cities, to offer many benefits to the state in conjunction with LP-WAN. In this assignment we will refer to LP-WAN in wireless communication technology and the three famous technologies that support this technology, which are SigFox, LoRaWAN and NB-IoT and how to apply in the smart cities. In addition, we will report a threat that smart cities face nowadays, and specifically we will describe what the DDoS threat is and how it can affect the network of smart cities. Finally, we describe a recent incident DDoS attack, approaching the incident which is known Stuxnet

Key Words: *LPWAN, SigFox, NB-IoT, LoRa, Smart Cities, DDoS, Stuxnet*

Subject Area: Internet of Things

Abbreviations

ACCUS	Adaptive Cooperative Control in Urban (sub) System
AI	Artificial Intelligent
D-BPSK	Differential Binary Phase-Shift Keying
DDoS	Distributed Denial of Service
ICT	Information Communication Technologies
ICP	Integration and Coordination Platform
IoT	Internet of Thinks
LP-WAN	Low Power Wide Area Network
LoRaWAN	Long Rate Wide Area Network
NB-IoT	Narrow Band Internet of Thinks
WAN	Wide Area Network

Contents

I. INTRODUCTION

Research shows that there has been an increasing trend of large people moving towards urban living. This means that by 2030 according to forecasts, there will be a 60% increase of population living in urban environments; some of the systems can address the challenges (Gaur et al, 2015). The challenges created by this massive urban migration in terms of housing, electricity, heating, and schooling (not to mention job creation) are overwhelming. In order to develop intelligent solutions, a combination of smart networks (Internet of Data, Internet of Things, Internet of Services and Internet of People) can be used to minimize environmental impact while maximizing social well-being and promoting collaborative ecosystems (Appio, Lima and Paroutis, 2019).

One of the most crucial sectors of European countries is the public sector, which is the regulatory factor of their economic and social cohesion. One of the targets of the public sector is to simultaneously provide the best and eco-friendly services to the citizens, maintaining the budget to a cost-effective level (V. Delitheou et M. Maraki, 2011, p. 10).

The implementation of Information and Communication Technologies (ICTs) in the public sector combined with new innovative culture and changes should improve the total providing services to the citizens, by enhancing productivity and effectiveness (V. Delitheou et M. Maraki, 2011, p. 11).

Moreover, electronic Government implemented by the public sector can provide 24 hour a day, 7 days a week and 365 days a year services to the citizens, improving the two-way interaction.

According to Hiller and Belanger (2001), there are 5 stages-levels of electronic governance. and according to Lee and Layne (2001) there are 4 phases of development. In the Public Administration of European Union countries there are 4 levels-stages of electronic Governance scaling: 1) Information which are provided to the citizens by Public Administration, 2) Interaction through the Public Administration's websites 3) Two-way interaction which offer an electronic access to the citizens in those websites by their authentication and finally 4) the transaction by providing to the citizens a holistic electronic services via Public Administration's websites to the citizens/users.

However, the ecosystems of smart cities are not simply because the urban environment is described by incorporating several complex systems of infrastructure, human behavior, technology, social and political structures and economy (Gaur et al, 2015). Smart cities should be applying the new technologies or updating existing ones to provide necessary services and infrastructure to increase the social economic and environmental benefits that contribute to improve the quality of life and sustainable urban development.

The implementation of the IoT in an urban environment is of particular interest, as it responds to the intention of many national governments to adopt information and communication technology (ICT) solutions in the management of public affairs. They thus implement the smart city (Smart City), which has as its ultimate goal the best possible use of public resources, aiming to improve the quality of services offered, while reducing the operating costs of public bodies.The introduction of ICT in urban governance brings benefits to the management and improvement of traditional public services such as transport and parking, public lighting, surveillance and maintenance of public spaces, cultural heritage conservation, waste collection, hospital and school hygiene(Zaxaropoulou, 2020).

IOTs in smart cities can be implemented in numerous sectors related to citizens. Some of these sectors are Urban issues, transportation, healthcare, entrepreneurship, education, payments, financial issues (taxes, penalties, e.t.c.), infrastructures and environment protection. All those sectors should be developed through this implementation, providing simultaneously advanced services to the citizens V. Delitheou et M. Maraki, 2011, p. 29).

