Internet of Things Security: Layered classification of attacks and possible Countermeasures

La sécurité de l'Internet des objets : classification en couches des attaques et contre-mesures possibles

Otmane El Mouaatamid
SIME Lab, ENSIAS, Rabat, Morocco
otmane_elmouaatamid@um5.ac.ma

Mohammed Lahmer
SIME Lab, EST My Ismail University, Meknes, Morocco
mohammed.lahmer@gmail.com

Mostafa Belkasmi
SIME Lab, ENSIAS, Rabat, Morocco
m.belkasmi@um5s.net.ma

Résumé

L'internet des objets (IdO) est un domaine actif de recherche. Assurer la sécurité des données échangées figure parmi ses grands défis. Cet article propose une nouvelle classification des attaques selon les couches OSI et l'objectif de sécurité à atteindre afin de développer de nouvelles techniques et procédures pour lutter contre ces attaques.

Abstract

Internet of Things is undoubtedly a well-known research area. In fact, ensuring security of data exchange is among the great challenges of the Internet of things. In this paper, we endeavour to introduce a new classification of attacks in compliance with the OSI layers and the objective of security that we seek to attained in order to develop novel techniques and processes to fight against these attacks.

Mots-clés

Internet des Objets, WSN, RFID, Sécurité, Attaques, Contre-mesures.

Keywords

Internet of Things, WSN, RFID, Security, Attacks, Countermeasures.

1. Introduction

The term Internet of Things was first coined by (Ashton, 1999) which is a technological revolution that represents the future of computing and communications. Its development depends on a dynamic technical innovation in a number of important fields, from wireless sensors to the nanotechnology based architecture (Akyildiz *et al.*, 2002); (Awerbuch and Scheideler, 2004); (Chaczko *et al.*, 2015). Today, we find this kind of technology in a wide range of potential applications, including smart city, control actuation and maintenance of complex systems in industry field, health, and transport. The IoT touches every facet of our lives. Security and privacy are two of the most crucial challenges that IoT is facing (FTC Sta¬ Report, 2015). Since sensor networks are highly vulnerable against attacks (Deng *et al.*, 2005), it is very important to have some mechanisms that can protect the network, devices, and users from all kinds of attack. It must be certain that the system is protected from any kind of attacks.

RFID (Radio Frequency Identification) and WSN (Wireless Sensor Networks) are two technologies used by IoT. Combining both RFID and WSN is of paramount importance as they can add additional services to each other. For instance, the identification of location can be performed using the RFID, whereas, WSN can be used to sense the objects surrounding environment. Many applications can get benefits from the integration of these two technologies, such as healthcare system and food chain tracking. But this combination can lead to multiple vulnerabilities that can jeopardize the benefit of these two technologies. Thus, security of Internet of Things is of paramount importance. The existing works in the literature focus only on the RFID or WSN. For instance, (Mitrokotsa *et al.*, 2010) give a classification of attacks for only RFID systems. Indeed, their classification is based only on the OSI layers whereas in our classification we classify the attacks based on both the security goals and attacks targeting each OSI layer. The authors (Sadeghi *et al.*, 2012) focus only on attacks that target the network layer in WSN.

In this paper, our contribution consists of classifying both WSN and RFID attacks and suggesting some countermeasures for these attacks. Our classification is based on both security requirements such as privacy, confidentiality, non-repudiation and the threats which seek a specific OSI layer. To the best of our knowledge, none of the existing papers address the attacks and countermeasures of both WSN and RFID according to the goal of security and the OSI layer. They tackle only one of them and they focus on attacks more than giving a detailed description of possible solutions.

The remainder of this paper is organized as follows. In the first section, we present an overview about Internet of things and their technologies, application areas, architecture and standardization. In the second section, we present features and goals of security for IoT. In the third section, we classify some WSN and RFID based on IoT attacks into three categories : Denial of service (DoS), Privacy, and Impersonation. Some attacks target both WSN and RFID. The last section suggests countermeasures for these attacks.

2. Internet of Things and Security

The CERP-IoT (Cluster of European Research projects on the Internet of Things) defines the Internet of things, such as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network (Sundmaeker *et al.*, 2010). This vision of the IoT will introduce a new dimension to the information and communication technologies. In addition to the two temporal and spatial dimensions that allow people to connect from anywhere at any time, we will have a new "object" dimension that will allow them to connect to anything. The IoT will cover a wide range of applications and almost touch all areas that we face every day. This will allow the emergence of smart spaces around a ubiquitous computing. These smart spaces include: cities, energy, transport, health, industry, and agriculture, etc. (Mitchell *et al.*, 2013).

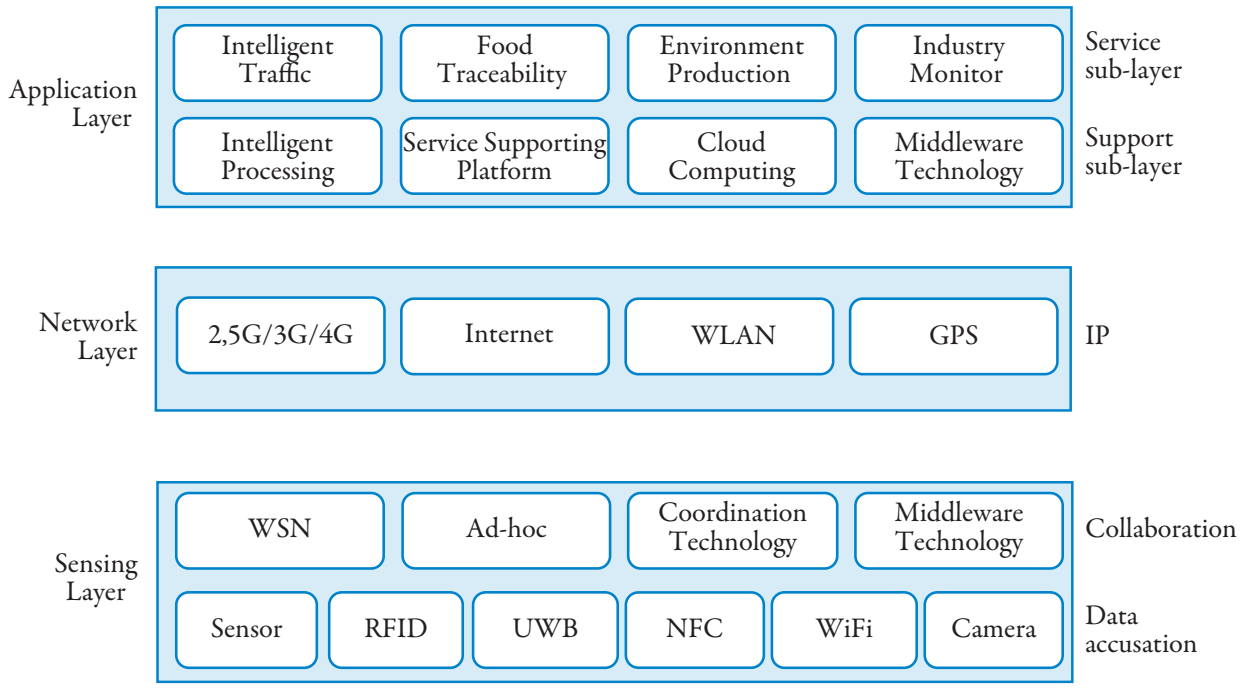

Figure 1. The IoT architecture model.

