A Lightweight Framework for Secure Life-logging in Smart Environments☆

Nikolaos E. Petroulakis[a], Elias Z. Tragos[a], Alexandros G. Fragkiadakis[a], George Spanoudakis[b]

[a]*Institute of Computer Science, Foundation for Research and Technology-Hellas, Heraklion, Greece*
[b]*School of Informatics, City University London, London, UK*

Abstract

As the world becomes an interconnected network where objects and humans interact with each other, new challenges and threats appear in the ecosystem. In this interconnected world, smart objects have an important role in giving users the chance for life-logging in smart environments. However, smart devices have several limitations with regards to memory, resources and computation power, hindering the opportunity to apply well-established security algorithms and techniques for secure life-logging on the Internet of Things (IoT) domain. The need for secure and trustworthy life-logging in smart environments is vital, thus, a lightweight approach has to be considered to overcome the constraints of smart objects. The purpose of this paper is to present in details the current topics of life-logging in smart environments, while describing interconnection issues, security threats and suggesting a lightweight framework for ensuring security, privacy and trustworthy life-logging. In order to investigate the efficiency of the lightweight framework and the impact of the security attacks on energy consumption, an experimental test-bed was developed including two interconnected users and one smart attacker, who attempts to intercept transmitted messages or interfere with the communication link. Several mitigation factors, such as power control, channel assignment and AES-128 encryption were applied for secure life-logging. Finally, research into the degradation of the consumed energy regarding the described intrusions is presented.

Keywords: Smart Objects; Internet of Things; Life-logging; Security; Smart Environment; GNUradio

1. Introduction

In an interconnected smart world humans and devices interact with each other, establishing a smart environment in which the exchange of data and decisions is continuous. Smart devices and in general the *Internet of Things* (IoT) are considered to be one of the key elements of the 21st century. The Internet has given us the opportunity to enhance aspects of everyday life using computers, smart phones, social networks, etc. A Smart Environment can be considered as a digital ecosystem consisting of two layers: (i) the first one is the reality, involving communications between people, daily duties or entertainment; (ii) the second layer is the virtual life, in which humans and objects are interconnected to a local network (or the Internet) and their communication is achieved through various collaborating technologies offering seamless connectivity. Decisions are taken by programmed devices or by users who have the capability to monitor, manage, adjust and interact with their automated smart environment.

The term *smart object* refers to small ubiquitous devices, such as sensors, actuators, RFID tags, smart phones and embedded systems or any other type of objects that are equipped with "intelligence". With the exception of modern smart phones, most smart objects have limited resources in terms of processing or computational power, available memory, storage, networking capabilities, routing and energy. Furthermore, most devices are incompatible with standard networking protocols, which makes them susceptible to a number of security threats. Finally, smart objects are able to be internetworked with other devices, using either the IP or other non IP protocols.

One of the greatest challenges for future networks is the ability of smart objects to get connected to a local network or the Internet under the IoT domain. The idea is transparent but faces many unresolved issues due to the different technologies of smart objects which try to interact with almost incompatible, but well-established networking technologies. One of the most important topics for the IoT is the need for connectivity with other networks and devices. The need to assign IP addresses in each of these devices is mandatory for many researchers and companies. IPSO alliance [3] has made a great effort to specify the rules and the prerequisites for advocating the use of IP networked devices. However, the limited resources of smart objects due to their design and tiny size makes it difficult to adopt well known protocols such as the TCP/IP.

In the IoT domain, users have the potential of connecting their life with objects physically or virtually. As a result, users have the chance to use, monitor and manage smart devices and

☆This submission is an extended version of our conference papers "Life-logging in Smart Environments: Challenges and Security Threats" which appeared in the IEEE ICC-WS Conwire 2012 [1] and "An Experimental Investigation on Energy Consumption for Secure Life-logging in Smart Environments" which appeared in the 17th IEEE Camad 2012 [2] and has been invited for the ISTR journal publication.

communicate with other people or objects. The act of recording everyday life of people, their personal information and data and the process of exchanging this information with others throughout a network introduces the term of *life-logging*. Although the term sounds new, it has been used since the old days, when people used to keep data and records about their lives' experiences and manage them effectively. The life-logging procedure can be separated into a two-phase approach in which the first is the recording of personal data from devices (i.e. sensors and actuators) and the second is their uploading onto a virtual space such as a social network.

Life-logging in smart environments faces several challenges, with security being the most critical one. There are several security issues regarding life-logging in an interconnected smart world due to the lack of efficient security standards for smart objects. Just as real-life networks encounter challenges in security, privacy and trust, the same can occur in a smart environment. Life-logging creates the possibility of disclosing things about someone's life that should not be revealed. Security risks arise because of the lack of suitable security protocols in smart devices. Smart objects have many security vulnerabilities caused by their limited resources for supporting well-established cryptography and security algorithms. In an insufficient security environment new lightweight approaches should be considered in order to overcome the lack of trust and privacy, thereby avoiding security dangers.

The issue of energy consumption for securing smart object such as wireless sensor networks (WSN) is an open challenge which has been discussed in bibliography in works such as [4, 5]. Experimental investigations concerning the energy consumption of WSN have been made on [6, 7]. Theoretical analysis and simulation results for mitigating mechanisms to detect jam attacks in wireless sensors networks are presented in [8, 9]. Moreover, experiments for intrusion detection of jamming attacks and passive listening in 802.11 using software defined radios, are described in [10, 11, 12]. Finally, channel assignment based on energy detection and received signal strength in wireless networks are presented in [13]. The decrease of energy due to the security protocols and the attempt to mitigate attacks from eavesdroppers, passive listeners and denial of services such as jamming attacks are critical points for research. To our best of our knowledge, the contribution of this research advances the state of the art by the development of an experimental test-bed including all the previous different described research areas. The setup consists of two users interconnected with their smart devices and one smart attacker, a software defined radios (SDR), whose main objective is to break any security wall on the communication channel either as a passive listener or as a jammer. The investigation due to different security threats, need different types of mitigation techniques such as channel assignment, power control and encryption.

The remainder of this paper is organized as follows. In Section 2 we present the factors of life-logging in a smart environment in which life-logging is applied to different technologies of smart objects to the IoT. In Section 3 we discuss the security challenges and vulnerabilities of life-logging in a smart environment and we analyze the security challenges due to energy constraints of smart objects In Section 4 we suggest a lightweight framework consisting of the most important pillars to overcome the described security challenges. In Section 5 we present the experimental setup containing the communication model of users, the attack model and the test-bed description. In Section 6 we describe different experimental scenarios to measure and compare the energy consumption of life-logging in smart environments concerning different security threats. We conclude this paper in Section 7.

2. Life-logging in smart environments and the Internet of Things

In a modern ecosystem devices, buildings and people have the potential to create a smart environment using internal and external interfaces of various technologies. The importance of smart infrastructure in the context of smart cities has attracted several companies to develop initiatives such as the IBM's vision of Smart Planet [14] and the Smart+Connected Communities of Cisco [15]. The structure of smart environments consists of three basic ingredients: (i) smart objects that interact with the environment, (ii) the interconnection of smart objects with the network; either the traditional Internet or the IoT, and (iii) the procedure of life-logging in this interconnected smart environment. The structure of the described smart ecosystem is depicted in Figure 1, consisting of a network infrastructure layer, an object ecosystem layer and an overlay layer.

