Security Challenges of the Internet of Things

Lisa Goeke

Bachelor's Thesis

Business Information

Technology

2017

Haaga-Helia
University of Applied Sciences

Abstract

May 18, 2017

Author(s) Lisa Goeke	
Degree programme Business Information Technology	
Report/thesis title Security Challenges of the Internet of Things	**Number of pages and appendix pages** 32

The ‘Internet of Things’ is the buzz phrase that describes a new era of computation. Briefly, the Internet of Things can be defined as the interaction of smart objects that are connected to the Internet.

These objects can sense, share and process information, upload them in the cloud, and make them available to the user via a large amount of different applications. Despite all of these promising innovations, the Internet of Things, as every other technology, faces multiple security challenges.

The objective of this paper is to give an overview of the Internet of Things, and to elaborate on all currently know security challenges the Internet of Things, as of today, is facing. All findings are based on the literature available for the key components of the Internet of Things.

This paper provides detailed insight into the key components of the Internet of Things, ranging from Radio Frequency Identification, over Near-Field Communication, to Wireless Sensor Networks.

Furthermore, the paper provides insight into the different fields of application these components are used by, and elaborates the security risks each component faces. All currently known countermeasures, that can protect the components of the Internet of Things from security attacks, and provide a secure version of the Internet of Things, are discussed in this work.

This paper evaluates the countermeasures available to protect each component of the Internet of Things from security risks. Information about security challenges still to be overcome, and countermeasures, not sufficient to protect the Internet of Things from attacks, are provided in the concluding chapter. Based on the current literature, this paper provides an answer to the question whether the Internet of Things as of today can already be considered secure.

Keywords
Internet of Things, Radio Frequency Identification, Near-Field Communication, Wireless Sensor Networks, Security

Table of contents

Abbreviations

ADC	Analogue to Digital Converter
DoS	Denial of Service
EPC	Electronic Product Code
IoT	Internet of Things
IPSO	IP for Smart Objects
MAC	Media Access Control
NFC	Near-Field Communication
PIN	Personal Identification Number
RFID	Radio Frequency IDentification
UID	Unique Identifier
WiFi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WSN	Wireless Sensor Networks

1 Introduction

The Internet of Things can be described as a network that consists of interconnected smart objects. These objects have the possibility of sensing their surroundings, and they can share and process information, which can be made available to different applications. (Gubbi, Buyya, Marusic, & Palaniswami 2013, 4).

The Internet of Things might introduce a completely new era of computation even though it is still in its earliest stage. How our daily life and lifestyle might change based on the technologies of the Internet of Things can't yet fully be imagined. Greengard (2015, 1) gives an insight into how different our day-to-day life could be when supported by the IoT:

Starting our day in the early morning our vibrating wristband could wake us up and provide detailed information about our sleeping pattern, available on an application on our smartphone. Another application can scan the barcodes on the packages of our foods and beverages when having breakfast to provide information about the nutritional content. When hitting the gym, with the help of a unique ID, we can gather information about the calories lost and how this affects our body weight or body fat content. The data is sent to the cloud and can be reviewed and analysed on an application on our smartphone. Although this might sound like fiction, Greengard describes this scenario as a realistic morning routine in his everyday life. (Greengard 2015, 1).

The scenario described involves a large number of interconnected devices, which make use of different technologies. Despite the IoT's promise of making our daily life easier and more efficient, every technology comes with security issues, which have to be overcome in order to use the technological innovation securely.

This paper is structured as follows. The first chapter will define the objective of this paper, provide the research questions, and define the scope of this work. The second chapter gives an overview of the Internet of Things including its current fields of application, the known risks as of today, and a definition from a technical point of view. The chapters three to five present the key components of the IoT. Every chapter will define the component, give examples on the usage within the IoT, and elaborate on the security issues and countermeasures currently available.

1.1 Thesis objectives

The objective of this paper is to give and overview of how secure the Internet of Things as of today is, and what security challenges have to be considered in order to deliver a basis for a solid and secure IoT. This paper will help to understand the components the IoT is built of, the way they work, and which risks each component faces. This approach leads to the following research questions:

- What are the security challenges of the IoT's key components ranging from Radio-Frequency Identification (RFID) over Near-Field Communication (NFC) to Wireless Sensor Networks (WSNs)?
- What are the currently known countermeasure for each component and how effective are they?
- Can the IoT as of today already be considered secure?

This paper will answer these research questions based on the currently available literature about the IoT.

1.2 Scope of the thesis

The paper will focus solely on the IoT's key components, Radio Frequency Identification, Near-Field Communication, and Wireless Sensor Networks. All components will be explained in detail, including information about their usage within the IoT as well as about their risks. The scope of this thesis includes all effective countermeasures to overcome the current security issues, which will be described for each component. Furthermore, the countermeasures and their effectiveness will be summarized and evaluated.

The outcomes and findings of this paper are based on the current literature available about the Internet of Things.

1.3 Out of scope

This paper focuses solely on the security challenge of the key components of the Internet of Things, and does not include any security challenges that affect the middleware of the IoT, which lays on the connectivity layer, acting as the bridge between the connected devices and the applications. Out of scope of this thesis is any security issue that can occur in any of the short-range communication feature, such as Bluetooth, ZigBee or WiFi. Due to the vast amount of applications that sit on the top layer of the IoT, this paper will not include any security challenges that affect IoT applications either. Any negative impacts, caused by the users of the IoT, are not part of this paper.

2 The Internet of Things

The Internet of Things - a buzz phrase used to describe the introduction of a new era of computing. But how can the IoT be defined? Taking a look at both components of the phrase, the Internet is a part of most people's everyday life. It provides means of communication, lets us interact and network using social media, provides applications and games to make our everyday life easier and more pleasant. Furthermore, it is getting accessible to a broader audience. (Miorandi, Sicari, De Pellegrini & Chlamtac 2012, 1497)

The other key word of the phrase *Internet of Things* describes smart objects that have the following characteristics.

- *Things* are entities that can be identified uniquely
- They can be defined by their physical nature in shape, size, etc.
- They can communicate by receiving and sending messages
- They can perform basic to complex computation
- They might be able to sense their environment (i.e. temperature, light)

(Miorandi, Sicari, De Pellegrini & Chlamtac 2012, 1497).

According to Gubbi et al (2013, 4) these *things* can interact with each other. They can gather information about their surroundings and communicate the information sensed to other objects, by the exchange of data streams. In addition to purely exchanging data, most of these smart objects can even react to events happening in the physical environment around them. These reactions can trigger actions that can be used by services available to human beings without them giving any input into the system. (Gubbi, Buyya, Marusic, & Palaniswami 2013, 4).

These *things* can reach from items that are part of our daily life such as smartphones, tablets or laptops to objects that are attached to items we use in our homes or vehicles, which can be connected to another device or the Internet.

The interconnectivity of *things* allows this new era of technology to move from the vision of the Internet to a more complex one. Instead of supporting connectivity at any-time, any-place and for every-one the Internet of Things makes a move from every-one towards every-thing. (Coetzee & Eksteen 2011, 2-3).

To support this change various new components have to be introduced. According to Atzori et al (2010, 3) Radio Frequency Identification (RFID) can be considered the driving

technology behind the IoT. RFID systems include a reading device and several RFID tags which can be attached to any objects around us. (Atzori, Iera & Morabito 2010, 3).
Other examples of RFID use are retail and supply chain management, in transportation as ticketing systems, or in bank cards and cargo (Gubbi, Buyya, Marusic, & Palaniswami 2013, 5). With the help of a reading device it is possible to extract the information stored in the tags (Atzori, Iera & Morabito 2010, 4).

Another key component of the IoT is the so-called Near-Field-Communication (NFC). This technology is used as an electronic support for RFID systems and has gained popularity in electronic payments. NFC eliminated the problems that occurred when using RFID systems on its own. Leading vendors, such as Walmart and Tesco, that took RFID into use to automate their retail had to face the technology's limitations. One major issue that occurred during those trials was, that other materials interfered with the tags when identifying them. NFC systems operate wireless and can be attached to any item. An example of NFC systems in today's time is Apple's iPhone 6, which comes with NFC and can be used with ApplePay. (Want, Schilit & Jenson 2015, 30)

The third component that plays a pivotal role in the IoT are sensor networks. These networks consist of a vast number of nodes which can sense their environment, communicate with each other, and report back to a base station. Compared to RFID systems, sensor networks do not need a reading device. They are used to monitor the environment as they can sense their surroundings, such as location, movement, or temperature, in military applications, or in transportation systems. Sensor networks do not only operate on their own but can cooperate with RFID systems, which helps to connect our physical and digital worlds (Atzori, Iera & Morabito 2010, 4).