2.1. IoT Architecture

The IoT is characterized by a comprehensive perception, a reliable transmission and intelligent processing. Figure.1 shows the three-layer architecture of IoT : applications, network and sensing layer. The sensing realizes a comprehensive perception by collecting real-time dynamic data through various sensors (including tags) while the network layer is mainly responsible for the reliable data transmission, relaying data acquired from the sensing layer to the application layer. Using distributed computing technologies, including cloud computing, the application layer performs massive data processing and intelligent analysis for the purpose of intelligent control (Zheng *et al.*, 2011).

2.1.1. Internet of Things : Business scenarios

IoT systems are affecting all matters of our everyday life (Mitchell *et al.*, 2013). In fact, The IoT is making the whole world one place where everyone is interacting with one another. An example for such interaction is the physical entities that could exist in many different social environments (work, family, individual, leisure, etc.), which make determine clear boundaries difficult as shown in figure 2.

In order to show the impact of IoT, we present, thereafter, some scenarios where IoT technologies have a special relevance, taking into account that these scenarios frequently share the same applications, sensors, devices, and most certainly, users. These scenarios have been provided by the Internet of things Architecture (IoT-A) (Walewski *et al.*, 2011).

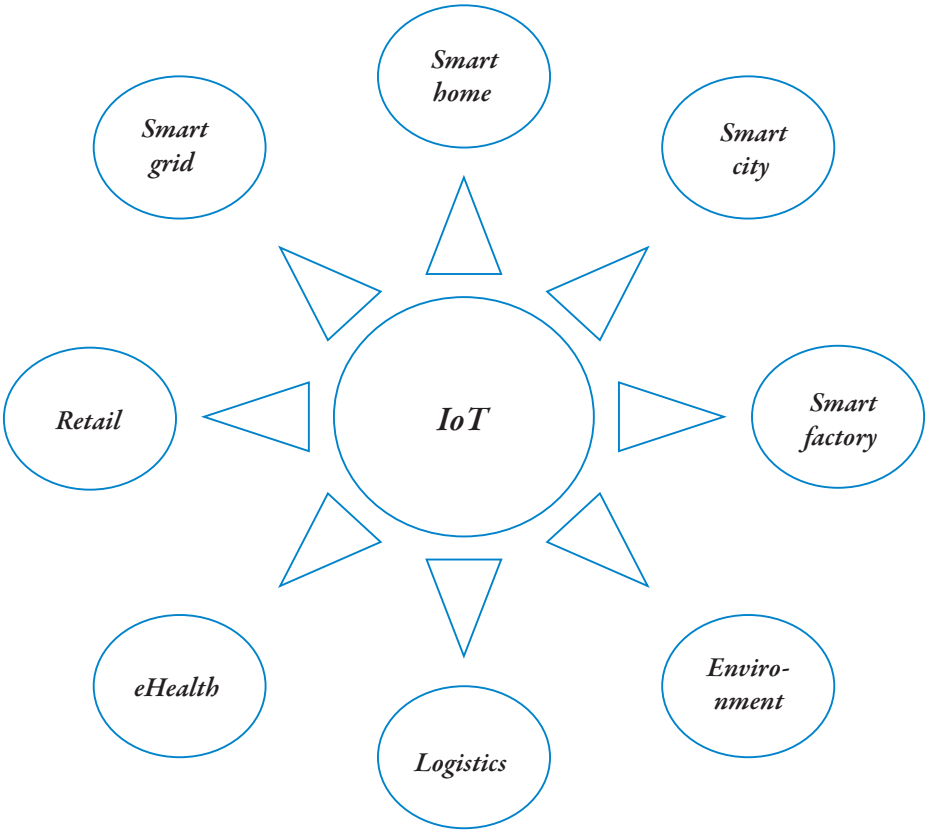

Figure 2. IoT business solutions

Smart home: Future smart homes will be conscious about what happens inside a building, mainly impacting three aspects: resource usage (water conservation and energy consumption), security, and comfort. The goal with all these is to achieve better levels of comfort while cutting overall expenditure. Moreover, smart homes address security issues by means of complex security systems to detect theft, fire, or unauthorized entries. The stakeholders involved in this scenario constitute a very heterogeneous group. There are different actors that will cooperate in the user's home, such as Internet companies, device manufacturers, telecommunications operators, media service providers, security companies, electric-utility companies, etc.

Smart city: A smart city can be defined as an urban community within which citizens, organizations and governing institutions deploy ICT to transform their locality in a significant way (Deakin, 2013). A smart city enables to implement a management infrastructure (water, energy, information and telecommunication, transport,

emergency services, public facilities, buildings, management and sorting waste, etc.). Likewise, a smart city is communicating, adaptable, sustainable, effective, eco-friendly, and ultimately automated to improve the quality of life of citizens.

Smart factory: The IoT is integrated into the objects of every day. It is the trend that is going to expand in the future. In this context, the IoT will allow companies to track all their products by means of RFID tags as they move through the global supply chain. As a result, companies will be able to reduce their Operational Expenditure (OPEX) and enhance their productivity. Hence, IoT will allow to automate procedures. As a consequence, the number of employees will be reduced. Workers will be replaced by complex robots, as efficient as humans. At the same time, these technologies will create new job opportunities for a big number of technicians to program and repair these machines.

Smart grids: Smart grids are fluid distribution materials networks (electricity, water, gas, oil ...) and / or information (telecommunications) that have been "augmented" (rendered intelligent) by computer systems, sensors, computer and electromechanical interfaces giving them a two-way exchange capacity and sometimes some capacity for autonomy in computing and materials flow management and information processing.

Environment: Smart environments are environments where sensors and actuators are integrated to react to events and to adapt to those present. For example, a smart home can adjust the temperature and lighting based on health, mood, and preferences of people and animals inside each piece.

