ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

Location Privacy in the Internet of Things

Thesis for MSc Degree of Security in Digital Systems

Author: Vasiou Maria

Supervisor of University of Piraeus: Prof. Labrinoudakis Costas

Supervisor of NICS Lab: Post-Doc Researcher Rios Ruben

November 2018

Acknowledgement

First of all, I would like to take the opportunity to express my gratitude to my supervising professor, Constantinos Labrinoudakis for his assistance and his support in the conduct of this thesis. Furthermore, I would like to thank him for giving me his guidance from choosing the best subject for my Thesis, until the completion of it, even from distance. His point of view and the confident that he would be there whenever it would be needed, were really important to me.

Afterwards, I am extremely thankful and indebted to my thesis advisor, Ruben Rios, post-doc researcher at NICS Laboratory, whom job I really admire. He was an influence for me and I would like to thank him for providing me with rich educational material, numerous of papers and as well as his own book, and also to thank him for his continuous guidance.

Moreover, I would like to especially thank prof. Javier Lopez, the head of NICS Laboratory at Malaga, for providing me with all the necessary facilities for my research. Except for that, he was next to me from the very beginning, even before my arrival to Malaga and helped me to adjust to the new environment and to face every issue that raised during my stay to the Laboratory. Also, I would like to thank each and every member of NICS Laboratory for their help and their kindness, which made me feel like I was a member of the Laboratory.

Of course, I am really grateful to my beloved friend and fellow Irini, without whom I would not have taken the opportunity to accomplish my Master Thesis via the Erasmus Program at the University of Malaga. Being her my fellow traveler to this adventure was really important to me, as she was encouraging me in order to complete my thesis, and without her nothing would be the same.

Last but not the least, I would like to thank my family, my parents and my sister for supporting me spiritually, throughout writing this thesis and my life in general. Also, I would like to thank my grandparents, and especially my grandfather who is not here anymore and who raised me and gave me all the experience of life that he had.

I also place on record, my sense of gratitude to one and all, who directly or indirectly, have lent their hand in this venture.

Abstract

The aim of this research is to find a solution for location privacy protection in the Internet of Thing network and especially in the problem of source location privacy problem. As nowadays, privacy in cyber world stimulate a stake, with many regulations and rules to get implemented in order to protect personal data and privacy of individuals, we tried to give a solution to a specific type of this problem, in terms of Privacy by design. We tried to reach our goal, starting from a really detailed comparison between the Internet of Things network and its predecessor Wireless Sensor Networks. We came up with three new features that the Internet of Things network provides, which are mobility, energy consumption and outside connectivity and then by adding them to the already existing solutions for source location privacy in Wireless Sensor Networks, we assumed that these protocols are not able to be implemented in the Internet of Things network on their current form. So, we created a new version of the Phantom Routing Protocol for the Internet of Things, which was firstly designed for Wireless Sensor Networks. Although, there is enough work to be done, we think that Phantom Routing Protocol for the Internet of Things is a good start for the design and implementation of solutions that protect privacy in the Internet of Things from the beginning of use of this new technology, in order to avoid privacy and personal data violation.

Contents

Table of Figures

1. Introduction

Nowadays there is a total different perspective in everything that is related to new technologies. Few years have passed from the first time that personal computers entered in our houses, then everyone had a mobile phone and after that every mobile phone is a small computer. Every person in the earth has a smart phone, connected almost always to the internet, communicating with hundreds of other applications and smart phones, and having in their storage an enormous amount of any kind of data, as well as personal and sensitive data of their holders. But, except for the smart phones, many other kind of devices are having such characteristics. For example, TVs, sound systems, air conditions, refrigerators are only some of the numerous types of devices that are having the ability of connectivity to the Internet via Wi Fi.

In this new situation the benefits of the new technologies for the people have increased, as more and more procedures have been automated and interconnected demanding of people less and less actions, making their lives easier and simpler. On the other hand, with all of these data collected and stored to devices, and their transmission through the internet, threats in the cyber world have increased significantly. Security and privacy are two major stakes in the cyber world, especially now with the implementation of the new technologies and the Internet of Things, where all the devices could be connected among them, without human involvement, it is really important to keep a high level of security and privacy.

As we already mentioned the Internet of Things network is smoothly migrating from an Internet of people towards an Internet of Things. According to Cisco [40], 50 billion things will be connected to the Internet in 2020, thus overshadowing the data generated by humans. This is limited by the birth rate: in 2020, it is expected to have 8 billion people worldwide [41].

The things to be connected to the Internet largely vary in terms of characteristics. This ranges from very small and static devices (e.g., RFIDs) to large and mobile devices (e.g., vehicles). Such heterogeneity induces complexity and stipulates the presence of an advanced middleware that can mask this heterogeneity and promote transparency. In particular, Wireless Sensor Networks (WSNs) are connecting things to the Internet through a gateway that interfaces the WSN to the Internet. [40]

The concept of the Internet of Things network provides a method of communication between uniquely identifiable objects. These objects can be anything having the capability of communication. The vision of the Internet of Things network allows participating objects to transport themselves, to optimize their performance and energy, and to reconfigure themselves in a new environment. Therefore, the technologies, such as sensors, smart phones, nanoelectronics and other wireless identifiable devices, are the essential part of an Internet of Things architecture. These wireless devices combine the characteristics of sensor networks and other wireless technologies to react autonomously to real-world situation without human intervention. The development of efficient energy sources and energy generation devices will be the essential factor for the effective and long-lasting usage of IOT objects. Moreover, the intelligence of Internet of Things devices from the perspective of context awareness and inter-device communication is extremely important. On the basis of this communication and interpretation, Internet of Things devices will reach a logical conclusion for performing an action. Apart from the above-mentioned issues, integration, interoperability, and security are major concerns for implementing the concept of the Internet of Things network. [29]

So in order to understand better the Internet of Things network, we need to understand Wireless Sensor Networks firstly. It is of high importance to know their structure, their components, how they work, the software which is used on them, all the kind of protocols and every other characteristic that they have, as many of them are inherited in the new technology of the Internet of Things. This fact is able to help as in our research, which includes the opportunity of using features that were used in Wireless Sensor Networks for protecting Location Privacy in Wireless Sensor Networks, to the Internet of Things, as they are or with some changes made on them.

1. a. Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are comprised of a large number of small, costless devices (sensor nodes or motes) which are able to monitor the physical phenomena taking place in their vicinity and to wirelessly communicate these data to a high-capacity device (base station or sink) with the ability to process and analyze all the collected information. In this way, WSNs might resemble living organisms since they are capable of getting stimuli from their surroundings and processing that information in order to eventually perform some action. Under this metaphoric view of WSNs, sensor nodes represent the senses, the communication channels can be regarded as the nerves, and the base station depicts the brain. [28]

The various types of sensors that might be coupled to a sensor node are extensive, such as temperature, humidity, pressure, acoustic, and radiation sensors. This makes WSNs a rather versatile technology capable of performing many diverse tasks which, together with the low cost and size of the devices, becomes the ideal technology for monitoring diverse environments and assets. Precisely, this reason makes WSNs suitable for many different areas, namely air quality monitoring and environmental data collection, efficient crops management, detection and prevention of forest fires, homeland security, healthcare, and industrial processes monitoring, among many other. [28]

As we already mentioned, Wireless Sensor Networks are the networks which their main characteristic is the ability of monitoring, sensing and measuring physical parameters. This happens because these networks are consisting of sensors which are collecting and generating data from their environment. Although, such devices have limited battery, and processing capabilities as well, and due to the location that they are installed it is difficult most of the times to replace their batteries. [29]

In such a network, a large number of sensor nodes are deployed to monitor a physical phenomenon, and the position of the sensor does not need to be predetermined. The placement of these nodes can be random for any application. However, the networks need to have the ability of self-organization in case of a random deployment, and the protocols need to be developed by considering this fact. [29]

Consequently, Wireless Sensor Networks can be deployed on a several number of applications, such as healthcare applications, environmental monitoring, disaster management and smart grid deployment. [29]

So, as we could imagine, in order to make reality such a network, wireless ad hoc networking techniques need to be developed and then to be integrated in the devices. Furthermore, specific protocols need to be implemented to each wireless sensor network according to the targeted applications. For example, if there is need of a wireless sensor network deployed for medical healthcare, this network needs to track doctors, monitor vital signs of patients, and transmit these important measured parameters to the doctors. On the other hand, for disaster management applications a wireless sensor network needs to track and guide the first responders inside a building. [29]

There are some specific characteristics of sensor networks which are existing the same for the most of them. The number of sensor nodes in a sensor network is not well defined and it can be much larger than the number nodes in an ad hoc network. According to the density of the deployment of sensor nodes, usually the deployment is dense, but again is not strictly defined. In general, the failure can occur in sensor nodes and the sensor network topology may change frequently. Last but not least characteristic, is that the most of the sensor devices have limited energy and computation capabilities. The sensor network may comprise a large number of nodes that are close to each other. For energy consumption minimization, multihop communication can have better results in comparison with single-hop communication. [29]

Now, if we want to see deeper in the Wireless Sensor Networks, we should consider to the wireless sensor nodes specifically. We could say that they consist of a number of main components. Firstly, as we already know and we can easily imagine a sensor node has sensors. Sensors are used for sensing physical phenomena. Also, they have an A/D converter which is used to convert the analog data received from the sensor. Transceivers are as well a component of sensors, and they are needed in order to send and receive the sensed data. Furthermore, a processor is used for processing, forwarding, and transmitting the sensed data, and a battery which supplies the energy to various components of the sensor node. [29]

As for the classification of Wireless Sensor Networks, we could define four main types of sensor networks. First of all, the classical applications of wireless sensor networks which include measurement of physical environmental parameters such as temperature, humidity, pressure, and noise levels that can be used to realize an environmental monitoring application. These devices are used for continuous monitoring and reporting of these parameters, and in the case of any unusual situation, the remedial activity can be started by the central base station that is receiving this data. [29]

The next type of Wireless Sensor Networks is the wireless multimedia sensor networks (WMSNs). The existence of this type of networks is due to the availability of cheaper cameras and microphones. It has led to the interconnection of these devices that can gather multimedia content, such as images, video, and audio streams that can be used to extract particular information. The main difference between WMSNs and classical WSNs is the bandwidth requirement, as large volumes of data need to be sent on the network. The other characteristic is that traffic is delay intolerant. The applications for realizing a WMSN may consist of surveillance networks that have the capability of processing, capturing, sending, and receiving the multimedia data. Law enforcement agencies can use such a network for monitoring different events and localities. Another example is that of a traffic monitoring system that also is used for enforcing the maximum speed limit and congestion avoidance systems in cities and highways. [29]

Then we have the Wireless Underground sensor networks which can be used to monitor various physical parameters, such as water and mineral contents for agriculture applications. The measured parameters can be transferred to a central device called the sink by using a wireless connection. This makes the solution very attractive, as it is not needed to deploy a wired connection for data delivery. However, these devices need to be energy-efficient, as the battery replacement is difficult and costly in such a network. The other issue is the communication channel quality and the error rate, which can be improved by using special antennas and signal processing techniques. The other applications include the monitoring of underground plumbing infrastructure and landslide or earthquake monitoring through buried sensors. [29]

Last type of Wireless Sensor Networks are the networks that have underwater monitoring applications, such as disaster prevention, surveillance applications, and pollution monitoring. This network consists of sensor devices that can collaborate to realize the mentioned applications. The network should possess a capability of self-organization, and each device has to coordinate its operation by sharing location, configuration, and movement information. Thus, the nodes adapt inside the network based on their position in the network. The major applications include environmental monitoring where the network can monitor the chemical level in streams, rivers, lakes, and oceans. Monitoring of ocean currents and winds may lead to the application of such a network in climate prediction. Underwater sensor networks have other applications in undersea exploration missions, disaster prevention in coastal areas, and distributed surveillance of an area. [29]

There are a lot of security concerns that are associated with the WSN that need to be addressed. It mainly consists of node compromise, unauthorized access, and denial-of-service attacks. [29]

1. Node compromise: The Wireless Sensor Network consists of thousands of nodes working together to gather specific information from the surrounding area. Due to the dynamic dispersion of these nodes, it is impractical to monitor each node to see whether it is compromised. Another problem is the inclusion of false nodes in the network that will corrupt the sensed data by adding false information to it. As the sensor devices have strict energy constraints, the solutions to minimize such attacks would be expensive, as they require more energy. Moreover, as it is well understand, if these devices are connected to the Internet through the Internet of Things, new threats will be added through Internet connection that may corrupt the sensed data. Therefore, the research for integration of Wireless Sensor Networks into the Internet of Things needs to look into these issues. [29]

2. Unauthorized data access: The other issue with the WSNs is that data can be read by an intruder if it is sent in an unencrypted format. The standard way is to use the encryption algorithms for transmitting each packet over the network. However, it is an issue for energy-constrained devices, as they cannot spend most of their energy on data encryption; thus, new schemes need to be developed. Moreover, a network may receive several unauthorized data requests, and the network should be able to check the authenticity of each request. Therefore, this is one of the research directions that have to be looked into while integrating Wireless Sensor Networks with Internet of Things. [29]

3. Denial of service: A malicious outsider may also launch an attack so that the entire network is unable to perform its tasks. The types of attacks may include sending useless attacks so that the device's energy is depleted quickly. There are a number of solutions to minimize such attacks; however, the solution combining Wireless Sensor Networks and the Internet of Things network needs to look into this issue as well. As we could imagine. These issues are needed to be addressed before integration of the Wireless Sensor Networks into the Internet of Things network. [29]

The other issue that will be faced while integrating Wireless Sensor Networks with the Internet of Things network is the nature of hardware devices. As we already mentioned, the sensor devices consist of transceivers, batteries, processing devices, and sensors. The possible issues may consist of energy consumption minimization, maximizing the node's processing capability, and having the hardware security of the device. [29]

1. Energy: The job of a sensor device is to have minimal energy consumption while performing the sensing, transmission, and analyzing job. This is so because the batteries of these devices cannot be changed easily due to their geographical location. Thus, there is a need to have research for developing small-sized batteries having a huge amount of energy [30].

2. Processing: The sensor devices have to implement a range of applications, starting from simple environmental parameter measurements to the capture of multimedia data. Based on application requirements, the sensor devices need to have an ample amount of processing resources to meet the overall objective. Thus, another area of research is development of energy-efficient devices capable of the timely processing of data [31].

3. Sensor device's security: Wireless Sensor Network's devices are realized using an electronic device that has a microprocessor to perform its tasks. These autonomous devices may be exposed to security attacks; thus, there is a need to design them so that they are less susceptible to attacks based on the targeted applications. These attacks can be done by tampering the device to make it malfunction or by reading the information leaked by the device. Such types of attacks are called side-channel attacks. If a sensor node is physically accessible to the end user, it is vulnerable to side-channel attacks. The side channel can be accessed by equipment that can interact with it. One example is the case of simple power analysis (SPA), where a block of data can be correlated with its instantaneous power consumption. This helps in determining the sequence of instructions being executed and thus is useful in planning an attack. [29]

As for the software that is embedded in the Wireless Sensor Networks, the coordination of thousands of sensor devices under limited energy constraints is also a challenge. The developed algorithms have to consider these energy constraints in order to realize an efficient network. There is a need to have necessary data processing (e.g., compression and aggregation) before sending it to the next node so that the transmission energy consumption of a node can be minimized [32]. The network should be self-organizing with minimal human interaction. These challenges are unavoidable in any network, and robust solutions need to be presented.

Finally, there is a need to develop smart applications for meeting a desired sensing goal [33]. Some of the important software challenges that might be faced while integrating WSN into IoT are described below. The three main challenges are Heterogeneity and Integration, Scalability and Data Mining. As it is already known, one of the important characteristics of an IoT-based network is the integration of heterogeneous devices for achieving a certain goal. These diverse heterogeneous devices make the integration process complicated. There are different Internet of Things platforms that devise their own mechanisms for incorporating the data streams for other nonproprietary sources [34,35]. The other approach, used by Sensinode [36] and SmartThings [37], is to use their own proprietary hardware, which is only compatible with their respective platforms. In order to create a large network of devices and attract developers (in sensor and actuator technologies), there must be a mechanism to integrate the proprietary and open-source devices and platforms. This can be achieved to some extent by abstracting the technical details of the platform to the developer. [29]

The term scalability refers to the adaptability to changes with respect to the load, increasing number of devices, or users. In the case of IoT, the platform deployed at a smaller scale, such as smart gateways, can allow access to any necessary devices. These gateways are limited in resources, especially hardware resources. As a result, the devices may not be able to connect when a saturation stage is achieved. Therefore, we need to find a trade-off for small- and medium-scale deployments in order to optimize the performance with an increasing number of devices. The other way could be to use cloud services to manage the large number of devices per user. [29]

One of the important concepts in the Internet of Things phenomena is semantics. For managing a number of things that are generating a large amount of data, it is necessary to implement the techniques for extracting useful data and then making a decision. Simple filtering mechanisms are typically defined by means of first-order rule engines or data source combinations (e.g., aggregation or fusion of data sources) by applying functions to aggregate them. Data filtering techniques are very often related to the detection of events. Other approaches take advantage of semantic web techniques in order to disseminate data by performing complex inferences [38].

But we could pause our analysis of Wireless Sensor Networks, at this point in order to explain the form of the Internet of Things network as it is seems to be until now. So, we would be ready for the next step of the comparison of Wireless Sensor Networks and the Internet of Things network, in much detail, which will help us later, according to how similar or not these two technologies are, to find out if privacy solution for Wireless Sensor Networks are effective to the Internet of Things network.

1. b. The Internet of Things

The Internet of Things network is appearing as a new paradigm that is getting huge attention in the context of modern wireless communication. In this situation, the surrounding objects will be part of the network. As a result, the information and communication system are invisibly embedded in the environment around us. The basic concept behind the Internet of Things network is the pervasive presence of different objects around us. These objects include radio frequency identification (RFID) tags, sensors, actuators, and mobile phones. These objects will cooperate with each other to achieve a common objective [45]. As we already mentioned, although the Internet of Things network paradigm has its own concept and set of characteristics, it also shares cohesion with other areas of computer science. The Internet of Things network combines different technologies that include sensors, semantics, the cloud, data modeling, and storing and communication technologies. [46].

An important technology that is used in the Internet of Things network is RFID. RFID which permits the microchips to transfer the identification information through wireless channels. RFID is extensively used in logistics, pharmaceuticals, retailing, and so forth, for identifying, tracking, and monitoring the objects attached with tags [47]. Apart from RFID, Wireless Sensor Networks are also considered the base technology for IoT. The Wireless Sensor Networks use interconnected intelligent sensors to monitor traffic-, industrial-, and healthcare-related applications.

As the research in the area of the Internet of Things is still in progress, and as a new technology is always getting different features and characteristics, therefore, it is difficult to extract one standard definition. However, numerous definitions have been proposed by a few researchers. The following definitions are some of them. [29]

Definition 1: "The semantic origin of the expression is composed by two words and concepts: Internet and Thing, where Internet can be defined as the world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP), while Thing is an object not precisely identifiable. Therefore, semantically, Internet of Things means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [42].