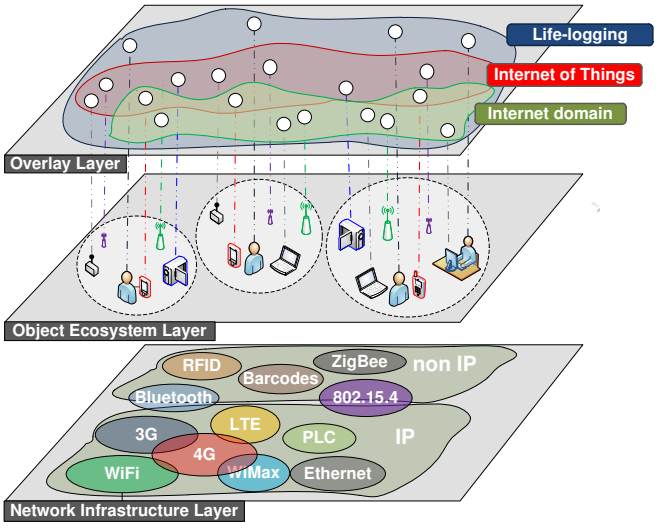

Figure 1: A life-logging smart ecosystem

2.1. Smart objects

The term *smart objects* was introduced for the first time by Neil Gershefelds in his article *When Things Start to Think* [16]. Their primary characteristics have been described as their unique identity and their capability of communicating with other objects and detecting the nature of the environment. Smart objects are small communication devices with micro-electronic components, low-power radio, limited energy

resources and a tiny microprocessor. Smart devices encompass innovations such as intelligent tags (RFID), sensors that measure physical quantities and convert them into analog or digital signals (temperature, pollution, motions), actuators that control equipment and embedded devices that perform specific functions [17]. Furthermore, smart objects can be combined with mobile devices such as laptops, PDAs, mobile phones or smartphones, as well as Bluetooth devices. In the Future Internet different wireless technologies (WiFi, 3G/4G, 802.15.4, RFID etc) or wired ones (ethernet, PLC) might interact and create a machine to machine ecosystem.

The most common communication technologies and protocols of smart objects transmit on the unlicensed spectrum. *Bluetooth* (IEEE 802.15.1) is a standard normally used in mobile phones, in hands-free headsets for transferring data or as a replacement of IrDA on remote controls. However, IrDA hardware is still less expensive and does not share the same security problems encountered with wireless technologies such as Bluetooth. *Wireless sensors* use the IEEE 802.15.4 protocol, which characterizes the Low Rate Wireless Personal Area Network (LR WPAN). ZigBee is an extension of 802.15.4 supported by ZigBee Alliance [18], which enables the connectivity of the devices in a mesh network architecture and is able to support thousands of sensors, in comparison to the normal IP-based protocols, which have a limited range. Low power IEEE 802.11 uses chips that are optimized for low power consumption, especially when the device is on standby mode. Powerline Communication (PLC) systems (IEEE 1901) exploit conductors used for electric power transmission for data transmission. Radio-frequency identification (RFID) technology includes a small RF transmitter and receiver, that usually operate at a low frequency and are mainly used for identifying or tracking objects [19].

There are two basic categories: the IP-based and the non IP-based objects. The IP based objects normally have high capabilities and are able to connect to the Internet by running operating systems and they only have energy and memory constraints for supporting the TCP/IP protocol. Sensors have natural limitations such as limited energy resources, low memory and processing capability, which make them difficult to provide full IP protocol stack support. For that reason, suitable OSs have been developed for tiny embedded systems and sensors with limited requirements such as Contiki, TinyOS and FreeRTOS [20, 21, 22, 23]. For the connectivity and communication of non-IP objects, protocols, such as ZigBee [18] have been developed for short-range low-power and low bit-rate radios and sensors. Non IP-based devices such as RFID tags can be: (i) passive, which do not incorporate a power supply, because the electrical power induced by the reader is enough to transmit data, or (ii) active, which use their own battery for data transmissions [24]. The main disadvantage of the non IP-based sensors is the lack of network connectivity without the need of gateways

2.2. Interconnecting smart objects with the Internet of Things

One of the most important pillars of Future Networks is the *Internet of Things* (IoT), which has attracted many supporters in the research community and industry. The European Commission has made a deal of great effort to fund project proposals, especially in the 7th Framework Programme, related to the IoT and Future Networks [25]. The term *IoT* was coined in 1999 by Kevin Ashton [26] with the vision of interconnecting previously unconnected and isolated objects to the Internet. The IoT has the potential to be incorporated into the network devices with minimal capabilities like smart objects. Moreover, the IoT aims to connect not only things but also networks as well, creating "networks of networks". For instance, such a network of networks could be a small sensor network connected with wireless access points managed by a mobile smart-phone. Collected data can be added to a database, in which remote devices may interact. IoT is able to interconnect wireless sensor networks, telemetry, embedded systems, mobile telephony, computer networking, mobile computing and ubiquitous computing [20]. There are two ways for a node to be attached to an IoT network: (i) by using a IoT gateway and (ii) by direct contact with other smart objects, using a communication interface such as ZigBee.

The three most important characteristics of IoT are: (i) the ability to instrument ordinary objects with a chip and a communication device, (ii) the interconnection capability, and (iii) a way to provide intelligent services. One critical challenge is to combine heterogeneous IP or non IP-based objects under the same network and connect them to the global Internet. The Internet Engineering Task Force (IETF) [27] and the IPSO Alliance [3] with the support of companies such as Cisco, Ericsson, Oracle, Intel, Google and Motorola, aim to standardize IP (and more specifically IPv6) for embedded systems in order to homogenize heterogeneous smart objects. The incompatibility between smart devices and their supported technologies, especially in different layers, leads to difficulties in their collaboration, as well as in their secure and trustworthy interdependence with their environment and logged in followers.

2.3. Life-logging

The main concept of *life-logging* improves the way people record and exchange their data, communicate with others and log into applications or devices. Since ancient times, people used to keep records of their everyday life and their personal activities within a community. Calendars, books, diaries, letters and paintings can be added to the catalogue of life-logging devices. Over the last century new forms of life-logging data were added to the above list such as photos, sounds and videos. Especially in the '80s decade, the broad propagation of personal computers gave humans the opportunity to keep records and personalize their environment to bring interfaces closer to their personal preferences, accounts and applications. At the end of the '90s decade and the begin of 21st century, especially with the widespread adoption of the Internet, personal data such as email accounts, gaming data, login accounts, favorite web pages, documents, digital photo albums, online web services and applications were stored in personal devices. In the 21st century, social networks have attracted a great number of users keen to be life-logged (Figure 2).

Figure 2: Life-logging in history

The increasing amount of life-logged data and the need to integrate it has been one of the main issues of IoT in the last decade. Authors in [28] analyzed in 2004 the usage of life-logging activities for different applications and media such as sending and receiving emails, TV programs, GPS records, visited web pages and photographs, focusing on the problem of combining life-log activities from different media types. A few years ago, someone could have only a couple of network-connected devices compared to today and the near future when each person will have access to and control quite more network-connected devices. The need to connect, manage and interact with a plethora of devices means having a life-account in which it is possible to connect to different applications and accounts. Social networks have attracted a great number of computer-connected users who share similar concerns, ideas, personal moments, photos, achievements, news and data. One step further is the possibility of managing these data in a centralized or a distributed base by interacting with the smart environment. There are a number of examples of life-logging on smart devices such as the use of smart phones to check emails, the key to unlock your car, the device to open your garage door or a RFID card needed to enter the entrance of an office or lab.