Transportation/ Logistics: Intelligent Transportation Systems (ITS) are the applications of new information and communications technology in transport. They are called "intelligent" because their development is based on the functions usually associated with intelligence sensory, memory, communication, information processing and adaptive behavior. ITS are found in several areas of activity, such as in optimizing the use of transport infrastructure, in improving safety (including road safety) and security and in the development of services.

eHealth: Control and prevention are two of the main objectives of the future health care. Today, people already can have the opportunity to be followed and monitored by specialists, even if the two are not in the same location. Tracing people's health history is another aspect that makes IoT-assisted Health very versatile. Business applications could offer the possibility of a medical service, not only for patients, but also specialists who need information to perform their medical evaluation. In this field, IoT makes human interaction much more effective because doesn't only allow the localization, but also tracking and monitoring of patients. Providing information on the State of a patient makes the process more efficient, and also make people much more satisfied

Retail: IoT realizes the needs of customers and the needs of businesses. The comparison of a product price, or searching other products of the same quality at lower prices or shop promotions gives not only information to customers, but also businesses and affairs. Having this information in real time helps companies to improve their business and meet the needs of customers.

IoT is based on several technologies such as RFID, Near Field Communication (NFC), Sensors and Actuators Wireless Network (WSN), Machine-to-Machine communications (M2M), 3G/4G, IPv6 and 6LoWPAN. All of them play an important role in the development of IoT. In the remainder of our study we will be limited to RFID and WSN (Clauberg, 2004).

2.1.2. Wireless Sensor Networks (WSN)

WSN are structures of independent nodes whose wireless communication takes place over limited bandwidth and frequency. The nodes of wireless sensor networks are made up of following parts, such as Sensor, Microcontroller, Battery, radio Transceiver and Memory. Because of the limited communication range of each WSN sensor node, multi hop relay of information takes place between the source and the base station. The communication networks are dynamically formed by the use of wireless radio transceivers that facilitates data transmission between nodes.

2.1.3. Radio Frequency Identification (RFID)

In situation to the IoT, RFID is a method for storing and retrieving data remotely using markers called (RFID tag) or (RFID transponder). RFID system activated by a transfer of electromagnetic energy consists of the following two components: RFID tags and RFID readers.

RFID tags (Transponders): Radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. The RFID tag is also made up of memory units, which houses a unique identifier known as Electronic Product Code (EPC). As described in [14], the classification of the RFID tags types are active and passive :

- ***Active tag***: An active tag has an on-board battery and periodically transmits its ID signal.
- ***Passive tag***: A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader.

RFID readers (Transceivers): A radio frequency identification reader (RFID reader) is a device used to gather information from a RFID tag, which is used to track individual objects (Zharinov *et al.*, 2014).

2.2. The Security Features

As wireless networks become ubiquitous and their security becomes an important design of a secure solution that should meet some basic and significant requirements. We primarily focus on security requirements, and then we address the main security issues in order to ensure the deployment of a secure IoT.

2.2.1. Security concepts

The term security subsumes a wide range of different concepts (Borgohain *et al.*, 2015); (Garcia-Morchon *et al.*, 2013); (Veríssimo and Rodrigues, 2001). In the first place, it refers to the basic provision of security services including:

- ***Authentication***: The process of determining whether someone or something is, in fact, who or what it is declared to be. We distinguish two kind of attacks related to authentication namely, impersonation attack where an attacker pretends to be another entity, and Sybil attack where the attacker uses different identities at the same time.
- ***Authorization***: The process of giving someone permission to do or have something.
- ***Integrity***: Set of means and techniques to restrict the modification of data to authorized persons. Attacks related to data integrity are message alteration attack and message fabrication attack.
- ***Confidentiality***: Concept to ensure that information can only be read by authorized persons. Attacks on confidentiality consist of accessing illegally to confidential data.
- ***Non-repudiation***: Set of means and techniques to prove the involvement of an entity in a data exchange. Attacks on non-repudiation consist of a denial of participation in all or part of communications.
- ***Availability***: the objective is to guarantee the survivability of network services against Denial-of-Service attacks. The attack aiming at an aggregator can make some part of the network losses its availability because the aggregator is responsible to provide the measurement of that network part.
- ***Privacy***: The objective of this security requirement is to prevent private information from being leaked to malicious entities. Attacks on privacy are related to illegally gathering sensitive information about entities (e.g., eavesdropping).

2.2.2. Security concerns in IoT

Privacy for IoT: As much of the information in an IoT system may be personal data, there is a requirement to support anonymity and restrictive handling of personal information.
There are a number of areas where advances are required (Weber, 2010); (Mattern and Floerkemeier, 2010).

- Cryptographic techniques that enable protected data to be stored, processed and shared, without the information content being accessible to other parties.
- Techniques to support Privacy by Design concepts, including data minimization, identification, authentication and anonymity.

And there are a number of privacy implications arising from the ubiquity and pervasiveness of IoT devices where further research is required, including:

- Preserving location privacy, where location can be inferred from things associated with people.
- Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT related exchanges.
- Keeping information as local as possible using decentralized computing and key management.

3. Classification of Attacks on IoT

3.1. Types of attacks

We can classify generally five types of security attacks, namely Physical attacks, Side channel attacks, Cryptanalysis attacks, Software attacks and Network Attacks (Babar *et al.*, 2011).

Physical attacks: These types of attacks tamper with the hardware components and are relatively harder to perform because they requires an expensive material. Some examples are de-packaging of chip, layout reconstruction, micro-probing, particle beam techniques, etc.

Side channel attacks: These attacks are based on a side channel Information that can be retrieved from the encryption device that is neither the plaintext to be encrypted nor the cipher text resulting from the encryption process. Encryption devices produce timing information that is easily measurable, radiation of various sorts, power consumption statistics, and more. Side channel attacks makes use of some or all of this information to recover the key the device is using. It is based on the fact that logic operations have physical characteristics that

depend on the input data. Examples of side channel attacks are timing attacks, power analysis attacks, fault analysis attacks, electromagnetic attacks and environmental attacks.

Cryptanalysis attacks: These attacks are focused on the ciphertext and they try to break the encryption, i.e. find the encryption key to obtain the plaintext. Examples of cryptanalysis attacks include ciphertext only attack, known-plaintext attack, chosen-plaintext attack, man-in-the-middle attack, etc.

Software attacks: Software attacks are the major source of security vulnerabilities in any system. Software attacks exploit implementation vulnerabilities in the system through its own communication interface. This kind of attack includes exploiting buffer overflows and using Trojan horse programs, worms or viruses to deliberately inject malicious code into the system. Jamming attack is the one of the ruinous invasion which blocks the channel by introducing larger amount of noise packets in a network. Jamming is the biggest threat to IoT where a network consists of small nodes with limited energy and computing resources. So it is very difficult to adopt the conventional anti jamming methods to implement over IoT technologies.

Network Attacks: Wireless communications systems are vulnerable to network security attacks due to the broadcast nature of the transmission medium. Basically attacks are classified as active and passive attacks. Examples of passive attacks include monitor and eavesdropping, Traffic analysis, camouflage adversaries, etc. Examples of active attacks include denial of service attacks, node subversion, node malfunction, node capture, node outage, message corruption, false node, and routing attacks, etc.