Definition 2: "Things have identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environment, and user contexts" [43].

Definition 3: "The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service" [44].

When we refer to "things" in the Internet of Things Network we can define them as real/physical or digital/virtual objects that have an identity, exist and move in space and time. Things are usually identified by assigned identification numbers, names, addresses, and so forth. The concept of things is the essential part in the construction of the Internet of Things because things are responsible for interacting and communicating with themselves and with the environment while reacting to the physical world events and running the processes that trigger the action. [29]

It is true that in the Internet of Things networks the term things can have different perceptions depending on the domain in which it is used. For example, in industrial applications, the thing may typically be anything that participates in the product life cycle. It may refer to the trees, a building, condition measurement devices, and so forth, in an environmental application. The thing may also be related to devices within public spaces or devices for ambient assisted living and so on in society. [29]

Some general principles of the Internet of Things Network, we could say that are the following:

- The Internet of Things network consists of objects or things that are real-world entities or virtual entities having the ability to identify each other.
- These entities are able to exchange information with each other using the communication protocols and infrastructure.
- The Internet of Things network can use services that act as an interface to things. These things may have the sensors that can interact with different environments.
- Things in the Internet of Things network can communicate and collaborate with each other and with different computing devices.
- Things in the Internet of Things network can adapt to the environment by extracting the patterns from the environment and learn from other things. These entities of the Internet of Things network have the ability to makes decisions, evolve, and propagate information. [29]

Although the Internet of Things network has huge potential for developing numerous applications, only a few of them have actually been deployed. Some of the most important applications of the Internet of Things are Aerospace and Aviation, Smart Cities, Smart Homes, Smart Buildings, Automotive Industry, Environmental Monitoring, Logistics Applications, Food Traceability, Agricultural Applications, Media Coverage, Smart Water Monitoring, Vehicle Insurance, Material Recycling and Home Automation. [29]

Smart car
Smart city
Wearables
IoT applications
Smart health
Smart appliances
Smart farming
Smart buildings
Smart TV
Smart home

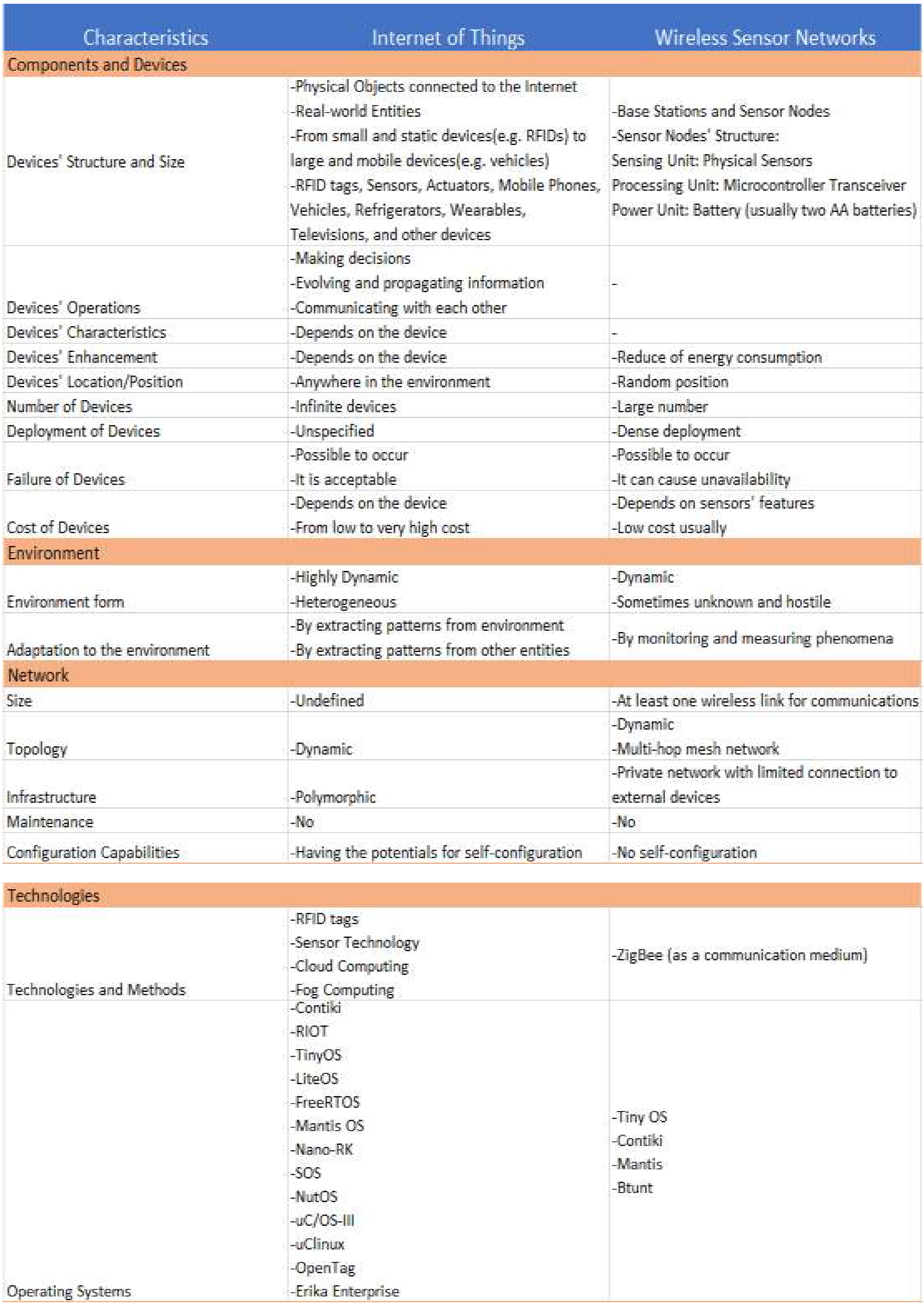
FIGURE 1: IOT APPLICATIONS

2. From Wireless Sensor Networks to the Internet of Things

From the first site, we can easily understand that these two very important technologies are highly connected together. Wireless Sensor Networks is the predecessor of the Internet of Things network and also a subset and a main component of the Internet of Things. Although, we still discuss about two different technologies, with different components, software, protocols and different approaches.

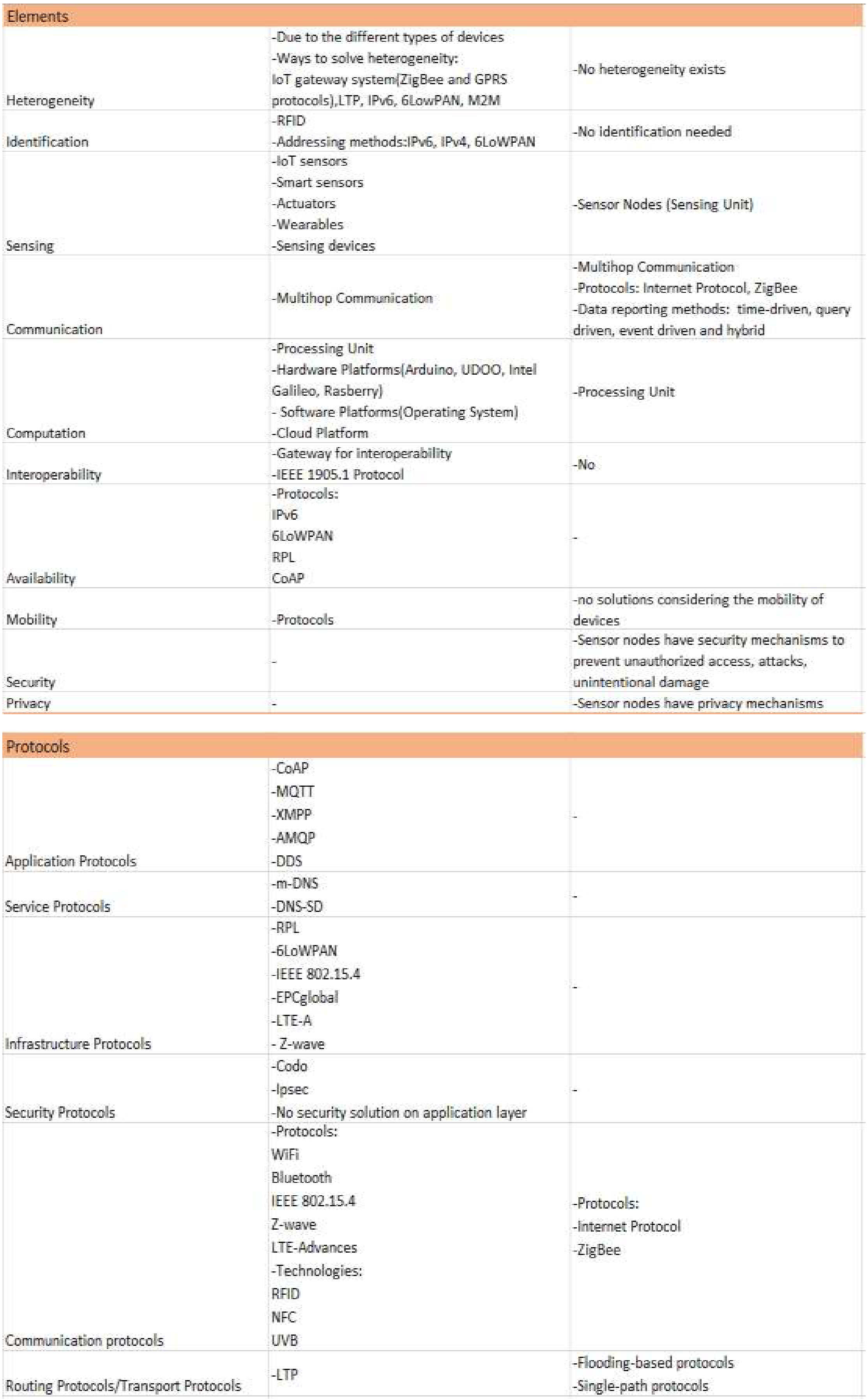
2. a Comparison between the Internet of Things and Wireless Sensor Networks

According to an intense search of many studies on both Wireless Sensor Networks and the Internet of Things, on every existing field on these technologies, we made a comparison of these technologies in order to study on their similarities and differences, understand them well and try to use them so as to solve our problem. This comparison helped us to conclude in second tense the new features that the new technology of the Internet of Things brought. A table follows with all this information and an explanation of them is presented below.



Characteristics	Internet of Things	Wireless Sensor Networks
Components and Devices		
Devices' Structure and Size	-Physical Objects connected to the Internet -Real-world Entities -From small and static devices(e.g. RFIDs) to large and mobile devices(e.g. vehicles) -RFID tags, Sensors, Actuators, Mobile Phones, Vehicles, Refrigerators, Wearables, Televisions, and other devices	-Base Stations and Sensor Nodes -Sensor Nodes' Structure: Sensing Unit: Physical Sensors Processing Unit: Microcontroller Transceiver Power Unit: Battery (usually two AA batteries)
Devices' Operations	-Making decisions -Evolving and propagating information -Communicating with each other	-
Devices' Characteristics	-Depends on the device	-
Devices' Enhancement	-Depends on the device	-Reduce of energy consumption
Devices' Location/Position	-Anywhere in the environment	-Random position
Number of Devices	-Infinite devices	-Large number
Deployment of Devices	-Unspecified	-Dense deployment
Failure of Devices	-Possible to occur -It is acceptable	-Possible to occur -It can cause unavailability
Cost of Devices	-Depends on the device -From low to very high cost	-Depends on sensors' features -Low cost usually
Environment		
Environment form	-Highly Dynamic -Heterogeneous	-Dynamic -Sometimes unknown and hostile
Adaptation to the environment	-By extracting patterns from environment -By extracting patterns from other entities	-By monitoring and measuring phenomena
Network		
Size	-Undefined	-At least one wireless link for communications
Topology	-Dynamic	-Dynamic -Multi-hop mesh network
Infrastructure	-Polymorphic	-Private network with limited connection to external devices
Maintenance	-No	-No
Configuration Capabilities	-Having the potentials for self-configuration	-No self-configuration
Technologies		
Technologies and Methods	-RFID tags -Sensor Technology -Cloud Computing -Fog Computing	-ZigBee (as a communication medium)
Operating Systems	-Contiki -RIOT -TinyOS -LiteOS -FreeRTOS -Mantis OS -Nano-RK -SOS -NutOS -uC/OS-III -uClinux -OpenTag -Erika Enterprise	-Tiny OS -Contiki -Mantis -Btunt

FIGURE 2.1: CHARACTERISTICS OF IOT AND WSNS



Elements		
Heterogeneity	-Due to the different types of devices -Ways to solve heterogeneity: IoT gateway system(ZigBee and GPRS protocols),LTP, IPv6, 6LowPAN, M2M	-No heterogeneity exists
Identification	-RFID -Addressing methods:IPv6, IPv4, 6LoWPAN	-No identification needed
Sensing	-IoT sensors -Smart sensors -Actuators -Wearables -Sensing devices	-Sensor Nodes (Sensing Unit)
Communication	-Multihop Communication	-Multihop Communication -Protocols: Internet Protocol, ZigBee -Data reporting methods: time-driven, query driven, event driven and hybrid
Computation	-Processing Unit -Hardware Platforms(Arduino, UDOO, Intel Galileo, Rasberry) - Software Platforms(Operating System) -Cloud Platform	-Processing Unit
Interoperability	-Gateway for interoperability -IEEE 1905.1 Protocol	-No
Availability	-Protocols: IPv6 6LoWPAN RPL CoAP	-
Mobility	-Protocols	-no solutions considering the mobility of devices
Security	-	-Sensor nodes have security mechanisms to prevent unauthorized access, attacks, unintentional damage
Privacy	-	-Sensor nodes have privacy mechanisms

Protocols		
Application Protocols	-CoAP -MQTT -XMPP -AMQP -DDS	-
Service Protocols	-m-DNS -DNS-SD	-
Infrastructure Protocols	-RPL -6LoWPAN -IEEE 802.15.4 -EPCglobal -LTE-A - Z-wave	-
Security Protocols	-Codo -Ipsec -No security solution on application layer	-
Communication protocols	-Protocols: WiFi Bluetooth IEEE 802.15.4 Z-wave LTE-Advances -Technologies: RFID NFC UVB	-Protocols: -Internet Protocol -ZigBee
Routing Protocols/Transport Protocols	-LTP	-Flooding-based protocols -Single-path protocols

FIGURE 2.2: CHARACTERISTICS OF IOT AND WSNS

Devices

Devices as it is normal are now different in the Internet of Things comparing to these which are used on Wireless Sensor Networks. Although, we need to mention that in reality the devices that are used on Wireless Sensor Networks are used as well in the Internet of Things, as we could say that Wireless Sensor Networks on many situations will be part of the Internet of Things. However, we will try to compare the new features that are now implemented on devices used in the Internet of Things and the sensors used in Wireless Sensor Networks.

Firstly, the devices that take part in the Internet of Things network can be directly connected using cellular technologies such as 2G/3G/Long Term Evolution and beyond (5G) or they can be connected through a gateway, forming a local area network, to get connection to the Internet. The latter is the case where the end-devices usually form Machine to Machine (M2M) networks using various radio technologies, such as Zigbee (based on the IEEE 802.15.4 Standard), Wi-Fi (based on the IEEE 802.11 Standard), 6LowPAN over Zigbee (IPv6 over Low Power Personal Area Networks), or Bluetooth (based on the IEEE 802.15.1). [2] The difference is that sensors on Wireless Sensor Networks cannot be directly connected on the Internet and they always need to be connected to a Base Station from which they can have connection to the Internet.

Moreover, another difference is that the communicating devices will have some new capabilities, such as that they will operate with different networking standards, may also experience intermittent connectivity with each other, and many of them will be resource constrained. A resource constrained device is a device that has limited processing and storage capabilities, and that often runs on batteries. [3] So we can conclude that this type of device has similarities with sensors on Wireless Sensor Networks.

We need as well to take into consideration that the first and foremost requirement of the Internet of Things is to provide connectivity between devices. This is because devices in the Internet of Things are representing, at the most of the times, the actual users of the Internet of Things network. Thus, achieving a seamless end-to-end D2D communication is imperative for the success of the Internet of Things. So, these devices, which are termed “smart objects/things,” may be the tiny and low-cost sensors, actuators, or RFID tags, which capture physical data and are capable of performing tasks or making decisions autonomously. [3]

As it is already mentioned, a device in the Internet of Things network can be also a mobile device such as smartphones. In certain instances, co-located devices that wish to exchange information may be using different communication technologies, which pose a challenge for the communication process. Most of these technologies use proprietary protocols, each with different implementations at the physical, data link, and network layers. [3] On the other hand, the main feature of the Wireless Sensor Network is that is implemented once and then is stable, so its devices, meaning sensor, are stable too. So, adding mobility to the devices of the Internet of Things network is creating a difference between these two technologies.

Last but not least, Wireless Sensor Networks and Sensor Networks in general, comprise of the sensor hardware (sensors and actuators), firmware and a thin layer of software. The Internet of Things network comprises everything that Sensor Network comprises and further it comprises a thick layer of software such as middleware systems, frameworks, APIs and many more software components. The software layer is installed across computational devices and the cloud. [4] So this characteristic added on the devices of the Internet of Things Networks make them different from sensors.

Environment

The environment of these technologies are quite similar. Both Wireless Sensor Networks and the Internet of Things network are implemented on dynamic environments. We could say, that the environment in which the Internet of Things network is implemented, from the moment that it is now in construction with more and more new devices and technologies arising, it can be characterized as highly dynamic. Whereas, the environment in which the Wireless Sensor Networks are implemented is sometimes hostile, as many times it can be unknown. For example, there is the possibility to through some sensors and try to build a wireless sensor network in a place where war conflicts are taking place and maybe soon or later the sensors will be destroyed. Another characteristic of the Internet of Things network is that is heterogeneous, which is something that can characterize the Internet of Things network in its entirety. Consequently, the need of adaption in this environment is really important so as the Internet of Things could work effectively. This could happen by extracting patterns from the already existing environment and from other entities which are already in the environment or they are implemented gradually. On the other hand, for Wireless Sensor Networks, the way to adapt on the environment is by monitoring and measuring phenomena happening, although it is more limited. Therefore, we could say that the environment for both the two kinds of networks are dynamic and unknown sometimes. The biggest difference on this field is the heterogeneity existing on the environment of the Internet of Things network.