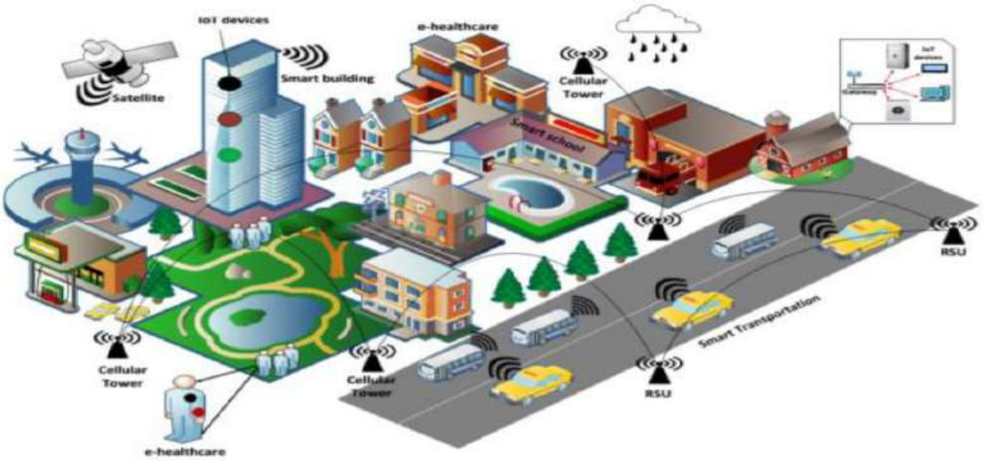


Figure 1: Smart City based on IoT

According to the above, we could say that the innovation ecosystem of smart cities consists of infrastructure of smart cities that can lead to unique collaborative ecosystems that consist of citizens, prosumers, industries, universities and research centers and may develop innovative products, services and solutions. So we notice that in contrast to the traditional marketplace that there are only two parties, supply and demand in a smart ecosystem involves more than actors engaged regarding private, public consumption, production education, research, entertainment and professional activities (Appio, Lima and Paroutis, 2019).

In conclusion, the ecosystem of smart cities represents a lifestyle based on the use of unprecedented technologies such as AI, IoT and Big Data and have become a priority in development strategies of many countries all over the word. It is not random that in 2025 around 10 million people will be living in 34 smart cities all over the word and that almost 70% of the world population will be living in such cities in 2050(Khalifa, 2020).

1. Communication Technologies in Smart Cities

1.1 LoRa

This section of assignment we discuss the three technologies that are applied to wireless technology communication which is called LoRa. However, let me say a few things about LoRa. LoRa is a long-range, low-power, low-bitrate, wireless telecommunications system, promoted as an infrastructure solution for the Internet of Things: end-devices use LoRa across a single wireless hop to communicate to gateway(s), connected to the Internet and which act as transparent bridges and relay messages between these end-devices and a central network server. This technology can be applied to the SigFox, LoRaWAN and NB-IoT technologies which are described immediately.

1.2 SigFox

As we refer above the SigFox technology is part of the LPWAN family of technologies, employed mainly for the development of the IoT networks, when we want send data that is oftentimes taken from the sensors with low ranging from a few bytes and reaching hundreds of kilobytes, and we achieve to cover high range tens of km, and at the same time to consumption very low energy (Lavric, Petrariu, and Popa, 2019). Specifically, the SigFox make use of the D-BPSK modulation for which a message has a fixed bandwidth 100Hz and the transfer speed of data is low, supporting either 4, 8 or 12 bytes, the maximum data rate is approximately 100 bps of Europe or 600 bps rate for USA.

Also, SigFox operates within an unlicensed frequency spectrum less than 1 GHz, with 868MHz in Europe and 915MHz in USA. This modulation technique is part of UNB modulation type and with Chirp Spreading that is used by the other two technologies LoRaWAN and NB-IoT ensure connection between nodes and BS with low-power consumption.

However, the SigFox infrastructure is still under construction in Europe, meanwhile new agreements are being worked upon by the biggest mobile network operators, so that great coverage stretch that aims at farther areas than those dealt with nowadays, can be realized (Lavric, Petrariu and Popa, 2019).