3.2. Classification of attacks on WSN and RFID

In this section, we classify attacks of WSN and RFID based on the layer that each attack is taking place, giving special characteristics (Figure 3 and 4). We discriminate attacks that are deployed in the physical-link layer, the network-transport layer and the application layer, as well as multilayer attacks, which affect more than one layer and in the last we suggest new classification in which, attacks are sorted based on the target of the attacker. For example, many attacks are designed for destroying the signal while some others are targeting the privacy issues. Based on this view, we classify attacks in three main categories: Denial of Service (DoS), Privacy, and Impersonation as shown in (Table 1).

3.2.1. Layered classification of attacks on the WSN

As summarized in Figure 3 and mentioned in the previous paragraph, there are several varieties of possible attacks in WSN that we have classified depending on which layer the attack happens.

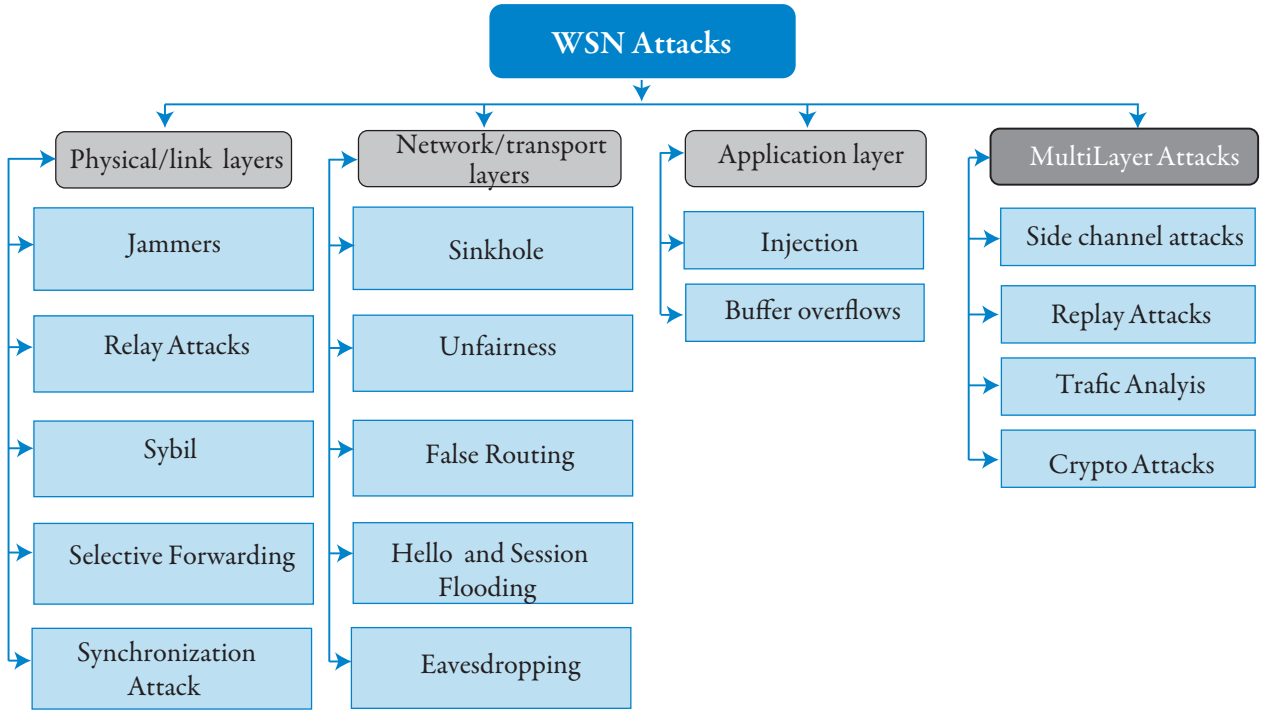

Figure 3. Layered classification of WSN attacks.

Hence, this classification has allowed us to easily locate each attack and then tackle the security issues according to the actions performed by the attacker. The attacker could be either an active attacker by performing an action that could jeopardize the benefit of the WSN, or a passive attacker whose objective is to eavesdrop the network. In this context, numerous techniques and tools have been developed to deal with WSN security attacks. The most existing attacks and vulnerabilities in WSN will be detailed later, whereas, in the last section, we will suggest some countermeasures against these attacks (Karlof and Wagner, 2003).

3.2.2. *Layered classification of attacks on the RFID*

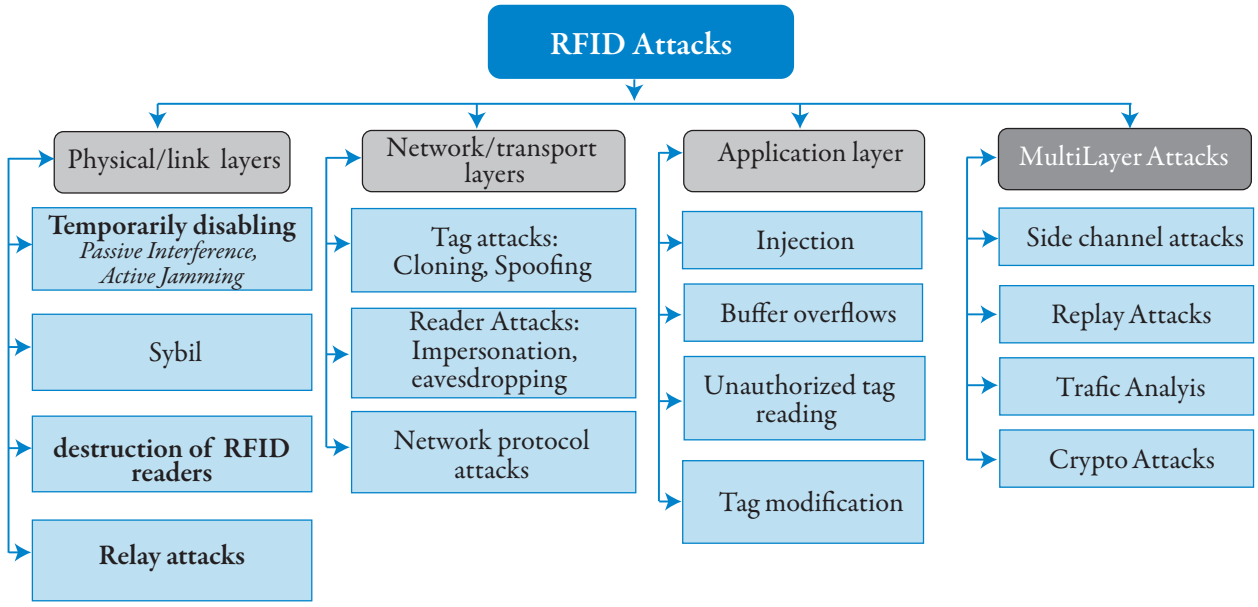

Figure 4. Layered classification of RFID attacks.