Network

A try made in order to find the similarities and differences between some basic characteristics that networks have. Firstly, concerning the size of a network could have, the size of the Internet of Things Network is undefined. This is normal as for the Internet of Things there are many options supporting that is one enormous network containing every smart device which could be connected to the Internet and consequently to it. Also, there is another point view about the Internet of Things networks, which is that the Internet of Things could be separated on sub-networks depending on which devices are connected with each other at that time and in this way we could talk about the sizes of the sub-networks, which are as well difficult to be defined. For Wireless Sensor network, the size is also undefined, as it is as well consisting of many sub-networks connected to each other. The only standard contribute in order to create a Wireless Sensor Network, is having at least one wireless link for communications. As we mentioned above, the Internet of Things network cannot exist without Sensor Networks, because Sensor Networks provide the majority of hardware (e.g. sensing and communicating) infrastructure support, through providing access to sensors and actuators. There are several other technologies that can provide access to sensor hardware, such as wireless ad-hoc networks. However, they are not scalable and cannot accommodate the needs of the Internet of Things network individually, though they can complement the Internet of Things network infrastructure. Sensor Networks are a part of the Internet of Things network. [4] In the Internet of Things network we could assume that there are lots of sub-networks, connected and communicated to each other and to devices.

For the topologies of both the two technologies we could say that they are dynamic. We could even say that especially for the Internet of Things network, the topology is undefined, as it is a new technology the topology of which is still under process. Although, there are many different options about how this could be. In general, the network topology in the Internet of Things network could be single-hop, multi-hop, star, mesh or multi-tier. [5] In traditional Wireless Sensor Networks, routing table or routing history, it uses a map to transfer the data to the destination as described in traditional WSNs protocols. In contrast, on the dynamic topologies, table routing, is no longer used, and rout discovery must be used instead of routing tables with considerable cost, regarding to energy, bandwidth and time. [6] However, in some situations, routing tables could be used even in the Internet of Things Networks, in order to enhance routing process and provide privacy.

Another difference between the Internet of Things network and Wireless Sensor Networks, which affects the form of their topologies, is that from their origin, Sensor Networks were designed, developed, and used for specific application purposes, for example, detecting bush fire. In the early days, sensor networks were largely used for monitoring purposes and not for actuation. In contrast, the Internet of Things is not focused on specific applications. The Internet of Things can be explained as a general purpose sensor network. Therefore, the Internet of Things network should support many kinds of applications. During the stage of deploying sensors, the Internet of Things would not be targeted to collect specific types of sensor data; rather it would deploy sensors where they can be used for various application domains. For example, company may deploy sensors, such as pressure sensors, on a newly built bridge to track its structural health. However, these sensors may be reused and connect with many other sensors in order to track traffic at a later stage. Therefore, middleware solutions, frameworks, and APIs are designed to provide generic services and functionalities such as intelligence, semantic interoperability, context-awareness, etc. that are required to perform communication between sensors and actuators effectively. [4]

Two figures of the architectures that could be used on the creation of both of these networks are presented. The figure is described of three types of architectures used on Wireless Sensor Networks. Firstly, there is the flat architecture which includes data transfers from static sensor nodes to the sink node using a multi-hop fashion. Then, the two-layer architecture, where more static and mobile sink nodes are deployed to collect data from sensor nodes, and the three-layer architecture, in which multiple sensor networks are connected together over the Internet. Therefore, from these types of network architectures we could imagine that the Internet of Things networks could follow the three-layer architecture. [4] The other figure of architectures that could be used on both the Wireless Sensor Networks and the Internet of Things is the event driven, the query driven and the time driven. Specifically in Wireless Sensor Networks, some sensors produce data when an event occurs (e.g. door sensor); the rest produce data continuously, based on specified time frames (e.g. temperature sensor). So, we could say that the architecture on Wireless Sensor Network are mainly event driven and time driven. In the Internet of Things all of the three types of architecture could be used, but we cannot have a clear point of view of which one will be used the most. However, the certainty is that the Internet of Things should handle billions of parallel and simultaneous events, due to the massive number of interactions. Consequently, real-time data processing is essential. [4]

Moreover, a classification of sub-networks participating in the Internet of Things network has been made, based on the types of devices which we be operating. Consequently, we have constrained and unconstrained networks. Constrained networks consist of devices with low power, memory, and data rate. Devices operate in the unlicensed spectrum and in environments where heat, moisture, and interferences are high. A constrained network may be one of the following: Short-range wireless network: This includes the IEEE 802.15 standards for wireless personal area networks (WPANs) and the IEEE 802.11 standards for wireless local area networks (WLANs). Low-power lossy network (LLN): This is a low-bit-rate WPAN under the IEEE 802.15.4 standards. Delay-tolerant network: This is deployed in performance challenged environments where continuous end-to-end connectivity cannot be assured. Such environments are spacecraft, natural disaster situation, or underwater. WSNs: These are made up of sensors that have been densely and randomly deployed to capture information, e.g., humidity or motion. The sensors have low power and self-organizing and collaborative capabilities. Unconstrained networks have high resources/capacity and high coverage range and data rates. They operate within the licensed frequency spectrum. Examples include the following: Cellular networks: wireless wide area networks such as third-generation, fourth-generation, and long-term evolution networks; WiMAX: IEEE 802.16 standards for wireless metropolitan area networks (WMANs). [3]

Concerning on maintenance of the networks, none of them are designed in a way to remain the same as when they have been implemented, and this depends on what we have mentioned before.

Finally, the last characteristic of a network could have and we examined is the configuration capability. In Wireless Sensor Networks, mainly because of the type of the devices (sensors) there is no possibility of self-configuration. On the other hand, in the Internet of Things network, as the smart devices that are used and which can be connected directly to the Internet, there are several potentials for self-configuration and the possibility of this to happen is high.

Technologies

Another field we tried to compare between the two networks are the technologies and methods that they use in order to operate. The Internet of Things network is using some main technologies which are the RFID tags, the Sensor Technology, the Cloud Computing and the Fog Computing, which are giving to the network all these needed features in order to be its devices connected to the Internet. On the other hand, all these technologies are not used in Wireless Sensor Networks, as the sensor do not need and they cannot have the same features as those which the smart devices have. The only technology that is used in Wireless Sensor Network is the ZigBee, which is used as a communication medium.

Considering the operating systems that are used by each of the networks, we concluded after extensive research to some operating systems, without making a clear conclusion of the benefits provided to the networks or their effectiveness, as we think that this is out of our scope and little could offer to our research. Although, we found that the operating systems which mainly are used in Wireless Sensor Networks are Tiny OS, Contiki, Mantis and Btunt. For the Internet of Things network the operating systems that are used or it is possible that will be used are Contiki, RIOT, Tiny OS, Lite OS, FreeRTOS, Mantis OS, Nano-RK, SOS, NutOS, uC/OS-III, uClinux, Open Tag and Erika Enterprise.

Elements

When we are referring to the elements of the Internet of Things networks and of the Wireless Sensor Networks, we mean the more high level properties and features which are composing a network and the elements on which we examined above. These elements that we tented to compare for the two technologies are

Heterogeneity, Identification, Sensing, Communication, Computation, Interoperability, Availability, Mobility, Security and Privacy.

First of all, the big difference which is arising when we look into the first component, is that in general, in the Internet of Things network there is heterogeneity mainly due to the different types of devices and the different operating systems, technologies, protocols and other components that are used in it. In order to solve the problems that may emerge from this heterogeneity the implementation of some protocols such as LTP, IPv6, 6LowPAN, M2M are used and also an IoT gateway system is created with the use of the ZigBee and GPRS protocols. On the other hand such a heterogeneity does not exist in Wireless Sensor Networks, as the devices are all the same, meaning they are sensors and less different components are used.

Another element, very important on the Internet of Things network is the Identification of the devices. This is so important, as there is the necessity of knowing of which exactly is the device which is connected to the Internet, or is connected to another device, or is trying to gain a connection to somewhere, in order to make all these connection right and finally the whole network to work in a correct way. As it is really hard to recognize each device and each smart thing from its name or its characteristics the RFID tags are used. RFID cards / RFID tags bear electronic identification data of different physical objects (e.g., goods, cars, and even wearable sensors), and can even be used to identify people. RFIDs consume very little energy by reflecting signals received from RFID readers. On the other hand, mobile and handheld devices (e.g., smartphone and PDAs) are changing the way we access and interact with things in the Internet, and is rendering the Internet into a ubiquitous service. Along with cloud computing, the capabilities of these devices will be further boosted by providing storage and computing power in the cloud. [40] Additionally to the RFID cards some addressing methods are implemented most of the times, such as IPv6, IPv4 and 6LoWPAN. On the other hand, in Wireless Sensor Networks identification by these means is not necessary, as we have only one type of devices where the result is the same if a message is transmitted from a node or from another one.

To both of these networks, in order of them to operate correctly and efficiently, Sensing is really important. In Wireless Sensor Networks, thing are really clear, as the sensor nodes, and especially the sensing unit of them, can provide the network with this feature. In the Internet of Things network sensing is providing with more ways, such as except the sensing nodes, the Internet of Things sensors, smart sensors, actuators, wearables and other sensing devices. The main conclusion is that sensing is essential for both of these networks.

Communication is also a very important component of these technologies. Without the right communication is difficult of these networks to operate without mistakes and breaks. It is certain for the Wireless Sensor Networks that the type of communication existing is multi-hop communication, and this happens because the sensor nodes do not have the ability to be connected directly to the Internet, so a message in order to be transmitted has to pass from a node to another so as to reach a base station and consequently the Internet and finally its destination. Generally, the multi-hop communication is the type of communication where the network uses for routing, two or more hops, as relays, to convey information from a source to a destination. On static wireless sensor networks, used for monitoring, multi-hop communication allows them to cooperate and deliver data between nodes outside the direct communication range. In this circumstance, multi-hop communication is really efficient and applicable to monitoring systems, as an enormous amount of data generated by the entire system can be collected to a base station easily and as it is taken in consideration the specific communication characteristics of each system. [9] On dynamic wireless sensor networks, similar to static WSN, multi-hop communication is considered as an effective low cost solution for coverage extension and capacity enhancement of wireless networks. Although, their disadvantage is that by using more than one relay, the implementation complexity of the system is being increased to a large extent. [10] Concluding, multi-hop communication in a WSN is most commonly used than a single-hop communication in order to consume less energy. Each node collects data from its environment and transports data to the receiver via a multi-hop network, performing the routing function. [11]

The protocols that are mostly used for this situation is the Internet Protocol and the ZigBee Protocol. Moreover, the methods that are used to report data in Wireless Sensor Networks and then cause a communication between sensors to start are time-driven, query-driven, event-driven or hybrid methods. Specifically, the time-driven model of data reporting, is suitable for applications which are in need of periodic data monitoring. So this means that sensor nodes will periodically switch on their sensors and transmitters, sense the environment, and transmit the data of interest at constant periodic time spaces. Query-driven model is the model where sensors react immediately to unexpected and drastic changes in the value of a sensed attribute, due to the response to a query that was generated by the Base Station or another node in the network. So, it would be well suited to time-critical applications. [7] Finally, the event-driven model, which is the most usual one, is suitable for time-critical applications while being energy efficient. In the event-driven model a sensor node starts reporting data to the base station immediately after an event of interest (i.e. a sudden change to the properties of a particular phenomenon) has been detected in its vicinity and stays silent otherwise. Consequently, if there are no events to be reported, the energy consumption of the nodes is moderately low. Moreover since the transmission power of the nodes is usually not sufficient to establish a direct communication with the base station, the data source uses multi-hop communications to deliver the sensed data. This means that in order to reach their destination, the packets sent by remote nodes go through multiple intermediate nodes, which act as data relays. [8]

Considering communication in the Internet of Things, we could imagine that we can meet both single-hop and multi-hop types of communication, and this happens as smart devices can be connected directly to the Internet or connected to each other and then to the Internet if it is needed. So, various types of communication take place in the field of the Internet of Things network such as device to device communication, device to human and vice versa. The most important requirement for the successful functionality of the Internet of Things network is to provide connectivity between the devices. [12] We also can assume that the communication between device to device and between devices to people is not usually multi-hop, in terms that the message is sent from one device to another immediately without a middle device to be interfered.

Many researches have been made for the ways of communication in the Internet of Things and many different types of communication have defined. One classification which is made is depending on which types of smart things are communicating. When we refer on the part of the Internet of Things network which includes sensors and sensor networks, machine-to- machine communication (M2M) which is a communication between multiple sensor devices and a single data collection device, is a common type of communication in the Internet of Things network. Most frequently adopted protocols in this situation are MQTT (Message Queue Telemetry Transport) and CoAP (Constrained Application Protocol). [18] However, various other types of communication may exist within the Internet of Things, and these include device-to-device (D2D), device to human and vice versa, and device to distributed storage. [3]The types of communication and the purpose of each type of communication within the Internet of Things network can be classified. The first classification of communication in the Internet of Things network is that the communication type, in which we have already referred, can be either single-hop or multi-hop communication. [19] More specifically, in the single-hop communication, devices communicate with each other directly, without any other device or sensor between them. For multi-hop communication, devices relay information for each other to achieve end-to-end communication between any source and destination device. Also, Devices probably will communicate with each other autonomously without any centralized control and collaborate to gather, share, and forward information in a multi-hop manner. [3] Another classification is that communication could be within the same network (intradomain) or across heterogeneous networks (interdomain). Within an intradomain network, devices may communicate to collect information or to report their state to one another. In addition, Device-to-device communication can be with or without human intervention. Communication between devices through the intervention of humans may be needed for interacting with humans or to trigger an alert for human decision making. Devices may communicate without human intervention to carry out an action or to identify or locate other devices. Devices may also directly communicate with humans to pass on information to them or to obtain information directly from human for decision making. Also, devices may communicate with a data storage agent to pass on captured data, update stored data, or retrieve stored data for automatic decision making. It is assumed that traditional routing protocols cannot solve the several networking challenges which open up from the new characteristics of the Internet of Things network. [3] The communication process in the Internet of Things network must support devices using different protocol stacks and radio frequencies. In addition, some of these connected heterogeneous devices often have inherent hardware and software constraints, e.g., low processing and transmission power, memory, and battery life. Hence, to have a seamless operation in the Internet of Things network, the communication process must support the exchange of information between heterogeneous devices and across heterogeneous networks. One solution is to allow interoperability between devices on heterogeneous networks with the use of gateways. However, gateways are complex to design, deploy, and manage and result in inefficient convergence of networks. To achieve efficient end-to-end D2D communication within the Internet of Things network, intelligent routing is required. [3] D2D communication in the Internet of Things network will typically be multi-hop in nature because devices have to relay traffic for one another, thus performing routing functions. This will necessitate cooperation between devices. Cooperation is a challenge that affects the achievement of optimal routing in D2D communication. Some devices may not collaborate to relay other device’s traffic because of reasons such as limited available power, security, and trust. [3]

The communication protocols which we found that are implemented or can be implemented in the Internet of Things and that can provide efficient communications between devices are Wi Fi, which allows smart devices to communicate and exchange information without using a router in some ad hoc configurations, Bluetooth which is used to exchange data between devices over short distances, IEEE 802.15.4, Z-wave which is used in remote control applications in smart homes as well as small-size commercial domains, covers about 30 meters point-to-point communication and is specified for applications that need tiny data transmission and LTE-Advanced which covers fast-travelling devices and provide multicasting and broadcasting services. [13] Some paradigms of technologies used to enable communication on the Internet of Things are RFID which realize the machine-to-machine concept, Near Field Communication (NFC) and Ultra-wide bandwidth (UWB).Concluding, the communication is different and similar depending on the situation, between these two networks.

As for Computational, which is another really important requirement for both the two networks, we concluded that for Wireless Sensor Networks the processing unit of the sensors, which participate in it has limited capacities and computational skills. On the other hand, for computational, in the Internet of Things are used processing units (e.g. microcontrollers, microprocessors, SOCs, FPGAs) and software applications. Also, there are used hardware platforms (e.g. Arduino, UDOO, Intel Galileo, and Rasberry) and Cloud platforms. Although, the difference in computational skills in the Internet of Things networks, compared with computational skills in Wireless Sensor Networks, is made by the existence of Cloud and Fog platforms, as they form an important computational part of the Internet of Things network. [13] In conclusion, the fact that the devices of the Internet of Things network have better computational skills of the sensors participating in Wireless Sensor Networks.

Interoperability is an element needed mainly because of the existence of heterogeneity, in order to different devices and technologies be able to communicate and be connected to each other even if they are not using the same interfaces, software and any other components they could have. So, as it was expected interoperability in Wireless Sensor Network is not being succeeded in a specific way as there is not such a need. For the Internet of Things interoperability is succeeded using gateways designed for interoperability and also the IEEE 1905.1 Protocol.

Moreover, Availability of the networks is one more requirement of those technologies. By availability we mean the capability of the network to be functional for each users without breaks and lose of connectivity. In Wireless Sensor Networks availability is not succeeded in a specific way, as happens with interoperability, because it depends on the nodes' life and their availability. If a sensor node runs out of battery, another one will receive the message that was meant for that node and if any node is not placed in a close distance then maybe the connection will get lost. But this is a non-definable scenario and there is not a specific way to ensure availability in any way. In the Internet of Thing network there are some protocols, which are implemented for many reasons and for providing and ensuring availability as well. There protocols are IPv6, 6LoWPAN, RPL and CoAP.

Mobility is the most important feature in the Internet of Things network and we could say that it is also the biggest difference between the Internet of Things network and Wireless Sensor Networks. For Wireless Sensor Networks no solutions considering the mobility of devices has been implemented, as sensor nodes are stable and there is not such a need. The nodes of the WSN are not mobile, in terms that they have a specific position, known or unknown, except a change in the topology of the network takes place. On the other hand, in the Internet of Things, from the moment that all devices which participate in it could move, or some of them, and in general every device in the Internet of Things is free to move independently in any direction, solutions covering the need of network's operation despite the fact that its devices maybe are on move are implemented, in most of the time by using some protocols. So, it is obvious that this is a big difference and a new feature that the Internet of Things network is inserting in these technologies, and this is the reason why we are going to analyze extensively mobility on the upcoming chapter.

About the features of Security and Privacy, a several number of solutions have been implemented on Wireless Sensor Networks in order to protect the network and the messages transmitting on it, but not always with great success. These fields, as well as almost all the above fields, are open for more research. However, it is certain that sensor nodes have security mechanisms to prevent unauthorized access, attacks and unintentional damages. Furthermore, sensor nodes have privacy mechanisms. When it comes to the Internet of Things network things are more blurry. The need of the protection of security and privacy is really significant, especially on this new technology, because of the many different technologies, devices and unknown behaviors that are going to co-exist in it. For the moment, security and privacy solutions have not been designed or proposed in an official way and this is a topic that we need to investigate more.

Protocols

Many types of protocols, for any reason, are implemented on both the networks as they help them to operate in a better way. In the Internet of Things network there are three categories of protocols that are not used in Wireless Sensor Networks. This happens because of the type of devices used on the networks. Consequently, due to the heterogeneity of devices and generally of the environment of the Internet of Things Application protocols, Service protocols and Infrastructure protocols are implemented. The application protocols are CoAP, MQTT, XMPP, AMQP and DDS. The service protocols that are used are m-DNS and DNS-SD. Finally, Infrastructure protocols are RPL, 6LoWPAN, IEEE 802.15.4, EPCglobal, LTE-A and Z-wave. However, from the moment that in Wireless Sensor Networks are not used there kinds of protocols, we assume that further analysis of them is out of the scope of this research.