A life-logging experience of interacting with devices is a daily issue for a variety of people. The scenario of [29], in which a runner with a heart rate sensor and a pedometer, records his data and transfer them through his WiFi-connected iPod to a web database in which his friend have access, is not a future scenario but is already reality. The increasing use and need for personal smart devices such as sensors and actuators indoor or outdoor create the need to develop applications with which a user may interact under the prism of the IoT. Whereas a couple of years ago smart phones were not affordable for many people, they now have a widespread penetration into the market with a variety of developed applications with interconnected capabilities in different environments. A very interesting framework platform for Android phones has been developed by Google under the Tungsten Project with the name *Android at Home* [30] in which IoT is applied for allowing individual users to log into their accounts and control their smart objects at home. Google's next challenge is the addition of "Android at Home" in Google Plus where life-logging in social networks will fulfill the intersection with smart objects and the IoT.

3. Security threats in smart environments

Security is assumed to be one of the key issues of smart environments. Not only is it critical for the connected devices and users but it is also dangerous for the gateways that are connected to them. The issue for security and emergency response in mission critical communications and infrastructure is always an important topic especially for mobile ad-hoc networks [31, 32]. In addition, military applications, factories and industries, bridges, medical and health and environmental applications are some examples where security threats should be taken into consideration. Moreover, the widespread use of smart objects in the home environment endangers disclosing private data. For instance, a wireless installed camera, for recording possible intruders, connected to an insecure home network could be a susceptible threat to disclose the private actions of a family. The fast growth of life-logging applications and the potential for integrating them into smart environments mandated that security issues need to be addressed. Secure and trustworthy life-logging in smart environments involves challenges, risks and threats on the communication layer under the IoT and finally on the end-users who log on and interchange data with their smart objects.

The general concept of CIA triad (Confidentiality, Integrity and Availability) supported by [20] and [33] can be applied successfully for the security of smart environments. *Confidentiality* focuses on keeping information private by encrypting it or ensuring that only the right people will have access to it. *Integrity* confirms that data has not been modified. Integrity is achieved by the use of Message Integrity Codes (MICs) or Message Authentication Codes (MACs). Finally, *availability*, guarantees that information is available when it is needed.

3.1. Security vulnerabilities and attacks in smart objects and the IoT

Smart objects, particularly sensor networks, are vulnerable by their very nature because of the lack of security support in the primary design of low lossy networks. Their previous status did not face the need to ensure secure transmissions. Information about measurements such as temperature and humidity is not so attractive for attackers. Nevertheless, the rapid growth of system automation, the massive production of sensors and smart devices and their integration in the smart environments reveal security deficits and raises possible threats from malicious users. Security add-on features in an insecure design cannot replace the capabilities of a securely designed network. Moreover, the limited resources of smart objects in terms of memory, CPU and energy make the inclusion of add-on security features even harder.

Security threats on smart objects do not vary much compared to normal wireless or wired networks. The main difference is that suitable security mechanisms are absent because of the lack of respective architectures and resources. The adversary model of life-logging involves stealing personal data, impersonating or launching DoS attacks. This model exists all over the Internet, irrespectively of the connection technology. Since smart objects are usually equipped with one wireless communication radio, respective security challenges are mostly compared to the wireless networks. Such security challenges exist in all different layers of OSI model [34] but the main difference of wireless networks to the wired ones is the medium. At the physical layer the most critical dangers involve eavesdropping, impersonating

in a secure or insecure communication channel and jamming attacks [33].

Security and privacy are critical points in sensors and actuators. A malicious node can easily intercept transmitted information or impersonate a receiver. Furthermore, privacy seems to be quite challenging because of the inability of the sensors to anticipate and sense possible eavesdroppers. If the messages exchanged between the nodes have a MIC in the headers and payload, it is impossible for an attacker to launch a successful impersonation attack but it is possible to become a passive listener or launch Denial of Service (DoS) attack. On the other hand, if the payload message is encrypted then a malicious node that has the encryption key can launch an impersonation attack but not to become a passive listener. The disclosure of sensitive information about the location, track and identity of a user may cause significant problems for him and his interconnected network and users.

Authentication is a very important issue that is missing in many objects. Trusted Platform Computing (TPM) implemented in laptops is difficult to be applied because of the lack of suitable cryptographic algorithms developed for lightweight smart devices. Moreover, lack of authentication, encryption or integrity on the interconnected objects raises serious considerations. The Transport Layer Security (TLS) protocol and the Secure Socket Layer (SSL) protocol appear to be efficient cryptographic solutions but they cannot be easily applied because of the resource-constraints of the smart objects. The low processing mechanisms for data mining and services capable for authenticity, confidentiality and privacy of devices raise security issues and threats for revealing sensitive information to insecure devices and storages.

Low networking capabilities in bandwidth, throughput and data rate along with the minimal computation power for real time aggregations and buffering, which are needed for secure networking, make the smart objects susceptible to attacks at the network layer. At the MAC layer security issues occur due to collisions and channel occupations, which may disable transmission opportunities for some users, exhausting the batteries of the devices in parallel. At the physical layer jamming, DoS, traffic analysis, injection and tampering are very serious security threats for smart objects. Especially, the inability of many objects to acquire IP addresses makes them vulnerable to attacks (such as DoS) that in powerful IP hardware devices, running efficient security protocols, can be avoided successfully.

Finally, the *topology* in a IoT multi-hop and multi-route domain is completely different that in the traditional Internet where service providers route and manage the traffic, avoiding malicious attacks and securing not only specific computers but also the whole network. These issues seem to be challenging for the IoT domains where there is no central control of the networks. The lack of IP for a number of smart objects raises security issues on the routing protocols where black holes, spoofing, forwarding and sinkholes attacks are launched.

3.2. Security challenges due to limited resources and energy constraints of smart objects

The tiny capabilities of smart objects in terms of computational power, memory and energy create difficulties in applying well-established security protocols. Smart objects and sensors are vulnerable to attacks because of the lack of security support in the primary design of low lossy networks. The most critical factor for secure communication between smart objects is the required energy. Mechanisms for mitigating security threats result in consuming more energy form their already limited energy resources. Nevertheless, if no security encryption exists, a malicious node can easily intercept transmitted information or impersonate a receiver. Furthermore, privacy seems to be challenging because of the smart objects' weakness to anticipate and sense possible listeners. However, the use of AES-128 (Advanced Encryption Standard) link-layer security mechanism of IEEE 802.15.4 seems to have lightweight properties but the necessary time to encrypt and decrypt interchanging messages increases significantly the energy consumption. The encryption algorithm used in 802.15.4 is AES with a 128b key length (16 Bytes). Moreover AES algorithm is not only used to encrypt the information but to validate the sent data. This concept is called Data Integrity and it is achieved using a MIC (or a MAC) which is appended to the message. This code ensures the integrity of the MAC header and the attached payload data. On the other hand, jamming attacks can be detected using suitable algorithms based on dropped packets or the decrease of the signal to noise ratio [35]. In order to mitigate such attacks, two possible solutions may be applied: (i) an increase in the power level or (ii) a channel assignment procedure as described in [36]. The use of both mitigating factors severely affects the energy consumed in smart objects, as will be described extensively in the next sections.