Despite the facilities it offers, the wireless medium used in RFID network has some drawbacks that leave it vulnerable to different types of attacks that target this type of transmission medium. We classified these attacks based on the layer where each attack could be performed. The Figure 4 represents a classification of RFID network attacks. As mentioned above, we discriminate attacks that could be deployed to physical layer, network-transport layer and the application layer, as well as multilayer attacks, which affect more than one layer. According to the functionalities and features of each layer, an attacker chooses a specific attack to carry out. Among these attacks we point out the relay attacks, destruction of RFID readers, Sybil attack and the temporarily disabling passive interference, active jamming… as security risks that could be faced on the physical/link layer. Regarding the threats associated to the network/transport layer we find the tag attacks such as cloning and spoofing, the reader attacks like impersonation, eavesdropping and the network protocol attacks. As to application layer several attacks can be considered such as injection, buffer overflows, unauthorized tag reading (Rieback *et al.*, 2006).

3.2.3. *Goal based Classification of WSN and RFID*

We can classify generally three types of security requirements in WSN and RFID according to the Goal (Table 1).

3.2.4. *Denial of Service (DoS)*

As mentioned in Table 1, there are four different ways of denying a service in the WSNs and RFID systems. There is a group of attacks called Jammers which try to reshape signal or change few bits of the packet by making interferences during communication. There is a group of attacks called network congestion which try to make network congested. There is a group of attacks called packet dropping, the goal of these attacks is dropping or discarding the packets, and there are attacks called network consumption, these attacks are specifically designed for draining the nodes energy (Ghildiyal et al, 2014)

		Technologies / Attacks	WSN	RFID
Denial of Service	*Jammers*	Physical Layer Jammers	✓	
		Link Layer Jamming	✓	
	Network Congestion	Unfairness	✓	
		Spoofing	✓	
		Wormhole	✓	✓
		Unauthorized Tag Reading		
		Sinkhole	✓	
		False Routing	✓	
		Unauthorizedtag reading		✓
	Packet Dropping	Selective Forwarding	✓	
		Synchronization	✓	✓
	Energy Consumption	Hello Packet And Session Flooding	✓	
Privacy	*Data oriented*	Eavesdropping	✓	✓
		Skimming		✓
		Substitution		✓
		Clonage		✓
		Replay	✓	✓
	Context oriented	Traffic Analysis	✓	✓
		Tempering Attacks	✓	✓
		Tag modification		✓
Impersonation	*Physical node*	Physical Layer Identification	✓	✓
		Spoofing	✓	
	Virtual node	Sybil	✓	✓

Table 1. Goal based classification of WSN and RFID

Jammers

Jammers are one of the oldest and famous attacks in WSN. Jamming can happen in the deferent OSI layers. Note that jamming in each layer means targeting the specific packets related to that layer, e.g. ACK packets in layer two.

Physical Layer Jammers: The main target of these attacks is radio signal which is jammed with Radio Frequency (RF) transmitter. Because in RFID system the communication media is shared between the Tags /Reader and in WSN the communication is shared between the nodes, adversaries have a great chance to interfere and deny the service. There are three techniques for physical layer jamming (Xu et al, 2006), (Constant Jamming) where attacker sends nonstop random bits, (Deceptive Jamming) whose main target is to send continuous stream of regular packets. Attacker can also send the jamming signal in a random periodic format to save the energy of the jamming device (Random jamming). All The three techniques mentioned above are considered as active jamming, because, the jammer can be detected.

Link Layer Jamming: Link layer jammers are complicated and energy inefficient compared to physical layer jammers. The target of this attack is data packets whereas in physical layer the target is just any packet. As described by (Law et al, 2005) this attack in link layer is harder to detect. Note that, the link layer jamming might also focus on the controlling signal such as ACK message. These specific jammers are called collision makers. Link layer jammer tries to jam the data packets. Since different types of MAC protocol exist, the jammer should jam based on the type of the MAC protocol in WSN. The challenge for link layer jamming is in predicting the arrival of the data packets. Jamming for different MAC protocols has been proposed by (Law et al, 2005). This attack is known in WSN environment but in RFID system we just talk about an active jammer in physical layer.

Network Congestion

The main objective of this group attacks is to create the delay in delivering the data. These groups of attacks include all the attacks that are based on the way RFID systems and WSN are communicating and the way those data are transferred between the entities of an RFID network (tags, readers) or between nodes of a WSN. These attacks pose a major threat to networks in which the data freshness is playing an important role. Below, we review the main congestion makers.

Unfairness: unfairness is a repeated collision based on attack. It can also be referred to as exhaustion based attacks by (Ghildiyal et al, 2014). This type of attacks is famous in WSN, but unknown on the RFID system.

Wormhole: The wormhole attack is independent of Link layer protocols as it is considered dangerous and the attacker do not need to understand the link layer Protocol or be able to decode encrypted packets. Wormhole could be performed at the bits level or at the physical layer. Wormhole is a low latency connection (tunneling) between two adversary nodes, geographically located in different parts of WSN (Tayebi et al, 2013).

Sinkhole: It is a special kind of the group network congestion attacks (Tayebi et al, 2013). A compromised node tries to draw all or as much traffic as possible from a particular array, by giving itself more attraction to the surrounding nodes with respect to the routing metric.

False Routing: The main objective of this attack is that the adversary node tries to make and propagate false routing information. There are different ways to perform this attack. This attack is famous in network layer as described (Ghildiyal et al, 2014) there are four ways to implement this attack: Overflowing routing table with Nonexistence routes, poisoning either routing table or routing cache (this way only applicable for on-demand routing protocols), and finally rushing attack.

Dropping

The goal of this attack is dropping or discarding the packet, the attacker can use two ways (packet forwarding) or (De-synchronization).

Selective Forwarding: The goal of this attack is to select some packets, forward it and drop the rest of this packet. There is another type of this attack, the attacker can drop all the packets and do not forward any of them. This type is called BlackHole.

Synchronization Attack: In this study, we classified attacks based on the OSI Model layers, these attacks can be used for link layer and transport layer of OSI model. The technique of Synchronization attacks for Listen-Sleep Slotted MAC protocols has been suggested by (Lu et al, 2008). In this attack, the adversary node tries to extend its listening slot and propagates the extended listening slot to the other nodes.

Consumption

In WSN the problem of energy consumption is much known, all groups of DoS attacks make node to eat up its battery power.