The following chapters will define the Internet of Things, give an overview of the different visions of the IoT, and provide insight into the possibilities that the IoT offers today, and possibly in near future.

2.1 Finding a common definition

As the Internet of Things is still in its early stages there is a variety of definitions available. The RFID group defines the IoT as a worldwide network, which consists of objects that can be addressed uniquely. These objects can communicate with each other based on the standard protocols available. Another definition by Cluster of European research projects on the Internet of Things spotlights the *things* by describing them as the participants that play an active part in the information process of the IoT. (Gubbi, Buyya, Marusic, & Palaniswami 2013, 4).

Gubbi et al (2013, 4) define the Internet of Things as devices that can sense, share, and process information that can be used by innovative applications. They define the IoT from the user's viewpoint without restricting it to any standard protocol (Gubbi, Buyya, Marusic, & Palaniswami 2013, 4).

All of these definitions put the focus on different parts that form the Internet of Things, from network over objects to users. Atzori et al (2010, 2) combine these different viewpoints in their definition, and claim, that the full potential of the IoT lays where the Internet-oriented, things-oriented-, and semantic-oriented IoT overlap. The following graphic gives an overview of the components of these different viewpoints.

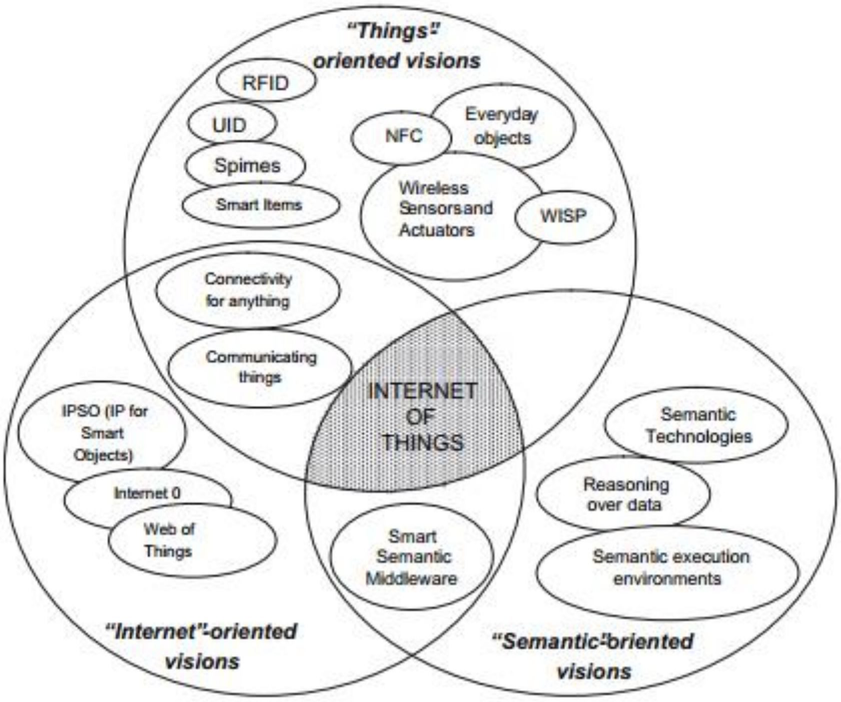
"Things"-oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

Figure 1: The components of the different IoT visions (Atzori, Iera & Morabito 2010, 3)

2.2 Applications

The Internet of Things can provide a vast amount of applications which are likely to influence our lifestyle and improve its quality. Most of the currently available applications can be divided into the following groups: transportation and logistics, healthcare, and smart and personal environments. (Atzori, Iera & Morabito 2010, 7).

An important sector that can benefit from the changes of the IoT is logistics. Thanks to RFID and NFC real-time tracking, at any stage of the supply chain, is possible. This ensures that the business can react to any change in the supply change right away. This allows businesses to plan more efficient so that a full safety stock will be unnecessary.

Another domain that will be affected by the changes of the IoT is transportation. Vehicles can be equipped with all kinds of different sensors, to ensure safety through collision avoidance systems. Considering private transport and freight companies the IoT can provide real time information about traffic jam, so that drivers can choose faster routes.

Another important sector that can benefit from the changes is the healthcare sector. The IoT allows tracking of moving tags, which can be attached to any person or object. This means that it would be possible to follow any item’s- or person’s movement and could prevent from left-in items during surgery, or theft of medication and instruments. Additional to tracking, sensors that are implanted or part of the out-patient care can be used to monitor a patient’s condition in real-time and from everywhere.

Besides transportation, logistics and the healthcare sector, there are further domains that can be supported by the IoT, such as the smart environments. These include homes, offices, or industrial plants. The IoT can help to save energy by regulating the heating systems, or automatically turn off devices that are not in use. Additionally, it can avoid incidents by monitoring the devices in question and triggering alarms if necessary.

The last sector that can benefit from the innovations of the IoT is the personal sector. RFID systems can help us find our lost items by checking the last recorded location. Furthermore, the user could search for keywords and if the condition matches the location the item could be found. This option of item tracking can even be used to detect theft. In case an item, that is part of a restricted area, has been removed from this area without authorization an alarm can be triggered to announce the possible theft. (Atzori, Iera & Morabito 2010, 7-10).

Figure 2 shows in which sectors the IoT is currently available.

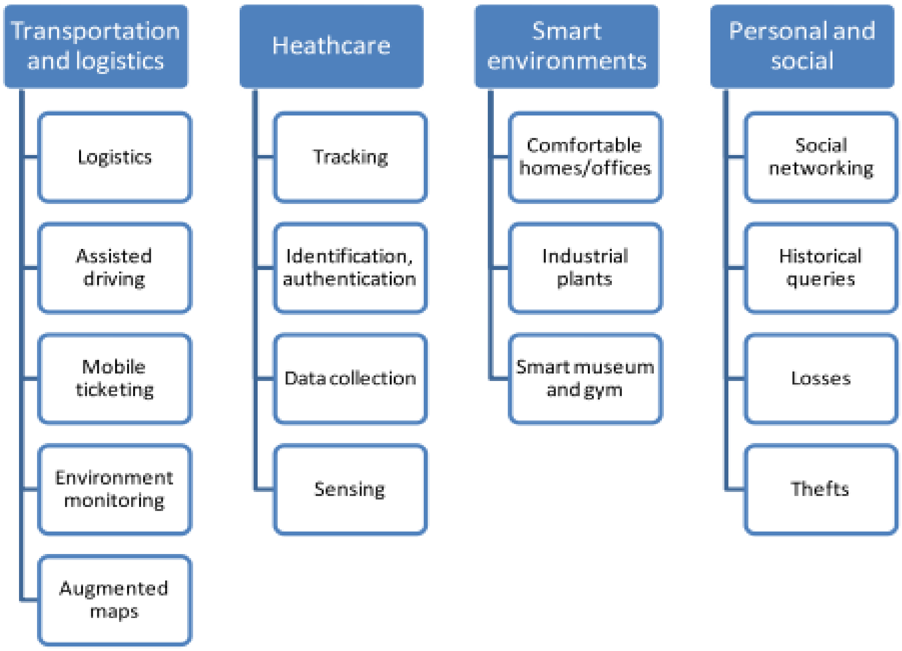

Figure 2: The current sectors included in the IoT (Atzori, Iera & Morabito 2010, 8)

2.3 Known risks

Despite all the benefits that the IoT provides there are well-known risks that have affected current IoT applications. This chapter provides some examples of incidents that have occurred in the sectors described in the previous chapter.

Taking a look at the sector of smart environment, Smith (2017, 13) describes the scenario of a hotel that replaced their old light switches with some android tablets, so that guests could turn on and off the lights for their rooms by using the tablet. A hotel guest that managed to sniff the Ethernet though was suddenly able to use this feature for all hotel rooms, turning on and off the lights in other guests' rooms.

Considering transportation there have been a couple of incidents with cars, ranging from opening a locked car and stealing the owner's expensive possessions to taking control over a car being driven on the motorway. Further incidents in the transportation sector have been reported for aeroplanes. The security researcher Chris Roberts managed to break into an aeroplane's controlling system, from his seat inside the plane.

A further sector that has been affected by even deadly incidents is the industrial environment. In both countries, the United States and Germany, there have been known incidents with factory robots leading to workmen's death.

Another sector that had to face the security risks of the IoT is the medical sector. Security issues in the software used for implanted insulin pumps or pacemakers have been known for a longer time. Another incident found by researchers in 2016 was the discovery of security holes in the drug-dispenser's software that allowed people to obtain harmful drugs.