3.3. Risks and security issues of life-logging

The trend of life-logging encounters a number of security issues which need to be resolved in order to step forward into the interconnected world and the Future Internet. To highlight the benefits and the risks of life-logging, authors in [32] present a future scenario in which they detail benefits, challenges, risks and threats of life-logging in real life. The scenario occurs in 3-5 years from now when the members of a family live in an integrated smart world in which life and objects have acquired a stable and tailored relationship. Several possible risks and threats are depicted in this scenario involving life-logging in a variety of activities, services and devices. Social networking, as a part of their lifestyle and as a tool for socializing or for work, has substantially enhanced the virtual reality in a cyber space world.

There are several security threats that could arise from life-logging in the Internet. Authors in [37] address the most common life-logging security and privacy risks, including: (i) the surveillance of someone's life, (ii) memory hazards, meaning that mistakes in life can not be forgotten easily, (iii) long term availability of personal information, even if his life and ideology has changed, and (iv) the problem of stolen life-log information. Moreover, the danger of a lost password or a stolen

one, is believed to be one of the most serious threats for most people. Such an incident could enable an attacker to gain access to a person's accounts, starting from his social networking profile or emails, up to his bank account.

Life-logging from a computer or a laptop on to the Internet differs from life-logging in a smart environment because of the unsolved security threats which occur in the unsafe smart environments. Secure life-logging in smart environments is relatively straightforward compared to the security of smart objects and the IoT. As discussed in previously, there are many vulnerabilities in a heterogeneous ecosystem in which every device faces different challenges in security and privacy. The discrepancy between technologies and the attempt to interconnect them have brought new security challenges and gaps which need to be filled.

4. Defining a lightweight framework

The increasing trend for the addition of life-logging applications into the smart environment and the discussed security threats require efficient countermeasures to ensure security, privacy and trustworthiness in life-logging applications. The key way to overcome these constraints is the development of a lightweight framework for ensuring security, privacy and trustworthy life-logging in smart environments. We describe the basic pillars of this framework including the use of lightweight versions of IP protocols, privacy by design and cryptography.

4.1. Lightweight IP protocols for securing smart objects

Security threats in life-logging under a smart environment and the IoT occur mainly because of the lack of suitable security protocols. Considering smart objects' limited capabilities, proper algorithms and techniques need to be implemented in order to achieve maximum security and privacy. The IPSO Alliance advocates the use of the IP protocol for establishing a secure exchange of data. In order to achieve security in smart objects, the IPv6 over Low power Wireless Personal Area Networks (6lowPAN) protocol is proposed [38]. Smart objects are able to connect throughout the lightweight 6lowPan protocol which gains its advantage from the use of AES-128 link-layer security mechanism of IEEE 802.15.4. However, the IP fragmentation allows the use of available buffer from malicious users to send large or invalid packets. Even if in the transport layer 6lowPAN is shown to have efficiency, in the network layer, Internet Protocol Security (IPsec) and Secure Neighbor Discovery (SEND) appear to be more suitable to attain network security in IPv6 [39]. Authors in [40] suggest a security adaptation layer to overcome security issues when connecting the IoT network to the Internet. The adaptation layer is based on one similar to the 6lowPAN concept or IPv6 in which gateways connected to different domains are able to translate standard IP security protocols to domain-specific protocols variants.

4.2. Lightweight design for ensuring privacy

Privacy is a major concept of life-logging especially in insecure smart environments in which a variety of data from users and devices are exchanged and collected. The massive production and transfer of sensitive data such as personal photos, messages and videos encounter the danger of disclosure. In order to ensure privacy on smart environments the principles of privacy should be applied in a lightweight privacy by design approach. The basic principles for ensuring privacy in smart environments of life-logging are detailed in [41]:

- *Openness* is established when recorded data are transparent and no secret data are stored.
- *Participation of Individuals* ensures that records are available to them.
- *Limits of Recorded and Appropriate Data* have to be assigned for specific applications.
- *Data Quality* of recorded data should be related and accurate to the application.
- *Limits of Use* indicates that records should be used only by authorized users and for an assessed purpose.
- Personal data should be *Secured Appropriately* on storage devices.
- *Accountability* of record keepers has to be ensured.
- The last principle which should be emphasized is *Awareness* from the user point of view.

Since privacy is not a convenient issue to be resolved, especially in smart environments, the principles of privacy should be implemented under an international framework and standards. Smart environments (more precisely the IoT) should be designed under the concept of Privacy by Design (PbD) defined by Ann Cavoukia [42] who suggested that privacy should be embedded into the design of technologies ensuring privacy and control over one's information and not solely by compliance with regulatory frameworks.

4.3. Lightweight cryptography for trustworthy life-logging in smart environments

Cryptography is considered as a key element for trustworthy transactions in smart environments. One of the most important issues in life-logging is the users' authentication and their devices connected to the IoT. For establishing authentication and authorization in the IoT the use of Lightweight Cryptography (LWC) is crucial. The LWC algorithms and protocols have been designed especially for constrained environments where the resources are limited such as in RFIDs, Sensors, tags, smart cards etc. Based on [43], the proposed lightweight cryptography is supported for two main reasons: for the efficiency of end-to-end communication and for the applicability to lower resource devices. Constraints of low resource devices, such as battery limitations and narrow computation power, require lightweight symmetric key cryptography to decrease power consumption of devices. Moreover, the footprint of LWC primitives is smaller compared to the conventional ones. Even though it is possible

for some nodes to store footprints in memory and run cryptographic algorithms, it is crucial the low-power and low-cost devices to embed applications instead of hardware circuitry because of the limited resources of smart objects. Symmetric and asymmetric key cryptography can apply lightweight properties for trustworthy life-logging in the IoT.

Symmetric Key Cryptography can be separated into three categories: (i) block ciphers, (ii) stream ciphers and (iii) hash functions. Block ciphers with lightweight properties have been proposed for AES and Data Encryption Standard (DES) such as CLEFIA [44] and PRESENT [45]. Stream cipher algorithms with lightweight properties have been proposed and developed in the ECTRYP II eSTREAM portfolio [46]. The hash algorithm SHA-3 [47] do not satisfy lightweight requirements. Lightweight hash functions are possible to construct based on lightweight block ciphers.

Asymmetric Key Cryptography is difficult to be implemented because the amount of data for public key cryptography in smart objects is much larger than in symmetric key cryptography. Efficient security such as Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC) cannot be implemented efficiently in smart objects because of the limitations for storing additional footprints. ECC is more likely to be implemented because of its smaller operand lengths and relatively lower computational requirements [48]. Nevertheless, it is possible to implement public key cryptography in smart environments but it is difficult to execute in reasonable time.

Considering the major need for authentication and authorization for users and devices in smart environments, cryptography will always be a challenge. Well-established or new algorithms may well have to be implemented efficiently in order to overcome the limitations of smart objects with lightweight capabilities. However, as strong as the cryptographic algorithms are, they will never get over the vulnerability of an insecure or inexpert user with a lack of basic security and privacy precautions.

5. Experimental investigations on energy consumption for secure life-logging

To investigate the impact of security attacks on energy consumption, an experimental test-bed was developed. The topology of the model consists of three users: (i) Bob, (ii) Alice and (iii) Eve. Bob and Alice are interconnected each with a smart device. The life-logging procedure is applied to their communication in which they share data, personal preferences and habits. The transmitted information may be sensitive, like security codes or personal data and secrets. Under this communication model, an attacker (Eve) appears to have as main target to break any available security wall and steal users' personal data or destroy the communication.