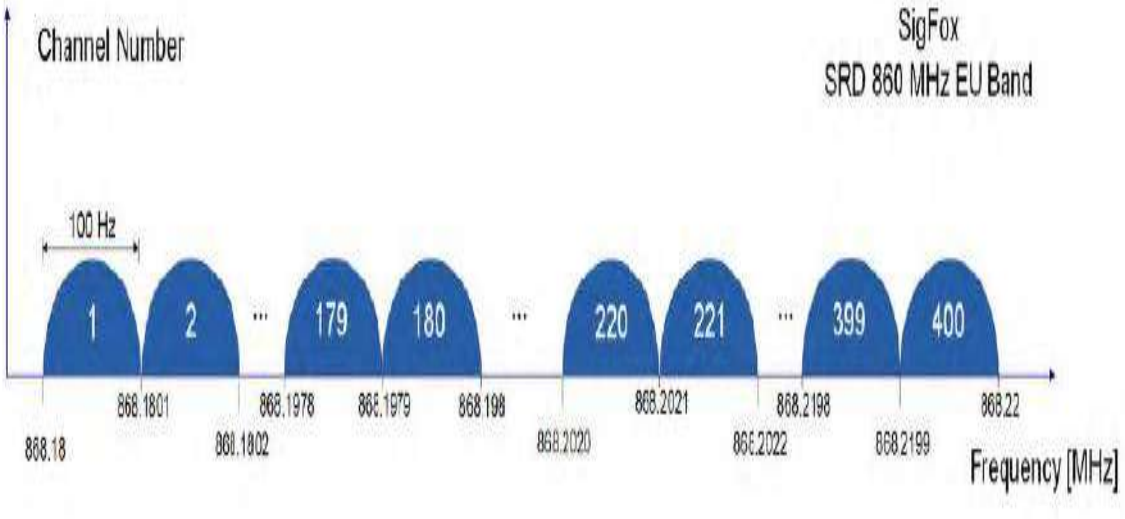


Figure 2 SigFox channel allocation

1.3 LoRaWAN

Let's get acquainted with LoRaWAN. LoRaWAN L is a MAC protocol, which is built to use the LoRa physical layer. It is designed mainly for sensor networks, where sensors exchange packets with the server with a low data rate and relatively long-time intervals that are sometimes per hour or even days.

LoRaWAN is defined by specification components to achieve the main goal which is to transfer packet data with energy low consumption and in a wide area. For this reason, end –devices have sensors with low power consumption and ability to communicate with gateways using the physical layer LoRa. Also, each gateway can forward packets coming from end –devices to a network over an IP backhaul interface allowing a bigger throughput, such as Ethernet or 3G and at the same time can have the ability a data packet be received or forward by more than one gateway.

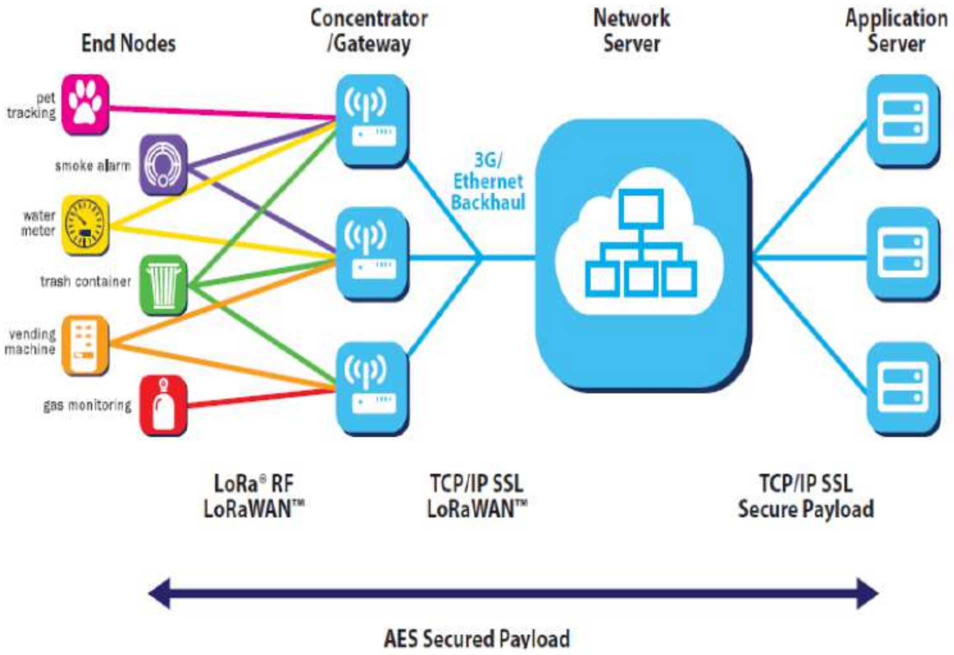


Figure 3 LoRaWAN Network Architecture

It is worth mentioning that LoRaWAN has three different classes of end-devices to address the various needs of applications.