Considering Security protocols in the Internet of Things some protocols that are referred on some paper of their implementation in this network for providing security are Codo and Ipsec, although no security solutions exist on application layer. As we have already mentioned, these protocols we believe are not enough to provide the wanted security to the Internet of Things network and further research is needed. On the other hand, in Wireless Sensor Networks such protocols are not existing, but security mechanisms are implemented.

Finally, as we analyzed on the previous section the communications protocols, the last category of protocols that we are going to analyze is the Routing of Transport protocols that are used on both networks. In the Internet of Things network the routing protocols which are likely to be used is the LTP and the RPL. On the other hand in Wireless Sensor Network there are mainly to types of routing protocols that are used and these are the flooding-based protocols and the single-path protocols.

Specifically, we are going to analyze routing in Wireless Sensor Networks. Wireless sensor networks usually consist of a large collection of nodes which route the gathered data over multiple hops to an individual sink. Also, there is a variation between the relays that a node has with the other nodes of the network, depending on the distance between them and their capacities. So, these facts combined together, could be considered as a disadvantage in the routing procedure as they lead to the creation of communication/routing patterns which an attacker can take benefit of.

There are main types of routing methods in Wireless Sensor Networks. The first one is the Flood-based routing method. In this simple routing method, the node that has a message to transmit sends it to each of its neighboring nodes, who retransmit this message to their neighbors. So, every message received by a node is forwarded to all its neighbors except to the one that is sent, and eventually the message visits all the nodes in the network. This approach is reliable in terms of the redundancy that provides, but it also has the disadvantages of energy inefficiency as all the nodes of the network participate in the transmission of a single message that is usually intended to the base station, packet duplicates at the destination and packet collisions especially when the number of simultaneous data sources is high [8] [14]. The other routing method which is used in Wireless Sensor Networks is the Single-path routing method, or shortest path routing method as it is known. This routing method allows each node to transmit a message to only one or to a small subset of its neighboring nodes. [14] So, whenever a node has event data to transmit, it sends a message to a neighboring node that is closer to the base station than itself. This operation is repeated for every node in the communication path until the data are eventually delivered. In this way, single-path routing protocols minimize the number of nodes participating in the routing procedure. [8] Consequently, this method is more energy efficient because it uses the minimum number of relays, but the disadvantage of this is that these kind of protocols tend to use the same communication path for every message, which extremely simplifies traffic analysis attacks. [15] Another disadvantage is that this type of routing method usually requires either extra hardware support or pre-configuration phase. [14]

For Routing protocols that are going to be used in the Internet of Things or their types, there are many point of views, as we concluded from our research. In general, the devices of the Internet of Things network are equal and there is not a central control node with specific responsibilities, as there is the Base Station or the sink in WSNs. So, each device in the mobile Internet of Things network can act as a host and as a router, which is the reason why routing protocols are needed in order to enable the devices to communicate effectively in a decentralized and self-organized way. [16] Routing mechanisms that can be used are one-to-one, one-to-may and many-to-many. [13]

Many different types and categories of routing protocols and techniques are presented on a several number of papers and researches. One type of routing is the Source-initiating on-demand routing (e.g. AODV, DRS). In AODV protocols, when a source device needs to send a message to some destination device, it broadcasts route request message to its neighbors. Then, its neighboring devices will broadcast the message to their own neighbors. During this process the device records the source of the received message in its routing table, in order to be constructed the reverse path for the route reply message. The destination responds with a route reply message to the neighbor. Similar to AOCV, in DRS protocols, when they receive a message to a destination device from a source device, at first they check if there has been a previous connection, and as a consequent there is already a route. If there is such a route the source node will use it, or else it is going to find a new one by broadcasting a route request. [16] The other type is the table-routing (e.g. OLSR). In this type of protocols the devices need to exchange information between to each other periodically to update and build their own network topology through distributed computing. Some devices are elected as routing nodes and they are not participating in routing computation. [16] Another classification of routing methods which are used in the Internet of Things network are proactive and reactive routing protocols. Proactive routing protocols gather routing information beforehand in order to have a general overview of network's topology at any time. The periodic distribution of beacons provides nodes with insight about the existence and quality of connection to their neighbors. On the other hand, reactive protocols search for routes on-demand, which means that only when a transmission towards another node is started, the route discovery process (towards this specific node) is triggered. In consequence, topology information is only exchanged when needed, saving energy. [17] This type of routing has similarities with the event-driven model which is used on WSNs. Moreover, there are also other types of routing. So, we have Hop-by-Hop routing, in which during the packet forwarding, each router stores a small part of each route it is participating in. This small part consists of the destination of the route, and over which of its neighbors the packets should be forwarded. [17] Source routing where during the packet forwarding, the entire path of a route is embedded in its packet header. [17] Another type is the Multipath routing which means that when a protocol employing multipath routing, seeks to end and use alternate paths towards every destination. This distributes the cost of forwarding packets among more nodes, saving the energy of individual, highly-frequented nodes. [17] Finally, the last type is Probabilistic routing, where routing decisions are calculated based on probabilistic values. [17]

However, in our research, as there is not any certainty about which exactly types of routing protocols and routing methods are going to implemented in the Internet of Things network, we assumed that the RPL routing protocol is the one that is going to be used, as is the most possible one to be used. RPL (Routing Protocol for Low Power and Lossy Networks) supports simple and complex traffic models like multipoint-to-point, point-to-multipoint and point-to-point. RPL keeps at least one path for each node to the root and uses control messages. RPL routers work under one of two modes operation the Non-Storing and the Storing mode. So, we are going to analyze further this protocol on the following chapter, as RPL compared to the routing protocols that Wireless Sensor Networks use, it is obvious that there are many similarities and this is a clue that is really important for us, as we trying to solve the problem of location privacy in the Internet of Things.

2. b. New Features in the Internet of Things

After the comparison between the features of the Wireless Sensor Networks and the Internet of Things, we are able to conclude the main differences between them and consequently the new features of the Internet of Things, which are playing the most important role considering the location privacy protection and the possibility of using the solutions for location privacy protection in Wireless Sensor Networks, in the Internet of Things as well.

The first and the most important new feature that we can observe in the Internet of Things is mobility. As we have already mentioned, in the Internet of Things network all or some devices, or maybe none of the devices in some situations, can be mobile. In contrast to this, sensors in Wireless Sensor networks are stable in their positions from their implementation until the end of the wireless sensor network's usage. Moreover, mobility in Internet of Things is polymorphic and it can be implemented in different ways. So, it can be occasional or continuous performed, which means that a device could be mobile and then stable, such as a vehicle, or a wearable which could be on move when the person, who is wearing it, walks and stable when this person sleeps.

Considering about mobility, we can imagine the many different changes that can occur in a network in different fields. At first, we can assume the changes that can arise in terms of context. By context we define all the concept related to the location of the devices in the network. So, by adding mobility, questions such as where the mobile device is located, which is the current position of the device and in what hands it is at a specific moment, are common and are needed to be answered. Furthermore, in terms of internet access and connectivity, we come up against questions such as if the mobile device is connected at all, and if it is connected to what wireless or wired network is connected to, at what bandwidth level is connected and with what security. Other kind of questions are the questions arising from the energy availability, such as where the mobile device is able to charge again, or how much energy does the mobile app need. Last but not least, due to mobility we face questions concerning security and privacy, such as what kind of security infrastructure the mobile device encounters when moving among different locations, and what private information do service providers have about user using a mobile device.

Although mobile devices, for example mobile phones and vehicles has been in our lives and in usage for many years, the fact that now changes is the increased number of sensors and actuators per mobile device, the increased density of mobile devices in users' environment, the increased interconnectivity and the increased reliance of users on mobile devices. All these elements create a new smart environment and they are totally and integrally connected to the users' daily routine. [1]

Consequently, when mobility is added we get dynamism, unpredictability, faults, hands-offs and disruptions when sensing, communicating, analyzing data and providing energy, security and privacy-aware mobile services. Although, the benefits of mobility are many on many ways. Mainly, we can imagine that against of a problem, could be solution to many problems concerning privacy and security.

Another new feature that is now arising comparing Wireless Sensor Networks and the Internet of Things network, is energy consumption. In Wireless Sensor Networks, as we already mentioned, sensor nodes are having batteries, which have a defined life cycle and some specific hours of work. As sensor nodes, are not self-configured and not rechargeable, their life and as a consequence their operability is going to end at some not specific moment. So, sensor nodes and Wireless Sensor Networks I general have energy limitations. On the other hand, in the Internet of Things, the devices that are used, which except sensor nodes that are being used as well, are having different characteristics, as we mentioned before. One of these characteristics is that most of the devices are rechargeable and it is really likely that they will have the ability to recharge relatively easily. For example, a device as a smart phone is rechargeable anytime with many ways. This fact leads us to the consumption that energy consumption in the Internet of Things network could be bigger than in the Wireless Sensor Networks, and that it is not such limited as in the Wireless Sensor Networks.

Last but not least, the third new feature that we noticed to arise in the Internet of Thing s network, comparing to the Wireless Sensor Networks is the Outside Connectivity. As we already mentioned, the Internet of Things network could be considered as one network compromised of many smaller sub-networks and due to the heterogeneity of the devices which participate in them, there is a big difference on how all these sub-networks and the different types of devices are connected among them. Also, the fact that maybe exist connection with devices and networks that are unknown, is a hint of the many threats that could be hidden concerning security and privacy of the Internet of Thing network.

2. c. Types of attackers in Wireless Sensor Networks and in the Internet of Things network

Another thing that we tried to figure is the types of attackers that we are going to deal with in the Internet of Things networks, considering cyber security and privacy attacks. Rios, Lopez and Cuellar have made an extended description and classification of the types of attackers that we may face at Wireless Sensor Networks. [8] So, after the detailed comparison between Wireless Sensor Networks and the Internet of Things network we tried also to describe the types of attackers in the Internet of Things network based on the types of attackers described for Wireless Sensor Networks.

In Wireless Sensor Networks as an internal attacker is considering the attacker who is a member of the network. Usually it is a legitimate node which behaves in an unintended or malicious way. [8] So, in the Internet of Things networks we assume that as an internal attacker is considering any device or entity that has authorized participation in the network of the Internet of Things network, but acts in a malicious way.

As an external attacker in Wireless Sensor Networks is considering the attacker who is an outsider of the network. Usually, it is an entity that does not belong to the network. [8] In the Internet of Things network, we believe that as an external attacker is considering the attacker who is outside the network, has no authority to participate in it, and he cannot compromise or control any devices.

Another classification of attackers is passive and active attackers. A passive attacker in Wireless Sensor Networks is an eavesdropper and limits his or her actions to merely observing the messages exchanged by the sensor nodes. [8] So, in the Internet of Things networks, we assume that a passive attacker is an eavesdropper who simply observes and analyzes the communications in the Internet of Things network and cannot conduct any active attacks such as denial of service attack.

An active attacker, in Wireless Sensor Networks, does not only listen but may introduce new packets, modify or block packets in transit, tamper with the devices, or a combination of these. [8] In the Internet of Things network, Lopez, Rios, Baob and Wangb have defined the active attackers as the attackers who are capable of disrupting the network operation for their own benefits, and this type of attacker is the one who must be considered more for attacking the Internet of Things, than passive attackers. [15] Also, they may have access to the internal memory of some of the devices that an individual owns or they collect information about the individual. So, they will also know the relevant information for the sake of configuration of the device and all sorts of user-related data. [15]

For local attackers in Wireless Sensor Networks, it is mentioned that they have the ability to control or monitor a part of the network. Also, especially in this type of networks they are called as mote-class adversaries and they have capabilities similar to an ordinary sensor node. [8] There are situations in which local adversaries resemble a global adversary. [15] Similar to the local attacker in WSNs, a local attacker in the Internet of Things network is an attacker who can control or monitor a part of the network, e.g. a number of devices connected to each other.

Finally, we have the type of global attackers. In Wireless Sensor Networks, a global attacker has the ability to control or monitor almost the whole or the whole network. A laptop-class adversary, as he is called in this circumstance, has access to more powerful devices with greater transmission range, processing power, memory storage, and energy budget than typical sensor nodes. [8] On the other hand, in the Internet of Things, as the Internet of Things systems may interact with remote services and devices, there is no adversary powerful enough to control all possible communication flows. [15] So, we can consider as a global attacker, an attacker who is capable of controlling a large number of devices or a large sub-network of the Internet of Things network, as according to the enormous amount of devices in the Internet of Things network we assume that it would be impossible for an attacker to control the whole Internet of Things network.

3. Location Privacy

After analyzing in many details the two technologies of Wireless Sensor Networks and the Internet of Things network, we will analyze now the element that we need to find ways to protect in them. This element is Location Privacy.

Many definitions are existing about privacy in general, as it is an issue that concerns people all over the world for many years and it is also a human right. Privacy is the guarantee that information, in its general sense, is observable or decipherable by only those who are intentionally meant to observe or decipher it. The phrase “in its general sense” is meant to imply that there may be types of information besides the message content that are associated with a message transmission. Source location, e.g. the location of the sensed event, is an important type of information whose privacy needs to be protected. [20]

Many problems are arising concerning privacy. One of the problems that is gaining more attention, is the location privacy problem, which aims to prevent attackers from obtaining the location of specific nodes of interest to him. [23]

The privacy threats that exist for sensor networks may be categorized into two broad classes: content-oriented security/privacy threats, and contextual privacy threats. Content-oriented security and privacy threats are issues that arise due to the ability of the adversary to observe and manipulate the exact content of packets being sent over the sensor network, whether these packets correspond to actual sensed-data or sensitive lower-layer control information. A first line of defense for protecting the content of sensor communications involves the use of appropriately designed network security protocols. [21]

Although issues related to sensor security are important, it is believed that many of the core problems associated with sensor security are on the road to eventual resolution. Contextual privacy issues, associated with sensor communication, however, have not been as thoroughly addressed. In contrast to content-oriented security, the issue of contextual privacy is concerned with protecting the context associated with the measurement and transmission of sensed data. In many scenarios, general contextual information surrounding the sensor application, such as the location of the message originator, are sensitive and need to be protected. The underlying challenge of source-location privacy is to make it difficult for an adversary to trace his way, hop-by-hop, back to the origin of a communication. [20] The same contextual privacy threats we are going to face on the Internet of Things.

In particular, location privacy in WSNs aims to prevent an adversary from being able to estimate the location of special nodes in the network, such as source nodes. Protecting such nodes from being localized is of vital importance since an adversary with that knowledge becomes very powerful. In some cases this information is innocuous (e.g. weather conditions) though there are many scenarios where the location information of the events being monitored is critical (e.g. homeland security). For example consider a sensor network deployed inside a building to improve users' quality of life. Due to user interaction with the environment, some (source) sensors will immediately generate network traffic in order to inform about the needs of the user and adapt building conditions accordingly. An external attacker might detect traffic variations in the network and thus localize the sources of messages, what finally allows him to approximate the location of the users as well as other private information. [23]

In Wireless Sensor Networks an attacker might capture and analyze network traffic to retrieve private information about the network itself and the data being collected. In fact, there is a link between these two aspects of privacy because the events being monitored by the network might be related to people. The main differences stands in which is the entity who might violate the privacy. In the case of social privacy, the user might not even be aware of being tracked since the devices collecting data are unobtrusively embedded into the environment, which turn the network owner into the privacy perpetrator. However, in the network privacy case, the adversary is an outsider who takes advantage of a sensor network deployed for legitimate purposes in order to obtain private information. [23]

Clearly, the packet payloads might be protected using traditional confidentiality and integrity mechanisms. In fact, this is a prerequisite for privacy protection. However, an attacker unable to obtain the information contained in the packets can still retrieve sensitive information just by observing and analyzing the communications. Pai et al. [26] show that simple observation of network traffic can reveal much information about the context in which the network is deployed. Different sensor nodes platforms communicate within different frequency ranges. Recent sensor platforms (e.g. Imote2) perform in the Gigahertz spectrum while older ones (e.g. cricket) perform at lower frequencies. This apparently innocuous information, can be used by an attacker to launch platform-specific attacks. Also the transmission rate can help an observer to determine the quantity and the nature of the events being monitored. For example, in the case of a body sensor network monitoring the heart rate of an individual with high blood pressure, the transmission of no messages might be an indicator of a heart problem. Moreover, the size of messages can be used to infer the type and precision of the data being collected. The size of packets reported by a sensor node monitoring the state of a light bulb (on/off) is smaller than those sent by sensors collecting data about the luminosity in a room. Also, some data aggregation protocols try to reduce network traffic by forcing nodes to reuse in transit packets to incorporate their own sensed data, thus increasing the size of the packets as they move closer to the base station. Finally, routing protocols might reveal the location of important nodes in the network such as the base station or the sources of messages, since sensor nodes usually send event data to a single or very few base stations in relative stable paths in order to preserve nodes' batteries. [23]

Another consideration about contextual privacy is made in [27] by Kamat et al. who claim that not only the occurrence of an event is sensitive information but also the time at which this event takes place (temporal privacy). This problem is more serious in the context of mobile asset monitoring, where an adversary can link the time and position of the events being monitored by the network and eventually he will be able to predict future behaviors. [23]

The location privacy problem in Wireless Sensor Networks could be described in general terms as the problem that arises when an adversary is trying to determine the location of some nodes which are having a special interest to him. In the Internet of Things network we could describe the problem of location privacy in a very similar way, as again the problem arises when an attacker wants to find the location of a device in this situation, with the greatest difference that the device could be stable or mobile.