5.1. Test-bed description

The test-bed contains three users each one equipped with a smart device. Bob and Alice are connected each with a Digi XBee Pro 802.15.4 device [49]. Both devices are connected (through their serial cable) with Matlab 2011b on a Windows XP management server. Suitable algorithms have been developed in order to satisfy the communication model. To measure the energy consumption of XBee a True-RMS polymeter with USB output was used for storing the current measurements of each experiment connected serially with Matlab as well. Eve is a malicious user which acts as an eavesdropper or as an attacker. This node is emulated with a Universal Software Radio Peripheral (USRP2) device from Ettus Research LLC [50] holding a XCVR2450 Dual-band Transceiver interchangeable daughterboard module that serves as the RF front end. The GNU Radio 3.3 software is installed for creating complex software-defined radio systems [51]. The GNU Radio software is installed on a Ubuntu 11.04 which manages the attack node. The IEEE 802.15.4 PHY implementation as well as UCLA Zigbee [52] GNU Radio extension was installed to capture and decode 802.15.4 messages. Jamming attacks are implemented using GNU Radio signal generator. Finally, the attacker model algorithms were implemented by the use of shell scripts. The described test-bed topology is depicted in Figure 3.

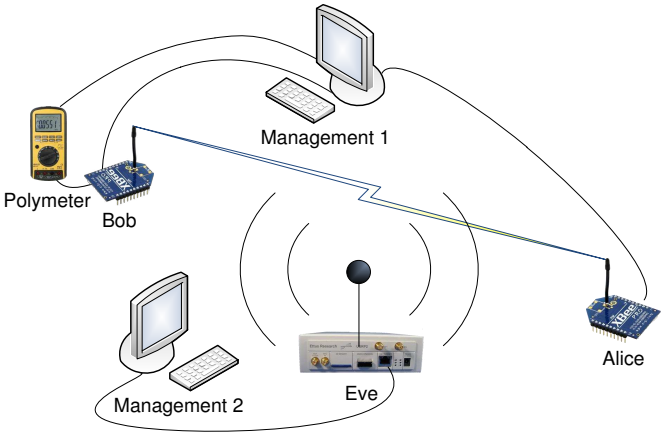

Figure 3: Test-bed topology

5.2. Energy consumption calculator

The experimental approach of this investigation has as a main object to measure the energy consumption of smart objects. For that reason, an application in Matlab was developed for real time energy consumption measurements. The polymeter device, serially connected with the computer and the Matlab, measures the electric current of connected devices, such as XBee modules. The developed tool is generic enough so that it can be used for a variety of consumed energy experiments and not only for the current one. It can plot (at real-time) four different kinds of measurements such as the electric current (in Ambere), the consumed power (in Watt), the consumed energy (in Watt-Hour) and the total sum of consumed energy (in Watt-Hour). One of the key features used to evaluate the described experiments, is its capability to record measured data for plotting them later. The described tool is depicted in Figure 4.

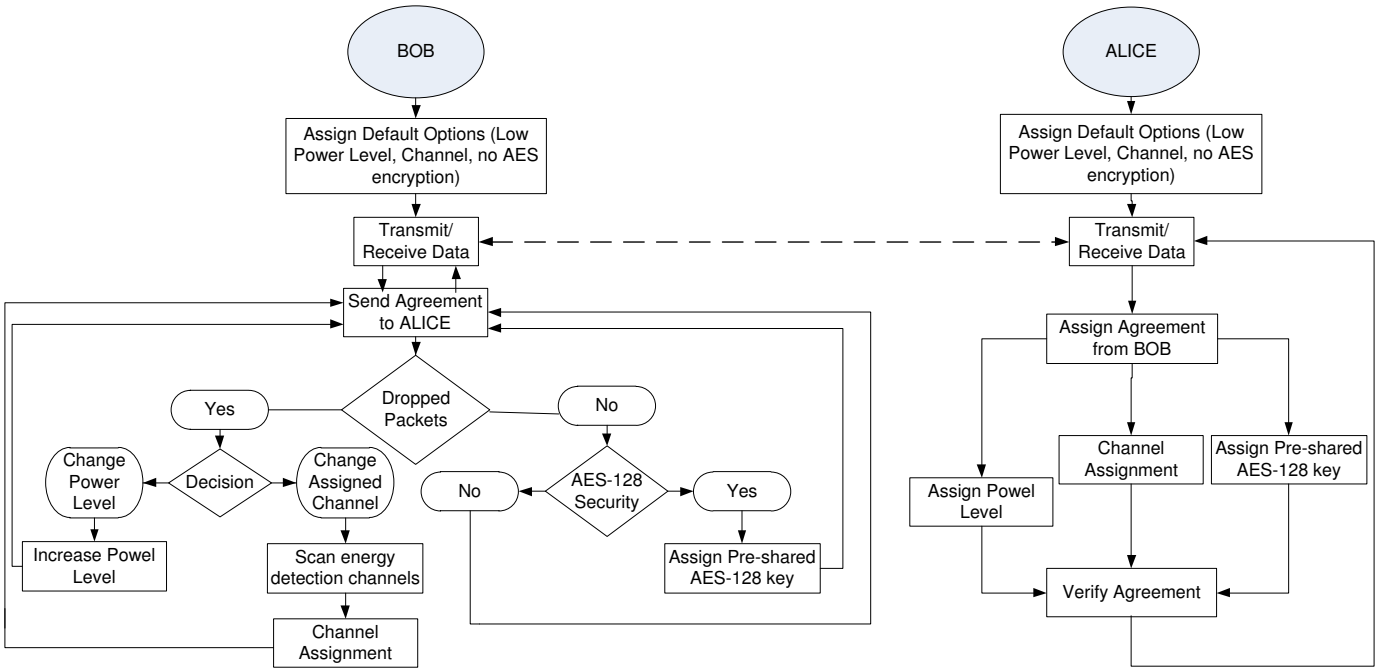

Figure 5: The communication flowchart model

Figure 4: Consumed energy calculator

5.3. Communication model

The main concept of this model focuses on mitigating security threats and attacks. In the specific model Bob acts as the coordinator and Alice as the end-user. In the first phase of the process, Bob and Alice assign the default identical options in power level and transmission channel without any security in order to consume the minimum amount of energy. When they start to interchange messages, if they anticipate dropped packets, they increase the power level to mitigate the issue. Power level cannot totally solve the problem if an attacker applies severe jamming attacks or if the channel is occupied by another transmission. For that reason Bob applies an energy detection scan to detect the most energy-free channel, informing Alice about the new channel. If an attacker exists, then he may identify the new communication channel, starting to jam the new channel. Bob will continue to apply energy detection techniques every time there are dropped packets until the users interchange the number of data they have to. This procedure incorporates the danger of disclosing personal data if there is no security on their transmission if an eavesdropper exists. Bob, being the coordinator, decides to enable the AES encryption on their data. So he requests Alice to enable the security option decrypting their messages with a pre-shared AES-128 key. The necessary computational power to decrypt and encrypt messages delay the procedure therefore the time to exchange the same number of messages is greater, increasing the required amount of energy. If the attacker cannot decode the messages, he will again start to apply jamming attacks causing dropped packets. Power level and channel assignment procedures will have to be followed again in order to mitigate the attack. These communication model scenarios, as described, are presented in Figure 5.