Class A: In this class, end-devices can schedule an uplink transmission based on a random variation before transmission. For downlink transmission from the server at any other time it has to wait until the next uplink transmission occurs. This class is most energy efficient and must be supported by all devices.

Class B: In this class, end-devices have open extra receive windows at scheduled times. Slotted communications synchronized with beacons from the gateway and network server are able to know when the end-device is listening.

Class C: The final class C, end-devices which can afford to listen continuously and with no latency for downlink communication (Augustin et al, 2016).

1.4 NB-IoT

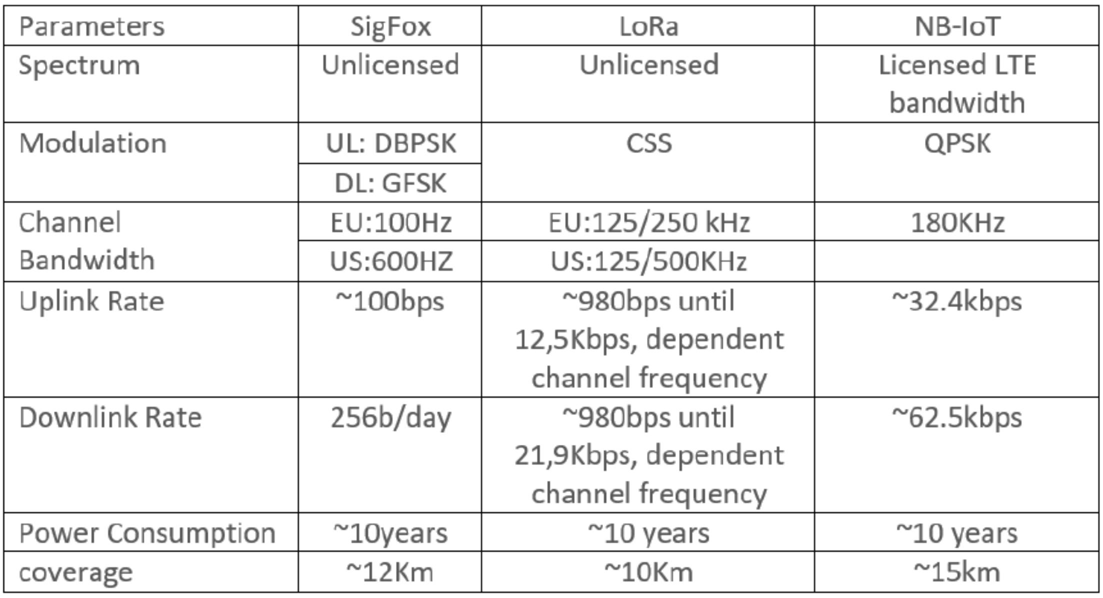
NB-IoT technology is a promising and necessary technology in IoT and consists of the main protocol for LoRa. NB-IoT evolves quickly, and its operations are based on cellular networks, which work in authorized frequency bands. As far as the technical characteristic, these downlink transmission rates supported by NB-IoT are within 250 kbits. Its channel bandwidth is limited to 180 KHz. Also, NB-IoT has strong anti-interference, high reliability, wide coverage and so on. Consequently, it works well for low-rate communication businesses. The main applications concern smart metering, smart grid and smart environment monitoring.

Narrow Band Internet of Things (NB-IoT) supports ultra low power consumption, wide area coverage and massive connections, which is the indispensable LPWAN technology today.

The Narrow Band Internet of things also known as LTE Cat NB1 can support the 3GPP security. Also, it can provide encrypted data and signaling protection with a physical SIM card that is connected to the device. Because of this, the NB-IoT is cost effective, provides low consumption power and wide range of coverage, makes it important in the IoT industry and consists of a protocol bridge and cooperation between LoRa network and Cellular network. NB-IoT is used to deploy a very high volume of low complexity, connected devices intended to transmit small data packages now and then. It affects smart cities, smart buildings, and consumers (Xin et al, 2019).