Further incidents with IoT devices have occurred when the infrastructure to support the innovation has been missing. Starting a car that requires to call home before it can start the engine was not possible anymore after the driver left to an area without full mobile coverage. Schools that provide tests via the Internet had a problem with the Internet connectivity which disrupted submitting the test results for all students. (Smith 2017, 13-20)

Despite its benefits the IoT provides a large surface of attacks. The following chapters give a detailed overview of the key components, RFID systems, NFC, and WSNs, explain the technologies, their possibilities and risks currently known, and provide technical solutions to these security issues. Concluding the paper will summarize the most severe security issues and give an evaluation of how secure the key components of the IoT currently are.

3 Radio Frequency Identification

During the past years, the technology of Radio Frequency Identification (RFID) has grown in popularity. Compared to other widely-used technologies, such as bar code labels, RFID does not require intervisibility. Furthermore, RFID does not only identify an object or item by a certain unique number but it also provides the possibility of additional, item descriptive data. (Want 2006, 25).

RFID systems consist of a database, a RFID reading device, and RFID tags affixed to various items to be tracked or identified. In a RFID-system, a reading device communicates with the database, usually via a secure channel. Furthermore, the reading device communicates with the RFID tags of the system. This channel is considered insecure and therefore strong security features need to be implemented. (Ha, Moon, Nieto & Boyd 2007, 3). The following graphic shows the components of an RFID system and how they interact (RFID advanced Research Alliances 2016).

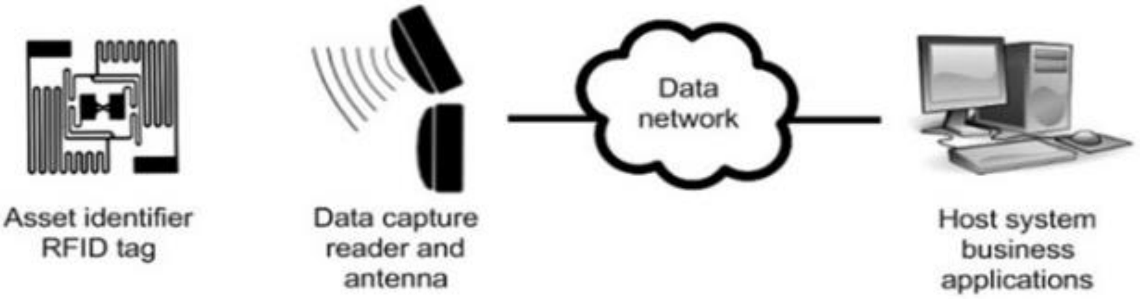

Figure 3: The components of an RFID system and their interaction (RFID advanced Research Alliances 2016)

3.1 Active and passive RFID tags

RFID tags can be roughly divided into two categories: active and passive. Passive RFID tags are usually cheaper in price as they do not contain a power source. Like active RFID tags, passive ones consist of an antenna and a chip coated by a protective cover. Since passive tags do not contain a power source they receive the power, necessary for communication, through varying magnetic fields induced by a reading device. (Want 2006, 25). Depending on the frequency on which passive tags operate they can reach ranges from approximately half a meter to several meters.

Active RFID tags are equipped with a battery which provides power necessary for transmission. This enables them to reach further ranges of approximately 100 meters. (Juels 2006, 2). Despite their advantage in range, due to their power source, active tags have a limited lifespan and are much pricier compared to their passive counterparts (Want 2006, 25).

RFID tags are, for example, used by retail companies to optimise their supply chains, and can even be found in e-passports (Juels, Molnar & Wagner 2005, 3). Further examples are implanted RFID tags in pets, access cards for locks in buildings, or certain types of credit cards, which allow contactless payment (Juels 2006, 2).

3.2 Basic and symmetric-key tags

According to Juels (2006), when considering security risks, it is important to divide RFID tags into two different categories: basic RFID tags (Juels 2006, 7) and symmetric-key tags (Juels 2006, 12).

Basic tags, including Electronic Product Codes (EPC), which are an alternative to bar code labels, are usually the cheapest option available. Hence their low purchase price these tags lack the option of cryptography. (Juels 2006, 7). Symmetric-key tags, on the other hand, are usually pricier than their basic counterparts and can therefore perform cryptographic one-way operations (Juels 2006, 12).

Despite of all possibilities that RFID offers it is important to take a look at the challenges that have to be overcome in order to use this technology safely. As privacy and security issues often go hand in hand this paper will discuss both issues in the following chapters.

3.3 Common attacks on RFID systems

The most common and sever attacks on RFID systems are de-synchronisation, untraceability, information leakage, and replay attacks. De-synchronisation attacks allow adversaries to trace tags and reveal their location by blocking the transmission of a certain type of communication between tag and reader.

Replay attacks enable attackers to misuse previously obtained, valid information. Information leakage can have a severe impact on its user, who might not even be aware of the tag’s activity. A user that carries an active tag unwittingly can reveal information about the ownership of certain, usually expensive products, or medication usage. (Ha, Moon, Nieto & Boyd 2007, 3).

The impact of such attacks on the system is severe and effective countermeasures will be explained in the following chapters.

3.3.1 Attacks on basic RFID tags

As aforementioned, the very basic RFID tags lack cryptography which results in plain sailing for attackers, hence they can simply gather a tag's data or clone it. (Juels 2006, 11).

Assuming an attacker succeeds cloning an EPC-compliant tag by using a skimming attack, that reveals the cloned tag's Electronic Product Code (EPC), the attacker is still in need of the tag's PIN to receive a valid output of the tag to execute the reader's commands. (Juels 2005, 7). The only option to receive the necessary PIN is guessing. Due to the PIN's length, guessing the right PIN is not in step with actual practice.
As non-EPC compliant clones can deceive the reader, by simply accepting any PIN as true, it is important to detect the clones. (Juels 2005, 8).

There might be circumstances under which it is preferable to rather use the reading device as means of communication between the tag and a trusted server. In this case, the reader communicates with the server providing it with a set of PINs. An attacker that manages to compromise a reading device, that can establish access to a server but not to a tag, faces the same problem as mentioned above; to clone a tag successfully the attacker has to guess which one is the valid PIN. Though, whenever the attacker can get access to the tag in question it is possible to learn the valid PIN by simply scanning the tag. (Juels 2005, 11).

Despite the previously described security issues there are further attacks on basic RFID tags. In case of non-permissible access to a database storing PINs, an attacker has the possibility of cloning all tags affected successfully. A further possibility to cloning tags is reverse engineering. To succeed an attacker needs to steal the tag to be able to learn the valid PIN which can then be used for the clone replacing the original one. (Juels 2005, 14).

3.3.2 Attacks on symmetric-key tags

A severe attack on RFID systems with symmetric-key tags is the man-in-the-middle attack. This attack is very effective as the attacker simply acts undetected between two communicating parties, in this case the reading device and the tag, controlling the entire conversation. The man-in-the-middle attack poses an inevitable threat to RFID systems as it bypasses any kind of cryptography.

3.4 Countermeasures for basic RFID tags

As basic RFID tags lack cryptography implementing secure countermeasures to enforce authentication and ensure consumer privacy is an important challenge (Juels 2006, 8). The following chapters will provide insight into lightweight authentication and how to discard basic RFID tags in order to ensure consumer privacy.

3.4.1 Lightweight authentication

Considering basic RFID tags the most challenging security issue is effective authentication. (Juels 2006, 11). To detect clones of attackers the so-called basic authentication protocol includes the feature of testing a tag by sending a set of random, falsified PINs including the correct PIN at a random place. If the tag's response is valid the tag can be revealed as a clone. (Juels 2005, 8). The simplest protocol of authentication, supposed to protect against cloning tags successfully or deceiving reading devices, assumes a trusted tag reading device and is suitable for the most basic type of RFID tags, such as EPCs. (Juels 2005, 8).

3.4.2 Removable tags and tag killing

Another solution to avoid revealing information about a tag's carrier, is to render the tag unusable. Currently, according to Juels (2006, 8) there are two possible scenarios to achieve this approach. One solution that is common in retail is to use so called removable tags that are often used as a price tag. These tags can simply be removed from the item once it has been purchased.

Another solution that is used with non-removable tags is tag killing. Tag killing is considered very effective and plays a pivotal role in consumer privacy. According to Jules (2006, 8) a future scenario would be to kill the tag right after the item has been paid. To kill a tag a reading device sends a command, including an associated, valid PIN code, to deactivate the tag. (Juels 2006, 8).