5.4. Attacker model

One of the most important parts of this investigation is based on a smart attacker. The main concept of the attacker is to break any security constraints of the communication between Alice and Bob. The first step is to identify the transmission channel. For that reason the 802.15.4 PHY multi-channel implementation was used. Under this procedure the attacker (Eve) scans the available channels until she finds the specific transmitted channel. The next step is to try to decode the transmitted 802.15.4 packets. Two possible scenarios may happen. The first is when

the communication between the users is without any AES-128 encryption, so the attacker is able to decode encrypted messages. The second case is when Bob and Alice share a predefined AES key. In this scenario if the attacker has stolen the shared key, she is able to decode the messages. If she does not hold the key, she can destroy the transmission by applying a jamming attack on the specific channel. When Bob and Alice anticipate a jamming attack, they change channel. In this case the attacker applies a multi-channel scan until she finds the transmitted channel. Finally, a malicious person can always apply jamming attacks independently whether there is encryption or not. Figure 6 depicts the flowchart model of the attacker.

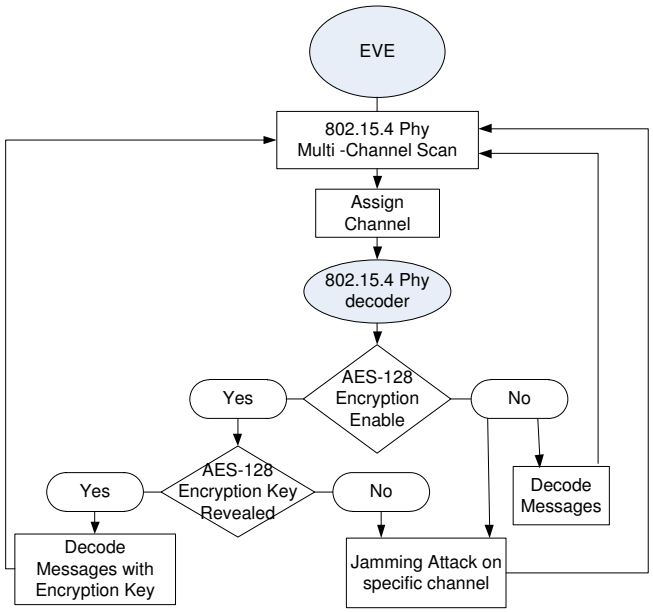

Figure 6: The attacker flowchart model

6. Performance evaluation

In this section the results from real experiments analyzing the security risks and emphasizing the energy consumption are presented. Different scenarios are presented in which the energy consumption is measured. The main concept involves the exchange of information and data between Alice and Bob either insecure or secure. The case in which a smart attacker (Eve) tries to steal exchanging data or to destroy the traffic, is investigated. Three different scenarios are presented to prove the vulnerabilities based on the energy consumption of different attack models. The maximum packet size in IEEE 802.15.4 standard (including the frame overhead which is 25 bytes) is 127 bytes or 102 bytes maximum data length [53]. Therefore, in the following experiments Bob sends to Alice 1000 packets of 102 bytes data length. The polymeter stores electric current and these values are used as the main measurements for this investigation. The power consumption is measured in watts (1) and in watt-hour (2).

$$P = VI. \tag{1}$$

$$WH = \int_0^t VIdt = \sum_{i=1}^{n} \frac{1}{2}(V_i I_i + V_{i-1} I_{i-1})(t_i - t_{i-1}). \tag{2}$$

Where P is the consumed electric power in Watts, WH is the consumed electric power Watt-Hour, V is the Voltage, I is the consumed Current and t is the time.

6.1. Transmission without attack

The first phase of this scenario includes the communication between Bob and Alice without any security encryption focusing on the power consumption on different power levels for each smart device. Bob transmits a packet to Alice who returns it back. The counter calculates the number of transmitted packets over the received ones. When there are dropped packets due to the distance of the users, the power level is increased. When there is a successful transmission Bob sends a new message to Alice. This scenario is applied to show the basic communication model. Under this model Eve is able to decode the exchanged messages as was described in the previous section by using the 802.15.4 PHY extension. Even if the users spend the minimum of the energy on this experiment the communication involves many security and privacy issues. Under this scenario an energy consumption investigation was carried out, measuring the different power levels of the modules.

The second phase of this scenario occurs when Alice and Bob become aware of the security level of their communication. They decide to decode their messages using AES-128 encryption. The result of exchanging information with AES encryption is the delay of transmitted data. This can be explained because of the limited computational power of XBee to encode and decode messages. The comparison of Figure 7a and 7b shows that the required time to transmit the same number of packets is 36% greater when AES encryption is enabled.

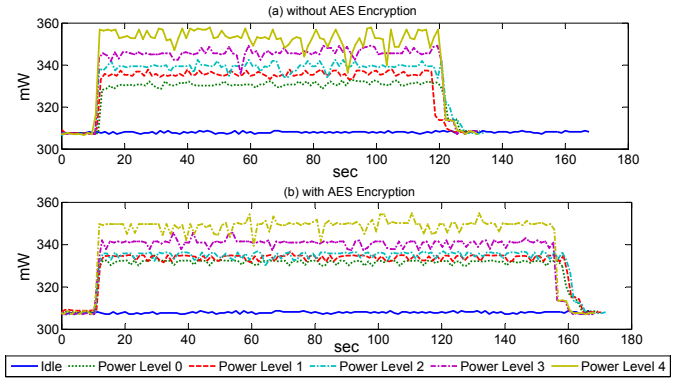

Figure 7: Energy consumption for different power levels (a) without AES encryption and (b) with AES encryption

6.2. Channel assignment on jamming attack

In the second scenario, the users realize that there are dropped packets in their communication due to the interference caused by external transmissions. This may happen when the channel is occupied or when a jamming attack occurs. Interference is reasonable since the XBee 802.15.4 uses the free band of

2.4GHz which shares the same band as the popular 802.11. The users apply the previously described communication model, in which, when dropped packets are anticipated, an energy detection process for finding the most suitable energy-free channel is executed. The attack model of Eve will observe that there is no transmission on the previously occupied channel but a new channel has been assigned. The next step is to detect the new channel and continue the attacks on the new channel. This loop will continue until Bob and Alice complete the number of packets that they want to transmit.

The second phase on this scenario describes the case in which Alice and Bob exchange messages with AES encryption. Since it is not possible for Eve to listen and decode interchanging messages her efforts focus on destroying the communication link. For this purpose a jamming attack is launched. This phase follows the same procedure as the first phase of this scenario but there is more delay for the transmission of 1000 packets because of the computation time to decrypt and encrypt messages. Figure 8 presents the comparison of energy consumption without and with AES encryption on different power levels.