Hello Packet and Session Flooding: Some routing protocols are using hello packets for establishing the neighborhood relationship or connection request. An adversary can constantly send a hello packet by using a high power radio transmitter. The nodes which receive the hello packet believe that the adversary node is their neighbor, even though the adversary node is located far away. Attacker can also send the session request to the victim nodes until they get exhausted or they reach their limit for maximum number of connections.

3.2.5. Privacy Attacks

The main goal of Privacy attacks is finding the information about devices or about persons. The privacy attacks are considered dangerous and they are classified into two groups, Data oriented and Context oriented, because the attackers are only interested in the information (Li et al, 2009).

Data oriented

Eavesdropping: The eavesdropping is a potentially dangerous attack because it allows an attacker to retrieve such confidential information exchanged between a reader and a card measuring the RF field emitted by the reader. Its development and implementation are quite simple since antenna connected to an oscilloscope can be used

to collect the exchanged binary data (Thevenon *et al.*, 2011). While the communication distance between a reader and a card is close to ten centimeters, a spy is able to recover the signal sent by a player over 20 meters (200 times the operating distance).

Substitution, clonage, and replay attack: The three attacks are grouped in the same group as their main characteristics are the same. All these attacks require data recovery on another card without contact. These attacks are often preceded by an eavesdropping attack or skimming attack which allows the attacker to retrieve the data stored in the memory of a transponder. This data can then be recorded onto a blank transponder to get a copy of the card previously attacked. Writing data on a blank card is quite simple since we can find on the internet all the equipment used to program any card, using a microprocessor.

Context oriented

Traffic Analysis: The attacker listens to the packets and tries to find the sensed data or ask to be sent. For example, in health application, an attacker may try to access the patient's confidential medical information.

Tempering Attacks: As described by (Sharifi *et al.*, 2013) the tampering attacks are well surveyed and classified into three difficult levels called easy, medium, and hard. The higher the difficulty level is, the most accessed and controlled over the victim hardware component. On the other hand, the easier attacks need less facility.

Tag modification: The most RFID tags use a writable memory. As a consequence, modifying or deleting valuable information could be performed easily by an attacker and it depends on the used standard and the READ/WRITE protection employed.

3.2.6. Impersonation

The last group is impersonation attack; the attackers want to impersonate themselves either as a physical node or a number of virtual nodes. This type of attacks might not sound very harmful for WSN, but destructive for RFID system and can be combined with DoS attacks and make them more destructive.

Physical Layer Identification: The main goal of the attacker is to impersonate a target device by generating packets or signals that contain factors which are sensitive to the fingerprint device. Therefore, the attacker can impersonate himself as one of targeted devices. This attack is used to detect the wireless devices in a network. It is based on the distinctive physical layer characteristics of a single device which are mainly due to manufacturing imperfection. The attacker uses two main techniques for device identifications. Transient based technique which is based on the unique features during the transient phase when radio is turning On (Danev and Capkun, 2009). The other technique is Modulation based techniques in which, modulation imperfection of wireless transceivers is the focusing point (Zeng *et al.*, 2010).

Sybil: In Sybil attacks, the attacker makes multiple identities and replicates a single node. These identities could be fabricated or stolen identities. Fabricated identities are fake identities which are randomly generated by the attacker. For example, if a node ID is represented by 32 bits, an attacker can randomly create 32 bits identities. In some networks where new nodes are not allowed to join, the attacker can steal the identities of legitimate nodes and use them for Sybil attack (Newsome *et al.*, 2004).

4. Common attacks countermeasures

This section is an overview of existing countermeasures to enhance security of IoT communication technologies. We identified countermeasures for WSN/RFID combined attacks based on different OSI layers, as shown in Table 2.

Attacks	Countermeasures
Jamming	Regulated transmitted power, Direct-Sequence Spread Spectrum, Direct-Sequence Spread Spectrum, and Hybrid FHSS/DSSS.
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use packet leach techniques.
Replay	Timestamps, one-time passwords, and challenge response cryptography
Traffic Analysis	Sending of dummy packet in quite hours: and regular monitoring WSN network
Eavesdropping	Session Keys protect NPDU from Eavesdropper
Sybil	Trusted Certification, Resource Testing, Recurring Fees, Privilege Attenuation, Economic Incentives, Location/Position Verification, Received Signal Strength Indicator (RSSI)–based scheme and Random Key Predistribution.

Table 2. Common attacks and countermeasures

4.1. Countermeasure against Jamming

4.1.1. Regulated transmitted power

By using low transmitted power, the discovery probability from an attacker decreases (an attacker must locate first the target before transmitting jamming signal). Higher transmitted power implies higher resistance against jamming because a stronger jamming signal is needed to overcome the original signal (Zhang and Kitsos, 2009).

4.1.2. Frequency-Hopping Spread Spectrum

Frequency hopping spread spectrum (FHSS) is a way of transmitting radio signals by fast switching a carrier amid many frequency channels, benefitting from the use of a shared algorithm known both to the transmitter and the receiver. FHSS brings forward many advantages in WSN and RFID systems, e.g (Mpitziopoulos and Gavalas, 2009).

- It reduces unauthorized interception and jamming of radio transmission between Tag and Reader in RFID and the nodes in WSN.
- It deals effectually with the multipath effect. One of the main drawbacks of frequency-hopping is that the overall bandwidth required is much wider than that required to transmit the same data using a single carrier frequency. However, transmission in each frequency lasts for a very limited period of time so the frequency is not occupied for long.

4.1.3. Direct-Sequence Spread Spectrum

Direct-Sequence Spread Spectrum (DSSS) transmissions are performed by multiplying the data (RF carrier) being transmitted and a pseudo-noise (PN) digital signal. This PN digital signal is a pseudorandom sequence of one and one values, at a frequency (chip rate) much higher than that of the original signal. This process causes the RF signal to be replaced with a very wide bandwidth signal with the spectral equivalent of a noise signal; however, this noise can be filtered out at the receiving end to recover the original data, through multiplying the incoming RF signal with the same PN modulated carrier. The first three of the above-mentioned FHSS advantages also apply into DSSS. Furthermore, the processing applied to the original signal by DSSS makes it difficult to the attacker to descramble the transmitted RF carrier and recover the original signal (Fang *et al.*, 2016).

4.1.4. Hybrid FHSS/DSSS

In WSN the Hybrid FHSS/DSSS communication between nodes represents the hoped anti-jamming measure. In general terms, direct-sequence systems achieve their processing gains through interference attenuation using a wider bandwidth for signal transmission, while FHSS through interference avoidance. Thus Hybrid FHSS/DSSS develop the solidity to combat the near/far problem, which arises in DSSS communications schemes. Another welcome feature is the capability to adapt to a diversity of channel problems (Mpitziopoulos and Gavalas, 2009).