3.5 Countermeasures for symmetric-key tags

To protect RFID systems from diverse attacks there are various protocols which can be applied to systems of symmetric-key tags. Symmetric-key tags can perform cryptography and have therefore better security options. The following sections give an overview of the two most effective protocols to overcome the problems of de-synchronisation, information leakage, and replay attacks. (Ha, Moon, Nieto & Boyd 2007, 3).

3.5.1 Low-cost and strong-security authentication protocol

Van Deursen and Radomirović (2009, 42) describe an authentication protocol introduced by Ha, Moon, Nieto and Boyd. The protocol's security is based on the assumption that the connection between the reading device and the database is secure. Furthermore, it is assumed that the communication between tag and reading device cannot be considered secure, due to eavesdropping. (van Deursen & Radomirović 2009, 42).

In this stateful protocol, the tag holds a secret ID as well as a value, either 0 or 1, indicating the success of the previous run. Besides holding a secret ID, the reading device furthermore holds the ID of the previous run and the hash of the current ID. The reading device generates a unique number used only once (nonce) and sends it to the tag. Thereupon, the tag generates such a number as well. In addition, if the previous execution was successful, leading to a tag's value of 0, the tag sends a response including the hashed ID and its nonce. Furthermore, the tag sets its state to 1.

In case of a previously unsuccessful execution, the tag keeps its state set to 1 and sends, apart from its nonce, the hashed function of its ID, nonce, and the reading device's nonce. To accept the tag, the reader needs to check the tag's response, excluding the tag's nonce. If the response, consisting of either the hash of the current ID, or the hashed function of the ID, the tag's nonce and the reader's nonce, or the hashed function of the previous ID, the tag's nonce and the reader's nonce, matches any of the values that the reading device holds the tag is considered accepted.

After verification, the reading device updates the values that it holds and sends the value of the hashed function of its previous ID and the tag's nonce to the tag. If the response is equal to the hashed function of the tag's ID and nonce the tag updates its ID to the value of the hashed function of its ID and the reading device's nonce. Furthermore, it indicates successful execution of this run by setting the state to 0. (van Deursen & Radomirović 2009, 42-44).

3.5.2 Lee Asano Kim protocol

Lee, Asano and Kim (2006, 3) stress the importance of untraceability and anti-cloning. Untraceability prevents an attacker from tracing back information that a tag emits, which can then be used to discover certain patterns revealing a tag's secret data, such as its ID.

Their protocol is based on the assumption that both, tag and reading device, can store certain variables in different memories. Each tag contains a unique, random number which is stored permanently for authentication purposes referred to as the tag's ID. In case the tag's ID matches the ID saved in the database the tag is assigned a new value after each successful authentication. Furthermore, tag and reader can store a second pseudorandom number which will only be stored while the authentication process lasts, to ensure that each session has a different identification to prevent replay attacks. The database that communicates with the reading devices saves the current ID of each tag as well as its previous. (Lee, Asano & Kim 2006, 3)

The authentication process of the protocol can be described as follows. The reader sends a randomly generated number, valid for the current round, to the tag. The tag sends the same type of number to the reader. Furthermore, the tag generates a hash function out of the number received from the reader, its own number and its ID and sends this hash to the reader.

The database, the reader communicates with, checks that the tag's ID matches the hash of one of the database's fields. The database updates its fields in case the received hash matches the tag's ID. In this case, the current tag's ID is stored in the field for the tag's previous ID and the received hash serves as the new ID. Out of the reader's random number, the hash of the tag, and the tag's permanent ID the database calculates a new value by using a hash function and sends this number to the reader. With the help of this number, the reader updates the tag's ID to the hash of the number received from the database. (Lee, Asano & Kim 2006, 3-4)

3.6 Conclusion

Although the protocol by Ha, Moon, Nieto and Boyd seems to ensure full authentication there are a couple of security issues that are not covered by the protocol. The first security issue that the protocol cannot fully protect against is false authentication. As a tag always responds to a reader's request with its hashed ID, attackers can obtain this hashed ID if the tag's status is set to 0, as there is no further authentication done. In case attackers can use their own reading devices, before the tag can communicate with a trusted reader that will update the tag's ID, they may impersonate the tag in case they are able to observe the tag's hashed ID and prevent the trusted reading device from updating it. (van Deursen & Radomirović 2009, 44-46).

Another attack, the protocol can't protect against, is desynchronization. This security flaw involves the man-in-the-middle attack and can lead to the reader and tag updating their IDs to different values, which leads to the tag being unusable as it cannot be authenticated in the next sessions anymore. Again, this attack assumes that the tag's state is set to 0. An attacker that succeeds modifying a reader's nonce before sending it, together with the other original values, to the tag can take advantage of the security flaw as there is no verification done that the tag receives the correct nonce sent by the reading device. This leads to the fact that, after execution of the protocol, the reading device and the tag will update their IDs to different values as the tag receives a different nonce than the original one sent by the reader. (van Deursen & Radomirović 2009, 48-50)

The protocol by Lee, Asano and Kim provides the most enhanced authentication currently known for RFID systems. Even though an attacker could eavesdrop on the communication and gather all values of the generated numbers, exchanged between the tag, reading device, and the server's database, that stores all values, the attacker is not able to distinguish between those numbers without being aware of the values stored in the database. The randomly generated number by the tag, described in the beginning of the protocol, prevents an attacker from cloning tags successfully as the number changes for every session. (Lee, Asano & Kim 2006, 5).

This protocol provides a solution against the man-in-the-middle attack as the database includes not only the current tag's ID but even it's previous. Even if an attacker manages to update the tag with a different ID than the one in the server's database to try to render the tag unusable as it cannot be recognized anymore, once the tag's ID differs from the readers, the tag can still be authenticated by its previous value that is stored in the database, additional to the tag's current ID. This ensures recognition of the tag and prevents the system from the impact of the man-in-the-middle attack. (Lee, Asano & Kim 2006, 5). According to Lee et al (2006, 5) their protocol provides enhanced authentication which can protect RFID systems from diverse attacks, including the common attack of tag cloning.

4 Near-Field Communication

Near-Field Communication (NFC) is a technology that is used upon Radio Frequency Identification (RFID). NFC allows devices to interact with each other using a wireless, short range connection. NFC enables communication by simply placing the devices in question close to each other allowing the transmission of data. In technical terms this means that the devices perform a handshake. (Agrawal & Khanna 2012, 1).

According to Haselsteiner and Breitfuß (2006, 1) the devices and their communication mode can be divided according to the devices state. Compared to their passive counterparts, active devices are equipped with a power source. In case both devices are active the radio frequency field is generated by the device sending data. If only one of the devices is an active, and the other a passive device, the radio frequency field is generated by the active device only. (Haselsteiner & Breitfuß 2006, 1). When performing a handshake, the active device, usually referred to as the initiator, sends a message to the second device which can either be active or passive. Based on this message the second device replies and the connection is established. (Haselsteiner & Breitfuß 2006, 2).

NFC is said to be very user friendly as there is no need to configure the devices beforehand. Placing the devices close to each other is sufficient to establish a connection in a very short time, usually within milliseconds. Furthermore, NFC can be used with other wireless technologies including WiFi, ZigBee, and Bluetooth. (Agrawal & Khanna 2012, 2).

4.1 Risks

Despite all the previously mentioned advantages NFC is prone to various attacks which can have a severe impact on the system. These threats are based upon common network security issues, such as eavesdropping, or the so-called denial of service attack. (Agrawal & Khanna 2012, 4).
The following chapters give a detailed overview of all common security threats.

4.1.1 Eavesdropping

Eavesdropping is a security issue that effects all wireless technologies. As NFC communicates through radio frequency waves, eavesdropping poses a threat to NFC. Typically, two communicating devices are not further than 10 cm away from each other. Despite the short distance, an attacker that receives and decodes the signal can eavesdrop on the communication, no matter how short the distance. (Haselsteiner & Breitfuß 2006, 4).

Nevertheless, according to Haselsteiner and Breitfuß (2006, 4) it is not possible to predict how close an attacker has to be for receiving the signal. This depends on various parameters of both, the sending and the receiving device. Amongst others, these parameters cover the characteristics of the antennas of the sending and receiving devices, the quality of the devices in general, and the location of the system setup. (Haselsteiner & Breitfuß 2006, 4).

In addition to that, an attacker has to consider the sending device's mode. A device that is generating its own radio frequency field, a so called active device, is much easier to eavesdrop on than a device that is using another device's field. This is simply because the reach of an active device is ten times higher. (Agrawal & Khanna 2012, 4).