NB-IoT holds a special position opposite technologies in the unlicensed spectrum because the NB-IoT is able to significantly reduce the common interference problem. In this way, its functions can guarantee which services will operate on given frequencies and bands, and in combination with prioritizing data guarantee high quality of service (QoS). In addition, NB-IoT allows a very large number of network objects per radio cell, about 50,000 devices. NB-IoT is also doing well as it comes to downlink transfer and upload data and for these reasons NB-IoT will significantly play a role in the close future of wireless technology communication (Brdulak, 2020).

Finally, after completing the report on LoRa and the technologies that support it, we present a comprehensive table with the main features of the above technologies.



Parameters	SigFox	LoRa	NB-IoT
Spectrum	Unlicensed	Unlicensed	Licensed LTE bandwidth
Modulation	UL: DBPSK	CSS	QPSK
	DL: GFSK		
Channel Bandwidth	EU:100Hz	EU:125/250 kHz	180KHz
	US:600HZ	US:125/500KHz	
Uplink Rate	~100bps	~980bps until 12,5Kbps, dependent channel frequency	~32.4kbps
Downlink Rate	256b/day	~980bps until 21,9Kbps, dependent channel frequency	~62.5kbps
Power Consumption	~10years	~10 years	~10 years
coverage	~12Km	~10Km	~15km

Table 1: Main Features

2. Threat on Smart Cities

One of the hot issues for discussing smart cities is security and privacy. So each smart city is concerned about the threats that it comes to face and these concerns are bigger due to increasing rapidly worldwide the IoT and smart cities. In this field we discuss the DDoS attack, and we refer to a recent incident which is known as Stuxnet.

2.1 DDoS Attack Threat against Smart City

The smart city ecosystem comprises three layers that can be exposed in threats and attacks. These layers are core, communication, and the edge. Core layers is the technology platform (cloud, IoT data perform) that processes data and generates business logic to make sense of the data flowing from the edge. The communication layer is the channel (Bluetooth, NFC, LTE, Wi-Fi Direct, etc.) establishes a constant two-way data exchange between the core and edge to seamlessly integrate the various components of the ecosystem. The last layer but not least is the edge that comprises devices such as smartphones, sensors as well as IoT applications such as smart lighting and smart trash collection. In the jargon of IT, edge is a front end of smart cities. The security goals of a smart cities are confidentiality, integrity and availability of data, systems and processes

Let me talk about the attack which compromises the availability. The Denial of Services (DoS) and Distributed Denial of Service (DDos) attack, one to one or more to one, is an attack that comprise the network layer when attackers attempt to overwhelm the network resources of the targeted victim with bandwidth consuming assaults such as TCP UDP ICMP. However more sophisticated attacks are those that attack the application layer and the protocols such as HTTP, DNS, VoIP, or SMTP.

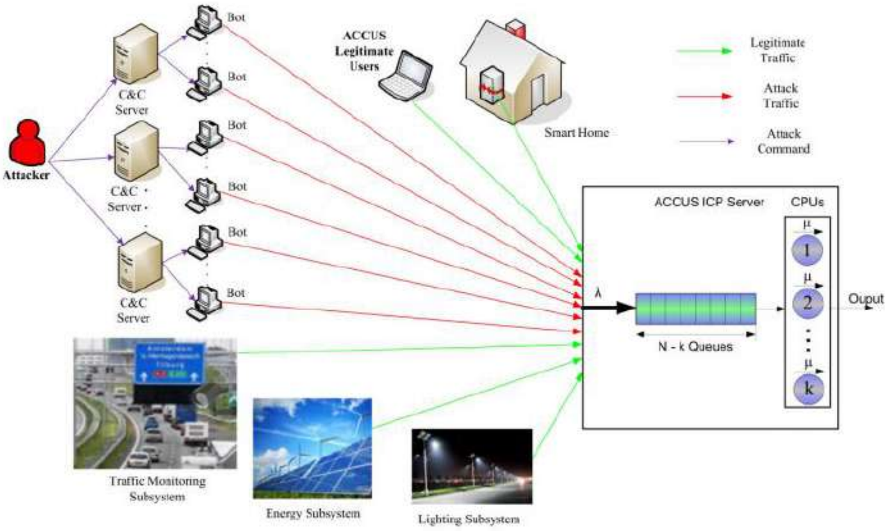


Figure 4 DDoS Attack

As we see in picture 4, the DDoS architecture consists of thousands of botnets that can be used by attackers to cause serious problems in performance of systems in a smart city. DDoS can launch multiple attacks from different locations and this fact led to the imperative for the detection and mitigation of threats for the safety of smart cities.