3. a. Source Location Privacy in Wireless Sensor Networks

Source-location privacy refers to the ability to protect the location of the sensor nodes reporting event data to the base station. [8]

The main goal of source location privacy mechanisms is to prevent an attacker capable of performing traffic analysis attacks from determining the location of a node reporting the presence of an event in its vicinity. Indeed, the interest of the attacker is not the node itself but the location of the event. However, he might use that information to get an approximation of the location of the event. [23]

The problem of source location privacy was first described in the well-known “Panda Hunter Game” [24, 25]. It proposes a scenario where a large sensor network is deployed to enable biologists to monitor the behavior of pandas in their environment. Whenever a panda comes into the hearing range of a sensor it starts transmitting messages to the base station. Although the sensor network is deployed for legitimate purposes, an attacker (the panda hunter) takes advantage of the already existing infrastructure to find and hunt pandas. [23]

The attacker might try to gain information about the location of the reported events either from the content of the packets or from the traffic pattern generated due to the operation of the network. Packets contain both information in the payload and the header. Assuming that the packet payload is cryptographically protected, the attacker might still retrieve sensitive information from the headers. Header information is used at every hop for routing purposes and thus contain information about the sender and recipient of the packet (see Figure 2). This information might be used to determine the location of these nodes. Therefore, it is necessary to protect the real identities of each sensor node taking part in a communication. [23]

3. b. Need of Location Privacy Protection in Wireless Sensor Networks and in Internet of Things network

Providing location privacy in a Wireless Sensor Network is extremely challenging. On the one hand, an adversary can easily intercept the network traffic due to the use of a broadcast medium for routing packets. He can then perform traffic analysis and identify the source node that initiates the communication with the base station. This can reveal the locations of critical and high value objects (e.g., soldiers) being monitored by the sensor network. On the other hand, the resource constraints on sensor nodes make it very expensive to apply traditional anonymous communication techniques for hiding the communication from a sensor node to the base station. [22]

The routing problem for Wireless Sensor Networks differs substantially from that of traditional ad-hoc wireless networks because sensor nets typically involve many resource constrained nodes that are densely connected by low-power radios and operate in aggregate over multiple hops to achieve some application-specific communication pattern. A basic data gathering communication pattern is a large collection of nodes route periodically sampled data over multiple hops to an individual sink. [23]

The source-location privacy problem in WSNs was first considered by Ozturk et al [20]. They analyzed several routing protocols widely used in WSNs and found out that they provide a poor protection level. [28]

Same problems appear in the Internet of Things Network, where it is more likely to be used the RPL as a routing protocol, as it is considered the de facto routing protocol for the Internet of Things (IoT). [48] First of all, RPL is a single path routing protocol and this protocol only finds an optimal or a better path. [49]

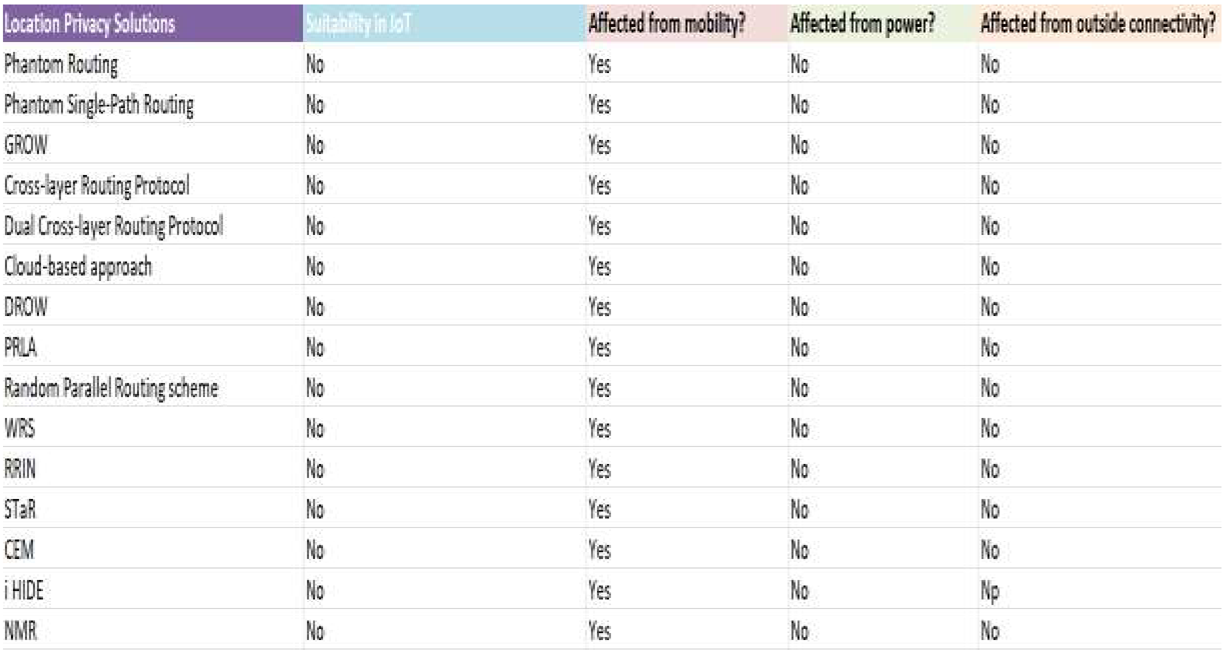
Lots of paper have been written about how RPL works. One of them which explains this quiet easily is the “A comparative performance study of the routing protocols rpl, loadng, loadng-ctp with bidirectional traffic for ami scenario” written by Elyengui, S, Bouhouchi, R and Ezzedine, T.[51] Although, we need to focus on the implementation of RPL, which reposes on Expected Transmission (ETX) as a routing metric. The minimum ETX value specifies the path that is selected by RPL. ETX is a maximum number of retransmissions needed to deliver the individual packet successfully toward destination. For example, a packet needs two transmissions to reach destination, evidently the best path has minimum ETX that is equal to 1. For sink node, ETX is equal to zero. ETX is calculated by two elements, link estimator which is responsible to calculate ETX for neighbors and neighbors that calculate their own ETX by accumulating all ETX in the path from neighbors to root. The first one called 1 hop ETX (ETX1hop) and the second one called multihop ETX (ETXmulti-hop). Each node can estimate for each route the cost ETX by adding the multi-hop ETX and 1 hop ETX. If the cost calculated is low means that it is the desirable route. [50] So, we can easily understand that RPL has many similarities to shortest-path routing, which is the type of routing that mostly is being used in the Internet of Things network. We assumed that, as this protocol prefers the path which has the less expected transmissions, meaning the one that passes though the smallest number of nodes. Consequently, we will need to face the same problem with traffic patterns as the ones we faced on the shortest-path routing protocols. Also, the routing metrics that the RPL provides [50], reinforce our aspect for the traffic patterns existence.

Therefore the problem on all of these protocols is that they make a traffic pattern and all the nodes are collected on the same points, which make it easy for the attacker to trace back and find the source node and consequently its location. So, the need of location privacy protection is the same and in the Internet of Things network, as in Wireless Sensor Networks.

3. c. Source Location Privacy Solutions in Wireless Sensor Networks

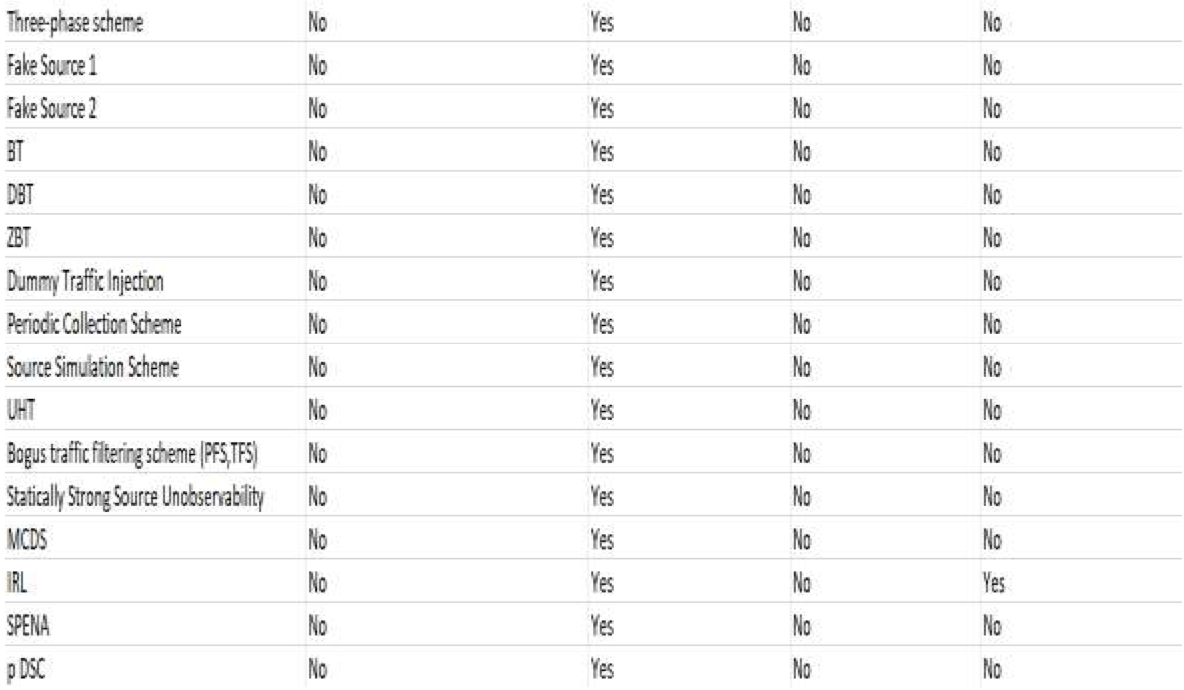
In the chapter 3 of the book “Location Privacy in Wireless Sensor Networks” of Rios R., Lopez J. and Cuellar J., [8] they are presenting very detailed a several number of solutions for location privacy in Wireless Sensor Networks. We tried to examine all the solutions which were made in order to protect source location privacy in Wireless Sensor Networks to see if they are suited in the Internet of Things network in order to protect again location privacy, by taking also into consideration the new features in the Internet of Things, meaning mobility, energy consumption and outside connectivity, that we mentioned on previous chapters.

In the following table we gathered all these solutions and we tried to briefly conclude if they are suitable for the Internet of Things network, if they are affected by mobility, by energy consumption or by outside connectivity. When we think about affection we mean affection in a bad way, in sense of the inability of the solution to be implemented to the Internet of Thing network as it is, due to one of the features. Although these conclusions, are made of a general sense and not from an extensive analysis and study of all of these solutions, we believe that almost all the solutions for source location privacy protection are affected in a bad way from mobility, as they cannot be implemented exactly as they are designed for Wireless Sensor Networks, from the moment that every device could be mobile. As for the energy consumption, in the Internet of Things network there is capability of more energy consumption for each device, which could be a positive element for the implementation of these protocols. Equally, outside connectivity, does not seem to harm the implementation of these protocols directly.



Location Privacy Solutions	Suitability in IoT	Affected from mobility?	Affected from power?	Affected from outside connectivity?
Phantom Routing	No	Yes	No	No
Phantom Single-Path Routing	No	Yes	No	No
GROW	No	Yes	No	No
Cross-layer Routing Protocol	No	Yes	No	No
Dual Cross-layer Routing Protocol	No	Yes	No	No
Cloud-based approach	No	Yes	No	No
DROW	No	Yes	No	No
PRLA	No	Yes	No	No
Random Parallel Routing scheme	No	Yes	No	No
WRS	No	Yes	No	No
RRIN	No	Yes	No	No
STaR	No	Yes	No	No
CEM	No	Yes	No	No
i HIDE	No	Yes	No	Np
NMR	No	Yes	No	No

FIGURE 3.1: LOCATION PRIVACY SOLUTIONS AND NEW FEATURES OF IOT



Three-phase scheme	No	Yes	No	No
Fake Source 1	No	Yes	No	No
Fake Source 2	No	Yes	No	No
BT	No	Yes	No	No
DBT	No	Yes	No	No
ZBT	No	Yes	No	No
Dummy Traffic Injection	No	Yes	No	No
Periodic Collection Scheme	No	Yes	No	No
Source Simulation Scheme	No	Yes	No	No
UHT	No	Yes	No	No
Bogus traffic filtering scheme (PFS,TFS)	No	Yes	No	No
Statically Strong Source Unobservability	No	Yes	No	No
MCDS	No	Yes	No	No
IRL	No	Yes	No	Yes
SPENA	No	Yes	No	No
p DSC	No	Yes	No	No

FIGURE 3.2: LOCATION PRIVACY SOLUTIONS AND NEW FEATURES OF IOT

In more details, firstly for Phantom Routing protocol, since this protocol was made to enhance and solve the problems of both flooding-based and single-path routing protocols, it could be also helpful to solve the problems that RPL routing protocol presents in its application in the Internet of Things network. This solution came of the analysis of both flooding-based and single-path routing protocols which are used in WSNs and the conclusion of the analysis, which showed that these protocols had the same privacy protection level. The protection level that they provided was low, so the need of a new routing protocol was necessary. Due to the similarities of RPL and the protocols mentioned above, we assume that this need still exists. [8]

So, we tried to imagine, really in broad terms, how the new features of the Internet of Things network will affect this solution. As the message which a node is sending visits all the nodes in the network, a main disadvantage of this protocol in WSNs is the energy inefficiency. Although, because of the new features that exist in the Internet of Things network, we can assume that power consumption could be unlimited, and consequently this protocol could be suitable in the Internet of Things in these terms. As much as it concerns outside connectivity, the other new feature of the Internet of Things network, Phantom routing protocol could be suitable again in the Internet of Things network, as it is not affected of this feature. Messages can be sent to every node it is needed inside or outside the network in order to being succeeded the routing procedure. Although, in terms of mobility, as the nodes in the network will have the ability to move without control, joining or leaving the network anytime, this protocol will be affected.

For these reasons, we assume that Phantom routing protocol cannot be suitable in the Internet of Things network with the form that it has for Wireless Sensor Networks, and changes should be occurred in order to be a source-location privacy solution for the Internet of Things network.

Phantom Single-path Routing protocol is a new version of Phantom Routing protocol. The flooding phase is now replaced with a single-path routing, which results in even longer safety periods due to the fact that the adversary misses some of the single paths coming from different phantom sources. But the main limitation in this protocol is in the walking phase. Pure random walks tend to stay close to the source node and the definition of a large value of h does not solve the problem. Indeed, a large value h does not provide a direct improvement in the safety period; it only increases the energy waste. [8]

As it is referred above, this scheme increases the energy waste, comparing to the Phantom routing protocol or other routing protocols. Although, this is not a problem in the Internet of Things network as we assume the power of almost all the participants in the Internet of Things network is unlimited. Regarding to the outside connectivity, this scheme is suitable in the Internet of Things network, as there will be no difference in using the routing techniques to devices and sensors inside or outside the network. In terms of mobility, this scheme for the same reasons as for the Phantom routing protocol is not suitable in the form that is now. This is because the directed walk is possible to transform in a random walk and the scheme will not be able to offer the privacy level that it was expected to offer.

GROW tries to reduce the problem occurred by the pure random walks which stay close to the source, by using a two-way greedy random walk. The idea behind GROW is that using random walks is desirable for protecting source-location privacy because decisions are made locally and independently from the source location. However, using pure random walks as the only routing mechanism is impractical because the average delivery time of messages goes to infinity. First it creates a permanent path of receptors by transmitting a special packet on a random walk from the base station. Then, the source node sends subsequent data packets on a greedy random walk that will eventually hit a node from the path of receptors. From there, the packet is forwarded to the base station following the established path in reverse order. The protocol is said to be greedy because it uses a Bloom filter to store previously visited nodes in order to extend as far and as quickly as possible. Despite being designed as a greedy algorithm, one of main limitations of GROW is the substantial delivery time of the packets. [8]

As far as it concerns the energy consumption of this privacy location scheme, it has proved of the comparison between GROW and flooding-based phantom routing, that the first one consume much less energy. Although, in the Internet of Things network we assume that the energy levels of every device and sensor that participates in the network is very high, so GROW is not affected of the Energy Consumption.

Outside connectivity and GROW can be combined easily, even though it would be problems because of the large size of the network or networks, but not because of the inter connections or intra connections. Mobility, on the other hand, is a feature that could affect the implementation of GROW in the Internet of Things network as it is difficult to create a permanent path of receptors as the scheme requires.

A cross-layer routing protocol was designed to further mitigate the problem of random walks staying close to the data source. This is a phantom routing that hides the walking phase by routing data using the data link layer. Beacon frames are periodically broadcast to inform about the node presence and other network-related parameters. The cross-layer solution has two phases: MAC-layer broadcast and routing. In the first phase (MAC-layer broadcast), nodes perform in the same way as the naive solution. After a sensor node detects some event, it broadcasts the event information within MAC layer beacon frames for several hops (a system parameter H). Then, it switches to the second phase (routing). One node, referred to as the pivot node, passes the event information to the routing layer and sends it to the Base Station via routing. After the solid square node detects the event, it broadcasts the event information inside beacons for 4 hops (first phase). One node on the 4th hop is selected to send the event information to the Base Station directly through using conventional routing (second phase). If the same pivot node is used for routing all event information, the attacker will be able to easily trace back to the pivot node by observing routing layer traffic. Therefore, different pivot nodes are used to send different event information. This forms different traffic flows to the Base Station. The source node is responsible for selecting the pivot node. The source node knows which nodes are H hops away based on the cell information. It randomly picks one of these nodes as the pivot node for each event occurrence and adds that node id to the beacon frame. [8]

As far as it concerns the energy consumption, as for the previous location privacy solutions, this is not a problem, due to the fact that in the Internet of Things network devices and nodes have unlimited energy levels. According to the outside connectivity, again this scheme is not affected in its implementation in the Internet of Things network, for the same reasons. Mobility is affecting this location privacy scheme in the way it affects the Phantom routing protocol, as it is using in the second phase the classic routing protocols that are used in the Internet of Things network.

A double cross-layer broadcast solution is proposed in order to address the fact that in the cross-layer solution some privacy is sacrificed because attackers near the base station have a possibility of tracing back the pivot node. [8]

As far as it concerns the energy consumption, as for the previous location privacy solutions, again this is not a problem, due to the fact that in the Internet of Things network devices and nodes have unlimited energy levels. According to the outside connectivity, this scheme is not affected in its implementation in the Internet of Things network, for the same reasons. Mobility is affecting this location privacy scheme in the way it affects the Phantom routing protocol, as it is using in the second phase the classic routing protocols that are used in the Internet of Things network.

In cloud fake traffic approach the authors propose a cloud-based scheme for efficiently protecting source nodes' location privacy against Hotspot-Locating attack by creating a cloud with an irregular shape of fake traffic, to counteract the inconsistency of the traffic pattern caused by hotspots, and camouflage the source node within the group of nodes forming the cloud. The fake packets also enable the real source node to send the sensed data anonymously to a fake source node selected from the cloud's nodes to send to the Sink. Cryptographic operations are used to change the packets' appearance at each hop to prevent packet correlation and make the source node indistinguishable because the adversary cannot differentiate between the fake and real traffic, i.e., the cloud's traffic pattern looks random for the adversary. Moreover, tracing the packets back to the source node is nearly impossible because the real traffic is indistinguishable and the real source node sends its packets through different fake source nodes. [8]

According the energy efficiency, this scheme reduces the energy cost as clouds are active only during data transmission, the nodes generate fake packets probabilistically, and the intersection of clouds creates a larger merged cloud to reduce the number of fake packets and also boost privacy protection. Moreover, this scheme uses energy-efficient cryptosystems such as hash function and symmetric-key cryptography and avoids the intensive energy consuming cryptosystems such as asymmetric-key cryptography. However, energy consumption is not a problem in the Internet of Things network, as "smart things" can have unlimited energy. For outside connectivity, again there is not a problem. On contrary, cloud-based approach is supporting connection either in intranet or in internet. As far as it concerns mobility, this feature is affecting the implementation, as the scheme needs each node to group its one-hop neighbors in such a way that each group can send packets in different directions, which is not possible while nodes are mobile.

Change the pure random walk in favor of a direct random walk (DROW). They prevent packets from staying close to the source node and at the same time they reduce the energy waste and achieve a similar safety period. Nodes are separated in two categories on whether they are in the same direction or in the opposite direction to the base station. Thus, during the walking phase, the next hop in the path is still selected uniformly at random but only from the set of nodes in the direction of the base station. [8]

As far as it concerns the new feature of the unlimited energy in the Internet of Things network, this scheme is not affected. Compared to Flooding-based phantom, DROW has lesser the energy consumption because each message is forwarded to the base station along the shortest path. But, as we said before, in our situation energy consumption does not play an important role. For outside connectivity, this scheme does not face any limitations. Mobility is a new feature, that puts some limitations in this scheme, as it is required that every sensor node has to know the relative position of its neighbors. This is not always guaranteed in the Internet of Things network.