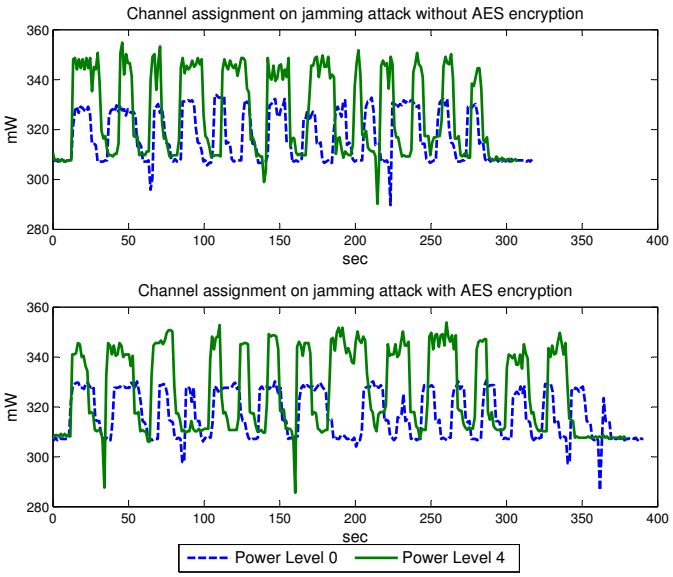

Figure 8: Energy consumption: channel assignment on jamming attack (a) without AES encryption and (b) with AES encryption

6.3. *Power increase and channel assignment on jamming attack*

The third scenario is similar with the previous scenario but the coordinator is able to execute an increment in the power level when there are 10 dropped packets on their devices. If the problem of dropped packets continues, a channel assignment procedure is applied. The gradual increase in the power level and the channel assignment procedure result to higher energy consumption. As the power increases, the energy consumption becomes higher. If the level of power reaches its maximum value, the coordinator applies a channel assignment. When the new channel is assigned, the power level is decreased to its minimum value. In Figure 9 the energy consumption on jamming,

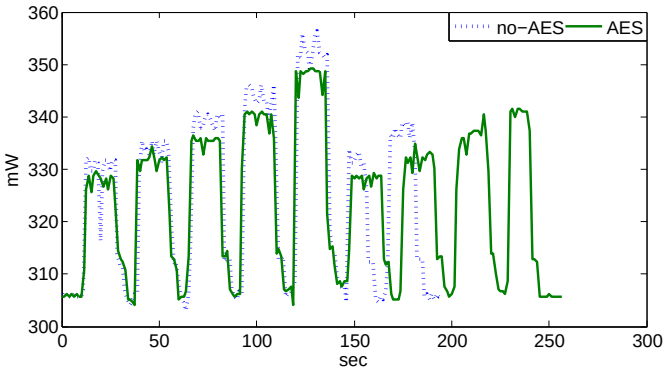

Figure 9: Energy consumption: power increment and channel assignment on jamming attack (a) without AES encryption and (b) with AES encryption

with and without AES encryption, is depicted. The graph shows the gradual increment of power until the nodes reach the maximum power level; so a new channel assignment is occurred decreasing the transmission power level to the minimum level in parallel.

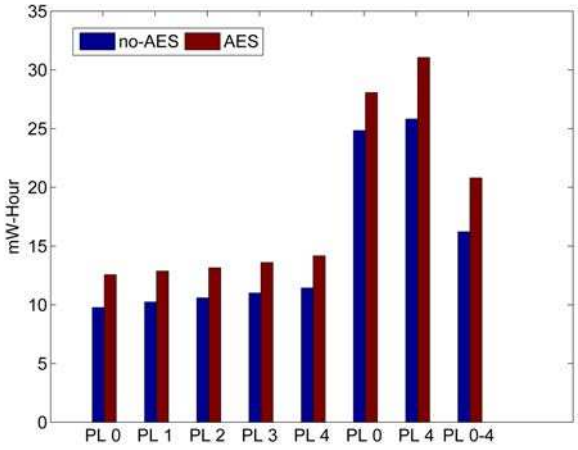

Figure 10: Energy consumption in milliWatt-Hour for different power levels (PL) of the three scenarios

6.4. *A comparison of the experimental results*

A comparison of consumed energy from all the previous scenarios in milliWatt-Hour is presented in Figure 10. For all the scenarios, there is an increment of about 15-30% when AES encryption is enabled compared with the transmission without AES encryption on the same power level and scenario. Moreover, for the first scenario the consumed energy is increased about 4% on each power level rise. For the second scenario, there is a rise of about 10% between minimum and maximum power level when channel assignment is occurred on jamming attacks. As it can be seen from the graph, the maximum consumed energy is needed for the second scenario (maximum power level, AES and channel assignment to mitigate jamming attacks) and the minimum consumed energy is needed for the first scenario (minimum power level, no AES, no jamming attack). The increment of the consumed energy is about 230%.

This final conclusion proves the value of this research concerning the correlation of security in addition with the energy consumption.

6.5. Evaluation of the experiments and future work

The experimental evaluation of this study has shown many valuable conclusions. The limited capabilities of smart devices severely affect the performance of the security framework. Especially the limitation in energy is assumed to be one of the most important issues for the smart objects especially if they run over batteries. The chosen method, measuring the electric current, proved to be the most proper and simpler way to measure the energy consumption. This method includes all the parameters which affect the performance of devices. Single measurements such as monitoring the CPU usage or memory use cannot reflect exactly the total consumed energy of the modules. Therefore, the developed setup was necessary in order to measure the consumed energy.

This research work has proved the prior assumption concerning the impact on energy consumption in smart objects due to different security mechanisms such as power control, encryption and channel assignment to mitigate passive listening and jamming attacks. Even if the experiments were done for specific devices such as XBee Pro, the same architecture can be used in order to measure energy consumption for a variety of different devices which mitigate attacks. The percentage of the effect may vary but the consumed energy will be increased. Nevertheless, the results are relative not only to the assigned parameters but also to the test-bed setup which is affected by the software used, operating systems and algorithms and the attempt to interconnect the plethora of different devices, software and algorithms. Much time was spent in the development of the communication model, the attacker model and the test-bed in order to be able to evaluate real experimental results. However, the development of such a setup will give the potential for further investigation, experiments, using a variety of different devices so as to construct a lightweight, energy efficient framework for secure life-logging in smart environments.

7. Conclusion

In this paper the topic of life-logging in smart environments was presented, giving details about the smart objets and their potential for interconnection in the Internet of Things domain. The plethora of smart objects and their connection with life-logging applications have raised new issues and security threats. Security challenges appear due to the lack of suitable security mechanisms and protocols in the Internet of Things because of the limited resources of smart objects. To overcome considerations in security, privacy and trustworthy life-logging, a lightweight framework was described. Furthermore, an experimental investigation on the energy consumption for secure life-logging in smart environments was described. The growing development of smart devices and their broad use by users has lead to new security challenges including not only security issues but in privacy as well. One of the most important restrictions in securing the communication on these devices is the limited resources. Under these conditions a communication model, an attacker model and an experimental test-bed were developed to investigate the consumed energy under different scenarios. The specifications of the users were defined in order to be able to mitigate eavesdropper's attacks of passive listeners and jamming attacks. The research has shown there is a great influence on the energy consumed to secure such attacks. A smart attacker was designed to break any security walls of such a communication. The conclusions of this investigation have shown weaknesses in this situation, increasing the need to secure life-logging in smart environments while overcoming the energy constraints.

References

[1] Nikolaos E. Petroulakis, Ioannis Askoxylakis, and Theo Tryfonas. Life-logging in Smart Environments: Challenges and Security Threats. In *the 2012 IEEE ICC Workshop on Convergence among Heterogeneous Wireless Systems in Future Internet (ConWire)*, Ottava, Canada, June 2012.