2.2 Dyn Attack

As we have mentioned above, in a smart city whose structures are based on IoT technology, heterogenic communication protocols and at the same time various cryptographic schemes are applied depending on the computing power for data encryption. Every DDOs attack has as its main purpose the undermining of the functions of a network with the aim of rendering non-functional the distribution of computing needs from the cloud to distributed routers for the terminal devices (Logota et al, 2018).

Dyn is a DDoS attack and an incident occurred in 2016. Specifically, the preparation of attack started on 30 September of 2016 when the Mirai botnet code was published online in the hacking community in Hack forums and in October the code shared the GitHub platform in order to avoid identifying the creator of Mirai code. At 7:00 a.m. on October 21st of 2016 the Mirai IoT botnet launched a DDoS attack against Dyn, a major DNS provider. The attacking hosts generated 1.2 terabits of malicious traffic forcing Dyn off the Internet for an hour (Jerkins, 2019). The figure 5 shows the areas where the attack took place.

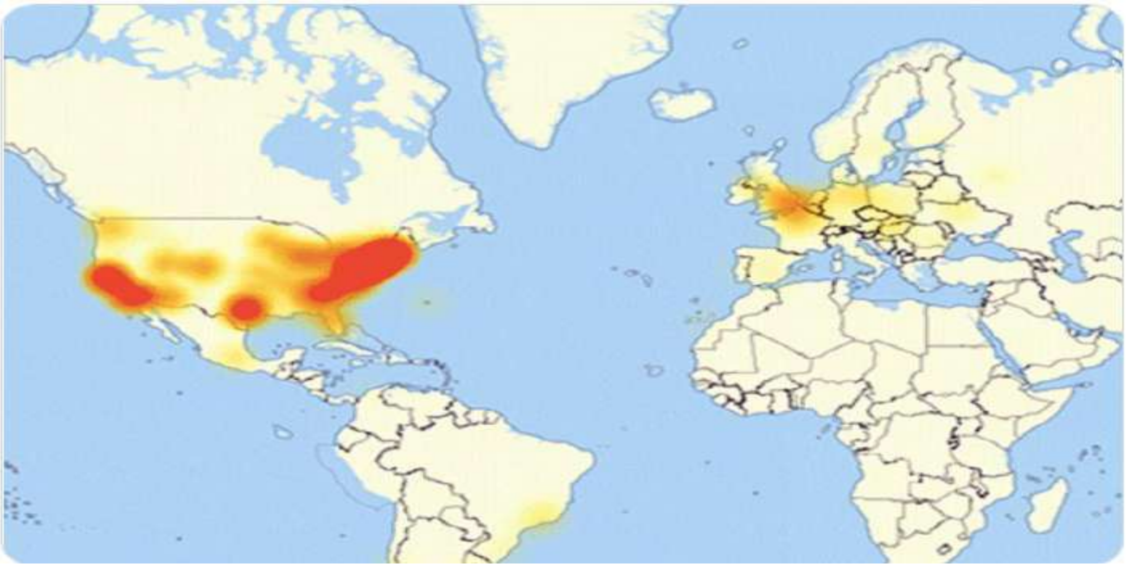


Figure 4 the area of Dyn DDoS Attack

Citizens of these countries woke up on 21 October and don't have access to Netflix, transacting business through PayPal, online gaming with Sony PlayStation Tweeter. This attack took place in the East Coast, Midwest, and California as well as Europe because the Dyn DNS was turned off for hours. In conclusion, this attack was just another DDoS attack which, by applying the method of publishing the code, resulted in leaving no fingerprints. The attack was carried out by hacker groups New World Hackers and Red Cult who have claimed responsibility for the incident with RedCult to promise that they will follow up with more attacks in the future (Kochetkova, 2016).

3. Suggestions

All those technologies that are analyzed in this text can be applied to smart cities. More specifically, municipalities throughout the Greek territory can adopt and implement these technologies in order to improve their citizens' quality of life, protecting the environment and saving energy and resources.

Further implementation and use of ICTs to the Public Administration via electronic Governance, and especially to Smart Cities, should improve the providing services to the citizens by developing the quality, accuracy and speed of them additionally to the enhancement of effectiveness. As a result, this implementation should provide a wider advantage to cities and the country's financial and social situation generally, simultaneously upgrading their status to global digital transformation status.