4.1.2 Denial of Service

A denial of service attack is done by disturbing the data exchange between the devices so that the data sent by the sending device cannot be decoded by the second device. Usually this is done by flooding the communication. (Agrawal & Khanna 2012, 4).

4.1.3 Data Insertion

Data insertions are always possible when the answering device is slower in answering than the attacker's device. In this case, the attacker can send the forged data before the actual valid data can be sent. In case the attacker's data and the valid data is sent at the same time, a flaw in data will occur. (Haselsteiner & Breitfuß 2006, 6).

4.1.4 Man-in-the-Middle attack

According to Haselsteiner and Breitfuß (2006, 6) a man-in-the-middle attack is possible only in theory. Nevertheless, for the reason of completeness, a theoretical scenario will be described in the following. There are two setups that are to be taken into consideration. The first conversation consists of the use of active and passive mode, while the second assumes both parties in active mode. (Haselsteiner & Breitfuß 2006, 6).

In an active-passive mode the active party generates the radio frequency field and sends the data to the second party. An attacker can eavesdrop on the communication and make the transmission impossible by disturbing the transmission. Once the transmission is disturbed the attacker sends the data, replacing the original, to the second party. To succeed the attacker needs to generate a radio frequency field. As the previous radio frequency field of the sender is still active the attacker would have to align both active fields perfectly to succeed, which makes the attack in active-passive mode impossible. (Haselsteiner & Breitfuß 2006, 6).

The second possibility of the man-in-the-middle attack includes both communicating parties using active mode. Again, as in the previously described active-passive mode, the attacker disturbs the transmission. Compared to the previous setup, in the active-active mode the sending party needs to turn off the radio field for the second party to receive the data. This enables the attacker to turn on its own radio field to send the forged data. In this setup both parties are listening to the communication waiting for the answer of the other party. This makes it impossible for the attacker to send the forged data without any of the parties noticing that the data is send from someone else. (Haselsteiner & Breitfuß 2006, 7). Again, according to Haselsteiner and Breitfuß (2006, 7) the previously described setup makes a man-in-the-middle attack impossible.

4.2 Security Implementations

This chapter gives an overview of the most effective security implementations on NFC systems. Furthermore, it will provide an example on how to secure the channel between two devices.

4.2.1 Eavesdropping

There is no countermeasure in NFC itself that could prevent a system from an eavesdrop attack. The only effective security implementation is a so called secure channel which will be described in detail under section 4.2.5. (Haselsteiner & Breitfuß 2006, 7).

4.2.2 Denial of Service

Denial of Service attacks are quite easy to detect. The power needed for data corruptions is remarkably higher so that NFC devices can detect the increase. (Haselsteiner & Breitfuß 2006, 7). In case a significant increase in power is detected, the NFC can be disabled by a simple switch included in every device (Agrawal & Khanna 2012, 4).

4.2.3 Data Insertion

To prevent an attacker from replacing valid data with forged data, there are various countermeasures. One possibility to prevent the attack is by having the answering device reply right away without any delay to make sure that an attacker does not get any time to reply with forged data. Another countermeasure that could detect and prevent an attack, is that while the channel for transmission between the two devices is open, the devices listen to the channel. In case an attacker inserts data, it could be heard on the channel. The last option to prevent a data insertion attack is a so-called secured channel which will be described under section 4.2.5. (Haselsteiner & Breitfuß 2006, 8).

4.2.4 Man-in-the-Middle attack

Due to the difficulties in both, active-passive and active-active mode, according to Haselsteiner and Breitfuß (2006, 8) a man-in-the-middle attack is impossible to perform. Nevertheless, due to the permanently generated radio frequency field, an attack in the active-passive mode is less likely to succeed so that for security reasons this setup is recommended to be used. (Haselsteiner & Breitfuß 2006, 8).

4.2.5 Secure channel

A secure channel between two NFC devices is fairly easy to set up and can protect the data sent from modifications. As it is nearly impossible to perform a man-in-the-middle attack, which is described under section 4.1.4**,** there are no further protective measures needed for setup. In general, a secure channel is based on a key agreement protocol such as the standard Diffie-Hellmann. In this protocol, both communicating parties hold a secret key, known only to them, which guarantees a secure transmission of data. (Haselsteiner & Breitfuß 2006, 8).

4.3 Conclusion

NFC faces severe security threats that NFC itself cannot prevent. Those threats include the modification of data and the eavesdropping attack. To overcome these security issues, it is recommended to use a so-called secure channel, which helps to provide a secure method for data transmissions. This secure channel uses a standard key protocol as, due to the resistance against the man-in-the-middle attack, it is most suitable. (Haselsteiner & Breitfuß 2006, 10).

5 Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are another key component of the Internet of Things. They are used in multiple applications including military applications, environmental applications, health applications, home applications, or other commercial applications.

Military applications include, amongst others, battlefield surveillance, damage assessment, and attack detection. In environmental applications WSNs are used to track movements of animals, monitoring of the Earth including forest fire or flood detections, or for geographical research. Health applications make use of WSNs for monitoring the processes in hospitals, monitoring and detecting human physiological data, or tracking the drug administration in hospitals. Small household appliances such as vacuum cleaners or microwave ovens can contain sensor nodes to ensure home automation used in home applications, based on the interaction of those devices. Examples of other commercial applications using WSNs are vehicle tracking and detection, robot control in automation, or centrally controlling air conditioning of office buildings. (Akyildiz, Su, Sankarasubramaniam & Cayirci 2001, 395).

Wireless Sensor Networks usually consist of two parts: The so called base stations, and a vast amount of sensor nodes. Sensor nodes again consist of the following four parts: A power unit, a transmission unit, a processing unit, and a sensing unit.
Usually the power unit is the only component which provides power to all other components of the node. It can either consist of a single battery or any energy harvesting device such as solar cells. The transmission unit connects the node to the network by constantly interacting with the processing unit. The processing unit consists of two components, a processor and a storage space. This unit interacts with all other units, receiving and processing information supported by the power unit. The sensing unit again consists of two sub components: a sensor, and a converter which converts the analogue inputs into digital ones, hence it is referred to as the analogue-to-digital converter (ADC).

As described in the previous abstracts, the nodes of a WSN often require information about locations, or it might be necessary to move certain sensor nodes to a new location. For these purposes, they might be equipped with a position finding system, often referred to as a location finding system, and a mobiliser.

Figure 4 shows the components of one sensor node (Wang, Attebury & Ramamurthy 2006, 3).

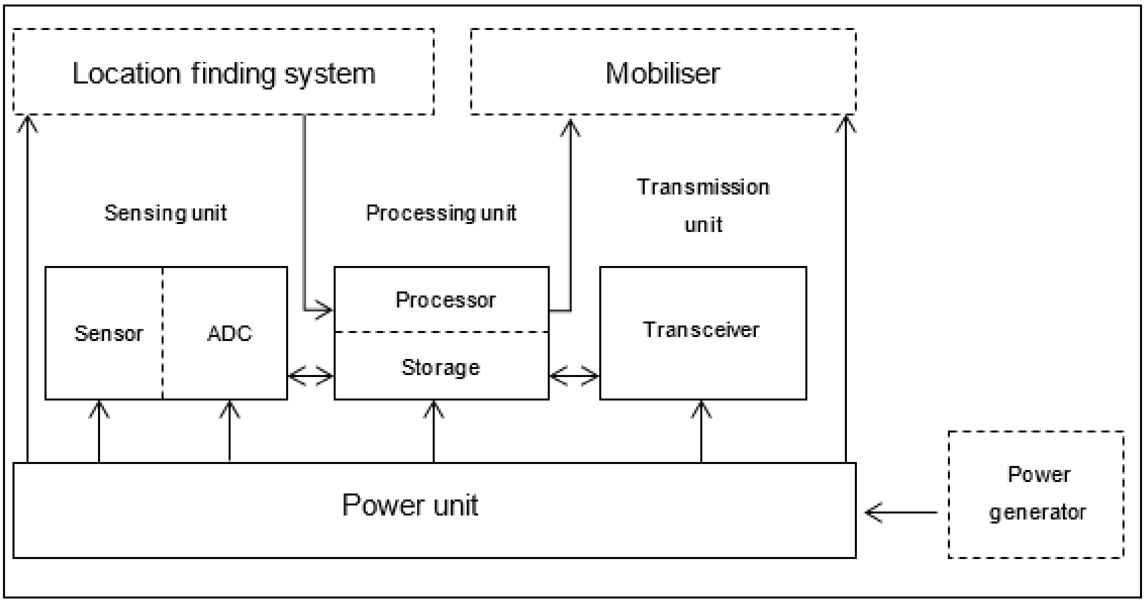

Figure 4: The components of one sensor node (Wang, Attebury & Ramamurthy 2006, 3)

Compared to the low-power, low-cost sensor nodes, base stations are usually a lot more powerful, including components comparable to workstations or laptops. A sensor network can contain multiple base stations which are used as both, gateways, and access points. (Karlof & Wagner 2003, 295). Although Wireless Sensor Networks share similarities with ad-hoc networks there are certain limitations that security challenges have to overcome (Karlof & Wagner 2003, 296).