4.2. Wormhole Countermeasure

A wormhole attack is considered dangerous as it is independent of MAC layer protocols and immune to cryptographic techniques. Strictly speaking, the attacker does not need to understand the MAC protocol or be able to decode encrypted packets to be able to replay them. Different papers in literature have developed countermeasures for wormhole attacks. The authors (Maheshwari et al, 2007) discussed them in two approaches. The first one is related to that Bound Distance or Time, and the second is based in graph theoretic and geometric.

4.3. Replay Countermeasure

In order to defend against replay attacks some simple countermeasures exist such as the use of timestamps, one-time passwords and challenge response cryptography. Nevertheless, these schemes are inconvenient and with doubtful efficiency considering the vulnerabilities to which challenge response protocols are susceptible to. Another approach is the use of RF shielding on readers in order to limit the directionality of radio signals and subsequently the appearance of a ghost. Another approach is based on the distance between the information requestor and the information owner. Implied that the signal-to-noise ratio of the reader signal in an RFID system can reveal even roughly the distance between a reader and a tag. This information could definitely be used in order to make a discrimination between authorized and unauthorized readers or tags and subsequently mitigate replay attacks (Mitrokotsa *et al.*, 2010).

4.4. Traffic Analysis Countermeasure

The way to defend against traffic analysis is to control the packet sending rate of every node in the network in such a way that every node sends packets with the same rate (Deng *et al.*, 2006). There is another way to defend traffic analysis is to ensure that the external appearance of a packet changes as it moves forward through a multi-hop sensor network. To do this, a cluster key is established among each set of neighboring nodes. The packet destination address, packet type, and packet contents are encrypted by a node, using its cluster key (Deng *et al.*, 2006). As a packet moves forward, each node first decrypts the packet and then re-encrypts it, using the cluster key. The current senders address remains in plaintext so that the receiver can choose the correct cluster key to decrypt the packet.

4.5. Countermeasure against Eavesdropping

Communications between WSN nodes and RFID (Tags and Readers) are vulnerable to the eavesdropping because very few nodes and passive tags are using the cryptographic protections. However, due to the short reading range of passive tags (Zhang and Kitsos, 2009), the eavesdroppers need to be the physical proximity of RFID tags, which is a sporadic activity. In order to protect against eavesdropping, data cryptography can prevent these security issues. Presently, sensor networks are supplied exclusively through symmetric key cryptography. The entire network is under risk if only one of its nodes has to be compromised by using symmetric cryptography. It means that the shared secret among those nodes is exposed. Another approach is to use a shared key between two nodes in the whole network. Then, it removes the network wide key. The disadvantage is additional nodes which cannot be added after the deployment process. In a sensor network with n nodes, each node needs to store (n-1) keys.

4.6. Countermeasure against Sybil attacks

There are different methods proposed against Sybil attacks but still there is no general solution to the Sybil attack. A number of approaches for various combinations of environments and attacks have been proposed (Levine *et al.*, 2006).
The most prominent techniques to resist Sybil attacks are as under.

- ***Trusted Certification***: is by far the very often cited solution to subdual Sybil attacks. It involves the presence of a trusted Certifying Authority (CA) that validates the one is to one correspondence between nodes on the network and its associated identity.
- ***Resource Testing***: is the most habitually implemented solution against Sybil attacks, despite it is ineffective for most systems.
- ***Recurring Fees*** or ***(Recurring Costs)*** is a variation method of resource examining where resource tests are conducted after certain specific time intervals to impose a specific "cost" on the attacker that is incurred for every identity that he controls. Using recurring costs or fees per identity is more effective to inhibit Sybil attacks than a one-time resource test.
- ***Privilege Attenuation***: is a technique to mitigate Sybil attack limited to Social Network System (SNS) as an application domain, this technique frequently used in (SNS) despite its disadvantages is only applied to monotonic policies. Significant run-time and storage overhead for generalized extensions of the idea (Fong, 2011) .
- ***Economic Incentives***: is a general technique used to mitigate Sybil attack, but this method is not efficient because it may encourage Sybil attackers that have no interest in subverting the application protocols, but that are interested in being paid to reveal their presence (Margolin and Levine, 2007).
- ***Location/Position Verification***: this technique is only limited to ad hoc networks. Methods employing this technique make use of the fact that any identities that are projected by any single physical device must be in the same location. Locations are verified using specific methods such as triangulation (Tangpong, 2010). So for an attacker with a single physical device, all Sybil identities will be in the same place or will appear to move together
- ***Received Signal Strength Indicator (RSSI)–based scheme***: is a technique used to mitigate Sybil attack. It does not deal with existing Sybil nodes in the network, Location calculations are costly. It is limited to Sensor Networks (Balachandran and Sanyal, 2012) .
- ***Random Key Redistribution***: is a technique limited in wireless sensor network but we can use it in other systems like RFID (Newsome *et al.*, 2004).

5. Conclusion

The Internet of things technologies are exposed to different types of attacks. An attacker can attack for different objectives. Attacks are categorized based on attacking goals and different OSI layers. In this paper, the most important attacks on WSN and RFID are identified, discussed, and presented in a systematic form to allow their comparison and trace the future research activities in this field. The use of conventional cryptography in the Internet of things is limited or even impossible. For that, our research will be oriented towards alternative solutions less costly and complex, including the use of codes in Cryptography. As known, the performance of an algorithm in IoT is of paramount importance. To this end, code based cryptography is most suitable for IoT as it has a very fast and efficient encryption procedure (Persichetti, 2012). In addition, there are no known vulnerabilities on this solution so it should be more secure even against quantum computer.

6. References

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). *A survey on sensor networks*. IEEE communications magazine, 40(8), 102-114.

Ashton, K. (2009). *That 'internet of things' thing*. RFiD Journal, 22(7), 97-114.

Awerbuch, B., & Scheideler, C. (2004). *Group spreading: A protocol for provably secure distributed name service*. In International Colloquium on Automata, Languages, and Programming . Springer Berlin Heidelberg. (pp. 183-195).

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). *Proposed embedded security framework for internet of things (iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, 2011 2nd International Conference on (pp. 1-5). IEEE.

Balachandran, N., & Sanyal, S. (2012). *A review of techniques to mitigate sybil attacks*. arXiv preprint arXiv:1207.2617.

Borgohain, T., Kumar, U., & Sanyal, S. (2015). *Survey of security and privacy issues of internet of things*. arXiv preprint arXiv:1501.02211.

Chaczko, Z., Jacak, W., & Łuba, T. (2015). *Computational Intelligence and Efficiency in Engineering Systems* (Vol. 595). G. Borowik (Ed.). Springer.

Clauberg, R. (2004). *RFID and sensor networks*. In Proc. RFID Workshop, St. Gallen, Switzerland (pp. 1-6).