First of all, LoRa as a long-range, low-power, low-bitrate, wireless telecommunications system, can be used to municipalities services such as automobility (public transports without driver, telemetry system in public transports' stops), cleaning services (sensors in litter bins which provide information to special panels), providing free internet via Wifi-LoRa in Municipality's territory and in tourism sector by providing all the appropriate information about the city to tourists (electronic list of city attractions, digital maps, weather forecast, etc.).

SigFox and LoRaWAN technologies are cost effective since they provide plenty of data in a low energy consumption.As a result, they will be used widely by municipalities in Greek territory in the near future, due to the fact that this technology's infrastructure is still under construction in Europe, in the same sectors with LoRa technologies.

According to Xin et al (2019), NB-IoT technology is a promising and necessary technology in IoT and consists of the main protocol for LoRa. Moreover, this technology is very cost effective and is used to deploy a very high volume of low complexity, connected devices intended to transmit small data packages now and then. Furthermore, NB-IoT technology provides the ability for downloading a vast majority of data in thousands of devices which can be used by citizens, tourists and municipalities in high quality. Based on this fact, it can be used widely by smart cities in the sectors of public transportation, security, data sharing and panel controlling through sensors.

REFERENCES

[1]. Appio, F., Lima, M., & Paroutis, S. (2019) "Understanding Smart Cities: Innovation Ecosystems, Technological Advancements, and Societal Challenges", ResearchGate, pp.1-11. Available at: DOI: 10.1016/j.techfore.2018.12.018

[2]. Augustin, A., Clausen, H., Townsley, M., and Yi, J. (2016) "A Study of LoRa: Long Range & Low Power Networks for the Internet of Things", ResearchGate, pp.9-10. Available at: DOI: 10.3390/s16091466

[3]. Brdulak, A. (2020) "Characteristic of Narrowband IoT (NB-IoT technology that supports smart city management, based on the chosen use case from the environment area", Journal of Decision System, [e-journal] 14(3), pp.4-5. Available at: DOI: 10.1080/12460125.2020.1791481

[4]. Delitheou, V. and Maraki, M. (2011) "E-local Government: Exploring citizens' attitude towards electronic municipal services", LAP Lambert Academic Publishing.

[5]. Gaur, A., Scotney, B., Parr, G., and McClean, S. (2015) "Smart City Architecture and its Applications based on IoT", Elsevier, pp.1090-1094. Available at: DOI 10.1016/j.procs.2015.05.122.

[6]. Hiller, J. S. and Belanger, F. (2001) Privacy Strategies for Electronic Government , Virginia: The Pricewaterhouse Endowment for The Business of Government.

[7]. Jerkins, J. (2019) "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code", IEEE, p.1. Available at: DOI: 10.1109/CCWC.2017.7868464

[8]. Khalifa, E. (2019) "Smart Cities: Opportunities, Challenges, and Security Threats", Research Gate, 14(3), p.79.

[9]. Kochetkova, 2016. "How to not break the Internet". [Online]. Available at: https://www.kaspersky.com/blog/attack-on-dyn-explained/13325/ [Accessed 18 February 2021]

[10]. Lavric, A., Petrariu, A., and Popa, V. (2019) "Long Range SigFox Communication Protocol Scalabity Analysis Under Large – Scale, High – Density Conditions", IEEE, p.35816-35822.

[11]. Layne, K and Lee, J. (2001) 'Developing fully functional E-Governanment: A four stage model', Government Information Quarterly, 18, p. 122-136.

[12]. Logota, E., Mantas, G., Rodriguez, J., and Marques, H. (2018) "Analysis of the Impact of Denial of Service Attacks on Centralized Control in Smart Cities", Instituto de Telecomunicações, p.1-3.

[13]. Skoufas, K., Mitrakos, D., and Spyrou, E. (2020) “Identifying DDoS Attacks from Fluctuations in Wireless Traffic in an Intelligent IoT Road Network”, ResearchGate, p.1. Available at: DOI: 10.1109/IWCMC48107.2020.9148242

[14]. Xin, C., Zhuo, L., Ying, C., and Wang, X. (2019) “Performance Analysis and Uplink Scheduling for QoS-Aware NB-IoT Networks in Mobile Computing”, IEEE, pp.44405.

[15]. Zacharopoulou, M., 2020. Smart Cities and IoT Technologies. PhD Thesis. Athens: University of Piraeus.