Due to the low-power, sensor nodes' power management is a critical problem in WSNs. The computation power of sensor nodes is much lower compared to nodes in an ad-hoc network. Furthermore, sensor nodes of a WSNs do not have the same capacity in memory as their ad-hoc network counterparts. The last major difference between ad-hoc networks and WSNs is the transmission range. Due to the fact, that nodes of a WSN are limited in power and technically not as powerful as nodes in an ad-hoc network their communication range is much shorter. All of these limitations make a lot of security algorithms, currently used in ad-hoc networks, impractical to use. (Wang, Attebury & Ramamurthy 2006, 4).

The following abstracts give an overview of the current constraints of WSNs, possible attack points, the most common attacks, and defence mechanisms.

5.1 Constraints in Wireless Sensor Networks

Wireless Sensor Networks face different constraints compared to ad hoc networks. To keep applications using WSNs competitive the production cost needs to be kept as low as possible. This leads to constraints in hardware as the components of a sensor network need to be of small size. Another constraint that needs to be considered is the environment in which WSNs are deployed. (Akyildiz, Su, Sankarasubramaniam & Cayirci 2001, 399 - 401). The following chapters give detailed insight into the constraints that make WSNs different from ad hoc networks.

5.1.1 Production cost constraints

The cost of a single sensor node in a WSN needs to be kept as low as possible to make applications using sensor networks competitive. Especially for sensor nodes that need to be equipped with a location finder and mobiliser**,** in order to meet certain applications' needs, the production cost can be a very challenging issue. Compared to a low-cost device, such as a Bluetooth radio, a single node in a WSN has to cost less than a tenth of that price. (Akyildiz, Su, Sankarasubramaniam & Cayirci 2001, 399).

5.1.2 Hardware constraints

As shown in figure 4, a single node in a WSN is made up of four basic components and, depending on the application, of two additional components. WSNs consist of hundreds or thousands of sensor nodes which requires them to be of small size. That requires all of those previously described components to fit into small cases, often smaller than a match box.

Depending on the application sensor nodes have to be adaptive to the environment they are placed into. This often means that, once deployed, those sensor nodes are hard to access, or not accessible at all anymore for their entire lifetime. This includes that those nodes have to operate unattended and consume as little energy as possible in order to ensure a long lifetime of the WSN. (Akyildiz, Su, Sankarasubramaniam & Cayirci 2001, 400).

5.1.3 Environmental constraints

Sensor network nodes must work under diverse conditions and environmental influences. They might be placed right inside the environment to track or observe it. Such environments include the interiour of devices or machinery, inside a moving device or vehicle, in a river, on the bottom of an ocean, or implanted into humans or animals. Sensor nodes could also be deployed in environments that force them to work under harsh environmental conditions such as extreme heat or cold, chemically or biologically contaminated areas, or in environment where sensor nodes must withstand noise which usually involves jamming. (Akyildiz, Su, Sankarasubramaniam & Cayirci 2001, 401).

5.1.4 Sensor network topology constraints

In WSNs, device failure is a challenging task and makes topology maintenance difficult, compared to ad-hoc networks. Sensor nodes can be deployed in diverse ways, depending on the application or environment they are used in. They can be put in place by using other devices such as aeroplanes or catapults, or by humans or robots. During the pre-deployment and deployment phase, it is important to take fault tolerance and flexibility into account.

Once those sensor nodes have been deployed, the WSN might face frequent topology changes due to the problem of insufficient energy supply, the position of certain nodes which might not be easy to reach anymore, or due to faulty nodes. During the re-deployment phase topology changes might be caused due to re-deployment or replacement of sensor nodes. To ensure security special routing protocols are required. (Akyildiz, Su, Sankarasubramaniam & Cayirci 2001, 401).

5.2 Classification of attackers

There are two types of attackers that can pose a threat to Wireless Sensor Networks. Mote-class attackers can get access to WSNs by using a certain number of malicious nodes which have similar capabilities as the nodes inside the network. The second type of attackers are the so-called laptop-class attackers. (Wang, Attebury & Ramamurthy 2006, 5).

Laptop-class attackers are much more powerful than mote-class attackers. While mote-class attackers can perform attacks in their immediate environment, laptop-class attacker could attack the entire network. Laptop-class attackers use more powerful devices, which usually have the capacity and components of a laptop or a similar device, including high-bandwidth and a powerful energy resource. (Karlof & Wagner 2003, 298). Additional to the previous distinction, attackers can be classified according to their access to the network as well as whether an attack is active or passive.

Active attacks include modification or creation of data streams while passive attacks are used to monitor those streams. Outsider attacks are performed from nodes that are not part of the WSN. Insider attacks on the other hand are performed using nodes that belong to the WSN. (Wang, Attebury & Ramamurthy 2006, 5). To successfully perform insider attacks, the adversary has to get hold of the key material in order to compromise the sensor node. Once the sensor node is compromised, laptop-class attackers can attack the entire WSN. (Karlof & Wagner 2003, 298).

5.3 Network assumptions and requirements

In the following abstracts the possible attacks on WSNs will be explained in detail, and countermeasures introduced. The following assumptions on WSNs will outline the weak points of the sensor network and the ones that can be considered trustworthy.
As sensor networks are wireless it can be assumed that attackers have the capabilities to eavesdrop on the communication between nodes. Furthermore, based on the deployment methods, it must be assumed that attackers can deploy their own nodes into a WSN and thus have control over multiple nodes of the network. As sensor nodes are very low in cost per unit it has to further be assumed that sensor nodes are not tamper resistant. (Karlof & Wagner 2003, 297). According to Wang et al. (2006, 5) base stations on the other hand can be considered trustworthy.

5.4 Attacks in sensor networks

Wireless Sensor Networks are vulnerable to different types of attacks which will be described in detail in the following chapters. The attacks occur on different levels of the protocol stack layer which can be described as followed.

The physical layer deals with the transmission of data streams, signal detection and data encryption and faces jamming and tempering attacks. The data link layer is responsible for multiplexing those data streams, for the detection of data frames, and for ensuring point-to-point or point-to-multipoint connections. Common attacks are resource exhaustion and unfairness.

The network layer ensures the forwarding of packets and address assignments. Attacks that occur on the network level are the following: spoofing, altering or replaying routing information, selective forwarding, sinkholes, the Sybil attack, wormholes, and HELLO-flood attacks.

The transport layer ensures a reliable transport of packages, and the application layer is responsible for managing data requests facing attacks such as flooding and desynchronisation. (Wang, Attebury & Ramamurthy 2006, 3).

5.4.1 Jamming

Jamming, often referred to as radio jamming, is a method used to attack wireless networks by interfering with the network’s radio frequencies. Adversaries that have a powerful source used for jamming attacks can disrupt an entire network. This is even possible if the source is less powerful but the jamming is distributed randomly. (Wang, Attebury & Ramamurthy 2006, 5).

5.4.2 Tampering

Due to the low-cost of sensor nodes tampering is another possible attack on sensor networks. Attackers that can gain physical access to a node can extract the node’s information and furthermore create a node of which the attacker has full control. Tamper-proofing nodes involves high costs, so that most security schemes consider nodes as not tamper resistant. (Wang, Attebury & Ramamurthy 2006, 5).

5.4.3 Resource exhaustion

Attackers can exhaust a node and their surrounding nodes by causing collisions between the transmission of data between multiple nodes. If the retransmission of data is not discovered and the network continuously attempts to transmits those packages, the energy resources of the nodes affected will be exhausted. (Wang, Attebury & Ramamurthy 2006, 6).

5.4.4 Unfairness

Unfairness involves the previously described link layer attack and can be considered a mild form of a DoS attack. In an unfairness attack an adversary tries to cause nodes to miss their transmission deadline which can impair and weaken the entire network. (Wang, Attebury & Ramamurthy 2006, 6).