To protect source-location privacy in energy-constrained wireless sensor networks, it was proposed to use DGWK (directed greedy walk) for packet delivery. When the source sensor node sends out a packet, the packet is unicasted to a parent node of source node by equal probability, which the parent node never forwards the packet. The intermediate node forwards the received packet to one of its parent nodes by equal probability, which the parent node never forwards the packet. Each packet from source sensor node is forwarded until it reaches sink in a directed greedy fashion. [8]

Compared to Flooding-based phantom, DGWK has only a litter the energy consumption because each message is forwarded to sink alone the short path. Although, energy consumption is not a problem in the Internet of Things network as we assume that it is unlimited. According to the outside connectivity, in this scheme there is not any limitation as it can be implemented for communications either in the intranet or in the internet. Mobility in this scheme is a feature that causes some problems in its implementation in the Internet of Things network, for the same reasons as in the previous scheme.

The phantom routing with location angle (PRLA) prioritizes the selection of phantom sources leading to larger inclination angles. Long random walks do not necessary increase the safety period unless the phantom sources are placed in a safe location to initiate the routing phase. A location is considered to be safe if it is not close to the straight line between the data source and the sink. [8]

Energy consumption is not a problem in the Internet of Things network as it is unlimited, so this scheme again does not face any limitation because of that feature. Outside connectivity once again it is not a problem for this privacy location scheme. As far as it concerns mobility, there are some limitations for the implementation of this scheme in the Internet of Things network.

Random Parallel routing scheme assigns each sensor node n parallel routing paths to the base station. Messages are evenly distributed to different paths in such a way that the adversary trace back time is the same at any path. Also, the paths must be sufficiently geographically separated in order to prevent the attacker from overhearing packets from various paths. The underlying idea is that if the adversary chooses one of the paths he is forced to stay on the single path. This improves the safety period, which is now equivalent to the sum of all the parallel paths. However, this approach is only theoretically feasible. In practice, the generation of n truly parallel path is a complex task, especially in large-scale sensor network deployments. It is also impractical for sensor nodes to store a large number of routing paths locally. Moreover, some of these paths may become useless over time due to the death of nodes or due to simple disruptions performed by an attacker in order to force the source node to use some particular paths. Finally, since the paths are parallel to each other, retrieving several packets from any of the paths provides a good idea of the direction to the source. A savvy adversary can use this information to significantly reduce the trace back time to the data source. [8]

From the moment that energy consumption in the Internet of Things network can be undefined, it is not considering as a feature that is affecting the implementation of this solution in the Internet of Things network. Outside connectivity is not a problem for this scheme. Mobility, on the other hand is a feature that can affect the implementation of this location privacy solution in the Internet of Things network. In this scheme it is required that the paths must be sufficiently geographically separated in order to prevent the attacker from overhearing packets from various paths. But this cannot be possible in the situation of the Internet of Things network.

The Weighted random stride (WRS) algorithm is similar to PRLA in the sense that both of them decide the next hop of the data path based on the inclination angle of its neighbors. Whenever a sensor node transmits a message to the base station, it uses two parameters to guide the path, a forwarding angle and a stride. First, the data source randomly picks a forwarding angle and chooses a neighbor that matches the angle. After receiving the message, the node uses the same forwarding angle to select a new neighbor. This progress continues until the stride, which defines the number of hops for a particular forwarding angle, reaches zero. Once the stride expires the recipient node selects a new forwarding angle and starts a new stride. In practice, instead of sensor nodes having to store the forwarding probabilities of all their neighbors, they are divided into closer and further nodes. Closer nodes are additionally divided into sectors and only nodes from these sectors are selected to forward the packet. In order to produce larger routing paths and thus deter the traceback attacks, sectors with larger inclination angles are prioritized. Within a particular sector, the node selects the neighbor that has the largest forwarding step. The main difference between this approach and PRLA is that in WRS there are no phantom sources from where the packets are finally routed to the base station using a single-path approach. [8] This scheme as the PRLA scheme is like shortest-path routing. They are making traffic patterns.

Routing through a random selected intermediate node (RRIN) where the network is divided into a grid and each node knows its relative location in the grid as well as the grid dimensions. Instead of making each node in the walking phase take routing decisions independently, the source node can pick a random point in the field and send the packet to that location. Two version of this scheme are proposed. In the first the intermediate point is chosen uniformly at random but it is forced to be placed at least at a distance d_{min} from the source. The main drawback is that there is the possibility that the intermediate nodes concentrate around the location of the source node and no mechanism prevents them from being picked from the proximities of the source-destination shortest path, which was one of the problems addressed by PRLA and WRS. In the second version, any location in the network has the same probability of being selected as the random intermediate point. The consequence in is that some intermediate nodes will be very close to the data source thus exposing its location while some others will be extremely far, not only resulting in energy-intensive paths but also in more chances for the adversary to trace packets. [8]

Mobility is affecting this scheme as due to the mobility nodes will not always be able to select an intermediate node according to its place in relation with the place of the real source, as it is needed in order to the scheme is going to provide privacy. Also, the nodes will not have the knowledge of their adjacent nodes. As for energy consumption and outside connectivity the conclusion is the same like for the other protocols which we mentioned before.

This scheme has been designed to reduce the energy cost associated with the selection of pure random intermediate nodes in the field. To that end the source node picks random points within a toroidal region around the base station, which guarantees that intermediate nodes are, at most, a given distance from the destination but also not too close in order to prevent trace back attacks. The main drawback is again the selection of random intermediate nodes. No mechanism ensures that these nodes are not often chosen close to the shortest path between the data source and the base station or behind it. The solution that is proposed is a two-phase routing scheme that addresses the source-location privacy issue by using a unique routing process. In the routing process, the source node randomly determines an intermediate node from a pre-determined region around the SINK node. This region is called the Sink Toroidal Region (STaR). From the random intermediate node, the message will then be routed to the SINK node through the shortest path routing. The STaR routing method is performed for every message the source node sends to the SINK node in the network. [8] This scheme has exactly the same problems and is affected from the same feature in the same points as RPIN because it is proved that are exactly the same except the fact that STaR is needed less power consumption, which is in the Internet of Things network is not a problem.

Cycle Entrapment Method (CEM) sends decoy messages in a loop to attract the adversary and distract him from the true path to the data source thus increasing the safety period. After the deployment of the network, each sensor node decides whether will generate a network loop with a given probability. Then the node selects two neighboring nodes and sends a loop-creation message that travels h hops from one of the neighbors to the other. All the nodes receiving the loop-creation message become members of the loop. During the normal operation of the network, a loop is activated whenever a loop member receives a real packet being routed from a source node to the base station. CEM is not a routing protocol itself but rather an add-on that can be used with different routing protocols to enhance source-location privacy. [8] In this scheme, we assume that, as well as in the other protocols which we have studied, the same things could happen due to the new features of the Internet of Things network.

Hiding in Distributed Environments (i HIDE) scheme is a scheme where the sensor network consists of a set of ring nodes that are interconnected with each other and with the base station by means of a wireless network bus. In I HIDE all the sensor nodes belong either to a ring or to the network bus. During the data transmission period, a source node that wishes to communicate data to the base station first sends the data to the nest ring member in a (counter-) clockwise direction. If the node belongs to multiple rings simultaneously it randomly selects one of them to forward the message. When the bus node receives the packet, it forwards it to the next bus node closer to the sink but the packet continuous to loop in the ring for a random number of hops. As the packet travels through the bus, each bus node decides, based on a given probability, to forward the packet into its own ring or to directly submit it to the next bus node. The main limitation is that because it has such a well-defined architecture and roles for the nodes, it is easy to learn the topology of the network and thereby identify the bus and the rings. Once a bus node has been reached, the adversary can wait until he observes that the bus node receives a message from another bus node that it forwards to the next one. This implies that somewhere in a previous ring there is a data source. In this way, the adversary can slowly reduce his uncertainty. [8] In IoT due to the mobility and the topology that it has is really difficult to be implemented such a scheme.

Network mixing ring (NMR) creates a ring of nodes surrounding the base station, which is not intended to trap the adversary but to mix real messages with fake traffic in order to make them indistinguishable to the adversary. Limitations of RRIN and STaR and also energy consumption but in IoT this is not a problem. This scheme provides both content confidentiality and source-location privacy through a two-phase routing process. In the first routing phase, the message source randomly selects an intermediate node in the sensor domain and then transmits the data packet to the randomly selected intermediate node before it is routed to a ring node. This phase provides the local source-location privacy. In the second routing phase, the data packet will be mixed with other packets through a network mixing ring (NMR). This phase offers network-level (global) source-location privacy. [8] For this scheme we think that there are similar affections by the new features, as for the previous ones.

This scheme consists of three phases: initialization, path diversification, and fake packet injection. These ring-based solutions require the network to be densely populated in order to enable the creation of full rings. [8] We suppose that the same changes could happen to this scheme if we tried to implement it in the Internet of Things network.

When a node has something to transmit it first floods the network with a data message containing the event data and a hop count. When this message reaches the base station, it floods the network with a new message to inform about the distance ds between the data source and itself. Once this message reaches nodes at the same distance than the data source, they transmit a choose message. This new message is forwarded to nodes further away, which decide to forward it based on a given probability. When the hop count of the choose message reaches 0, the recipient node generates a random number, and, if above the threshold the node becomes a fake data source. The result is that a number of nodes at distance larger than ds from the base station become fake source. [8] This scheme, Fake Source 1, is built on top of baseline flooding protocol which is not able to protect source location privacy. Also mobility is a problem as the position of the fake sources depends on the position of the real source, but in Internet of Things network the position of the real source might be mobile, so it is hard to define the position of the fake source as well. The set of fake sources is chosen at deployment time, is known a priori or requires network-wide knowledge to generate. This is not always possible in the Internet of Things network.

The following scheme is built on top of baseline flooding protocol which is not able to protect source location privacy. Also mobility is a problem as the position of the fake sources depends on the position of the real source, but in Internet of Things network the position of the real source might be mobile, so it is hard to define the position of the fake source as well. [8] For Fake Source 2 applies whatever is applied on Fake Source 1 scheme.

As for the rest of the schemes mentioned on the table, the same conclusions are made after studying them by taking into consideration the new features of the Internet of Things network, meaning mobility, energy consumption and outside connectivity, so we decided not to analyze more of them in this survey, because at the moment this is out of scope. In general terms, the sense of this research is that the already existed protocols and schemes which are designed to protect source location privacy in Wireless Sensor Networks are not able to be implemented exactly as they are in the Internet of Things network. Mainly, they are affected in a bad way from mobility, without meaning that mobility is not permitting them to be effective, but with the structure that they now have. There is the possibility, with the appropriate changes these schemes could work maybe better and be more effective due to mobility, but this is a case that has to be examined in particular for each scheme. According to outside connectivity and energy consumption, we think that these two features cannot affect in a bad way the schemes, on the contrary, they can enhance them.

4. Phantom Routing Protocol for Wireless Sensor Networks

4. a. Phantom Routing Protocol

As we already mentioned one of the solutions for the protection of source location privacy in Wireless Sensor Networks is the Phantom Routing Protocol. This protocol has written by Celal Ozturk, Yanyong Zhang and Wade Trappe at the Wireless Information Network Laboratory (WINLAB) of Rutgers University. [20] In this paper, the authors focused on protecting the source's location by introducing suitable modifications to sensor routing protocols to make it difficult for an adversary to backtrack to the origin of the sensor communication. In particular, they focused on the class of flooding protocols. While developing and evaluating the privacy-aware routing protocols, they jointly consider issues of location-privacy as well as the amount of energy consumed by the sensor network. Motivated by the observations, they proposed a flexible routing strategy, known as phantom routing, which protects the source's location. Phantom routing is a two-stage routing scheme that first consists of a directed walk along a random direction, followed by routing from the phantom source to the sink. Their investigations have shown that phantom routing was a powerful technique for protecting the location of the source during sensor transmissions. [20]

Consequently, we studied a lot and in depth the Phantom Routing Protocol. We quote the Phantom Routing Protocol and the analysis of it, as it was performed by its authors on their paper “Source-Location Privacy in Energy-Constrained Sensor Network Routing”, in order to understand well its structure and the thinking behind it. Before the explanation of the Phantom Routing Protocol the authors analyze the simulation model that they used and the panda-hunter game which is a generic sensor-network application for setting up the use case on which location routing protocols were applied in order to see their effectiveness. The panda-hunter game is presented below as it was written on the paper we mentioned before. In the Panda-Hunter Game, a large array of panda-detection sensor nodes have been deployed by the Save-The-Panda Organization to monitor a vast habitat for pandas. As soon as a panda is observed, the corresponding source node will make observations, and report data (e.g., what the panda is doing, etc.) periodically to the sink via multi-hop routing techniques. The game also features a hunter in the role of the adversary, who tries to capture the panda by back-tracing the routing path until it reaches the source. As a result, a privacy-cautious routing technique should prevent the hunter from locating the source, while delivering the data to the sink. [20]

The primary concern for the operator of the sensor network is the safety of the panda. In this sense, keeping the location of the source of a sensor reading unknown to the hunter is the primary underlying privacy goal. In order to explore this further, they examined the operation of the Panda-Hunter Game in more detail. In the game, the panda pops up at a random location, and stays there until it is captured by the hunter. Once the hunter gets close to the panda (i.e., within δ hops from the panda), the panda is considered captured and the game is over. At the beginning of the simulation, the panda will appear at a random location, and the corresponding sensor node, which becomes the source, will start sending packets to the sink reporting its behavior. The simulator uses a global clock to synchronize all the activities within the network. The source generates a new packet every T clock ticks until the simulation ends. The packets are of the same length and will be encrypted, and the hunter cannot break the encryption. The authors employed a simple approach to model the communication links: a message will reach all the neighbors (i.e. the nodes that are within the sender's radio range R) of the sender at the next clock tick with the probability p, where p denotes the reliability of the channel (also modeling MAC-layer collisions), and 1 – p denotes the loss factor of the channel. The simulation ends either when the hunter catches the panda or when the hunter cannot catch the panda within a threshold amount of time (e.g. the panda has returned to its cave). [20]

They assumed that the hunter is mobile with unlimited amount of power, yet a limited amount of memory. The hunter starts at the sink's location, where it is guaranteed that sensor packets must ultimately arrive. The hunter is constantly in a listening/receiving mode. Once it hears the first message, it knows which node among its neighborhood sent that message, and it will move to the transmitting sender node. It should be emphasized that, due to the multi-hop nature of routing protocols, a transmitter node may differ from the original message source. The authors further assume that the hunter has a message cache which stores the most recent M messages that have been heard. Every time the hunter moves to a new location, he continues to listen to the channel until he receives a new message. Multiple copies of the same message may traverse different portions of the network, and hence it is possible for the hunter to receive multiple copies of the same message at different times. The hunter will want to differentiate between new messages and previously observed messages. Therefore, they assumed that the hunter can tell whether a message is new or not by comparing it with all the messages in its cache. Further, since the hunter has limited memory, they assumed that he employs an LRU (Least Recently Used) cache replacement policy in order to ensure that the most recently heard messages (which are hopefully the most recent messages) are always kept in the cache. Once a new message is heard, the hunter makes another movement towards to its sender. If no new messages are heard within a specified period of time (T_{listen}), the hunter concludes that the current node he is at is not on the routing path, and must return to a former location. In addition, the authors also assumed the hunter has a location cache which records the locations of the last N nodes it has visited to avoid loops. As soon as the hunter gets reasonably close to the panda (within the capture range δ), we assume the panda is caught and the game/simulation will end. [20] So, more or less, this is the simulation model on which the authors deigned in order to perform and implement the phantom routing protocol, to observe if it is able to protect the location privacy. Although, in the Internet of Things Network there are several differences comparing to the Wireless Sensor Network, with mobility the most important difference, we used in general in general terms the same model, but now in our situation the panda and the nodes in the routing could be possible mobile. We analyze in more detail all the relative cases that could appeared in the Internet of Things network to the following section. In the Internet of Things network we can assume that sensors could be also smart things such as devices etc. which participate in the network and they can be as well in the routing path. Due to the mobility, the things that are changed to the simulation model above is the fact that the panda has the ability to move anywhere and anytime in the network, and the same ability have the rest sensors or devices that participate in the routing path that the source node is using to send its data to the sink node.

Then authors in order to explain the phantom routing protocol better presented and analyzed three basic routing techniques for location privacy. These three techniques are Baseline flooding, Probabilistic flooding and flooding with Fake Messages. For our research, and in terms of better understanding the phantom routing protocols, we will quote as the authors presented the Baseline flooding technique in their paper, as this technique is a part of the phantom routing protocol and it will be a part of our attempt to outline a phantom routing protocol for the Internet of Things network.