Danev, B., & Capkun, S. (2009). Transient-based identification of wireless sensor nodes. In Proceedings of the 2009 International Conference on Information Processing in Sensor Networks (pp. 25-36). IEEE Computer Society.

Deakin, M. (2013). *Smart cities: governing, modelling and analysing the transition*. Routledge.

Deng, J., Han, R., & Mishra, S. (2005). *Countermeasures against traffic analysis attacks in wireless sensor networks.* In First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05) . IEEE. (pp. 113-126).

Deng, J., Han, R., & Mishra, S. (2006). *Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks*. Pervasive and Mobile Computing, 2(2), 159-186.

Fang, S., Liu, Y., & Ning, P. (2016). *Wireless communications under broadband reactive jamming attacks*. IEEE Transactions on Dependable and Secure Computing, 13(3), 394-408.

Fong, P. W. (2011). *Preventing Sybil attacks by privilege attenuation: A design principle for social network systems*. In 2011 IEEE Symposium on Security and Privacy (pp. 263-278). IEEE.

FTC Sta¬ Report. (2015). *Internet of things: Privacy & security in a connected world*. Washington, DC: Federal Trade Commission.

Garcia-Morchon, O., Kumar, S., Struik, R., Keoh, S., & Hummen, R. (2013). *Security Considerations in the IP-based Internet of Things*.

Ghildiyal, S., Mishra, A. K., Gupta, A., & Garg, N. (2014). *Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks*. IJRET: International Journal of Research in Engineering and Technology, 2319-1163.

Karlof, C., & Wagner, D. (2003). *Secure routing in wireless sensor networks: Attacks and countermeasures*. Ad hoc networks, 1(2), 293-315.

Law, Y. W., Hartel, P., den Hartog, J., & Havinga, P. (2005, January). *Link-layer jamming attacks on S-MAC*. In Wireless Sensor Networks, 2005. Proceeedings of the Second European Workshop on (pp. 217-225). IEEE.

Levine, B. N., Shields, C., & Margolin, N. B. (2006). *A survey of solutions to the sybil attack.* University of Massachusetts Amherst, Amherst, MA, 7.

Li, N., Zhang, N., Das, S. K., & Thuraisingham, B. (2009). *Privacy preservation in wireless sensor networks: A state-of-the-art survey.* Ad Hoc Networks, 7(8), 1501-1514.

Lu, X., Spear, M., Levitt, K., Matloff, N. S., & Wu, S. F. (2008). *A synchronization attack and defense in energy-efficient listen-sleep slotted MAC protocols.* In 2008 Second International Conference on Emerging Security

Information, Systems and Technologies (pp. 403-411). IEEE.
Maheshwari, R., Gao, J., & Das, S. R. (2007). *Detecting wormhole attacks in wireless networks using connectivity information*. In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications (pp. 107-115). IEEE.
Margolin, N. B., & Levine, B. N. (2007). *Informant: Detecting sybils using incentives.* In International Conference on Financial Cryptography and Data Security .Springer Berlin Heidelberg. (pp. 192-207).
Mattern, F., & Floerkemeier, C. (2010). *From the Internet of Computers to the Internet of Things.* In from active data management to event-based systems and more .Springer Berlin Heidelberg. (pp. 242-259).
Mitchell, S., Villa, N., Stewart-Weeks, M., & Lange, A. (2013). *The Internet of everything for cities: connecting people, process, data and things to improve the livability of cities and communities.*
Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). *Classification of RFID attacks.* Gen, 15693, 14443.
Mpitziopoulos, A., & Gavalas, D. (2009). *An effective defensive node against jamming attacks in sensor networks*. Security and Communication Networks,2(2), 145-163.
Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). *The sybil attack in sensor networks: analysis & defenses.* In Proceedings of the 3rd international symposium on Information processing in sensor networks (pp. 259-268). ACM.
Persichetti, E. (2012). *Improving the efficiency of code-based cryptography.* (Doctoral dissertation, Department of Mathematics, University of Auckland).
Rieback, M. R., Simpson, P. N., Crispo, B., & Tanenbaum, A. S. (2006). *RFID malware: Design principles and examples*. Pervasive and mobile computing, 2(4), 405-426.
Sharifi, A., Khosravi, M., & Shah, A. (2013). *Security Attacks and Solutions On Ubiquitous Computing Networks.* International Journal of Engineering and Innovative Technology (IJEIT), 3(4).
Sadeghi, M., Khosravi, F., Atefi, K., & Barati, M. (2012). *Security analysis of routing protocols in wireless sensor networks.* International Journal of Computer Science Issues, 9(1), 465-472.
Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). *Vision and challenges for realising the Internet of Things.* Cluster of European Research Projects on the Internet of Things, European Commision.
Tangpong, A. (2010). *Managing Sybil Identities in Distributed Networks.* (Doctoral dissertation, The Pennsylvania State University).
Tayebi, A., Berber, S., & Swain, A. (2013). *Wireless Sensor Network attacks: An overview and critical analysis.* In Sensing Technology (ICST), 2013 Seventh International Conference on (pp. 97-102). IEEE.
Thevenon, P. H., Savry, O., Malherbi-Martins, R., & Tedjini, S. (2011). *Attacks on the HF physical layer of contactless and RFID systems.* INTECH Open Access Publisher.
Veríssimo, P., & Rodrigues, L. (2001). *Fundamental security concepts.* InDistributed Systems for System Architects .Springer US. (pp. 377-393).
Walewski, J. W., Bauer, M., Bui, N., Giacomin, P., Gruschka, N., Haller, S., ... & Magerkurth, C. (2011). *Project Deliverable D1. 2–Initial Architectural Reference Model for IoT*.
Weber, R. H. (2010). *Internet of Things–New security and privacy challenges*. Computer law & security review, 26(1), 23-30.
Xu, W., Ma, K., Trappe, W., & Zhang, Y. (2006). *Jamming sensor networks: attack and defense strategies*. IEEE network, 20(3), 41-47.
Zeng, K., Govindan, K., & Mohapatra, P. (2010). *Non-cryptographic authentication and identification in wireless networks*. network security, 1, 3.
Zhang, Y., & Kitsos, P. (2009). *Security in RFID and sensor networks.* Auerbach Publications.
Zharinov, R., Trifonova, U., & Gorin, A. (2014). *Using RFID Techniques for a Universal Identification Device.* In Proceedings of the 13th Conference of Open Innovations Association FRUCT and 2nd Seminar on e-Tourism for Karelia and Oulu Region (pp. 244-248).
Zheng, L., Zhang, H., Han, W., Zhou, X., He, J., Zhang, Z., ... & Wang, J. (2011). *Technologies, applications, and governance in the internet of things.* Internet of Things-Global technological and societal trends. From smart environments and spaces to green ICT.