5.4.5 Spoofing, Altering and Replaying

The aim of spoofing, altering and replaying routing information is to disrupt network traffic. The attacks mentioned can include the following: creation of routing loops, extension or shortening of routes, network partitioning, or the generation of false error messages. (Wang, Attebury & Ramamurthy 2006, 6).

5.4.6 Selective forwarding

In a selective forwarding attack adversaries make use of the assumption that nodes usually forward received messages faithfully. In this attack adversaries use malicious nodes to drop certain messages which means that they are not forwarded any further. To limit suspicion and avoid that surrounding nodes choose another route, in case they conclude the original has failed, attackers might select to modify or supress only a few packets and forward the remaining ones.

Adversaries have two possibilities to achieve this attack. They can be either be part of the path of the transmission of data, or they can overhear the transmission flow through neighbouring nodes. Even though both forms of attack are possible, the first option is more effective and easier to perform. (Karlof & Wagner 2003, 300).

5.4.7 Sinkhole attacks

The aim of a sinkhole attack is to ensure that all traffic of a certain area of the network flows through a compromised node the attacker has full control of. To create a sinkhole the attacker has to ensure that the node seems attractive to its surrounding nodes, by simulating the nodes to be a high-quality route to a base station. This ensures that nodes use the sinkhole to forward packets supposed to reach the base station. Using this attack, adversaries can easily supress or modify data packets. (Karlof & Wagner 2003, 300-301).

5.4.8 The Sybil attack

This form of attack is often used in geographic routing. In a Sybil attack an adversary comprises a node to appear as multiple identities. In a location routing system nodes exchange their coordinates with their neighbouring nodes to geographically route information, usually accepting any set of coordinates. This causes that the adversary can be in multiple places at a time. (Karlof & Wagner 2003, 301).

5.4.9 Wormholes

Attackers use wormholes to tunnel messages from one part of the network to a different one. Wormhole attacks usually include two distant nodes an attacker has full control over forwarding messages between them. If an adversary succeeds to place a wormhole close to a base station and convinces nodes that are usually multiple hops away to be much closer the attacker could disrupt routing in the entire network. Wormhole attacks can be used in combination with other attacks to make the attack more powerful. Those attacks include eavesdropping, selective forwarding, sinkholes, or the Sybil attack. (Karlof & Wagner 2003, 301).

5.4.10 HELLO flood attack

In a HELLO flood attack adversaries misuse the fact that in most routing protocols nodes use HELLO packets to announce themselves to their neighbouring nodes. This includes the assumption that those nodes are within normal radio range of each other. Attackers sending those HELLO packets, despite being in normal range, can make other nodes believe that they are the sending nodes neighbours. The neighbouring nodes will transmit their data packets to the node sending the HELLO packets but, since being out of radio range, the packet will never reach their destination, which makes it impossible for the network to maintain its state. (Karlof & Wagner 2003, 302).

5.4.11 De-synchronisation

In a desynchronization attack an adversary continuously sends spoofed packets to a host, that tries to request those missed frames to be retransmitted. This can cause the host to waste energy, trying to recover from false errors, in case the attacker manages to prevent data exchange completely. (Wang, Attebury & Ramamurthy 2006, 7).

5.5 Countermeasures

According to Karlof and Wagner (2003, 310) most attacks coming from the outside of the WSN can be prevented by applying link layer encryption using a shared key between the nodes and the base station. However, this countermeasure does not provide protection against insider attacks.

The following chapters will focus on countermeasures for the previously described attack mechanisms on WSNs, and give an insight into various solutions to the most common attacks against WSNs.

5.5.1 Jamming

There are two defence mechanisms known against radio jamming: frequency hopping, and code spreading. Frequency hopping involves rapidly changing frequencies when transmitting signals, which makes it impossible for an attacker to jam the unknown frequency. Code spreading is used for the same purpose but, as the signal is spread, this defence mechanism requires a larger amount of energy. Due to the low cost of WSNs and the limited energy resources both defence mechanisms cannot be applied. (Wang, Attebury & Ramamurthy 2006, 5).

5.5.2 Tampering

Like jamming, tempering is an attack occurring on the physical layer. Due to the low cost of WSNs there is no effective countermeasure known that could be applied to the design of current WSNs. In order to protect WSNs against attacks on the physical layer, all security schemes must consider this weakness. (Wang, Attebury & Ramamurthy 2006, 5).

5.5.3 Resource exhaustion

There are two countermeasures used to prevent resource exhaustion. The first countermeasure prevents from energy depletion by allowing the WSN to ignore requests that are outside the rate limits in the MAC layer. The second solution introduces a time slot in which the transmission of signals is allowed and prevents the WSN from continuously retransmitting the corrupted data. This solution is often referred to as time-division multiplexing. (Wang, Attebury & Ramamurthy 2006, 6).

5.5.4 Unfairness

Currently there is no countermeasure know that could completely prevent WSNs from unfairness attacks. Using smaller time frames for transmissions can lessen the impact of unfairness attacks on the WSN, nevertheless the attack itself cannot be prevented as adversaries can retransmit very quickly. (Wang, Attebury & Ramamurthy 2006, 6).

5.5.5 Spoofing, Altering and Replaying

An effective solution to prevent WSNs from spoofing, altering, and replaying information is to add a message authentication code and a timestamp to the message. This allows verification of the received data and furthermore avoids the information to be replayed. (Wang, Attebury & Ramamurthy 2006, 6).

5.5.6 Selective forwarding and sinkhole attacks

Selective forwarding and sinkhole attacks by an outside attacker can be fully avoided by applying shared key encryption. This countermeasure ensures that the adversary cannot join the WSN anymore. Nevertheless, the countermeasure is non-effective for inside attackers. (Karlof & Wagner 2003, 310).

5.5.7 The Sybil attack

As attacks coming from inside of the WSN cannot be prevented, it is important to verify the nodes' identities in order to detect masquerading. Due to the restrictions of WSNs traditional approaches, such as public key cryptography, are not feasible. A possible solution to overcome the problem of Sybil attacks on WSNs is the implementation of unique, symmetric keys that are shared between the nodes and the base station. These keys allow neighbouring nodes to verify their identity and establish a shared key which limits its communication to the authenticated neighbouring nodes. It is important to note that the number of keys per node should be limited by the base station to prevent adversaries from establishing a shared key with every node. In case a node exceeds the given number of shared keys with neighbouring nodes an error message will be sent to announce the problem. (Karlof & Wagner 2003, 310-311).

5.5.8 Wormholes

Most existing protocols do not protect from wormhole attacks which makes it very difficult to protect WSNs against this form of attack, especially when used in combination with other attacks. The only type of protocol that is resistant to wormholes is the geographic routing protocol. In this type of protocol the topology of the WSN is not constructed by the base station but by the traffic that reaches the physical location of the base station. Topologies that are constructed this way consider the physical distance between neighbouring nodes, and nodes that are beyond radio range can be revealed. (Karlof & Wagner 2003, 311).

5.5.9 HELLO flood attack

A possible countermeasure to HELLO flood attacks is an authentication protocol between neighbouring nodes that verifies the nodes' identities using the base station. Before an adversary can use a HELLO flood attack, an authentication with all neighbouring nodes has to be established. If the number of neighbouring nodes is above a certain limit the base station might detect the attacker. (Karlof & Wagner 2003, 311).

5.5.10 De-synchronisation

De-synchronisation attacks can be prevented by authenticating the packets that are send between the two hosts, preventing the attacker from sending spoofed packets. (Wang, Attebury & Ramamurthy 2006, 7).

5.6 Conclusion

The previously mentioned attacks on Wireless Sensor Networks have shown that encryption on the link layer, identity verification, and authentication are effective countermeasures against outside attackers. If applied correctly WSNs can be protected from Sybil attacks, HELLO flood attacks, selective forwarding, spoofing, and de-synchronisation.

Attacks performed by powerful adversaries from the inside of the WSN though pose a significant threat to the network, as there is no effective countermeasure known that could protect against these attacks. The most challenging attacks caused from the inside of the network are the sinkhole and wormhole attack. To protect WSNs from inside attackers, further countermeasures to cryptography have to be considered. Secure routing protocols need to be tailored to the needs and restrictions of WSNs. Currently, only the geographic routing protocol can protect the sensor network from inside attacks, such as the wormhole attack. (Karlof & Wagner 2003, 313).

According to Karlof and Wagner (2003, 313) to design a routing protocol, that can overcome the current security issues, stays an open problem that needs to be solved to securely use WSNs for multiple applications.