In the baseline implementation of flooding, they made sure that every node in the network only forwards a message once, and no node retransmits a message that it has previously transmitted. When a message reaches an intermediate node, the node first checks whether it has received and forwarded that message before. If this is its first time, the node will broadcast the message to all its neighbors. Otherwise, it just discards the message. Realistically, this would require a cache at each sensor node. However, since sensor messages are typically small, and the delay between source messages is typically longer than the maximum time needed for a message to traverse the network, the cache size can be kept small. It is thus reasonable to expect that each sensor device will have enough cache to keep track of enough messages to determine whether it has seen a message before. [20]

It is evident that flooding involves significant energy consumption. If it is supposed that there are n nodes in the sensor network, then the total number of transmissions that will take place (per new message) is upper bounded by n. They noted that the actual amount of transmissions that occur is also affected by the packet reception rate p, and it is entirely possible that some sensors will never receive a message and hence never transmit that message themselves. For reasonable values of p, the energy spent by the entire network on a single message transmission will increase linearly with the size of the network n. Further, under realistic conditions, where packet collisions, packet retransmissions, and packet drops frequently occur, flooding is an energy expensive approach to message delivery. In their simulation studies, the authors found the number of transmissions per message for p = 1 and verified that it is equal to the number of nodes in the network. [20]

Then, they presented the best strategy that an adversary could adopt in this case. The adversary should start at the sink, and wait until it hears a message. If it first hears the message, it moves to the immediate sender of the message until it gets to the source. In this algorithm, the adversary must be able to tell if the message it has received is a new one or not, which is accomplished using the LRU-message cache. [20]

At first glance, one may think that flooding can provide strong privacy protection since almost every node in the network will participate in data forwarding, and that the adversary may be led to the wrong source. However they believe that further inspection reveals the contrary. They emphasized that flooding provides the least possible privacy protection since it allows the adversary to track and reach the source location within the minimum safety period. For instance, if the shortest path length between the source and sink is 80, then the safety period is 80 as well. [20]

Then they provided an explanation for the poor privacy performance of flooding. The authors started by looking at the set of all paths produced by the flooding of a single message. This set consists of a mixture of different paths, some longer than others, and it is clear that the shortest path between the source and the sink is contained in the collection of paths produced by flooding. Therefore, the first message that the adversary receives while waiting around the sink will correspond to a message that follows the shortest path, and as a result the adversary will be able to jump to the forwarding node on the last hop in the shortest path. Now, while the adversary is sitting at this new position, the source produces the next message. Due to the fact that the adversary is on the shortest path, the adversary will subsequently receive the next message via the sub-path of the source-sink shortest path. Thus, the adversary will be able to jump to the previous forwarding node on the source-sink shortest path. Repeating iteratively, the adversary will capture every message on the shortest path, and ultimately reach the source via the shortest path. [20]

Then they tried to explain the poor privacy performance of flooding by looking at the message latency. Suppose the source sends out m events, e1, e2, · · ·, e_m. The sink will receive multiple copies of each event, depending on the number of immediate neighbors it has. Among all the receiving times for the same event, the sink records the minimum time stamp, and further computes the minimum latency between the source and sink. We use d_i to denote the minimum latency for event e_i. Then the average of the d_i values is called the average shortest latency. They observed that the average shortest latency is always equal to the number of hops as it takes 1 clock tick to travel each hop. This further confirms that the messages always arrive earlier from the shortest path, and thus the adversary can easily locate the source. [20]

One may argue that this observation might be just an artifact that results from the way we implement the flooding protocol. In the simulation, they assumed that every link incurs the same transmission delay of 1 clock tick. It is arguable that this fixed latency can lead to a fixed shortest path, thereby making the adversary's job easier. However, in order to demonstrate that their observation holds under more general and realistic network conditions, they also modeled the link latency as a number that is randomly selected with equal probability from {1, 2, 3} clock ticks, thereby allowing the shortest path between different event deliveries to vary. [20]

In their paper, they conducted simulations to study the privacy characteristics of flooding for a uniformly distributed network consisting of n = 10, 000 nodes. Regardless of the link latency, every event is transmitted the same number of times. Since the average link latency increases in the random latency scenario, the average shortest latency also increases. They observed that the latencies with random delay are roughly around 1.2 times longer than the fixed-latency configuration across different network setups. More importantly, in spite of the increase in the average latency, it is proved that the gap between safety periods for these two configurations is negligible (always below 10%). This result implies that the adversary can easily locate the source even when every link has a random latency, which supports the observation that the flooding technique does not provide privacy protection. (This is because different links in the network have the same delay distributions.) [20]

Then, more specifically, we are going to examine the Phantom Routing protocol as it was presented in the paper. [20] Firstly, Phantom flooding shares the same insights as probabilistic flooding (which was also analyzed in the same paper) in that they both attempt to direct messages to different locations of the network so that the adversary cannot receive a steady stream of messages to track the source. As they pointed out in their paper, probabilistic flooding is not very effective in achieving this goal because shorter paths are more likely to deliver more messages. Therefore, what they would like to do is somehow entice the hunter away from the source and towards a fake source, called the phantom source. [20]

In phantom flooding, every message experiences two phases: (1) a walking phase, which may be a random walk or a directed walk, and (2) a subsequent flooding meant to deliver the message to the sink. When the source sends out a message, the message is unicasted in a random fashion within the first h_{walk} hops (referred to as random walk phase). After the h_{walk} hops, the message is flooded using the baseline flooding technique (referred to as flooding phase). The algorithm is illustrated in Figure 4. The implementation of the flooding phase it is the same as it was discussed earlier. [20]

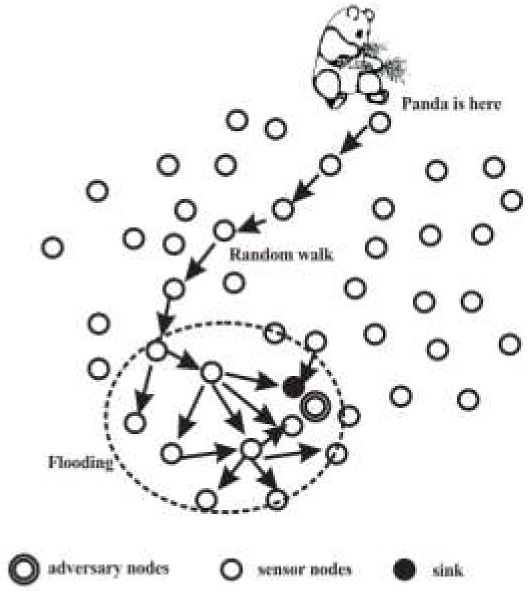


FIGURE 4: PHANTOM FLOODING ALGORITHM

Phantom flooding can significantly improve the network safety period because every message may take a different (shortest) path to reach any node within the network. As a result, after the adversary hears message i, it may take a long time before it receives i + 1. When it finally receives message i+1, the immediate sender of that message may lead the adversary farther away from the source. In the example shown in Figure 5, the adversary is already pretty close to the source before it receives the next new message. This new message goes through the random walk phase and reaches node A, and then goes through the flooding phase. The adversary receives this message from node B, and according to its strategy, it will be duped to move to node B, which is actually farther away from the source compared to the current location of the source. [20]

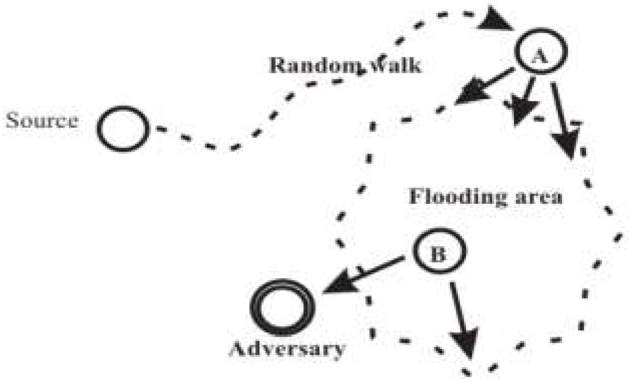


FIGURE 5: EXAMPLE SCENARIO OF PHANTOM ROUTING PROTOCOL

Another advantage of phantom flooding is that its privacy protection improves as the network size and intensity increase because the path diversity between different messages will become more substantial. [20]

It is not a trivial task to implement random walk. The purpose of the random walk is to send a message to a random location away from the real source. However, if the network is more or less uniformly deployed, and we let those nodes randomly choose one of their neighbors with equal probability, then the resulting random walk path is essentially an unbiased, discrete two-dimensional Brownian motion. Therefore, there is a large chance that the message path will loop around the source spot, and branch to a random location not far from the source (illustrated in Figure 6). [20]

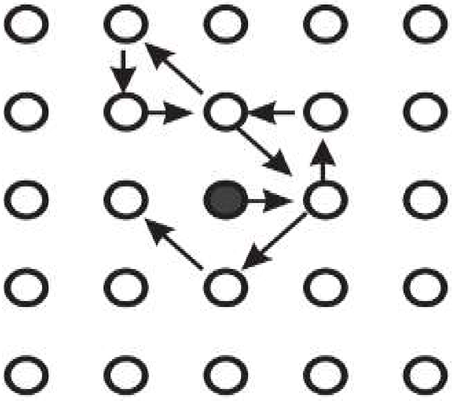


FIGURE 6: RANDOM WALK

Our simulation results further confirm this observation, but due to space limitations, the results are not shown here. In order to avoid random walks cancelling each other, we need to introduce bias into the walking process, and therefore we propose the use of directed walk to provide location-privacy. In directed walk, we separate the neighbors into two groups so that those nodes whose directions are opposite to each other do not belong to the same group, as illustrated in Figure 7. [20]

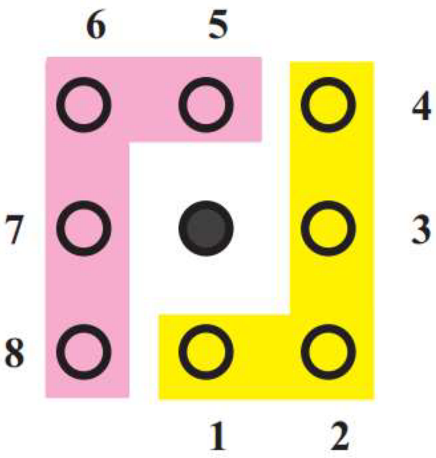


FIGURE 7: NEIGHBOR GROUPING METHOD

At the first step of the directed walk, the node randomly picks one group, and later steps will only choose neighbor nodes from that specific group. This method can remove the paths that loop back upon themselves in the random walk. As a result, the routing can leave the source area and reach a random location (illustrated in Figure 8). [20]

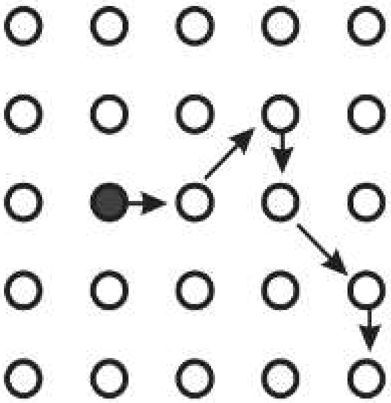


FIGURE 8: DIRECTED WALK

Directed walk requires a node knows the relative position of its neighbors. Such knowledge can be obtained by using ranging and angle of arrival (AOA) measurements. [20]

In this simulation, the authors varied the source location by varying the shortest path between the source and the sink as in earlier sections. They also varied the directed walk length (h_{walk}) to study its bearing on the privacy level. They have found that even with a directed walk length of 10, the Hunter cannot track the source location. So, the authors conclude that Phantom flooding success-fully protects the source location privacy. [20]

Compared to baseline flooding, phantom flooding does not increase the energy consumption because each node at most forwards the same message once. However, phantom flooding can potentially increase the average message latency because every message is directed to a random location first. They expected that the latency should be increased at least by the factor hwalk. As the network size increases, this relative increase is negligible. [20]

In conclusion, networks of energy-constrained sensor nodes are increasingly being deployed for monitoring and data collection applications. The very nature of sensor networks such as their location-dependency, their context sensitivity, and the challenges of the underlying wireless communication protocols has created a new set of problems surrounding the security and privacy of the sensor communications. An important aspect of the communication context is the source location. In many applications, if the adversary observes traffic within the network, he may be able to back track these messages to locate the event source, which can be a serious privacy breach for many monitoring and remote-sensing application scenarios. [20]

In this paper, the authors identified this important problem, and indicated that the source location privacy can be strongly influenced by the data dissemination techniques or routing protocols. They examined one of the most popular families of routing protocols in sensor networks, namely flooding. Based on their analysis and simulations, they found out that neither of these protocols are capable of providing source location privacy. [20]

They proposed a family of techniques for the flooding routing classes that enhance their privacy protection. After observing the privacy performance and energy consumption characteristics of these different methods, they proposed a very powerful strategy, known as phantom routing. Through their simulations, they showed that phantom routing is capable of keeping the adversary virtually lost within the sensor network, thus significantly enhancing source-location privacy, while not incurring any significant energy overhead. [20]

4. b. Advantages and Disadvantages of Phantom Routing Protocol

After the extensive study of the Phantom Routing protocols we tried to find the advantages and disadvantages of this protocol, as well as we tried to imagine what could happen after adding one by one the new features that are existing on the Internet of Things network and which were not existing in Wireless Sensor Networks. We made this scenarios because the Phantom Routing protocol was designed for Wireless Sensor Networks and was implemented on it, so we believed that this process would helped us to conclude if the Phantom Routing Protocol could be used as it is in the Internet of Things network in order to protect location privacy, or if some improvements are needed to be done, or a new algorithm of the protocol should be made, or even maybe this protocol is totally unsuitable for the Internet of Things.

First of all we tried to record the advantages of the Phantom Routing protocol. As the authors of this protocol mention the Phantom Routing protocol has several advantages when is implemented in Wireless Sensor networks. Firstly, the Phantom Routing protocol is able to significantly improve the network safety period, and consequently aid to the protection of source location privacy. This occurs because every message may take a different (shortest) path to reach any node within the network. Also, is referred that the privacy protection improves as the network size and intensity increase because the path diversity between different messages will become more substantial. This is a good hint as the Internet of Things network is tenting to be a big network so this could be implemented in a good and beneficial way. Moreover, it is proven that phantom routing with directed walk even with a directed walk length of 10, the hunter cannot trace the source location. Last but not least, the Phantom flooding, compared to baseline flooding does not increase the energy consumption because its node at most forwards the same message once.

As for the disadvantages of Phantom Routing protocol in Wireless Sensor Network we also find a several number of disadvantages, something that we could already imagine because of the big number of different routing protocols that have designed and of the continuous existence of the need of protecting location privacy, which means that the perfect solution for this problem has not been found yet.

Firstly, the first of the two phases of the walking process in Phantom Routing, is a random or a directed walk. Random walk is not a good choice, as it makes loops around the source so it is possible that the intermediate nodes would stay really close to the source and then it is easy for the adversary to trace back the road and eventually find the source node. Also, even with the directed walk, if we add mobility, we may have the same problem with the random walk, as the positions of the nodes would not be steady and we could not have two different groups of neighbors.

Then, the second phase of the walking process is baseline flooding. According to the privacy protection, flooding provides the least possible privacy protection, as it allows the adversary to track and reach the source location within the minimum safety period. This happens because in the collection of all the paths produced by flooding is included as it is normal the shortest path from the source to the sink. So, the first message that the adversary receives while waiting around the sink will correspond to a message that follows the shortest path, and as a result the adversary will be able to jump to the forwarding node on the last hop in the shortest path. Now, while the adversary is sitting at this new position, the source produces the next message. Due to the fact that the adversary is on the shortest path, the adversary will subsequently receive the next message via the sub-path of the source-sink shortest path. Repeating iteratively, the adversary will capture every message on the shortest path and ultimately reach the source via the shortest path.

Concluding, these two techniques combined together are supposed to provide better privacy protection, but if one of them does not work properly, the problems of the other one will appear as well. Furthermore, the Phantom routing can potentially increase the average message latency because every message is directed to a random location first. It is expected that the latency should be increased at least by the factor h_{walk}. Then, the same as the probabilistic flooding in Phantom routing there is the possibility of some messages be lost in the network and that would affect the network connectivity. Finally, in general, Phantom Routing increases the energy consumption.

4. c. Making scenarios by adding new features

Then, we tried to make some scenarios by adding some new features each time. So, we started to think about what could happen and what problems and benefits would arise if the base station could move. So, there is the possibility that the base station will move really close to the source node or maybe away from the source. But this cannot play an important role to the safety period. Consequently, we believe that if the base station was moving, it would be the same as if the base station would be steady, because the routing and the privacy depend on the routing path which takes place between the rests of the nodes. From the moment that the attacker will hear a message and moves to the node that the message came from, it does not make any difference if after that the base station will move, as the attacker would have already start to follow the path of the message back to the source.

After this, we tried to figure the scenario where some nodes can move and we came to some conclusions. In this situation, on the directed walk we cannot separate groups of neighbors as the position of the nodes could change and consequently the node would change group. This could direct to have a random walk instead of directed walk.

Moreover, if the node which is the next to transmit a message is moving to place where there are no other nodes around him it is possible to have a big latency until he moves again to place with neighboring nodes or another node move in his vicinity.

If the node is moving closer to the base station the safety period is possible to be further reduced as maybe even shorter paths from the phantom source to the sink as closer as a node is getting to the base station.

Furthermore, if the nodes and consequently the phantom sources are gathered on a particular area from where many paths from the source to the sink are passing, this area becomes a critical area, as if the attacker trace back a path in this area he will be able easily to receive more messages from the source and the safety period will be more reduced. Mobile nodes in this situation are a good and in parallel a bad option, because they can create or destroy a critical area quite easy. It would be a good option if nodes were moving out of an already existing critical area so there would not be a critical area anymore, or if they were moving away from the source node, so as the safety period would be increased and it would be more difficult for the attacker to trace back the messages. From the other hand, it is possible the moving nodes to enter an already existing critical area, so it would be much easier for the adversary to reach the source node.

The last scenario depending on the mobility or not of the nodes that we examined, was the one in which all nodes can move. In this situation, all the above problems would consequently appear, as well. If nodes that participate on the routing paths and the base station come closer to each other and if all are gathered in the critical area that would made it even easier for the attacker to reach the source node. But also, any mobile node even could leave from a critical area.

After created these scenarios and figured some of the consequences that could be occurred at the implementation of the Phantom Routing protocol we tried to think if we can solve the problems arisen by only introducing slight or maybe big changes on the phantom routing protocol. So, as we can say that we can use the Phantom Routing protocol in the Internet of Things network.

Firstly, the nodes even if they move or not, can inform the rest nodes of the network about their approximate position, their direction or their destination. In this way, we could have a kind of directed walk, so as there will not be loops around the source node. They could send this kind of information whenever they change position or they can give this information when another node is searching about its neighbors by making relative requests. This is more effective in terms of saving power, instead of the nodes sending continuously their information. The node which is in search for an intermediate node to transmit his message can make a request to his neighboring nodes, then they will answer with this information and he will decide if it is beneficial for him to send them his message. Although, this procedure may cause some delays until the node get the information that he needs for the other nodes in order to decide. Depending on the kind of application and how much critical is the time between the transmission, we can define a period of time in which the mode can be in search. If he gets over this time period or he transmits his message to a node which is not ideal, or he rejects it.

Secondly, in any situation in which it is possible, we could force the nodes in such a way to move or stay stable depending on their current position according to a critical area that has been created. For example, if during the transmission of a number of messages all originated from the same source node, the nodes that are used as phantom sources are close to each other, it is needed to force them move in order to leave the critical area, or to stop transmitting messages while they are in it and wait for other phantom sources to leave. Also, if other nodes which maybe later will be used as phantom sources, are tending to get inside the critical area. So, the problem now is how the nodes could know that they are in a critical area or maybe prevent the creation of a critical area.

The solution could be in the information that is sent between the nodes. With some parameters such as the current position of the node, the destination or the direction of the node, a number showing how recently this node is receiving and transmitting messages, and the average of the messages that he is receiving and the average of transmitting, we could have a current identity. Compare his identity to the identities of the neighboring nodes he could make a conclusion about if he is going to transmit his message or to move to a critical area. According to the average of receiving messages and the one of the transmitting messages of each node we could understand if a node possibly has been or has not been a phantom source. So, with this information we will not let him be again a phantom source or to reach other nodes that have been phantom sources too to reach him.

Otherwise, depending on the type of the device, according to this information we could give it a command of moving to a specific area where seams that have not been other phantom sources, so as nodes that have been used as phantom sources are spread on the field and not gathered on the same area.

If it is not possible to control the movement of a device somehow, we could try to control the messages that they receive and transmit. According to the information of the environment of the nodes and to their own information, if they are in a critical area, we can force them to reject for a period of time messages in order to avoid being a phantom source in a critical area. So, the messages are going to be transmitted from other nodes that possibly were not phantom sources recently in the past.

All this information of the nodes should be encrypted, so as the attacker could not read it even if he get it.