[2] Nikolaos E. Petroulakis, Elias Z. Tragos, and Ioannis G. Askoxylakis. An Experimental Investigation on Energy Consumption for Secure Life-logging in Smart Environments. In *the IEEE International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD)*, Barcelona, Spain, September 2012.

[3] IPSO Alliance. Enabling the Internet of Things, www.ipso-alliance.org, 2011.

[4] E Shi and A Perrig. Designing secure sensor networks. *Wireless Communications, IEEE*, (December):38–43, 2004.

[5] David Boyle and Thomas Newe. Securing wireless sensor networks: security architectures. *Journal of Networks*, 3(1):65–77, 2008.

[6] RSJ Reyes, JC Monje, and MEC Santos. Implementation of Zigbee-based and ISM-based wireless sensor and actuator network with throughput, power and cost comparisons. *WSEAS TRANSACTIONS on COMMUNICATIONS*, 9(7):395–405, 2010.

[7] Javier Alonso and Sergio Gómez. Experimental Measurements of the Power Consumption for Wireless Sensor Networks. *Internal Report UPC, June*, pages 1–14, 2006.

[8] Incheol Shin, Yilin Shen, Ying Xuan, MT Thai, and T Znati. Reactive jamming attacks in multi-radio wireless sensor networks: an efficient mitigating measure by identifying trigger nodes. *FOWANC09*, pages 87–96, 2009.

[9] V. Bhuse, a. Gupta, and a. Al-Fuqaha. Detection of Masquerade Attacks on Wireless Sensor Networks. *2007 IEEE International Conference on Communications*, pages 1142–1147, June 2007.

[10] E Bayraktaroglu, C King, and X Liu. On the Performance of IEEE 802.11 under Jamming. *Infocom/08*, 2008.

[11] Liran Ma, AY Teymorian, and Xiuzhen Cheng. Passive listening and intrusion management in commodity wi-fi networks. *GLOBECOM'07. IEEE*, 2007.

[12] Alexandros G Fragkiadakis, Elias Z Tragos, Theo Tryfonas, and Ioannis G Askoxylakis. Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype. *EURASIP Journal on Wireless Communications and Networking*, 2012(1):73, 2012.

[13] VA Siris and M Delakis. Interference-aware channel assignment in a metropolitan multi-radio wireless mesh network with directional antennas. *Computer Communications*, 2011. Query date: 2012-10-13.

[14] IBM. Smart Planet, http://www.ibm.com/smarterplanet.

[15] Cisco. Smart+connected communities, changing a city, a country, the world, 2010.

[16] N. Gershenfeld. *When Things Start to Think*. Owl Books, 2000.

[17] P. Wetterwald. Promoting the use of IP in networks of Smart Objects. *ETSI M2M Workshop*, 2010.

[18] ZigBee Alliance. www.zigbee.org.

[19] et al. Vasseur, JP. A survey of several low power Link layers for IP Smart Objects. *IPSO Alliance*, 2010.

[20] J.P. Vasseur and A. Dunkels. *Interconnecting Smart Objects with IP: The Next Internet*. Morgan Kaufmann Publishers Inc., 2010.

[21] TinyOS. www.tinyos.net.
[22] FreetOS. www.freertos.org.
[23] Contici-OS. www.contiki-os.org.
[24] R. Tesoriero, J.A. Gallud, M. Lozano, and V.M.R. Penichet. Using active and passive RFID technology to support indoor location-aware systems. *ICCE*, 2008.
[25] Internet of Things and Future Internet Enterprise Systems, http://cordis.europa.eu/fp7/ict/enet/.
[26] K. Ashton. That 'Internet of Things' Thing. *RFID Journal*, 2009.
[27] IETF. The Internet Engineering Task Force, http://www.ietf.org/ .
[28] T. Ushiama and T. Watanabe. A Life-Log Search Model Based on Bayesian Network. *ISMSE*, 2004.
[29] A. Manfred. Security in the Internet of Things. *RFIDsec Asia*, 2010.
[30] P. Wetterwald. Android@home. *Google I/O developer conference*, 2011.
[31] Alexandros G Fragkiadakis, Ioannis G Askoxylakis, Elias Z Tragos, and Christos V Verikoukis. Ubiquitous robust communications for emergency response using multi-operator heterogeneous networks. *EURASIP Journal on Wireless Communications and Networking*, 2011(1):13, 2011.
[32] I. Askoxylakis, I. Brown, P. Dickman, M. Friedewald, K. Irion, E. Kosta, M. Langheinrich, P. McCarthy, D. Osimo, S. Papiotis, A. Pasic, M. Petkovic, B. Price, S. Spiekermann, and D. Wright. TO L0G OR NOT TO L0G ? Risks and benefits of emerging life-logging applications. *ENISA*, 2011.
[33] K. Stammberger, M. Semp, M. B. Anand, and D. Culler. Introduction to Security for Smart Object Networks. *IPSO Alliance*, 2010.
[34] IOS/IEO Commission. Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model. *ISO/IEC*, 1994.
[35] A. Fragkiadakis, V. Siris, and N. Petroulakis. Anomaly-based intrusion detection algorithms for wireless networks. In *the 8th WWIC 2010*, June 2010.
[36] N. Petroulakis, M. Delakis, M. Genetzakis, T. Dionysiou, S. Papadakis, and V.A. Siris. Demonstration of channel assignment in a wireless metropolitan MESH network. In *the 10th IEEE WoWMoM 2009*, June 2009.
[37] R. Rawassizadeh and A M. Tjoa. Securing Shareable Life-logs. *Social Computing (SocialCom),*, 2010.
[38] J. Hui, D. Culler, and S. Chakrabarti. 6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture. *IPSO Alliance*, 2009.
[39] C. E. Caicedo, J.B.D. Joshi, and S. R. Tuladhar. IPv6 Security Challenges. *Computer*, 42(2), February 2009.
[40] R. Hummen, T. Heer, and K. Wehrle. A Security Protocol Adaptation Layer for the IP-based Internet of Things. *Interconnecting Smart Objects with the Internet Workshop*, 2011.
[41] P.A. Nixon, W. Wagealla, and C. English. Security, privacy and trust issues in smart environments. *Smart Environments*, 2004.
[42] A. Cavoukian. Privacy by Design: The 7 Foundational Principles. *http://privacybydesign.ca/*, 2011.
[43] M. Katagi and S. Moriai. Lightweight Cryptography for the Internet of Things. *Sony Corporation*, 2008.
[44] T. Shirai, K. Shibutani, and T. Akishita. The 128-Bit Blockcipher CLEFIA. *FSE*, 2007.
[45] A Bogdanov, L Knudsen, G Leander, and C Paar. PRESENT: An ultra-lightweight block cipher. *Systems-CHES*, 2007.
[46] The eSTREAM Project. http://www.ecrypt.eu.org/stream/, 2008.
[47] A. Regenscheid, J. Kelsey, and S. Paul. Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition. *NIST*, 2009.
[48] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel. A Survey of Lightweight-Cryptography Implementations. *IEEE Design & Test of Computers*, 24(6), November 2007.
[49] Digi XBee Pro. www.digi.com.
[50] Ettus Research. www.ettus.org.
[51] GNU Radio. http://gnuradio.org.
[52] T. Schmid. Gnu radio 802.15. 4 En-and decoding. *UCLA NESL, Los Angeles, CA*, 2005.
[53] LAN/MAN Standards Committee. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Computer Society*, (October), 2003.