6 Conclusion

Evaluating the security risks of RFID systems, it can be said that, the lower the tags are in price, the higher the security issues. Low cost, basic RFID tags cannot prevent attackers from extracting the information of a tag, revealing its data to the adversary while the tag is considered active. In case an attacker can get physical access to a tag, there is no security countermeasure that can prevent the attacker from cloning the tag, as all data necessary to succeed is revealed by the tag.

Although the proposed lightweight authentication protocol can detect clones, by scanning them, there is currently no protocol available that could protect RFID systems, with low cost basic tags, from revealing its data. An effective countermeasure to overcome this security flaw is tag killing. Once a tag has been killed it cannot reveal its information anymore, as attackers cannot track the item the tag is attached to. This ensures that the item's, often sensitive information, such as item description or price, does not fall into the wrong hands as this information should stay private to ensure the owner's security. Nevertheless, it might not always be possible to discard the tags of a system once the item is in the hands of a person. For systems, that require a tag to stay alive for the entire lifetime of an item or product, which can be used in rental chains including hire cars, or libraries, there is currently no effective countermeasure known.

RFID systems using symmetric-key tags have more security options available due to supported cryptography. Despite the vulnerabilities found in current countermeasures the protocol by Lee, Asano and Kim provides enhanced security which can overcome the security flaws known in other protocols. Summarizing, it can be said that RFID systems using symmetric-key tags only can be considered secure, while its basic counterparts lack security.

The technology of Near-Field Communication is vulnerable to all attacks that most wireless technologies face, ranging from eavesdropping over data insertions to denial-of-service attacks. Despite those security issues, with the introduction of the secure channel, NFC provides an effective countermeasure that can ensure a secure transmission of data. Nevertheless, there is the risk of a denial-of-service attack for which there is currently no effective countermeasure known, that would ensure the device or system to be available. Despite the DoS attack, NFC provides the necessary security implementations to consider this technology a solid and secure basis for the IoT.

Like RFID systems, WSNs face the problem of competitiveness which forces them to operate with low cost nodes which limits their energy resource. WSNs cannot protect from attacks on the physical layer, such as jamming or tampering, due to their scarce resources. Nevertheless, not only the hardware constraints play a role in this security flaw, even environmental constraints, such as noise, make attacks on the physical layer more likely to occur.

Not only the physical layer faces attacks no current countermeasure is known for, the link layer can be considered a weak part as well. The effects of an unfairness attack, that functions as a DoS attack, in order to make the network unavailable, can be lessened though not prevented.

Although effective cryptography can protect the WSN from outside attacks no countermeasure can protect the network when the attack comes from the inside. These attacks pose a significant threat to the security of the entire network.

Considering the IoT as of today it can be concluded that countermeasures, to prevent the IoT from attacks, leading to security issues effecting its users, are getting more effective. Authentication and cryptography can protect the IoT's key components RFID and NFC from severe attacks, nevertheless, they are not applicable to WSNs. Concluding it can be said that, as long as there are no effective security mechanisms provided that can protect WSNs from severe attacks, the IoT as of today cannot be considered secure.

References

Agrawal, U. & Khanna, B. 2012. Near field communication. SETLabs Bridfings, 10(1), pp. 67-74. URL: https://www.researchgate.net/profile/Binny_Khanna/publication/264048931_Near_Field_Communication_A_Technology_for_Short_Range_Communication/links/02e7e53ccb1831f2fa000000.pdf. Accessed: 22 December 2015.

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. 2002. Wireless sensor networks: a survey. Computer networks, 38(4), pp.393-422. URL: http://www2.ic.uff.br/~julius/compmov/SensorNetSurvey.pdf. Accessed: 15 January 2017.

Atzori, L., Iera, A. & Morabito, G. 2010. The internet of things: A survey. *Computer networks*, *54*(15), pp.2787-2805. URL: https://www.researchgate.net/profile/Luigi_Atzori2/publication/222571757_The_Internet_of_Things_A_Survey/links/546b36df0cf2f5eb180914e5/The-Internet-of-Things-A-Survey.pdf. Accessed: 19 October 2015.

Coetzee, L. & Eksteen, J. 2011. The Internet of Things-promise for the future? An introduction. In *IST-Africa Conference Proceedings, 2011* (pp. 1-9). IEEE. URL: https://www.researchgate.net/profile/Louis_Coetzee/publication/232168435_Turn_me_on_Using_the_Internet_of_Things_to_turn_things_on_and_off/links/568faa1308aead3f42f45509.pdf. Accessed: 19 October 2015.

Greengards, S. 2015. The Internet of Things. Massachusetts Institute of Technology. The MIT Press. Cambridge Massachusetts.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), pp.1645-1660. URL: https://arxiv.org/ftp/arxiv/papers/1207/1207.0203.pdf. Accessed: 22 October 2015.

Ha, J., Moon, S., Nieto, J. M. G., & Boyd, C. 2007. Low-cost and strong-security RFID authentication protocol. Emerging Directions in Embedded and Ubiquitous Computing, pp.795-807. URL: https://pdfs.semanticscholar.org/e2b5/0a448e78d91c7e7cc904fddbac07aac449fb.pdf. Accessed: 1 November 2015.

Haselsteiner, E. & Breitfuß, K. 2006. Security in near field communication (NFC). Workshop on RFID Security RFIDSec. URL: http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf. Accessed: 22 December 2015.

Juels, A. 2005. Strengthening EPC tags against cloning. In Proceedings of the 4th ACM workshop on Wireless security, pp. 67-76. URL: http://vs.inf.ethz.ch/edu/SS2005/DS/papers/rfid/juels-epc_cloning.pdf. Accessed: 23 October 2015.

Juels, A. 2006. RFID security and privacy: A research survey. Selected Areas in Communications, IEEE Journal, pp. 381-394. URL: http://www.mscs.mu.edu/~iq/papers/rfid/RFID%20Security%20and%20Privacy%20A%20research%20survey.pdf. Accessed: 19 October 2015.

Juels, A., Molnar, D. & Wagner, D. 2005. Security and Privacy Issues in E-passports. Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005, pp. 74-88. URL: http://www.library.ca.gov/crb/rfidap/docs/Juelsetall-SecurityandPrivacyofE-Passports.pdf. Accessed: 19 October 2015.

Juels, A. & Weis, S. A. 2009. Defining strong privacy for RFID. ACM Transactions on Information and System Security (TISSEC), p. 7. URL: http://www.securant.com/emc-plus/rsa-labs/staff/bios/ajuels/publications/rfid_privacy/rfidprivacy.pdf. Accessed: 1 December 2015.

Karlof, C., Wagner, D. 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), pp.293-315. URL: https://users.ece.cmu.edu/~adrian/731-sp04/readings/karlof-wagner-secrouting.pdf. Accessed: 15 January 2017.

Lee, S., Asano, T., & Kim, K. 2006. RFID mutual authentication scheme based on synchronized secret information. In Symposium on cryptography and information security. URL: http://caislab.kaist.ac.kr/publication/paper_files/2006/SCIS_Lee.pdf. Accessed: 1 December 2015.

Miorandi, D., Sicari, S., De Pellegrini, F. & Chlamtac, I. 2012. Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), pp.1497-1516. URL: https://irinsubria.uninsubria.it/retrieve/handle/11383/1762288/2389/IOT.pdf. Accessed: 20 October 2015.

RFID Advanced Research Alliances 2016. URL: http://www.therfid.com/rfid.html. Accessed: 7 May 2017.

Smith, S. 2017. The Internet of Risky Things. Trusting the Devices That Surround Us. O’Reilly Media Inc.

van Deursen, T., Radomirović, S. 2009. Security of RFID protocols–A case study. Electronic Notes in Theoretical Computer Science, 244, pp. 41-52. URL: http://ac.els-cdn.com/S157106610900259X/1-s2.0-S157106610900259X-main.pdf?_tid=7521aa3c-33f7-11e7-b948-00000aacb360&acdnat=1494252537_7af835abee23299349026a23d03d89d2. Accessed: 30 October 2015.

Wang, Y., Attebury, G., & Ramamurthy, B. 2006. A survey of security issues in wireless sensor networks. URL: http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1087&context=csearticles. Accessed: 15 January 2017.

Want, R. 2006. An Introduction to RFID Technology. Pervasive Computing, IEEE 5.1, pp. 25-33. URL: http://gtubicomp2013.pbworks.com/w/file/fetch/64846805/want-rfid.pdf. Accessed: 19 October 2015.

Want, R., Schilit, B.N. & Jenson, S. 2015. Enabling the internet of things. *Computer*, *48*(1), pp.28-35. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.6666&rep=rep1&type=pdf. Accessed: 22 April 2017.