Although, for this kind of solutions each node will need big enough memory in order to be able to keep messages that he could not send immediately and the information we described above.

Furthermore, another problem is the latency that possibly will be occurred on the network, as it would take more time for each node to check its neighboring nodes about how compatible they are before transmitting his message to them.

Lastly, energy consumption is increased because more information has to be transmitted on the network and computations will take place on the nodes.

When a node has been a phantom source we can force him to move to the opposite direction from the direction he flooded the message or if he cannot move he is rejecting the messages for a period of time until he is able to send messages again.

So, after all these consumptions, we tried to think if the good be better in order to this protocol operate correctly, by adding firstly some nodes with unlimited power. We believe that if nodes have unlimited power they can send continuously and periodically their position, their destination or their direction, to every other node in their vicinity. That would be very efficient so as the nodes could transmit their message with relative security that they will go to the path that they want and that loops around the source node will not be feasible. Also, maybe a solution would be adding nodes that send fake messages continuously.

Then we tried to think what could happen if we added some nodes with “unlimited” memory. Unlimited memory is a feature that could be used from the node in order to store a message when he is in a place where there are no other nodes around him or when he thinks that no one of his neighboring nodes’ position/destination/direction fits to the destination which he wants for his message to follow. In this case he has to wait until another node comes up or he moves to another place, so he has to have enough memory to store the messages. Also, unlimited memory is useful in terms of avoiding loops, by not transmitting the same message from the same nodes. So, a node can keep to his memory for a specific period of time the messages that he has already transmitted, and if he receives again the same message in this period he is going to reject it.

The other feature we tried to add is Internet connectivity implemented on some nodes, as if they were smart devices which are able to connect in the Internet directly. If this happened, nodes could send their messages immediately to a cloud, when it is needed, and then from the cloud the messages would be sent to the sink, so the path back to the source will not be distinct to the adversary.

A last feature that we thought that might could help in solving our problem is adding some nodes that are having antennas. If a node has not connectivity to the Internet and a neighboring node has an antenna, the node can sent its message to this node and then the node with the antenna could sent the message to cloud, and then the message would be sent to the sink.

Last but not least we tried to examine if in these scenarios and solutions that we made for each one there was any impact on network performance and if we should use the solutions that we made. The truth is that on real time applications when we cannot afford any latency or when the time is critical for the application, or location is changing quickly, we can not to use this solution. Depending on the kind of the application and how important is the location in order to protect it. So, we need to carefully find where and when we can implement these solutions in order to be effective.

5. Phantom Routing Protocol for IoT (Algorithm)

In terms of using the "Phantom Routing Protocol" in the Internet of Things, we tried to create an algorithm with the steps that must be followed, in order to eliminate the possibility of the attacker who is trying to disclose the location of the source. So, a new model of the phantom routing protocol created, by taking advantage of all the knowledge, the simulations and the differences between Wireless sensor networks and Internet of Things, which we got of the previous analysis of these two technologies and all of their characteristics.

The steps of the algorithm of the "Phantom Routing Protocol for Internet of Things" are the following:

1. The source node sends his message in a random fashion so there is a random walk of h_{walk} hops. In order to avoid the disadvantages of the pure random walk such as having loops around the source node with the consequence that the phantom source will stay really close to the source, we could implement directed walk. Although, as some of the nodes will be mobile, permanently or sometimes, and some others will be stable, directed walk need to be different in some points, comparing to the directed walk used for the phantom routing in WSNs. We assume, that every node in the network, mobile or not, can send information about his current position, his direction and/or his destination whenever he is going to be asked from a node who is willing to transmit his message to him, searching the ideal node, instead of sending his message totally random to a neighboring node. So, the node that is searching for the ideal node to make the transmission of his message will make a request for this kind of information, to all his neighboring nodes. When they will answer, providing him with the necessary information he will randomly select between the nodes who cover his needs, and he will reject he nodes who does not, for example nodes whose destination are nodes to the opposite destination of the one that he wants, or their position is really close to him etc. On the same way the directed random path will be created after h_{walk} hops and the last node of this random walk will be the phantom source.

Although, we already have some disadvantages in this phase. In the phase of the directed walk there is the possibility that the procedure of the transmission of the node's current "position-direction" information will cause some delays and as well some latency to the network. For this reason, we cannot let the node search for the ideal node indefinitely. After a define period of time, depending on the type of the application (if the time is crucial or not) we will give him the command to either choose random a node even if he is not ideal or to wait until something changes like his position or his neighbors.

2. When the phantom source is defined in a total random way, after the directed random walk, the message is delivered to the base station through baseline flooding, on the same way as in the Phantom Routing protocol for WSNs.

The main problem that comes up on this scheme is that there is a high possibility that many phantom sources will be gathered on the same area. If the nodes and consequently the phantom sources are gathered on a particular area from where many paths from the source to the sink are passing, this area becomes a critical area, as if the attacker trace back a path in this area he will be able easily to receive more messages from the source and the safety period will be more reduced. Mobile nodes in this situation are a good and in parallel a bad option, because they can create or destroy a critical area quite easy. It would be a good option if nodes were moving out of an already existing critical area so there would not be a critical area anymore, or if they were moving away from the source node, so as the safety period would be increased and it would be more difficult for the attacker to trace back the messages. From the other hand, it is possible the moving nodes to enter an already existing critical area, so it would be much easier for the adversary to reach the source node.

But in this situation is difficult for a node to know if his is in a critical area or not, or if he is going to move to a critical area. As it is impossible to foresee which node will be a phantom source or where a critical area will be created, we have to take advantage of the information that we already have about the nodes that already have been created.

3. After a node becoming a phantom source, he can be forced either to move, if he is able to move, to the opposite side from which he flooded the message, or to stay stable, if he does not move, but with rejecting all the messages he receives for a period of time, in order to not become again a phantom source.

4. If he changes position, he has to check before he is going to transmit another message of his new position, if on his new neighborhood there are neighbors who have been used as phantom sources. He can send a request to his neighboring nodes to send him back their information of the average of the transmitting and receiving messages. Comparing their averages between them, he could understand if some of them were or were not, during the define time of period, phantom sources. If they were, he has to decide either to stay but without transmitting messages or to move again to the opposite side from the one that he came and also the one that he is.

Note: Every node has to be able to keep some information for a certain period of time. This information should be: the average of the receiving messages, the average of the sending messages, his current position, his direction and his destination.

Nodes should have some credentials that are going to use when they receive this information after their request to their neighboring nodes, so as they will be able to reveal this information and will be able to understand if any of this node is a phantom source or not. This would be a kind of authentication for the legal nodes and a way to prevent the revealing of this information to an attacker.

This kind of information is going to be erased when a period of time has passed so it will then be useless.

5. In the case that the node who just became phantom source is stable, we will force him for a certain period of time to reject every other message is coming to him for transmission, in order to avoid becoming again and again phantom source for the same source node and consequently a define path will be created. Or else, he could keep the message until he gets informed that other neighboring phantom sources left from his vicinity.

6. In case that the source node is also moving during the period of time that we have defined, that could mean that the nodes that have been used for this source node could maybe reused if the movement of the source node is such a movement that will not use this node or nearby nodes for phantom sources so as to create a critical area. Although, in this case again we cannot predict the exact movement.

As a conclusion, we can assume that we will never be in the position to guarantee that a critical area will never be created or that a node which recently had been a phantom source will never be in such an area, but we try to minimize this possibility.

6. Conclusion

With the passing from the Wireless Sensor Networks to the new technology of the Internet of Thing network, many things have changed, new benefits have been raised, but also new disadvantages and threats have appeared. In this new cyber environment, security and privacy are two elements that constitute stakes. Already, the 100% of security and privacy in the cyber world is not existing. Every day we can see new cyberattacks taking place and violation of the privacy life of many people, by data leakages and other ways. This has led to new regulations and legal rules for the protection of personal data, such as General Data Protection Regulation (GDPR) and e-privacy regulation (which is not yet applicable), which aim to protect privacy and personal data of individuals and they stipulate substantial penalties (legal and economical) to anyone who violate them.

Although, we believe that rules and regulations for data protection and privacy protection are more than welcome to exist and being applied, but they are not enough controls for achieving this hard goal of data and privacy protection. Controls in terms of Privacy by design are really important to this direction and they can be more efficient as they are able to protect data and privacy from the beginning of the implementation of new technologies, which may possible harm privacy and personal data.

So, by examining in deep details the similarities and the differences between the technologies of Wireless Sensor Networks and the Internet of Things network, we concluded that the three major new features that the Internet of Things brings, and Wireless Sensor Networks do not provide, are mobility, energy consumption and outside connectivity. We took these findings for granted, and we tried to see what could happen if we added them, to the already existing solutions for location privacy protection in Wireless Sensor Networks. These solutions were types of routing protocols, designed to protect source location privacy, as the routing protocols that were being used in Wireless Sensor Networks were producing traffic patterns and it was easy for an attacker to find the source node and consequently to reach the location of the desired device.

We noticed that the same problem would occur to the Internet of Things, as the routing protocol that is more likely to be used, RPL protocol, also produce traffic patterns. After studied on every source location privacy protocol, we concluded that none of the existing protocols can be used as it in the Internet of Things due to the new features of the Internet of Things and especially the feature of mobility. Therefore, we made a new version of the Phantom Routing Protocol, as this would be appropriate to be applied in the Internet of Things network. Although, again this solution is not perfect and has so disadvantages which need to get solved, it is really encouraging from the perspective of Privacy by design, as by designing such protocols and implementing them from the beginning in the Internet of Things we can protect more efficiently privacy and personal data.

As future work, it is really substantial to continue the research on this suggested protocol for source location protection, the Phantom Routing protocol for the Internet of Things network, by studying again and more on the Internet of Things as it is a new technology that continuously is being developed and changing and then by implementing versions of this protocol to see how it works in practice, in order to be sure that it is effective and in a good direction for achieving our goal. Then, the attempt of examining the rest of the location privacy protocols and their transformation in protocols that could be applied in the Interne of Thing network as well, is very important and it could give many useful consumptions to the issue that is called Location Privacy Protection.

References

[1] Nahrstedt, K, Li, H, Nguyen, P, Chang, S and Vu, L (2016). Internet of Mobile Things: Mobility-Driven Challenges, Designs and Implementations. IEEE First International Conference on Internet-of-Things Design and Implementation.

[2] Karagiannis, V, Chatzimisios, P, Vazquez-Gallego, F and Alonso-Zarate, J (2015). A survey on application layer protocols for the Internet of Things. ResearchGate.

[3] Bello, O and Zeadally, S (2016). Intelligent Device-to-Device Communication in the Internet of Things. IEEE SYSTEMS JOURNAL, VOL. 10, NO. 3, SEPTEMBER 2016.

[4] Perera, C, Zaslavsky, A, Christen, P and Georgakopoulos, D (2014). Context Aware Computing for The Internet of Things: A Survey. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014.

[5] Bandyopadhyay, D and Sen, J (2011). Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Pers Commun.

[6] Ghaleb, S, Subramaniam, S, Zukarnain, Z and Muhammed,A (2016). Mobility management for IoT: a survey . EURASIP Journal on Wireless Communications and Networking.

[7] Al-Karaki, J and Kamal, A (2004). Routing Techniques In Wireless Sensor Networks: A Survey. IEEE.

[8] Rios, R, Lopez, J and Cuellar, J (2016). Location Privacy in Wireless Sensor Networks. United States of America: CRC Press. p1-22.

[9] Zou, Z, Nagayama, T, and Fujino, Y (2013). Efficient multihop communication for static wireless sensor networks in the application to civil infrastructure monitoring. Wiley Online Library.

[10] Butcharoen, S, Pirak, C and Mathar, R (2011). On the Performance of Cooperative Multihop Communications. IEEE.

[11] Yao, L, Kang, L, Shang, P and Wu, G (2013). Protecting the sink location privacy in wireless sensor networks. Pers Ubiquit Comput.

[12] Dhumane, A, Prasad, R, and Prasad, J (2016). Routing Issues in Internet of Things: A Survey. IMECS.

[13] Al-Fuqaha, A, Guizani, M, Mohammadi, M, Aledhari, M and Ayyash , M (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communication Surveys & Tutorials, Vol.17, No.4.

[14] Kamat, P, Zhang, Y, Trappe, W and Ozturk, C (2005). Enhancing Source-Location Privacy in Sensor Network Routing. IEEE.

[15] Lopez, J, Rios, R, Baob, B and Wangb, G (2017). Evolving privacy: From sensors to the Internet of Things.

[16] Xin H and Yang, K (2015). Routing Protocols Analysis for Internet of Things. IEEE.

[17] Steenbrink, L (2014). Routing in the Internet of Things. Ausarbeitung.

[18] Grgić, K, Špeh, I and Heđi, I (2016). A Web-Based IoT Solution for Monitoring Data Using MQTT Protocol. IEEE.

[19] Bandyopadhyay, D and Sen, J (2011). Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Pers Commun.

[20] Ozturk,C, Zhang,Y, Trappe, W (2004). Source-Location Privacy in Energy-Constrained Sensor Network Routing. WINLAB.

[21] Wireless securty workshop. See http://www.ece.cmu.edu/ adrian/wise2004/.

[22] Mehta, K, Liu, D and Wright, M (2007). Location Privacy in Sensor Networks Against a Global Eavesdropper. Arlington: The University of Texas at Arlington.

[23] Rios, R and Lopez, J (2010). Source Location Privacy Considerations in Wireless Sensor Networks. Malaga: NICS Lab.

[24] Kamat, P, Zhang, Y, Trappe, W and Ozturk, C (2005). Enhancing Source-Location Privacy in Sensor Network Routing. ICDCS 2005, 25th IEEE International Conference on Distributed Computing Systems.

[25] Ozturk, C, Zhang, Y and Trappe, W (2004). Source-Location Privacy in Energy-Constrained Sensor Network Routing. New York, NY, USA: SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. P 88–93.

[26] Pai, S, Bermudez, S, Wicker, S, Meingast, M Roosta, T, Sastry, S and Mulligan, D (2008). Transactional Confidentiality in Sensor Networks. IEEE Security & Privacy.

[27] Kamat, P, Xu, W, Trappe, W and Zhang, Y (2007). Temporal Privacy in Wireless Sensor Net- works. ICDCS '07: Proceedings of the 27th International Conference on Distributed Computing Systems.

[28] Rios, R and Lopez, J (2011). Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks. The Computer Journal, vol. 54.

[29] Khan, Z and Abbasi, U (2016). Evolution of Wireless Sensor Networks toward Internet of Things. Cornell University Library.

[30] D. Christin, A. Reinhardt, P. Mogre, and R. Steinmetz (2009). Wireless sensor networks and the Internet of Things: Selected challenges. Proceedings of the 8th Fachgespräch Drahtlose Sensornetze, Hamburg, Germany, p. 54–57.

[31] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci (2002). Wireless sensor networks: A survey. Computer Networks vol. 38, no. 4, p. 393–422.

[32] N. Kimura and S. Latifi (2005). A survey on data compression in wireless sensor networks. International Conference on Information Technology: Coding and Computing (ITCC) 2005, Las Vegas, NV, vol. 2, pp. 8–13.

[33] J. Blumenthal, M. Handy, F. Golatowski, M. Haase, and D. Timmermann (2003). Wireless sensor networks— New challenges in software engineering. Proceedings of IEEE Conference on Emerging Technologies and Factory Automation (ETFA) 2003, vol. 1, p. 551–556.

[34] R. Bhattacharya, C. Florkemeier, and S. Sarma (2009). Towards tag antenna based sensing—An RFID displacement sensor. Proceedings of 2009 International Conference on RFID, Orlando, FL, p. 95–102.

[35] G. Marrocco, C. Occhiuzzi, and F. Amato (2010). Sensor-oriented passive RFID, in The Internet of Things. Springer, Berlin, Germany, Part 4, p. 273–282.

[36] R. Bhattacharyya, C. Floerkemeier, S. Sarma, and D. Deavours (2011). RFID tag antenna based temperature sensing in the frequency domain. Proceedings of 2011 IEEE International Conference on RFID, Orlando, FL, p. 70–77.

[37] J. Gao, J. Siden, and H. E. Nilsson (2011). Printed electromagnetic coupler with an embedded moisture sensor for ordinary passive RFID tags. IEEE Electron Device Letters, vol. 32, no. 12, p. 1767–1769.

[38] K. Chang, Y. H. Kim, Y. J. Kim, and Y. J. Yoon (2007). Functional antenna integrated with relative humidity sensor using synthesized polyimide for passive RFID sensing. Electronics Letters, vol. 47, no. 5, p. 7–8.

[39] Khalil N, Abid M, Benhaddou, D and Gerndt, M (2016). Wireless Sensor Network for Internet of Things. cs.NI.

[40] D. Evans (2011). The internet of things: How the next evolution of the internet is changing everything.

[41] World population clock. (2013) Available: http://www.worldometers.info/world-population/

[42] European Commission, (2008). Internet of Things in 2020: Roadmap for the future, Technical report, Working Group RFID of the ETP EPOSS. Available at http://ec.europa.eu/informationsociety/policy/rfid/documents/iotprague2009.pdf (accessed on December 12, 2014).

[43] T. Lu and W. Neng, (2010). Future Internet: The Internet of Things, in 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, Sichuan Province, China, August 2010, vol. 5, pp. V5-376–V5-380. Available at http://dx.doi.org/10.1109/ICACTE.2010.5579543.

[44] P. Guillemin and P. Friess, (2009). Internet of Things strategic research roadmap, Technical report, Cluster of European Research Projects, September 2009. Available at

http://www.internet-of-things-research.eu/pdf/IoTCluster Strategic Research Agenda 2009.pdf (accessed December 25, 2014).

[45] D. Giusto, A. Iera, G. Morabito, and L. Atzori (2010). The Internet of Things, Springer, Berlin.

[46] National Intelligence Council, (2008). Disruptive civil technologies—Six technologies with potential impacts on US interests out to 2025, Conference Report CR 2008-07, National Intelligence Council, Washington, DC, April 2008, http://www.dni.gov/nic/NIC_home.html.

[47] R. van Kranenburg, E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, and M. Ratto, (2010). The Internet of Things. Proceedings of 1st Berlin Symposium of the Internet Society, Germany, p. 25–27.

[48] Iova, O, Picco, G, Istomin, T, and Kiraly, C (2016). RPL, the Routing Standard forthe Internet of Things . . . Or Is It? IEEE COMMUNICATIONS MAGAZINE.

[49] Wang, Z, Zhang, L, Zheng, Z, and Wang, J (2016). An Optimized RPL Protocol for Wireless Sensor Networks. IEEE.

[50] Hanane Lamaazi ; Nabil Benamar ; Muhammad Iqbal Imaduddin ; Antonio J. Jara (2016). Performance Assessment of the Routing Protocol for Low Power and Lossy Networks. IEEE.

[51] Elyengui, S, Bouhouchi, R and Ezzedine, T (2016). A comparative performance study of the routing protocols RPL, LOADng and LOADng-CTP with bidirectional traffic for AMI scenario. Cornell University Library.

[52] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT