An Experimental Investigation on Energy Consumption for Secure Life-logging in Smart Environments

Nikolaos E. Petroulakis, Elias Z. Tragos and Ioannis G. Askoxylakis
Institute of Computer Science, Foundation for Research and Technology-Hellas, Greece
{npetro,etragos,asko}@ics.forth.gr

***Abstract*—In a smart world, smart objects will play an important role giving users the chance for life-logging in smart environments. However, the limitations of smart devices with regard to memory, resources and computation power bring a variety of security challenges and constraints. One of the most important constraints is the consumed energy. In order to investigate the impact on energy consumption due to critical security attacks, an experimental test-bed was developed including two interconnected users and one smart attacker, who attempts to intercept transmitted messages or destroy the communication channel. 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.**

***Index Terms*—Energy Consumption, Smart Objects, Smart Environments, Internet of Things, Life-logging, Security, XBee-Pro, GNUradio, USRP2.**

I. Introduction

As the world becomes an interconnected network in which objects and humans interact, new security challenges and threats appear. The interaction between humans and devices in these smart environments is based on the continuous exchange of data and decisions. Smart devices appeared to be one of the key elements of the 21st century. The Internet has given us the opportunity to enhance aspects of its network such as computers, smart devices, smart phones, people, families and communities. A digital ecosystem has been developed consisting of two layers: (i) the first layer is the reality, involving communication between people, daily duties or entertainment; (ii) the second layer is the virtual life, in which human and objects are connected to a local network (or the Internet), in which communication is achieved through various collaborating technologies offering seamless connectivity.

Although the term ”life-logging” sounds new, it has in fact 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: (i) the acquirement of personal activities from devices such as sensors and actuators; (ii) their execution into a virtual space such as a social network interconnecting with other users. One of the most important issues of life-logging includes the possibility of disclosing information about someone's life, stealing his personal data and invading his privacy. In our previous work [1] we described extensively the challenges and security threats of life-logging in smart environments.

The list of smart objects includes ubiquitous devices like sensors, actuators, RFID tags, smart phones and embedded systems with and without IP. These devices have many constraints compared to high-powered smart phones or computers because of their narrow capabilities in computational power, energy efficiency, storage, memory, networking capabilities, routing and incompatibility with standard protocols, which encounter a number of security issues. One of the most important topics for the Internet of Things (IoT) is the need for connectivity with other networks and devices. The lack of IP connectivity in each of these devices is an inhibiting factor for securing smart environments. IPSO alliance [2] 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 initial design and tiny size makes it difficult to adapt well known protocols such as the TCP/IP.

The depreciation 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. Different security threats need different types of mitigation techniques. In order to investigate the consumed energy due to security threats, an experimental test-bed was developed including two users interconnected with their smart devices, and one smart attacker, whose main objective is to break any security wall on the communication channel either as a passive listener or as a jammer.

The remainder of this paper is organized as follows. In Section II we analyze the security challenges due to energy constraints of smart objects. In Section III we present the communication model of users, the attack model and the test-bed description. In Section IV we show 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 V.

II. Security Challenges due to Energy Constraints of Smart Objects

Security threats on smart objects do not vary much compared to normal wireless or wired networks. The main differ-

978-1-4673-3125-8/12/$31.00 ©2012 IEEE

ence is that suitable security mechanisms are absent because of the lack of respective architectures and resources. The adversary model of life-logging involving stealing personal data, impersonating or DoS attacks, exist all over the Internet, either wired or wireless. Since smart objects are usually equipped with one wireless communication radio, security challenges are mostly compared to the wireless networks. Security challenges exist in all different layers of OSI model [3] 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 [4].

Secure life-logging in smart environments is challenging due to the lack of sufficient resources in smart devices. Their tiny capabilities in computational power, memory and energy create difficulties in applying well-established security protocols. Smart objects, particularly sensors, are vulnerable by nature because of the lack of security support in the primary design of low lossy networks. Information about measurements such as temperature and humidity did not attract attackers to interfere. Nevertheless, the rapid growth of system automation and the massive production of sensors and smart devices and their integration in the environment reveals security deficits and possible threats from malicious users. Additional security add-on features in an insecure design cannot replace the capabilities of a securely designed network. Moreover, the limited resources in memory, CPU and energy of smart objects make the enhancement of add-on security features even harder.

The most critical factor for secure communication between smart objects is the required energy. Evaluations of energy-efficient techniques especially for the Medium Access Protocol on 802.11 and 802.15.4 are presented on [5] and [6]. Mechanisms for mitigating security threats result in consuming more energy from their limited energy resources. Nevertheless, if there is no security encryption 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. The Transport Layer Security (TLS) protocol and the Secure Socket Layer (SSL) protocol appear to be efficient cryptographic solutions but they are inadequate because of the limitations of smart objects in supporting them. However, the use of AES-128 link-layer security mechanism of IEEE 802.15.4 seems to have lightweight properties but the necessary time to encrypt and decrypt interchanging messages occur at higher levels of energy consumption. The encryption algorithm used in 802.15.4 is AES (Advanced Encryption Standard) with a 128b key length (16 Bytes). Moreover AES algorithm is not only used to encrypt the information but to validate the data sent. This concept is called Data Integrity and it is achieved using a Message Integrity Code (MIC) also known as Message Authentication Code (MAC) which is appended to the message. This code ensures the integrity of the MAC header and payload data attached. On the other hand jamming attacks can be detected with the use of suitable algorithms based on dropped packets or the decrease in the signal to noise ratio [7]. In order to mitigate such attacks, two possible solutions may work; an increase in the power level or a channel assignment procedure as described in [8]. The use of both mitigating factors severely affect the energy consumed in smart objects and will be described extensively.

III. Measurement System and Experimental Setup

To investigate the consequences on energy consumption from security threats of malicious users, an experimental test-bed was developed. The topology of the model consists of three users Bob, Alice and Eve. Bob and Alice are interconnected 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 channel, an attacker, Eve, appears to have as her main target to break any available security wall and steal users' personal data or destroy the communication.

A. 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 1.

B. Attacker Model

One of the most important parts of this investigation is based on a smart attacker. The main concept of the attacker

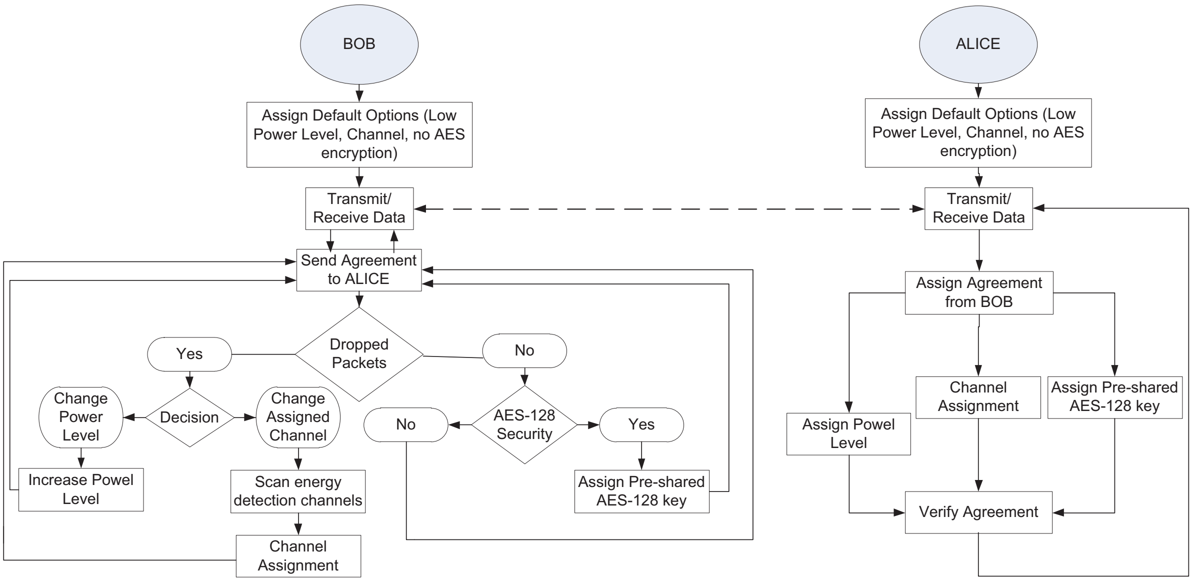

Fig. 1: The Communication Flowchart Model

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 2 depicts the flowchart model of the attacker.

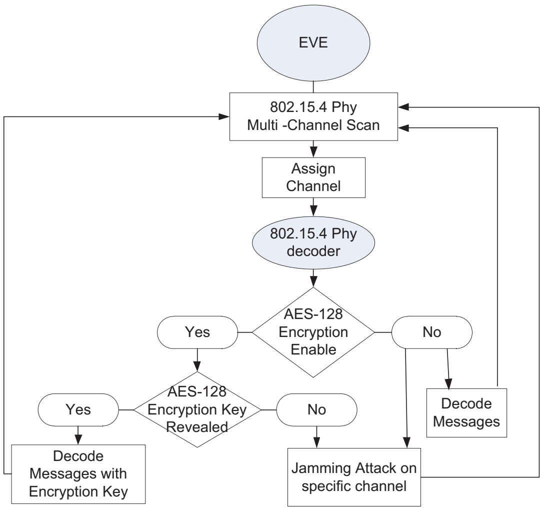
EVE
802.15.4 Phy Multi -Channel Scan
Assign Channel
802.15.4 Phy decoder
AES-128 Encryption Enable
Yes
No
AES-128 Encryption Key Revealed
Yes
No
Decode Messages
Decode Messages with Encryption Key
Jamming Attack on specific channel

Fig. 2: The Attacker Flowchart Model

C. Test-bed Description

The test-bed contains three users each one attached with a smart device. Bob and Alice are the users who are connected with a Digi XBee Pro 802.15.4 device [9] respectively. Both devices are connected (through their serial cable) with Matlab 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 2011b as well. Eve is a malicious node which acts as an eavesdropper or as an attacker. This node is a Universal Software Radio Peripheral (USRP2) device from Ettus Research LLC [10] holding a XCVR2450 Dual-band Transceiver interchangeable daughterboard module that serves as the RF front end. The GNU Radio 3.3 software is installed, suitable for creating complex software-defined radio systems [11]. The GNU Radio software is installed on a Ubuntu 11.04 which manages the attack node. The IEEE 802.15.4 PHY implementation as known as UCLA Zigbee [12] 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.

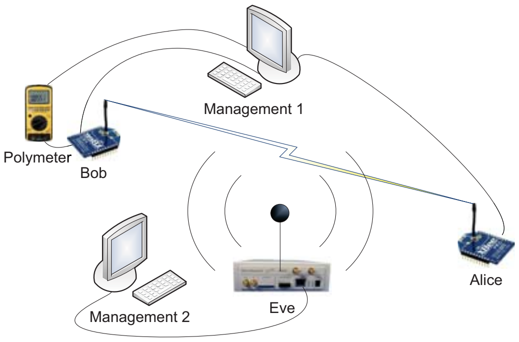

Fig. 3: Test-bed Topology

IV. 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. Four different scenarios are presented to prove the vulnerabilities based on the energy consumption of different attack models. The polymeter stores electric current and these values are used as the main measurements for this investigation. 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 [13]. Therefore, in the following experiments Bob sends to Alice 1000 packets of 102 bytes data length.

A. Transmission without Encryption

The first 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 or external interference, the power level is increased. When there is a successful transmission Bob sends a new message to Alice. Under this scenario an energy consumption investigation was carried out, measuring the five levels of conducted power which are: 0 (10 dBm), 1 (12 dBm), 2 (14 dBm), 3 (16 dBm) and 4 (18 dBm) as is depicted in Figure 4a.

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.

B. Transmission with AES Encryption

The second scenario occurs when Alice and Bob become conscious of the security level of their communication. They decide to decode their messages by the use of 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 energy consumption on different power levels is depicted in Figure 4b. The comparison of Figure 4a and 4b shows that the required time to transmit the same number of packets is 36% greater when AES encryption is enabled.

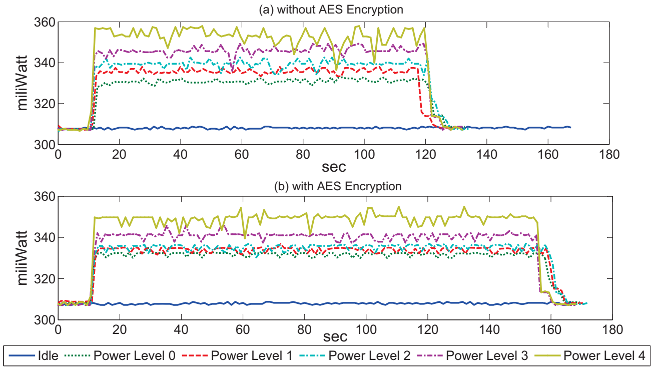

Fig. 4: Energy Consumption on Different Power Levels (a) without AES Encryption and (b) with AES Encryption

C. Transmission on Jamming Attack without AES Encryption

In the third 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. The users apply the communication model, as described above, in which when there are 10 dropped packets the coordinator executes firstly an increment in the power level on their devices and if the problem of dropped packets continues, an energy detection process for finding the most suitable energy-free channel, will be executed. When the new channel is assigned, the power level is decreased to its minimum value. The gradual increase in the power level and the channel assignment procedure will have an effect on higher energy consumption. 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.

D. Transmission on Jamming Attack with AES Encryption

The last 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 communication. For this purpose a jamming attack is made. The scenario follows the same procedure as the scenario 3 but there is more delay for the transmission of 1000 packets because of the computation time to decrypt and encrypt messages. Figure 5 presents the comparison of energy consumption between scenarios 3 and

4. As the power increase the energy consumption is higher. When the power level is maximum, the coordinator applies a channel assignment. As it can been seen in the figure when the packets are decoded by the use of AES encryption, the transmission time of 1000 packets is greater and the transmitter applies 2 more power level increment to mitigate the attack and complete the transmission of all packets.

In Figure 6 there is a comparison of consumed energy in miliWatt-Hour gained from the previous scenarios. The consumed energy is increased 4% on each power level rise. When the AES encryption is enabled, there is an increment of 25% compared with the transmission without AES encryption on the same power level. Finally, when a jam attack is occurred, the increase on the energy consumption is more than 43% compared to the transmissions without jam attack.

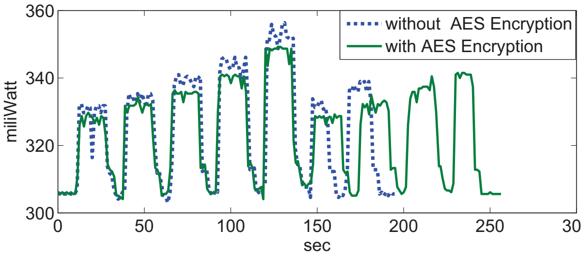

Fig. 5: Energy consumption on Jamming Attack (a) without AES Encryption and (b) with AES Encryption

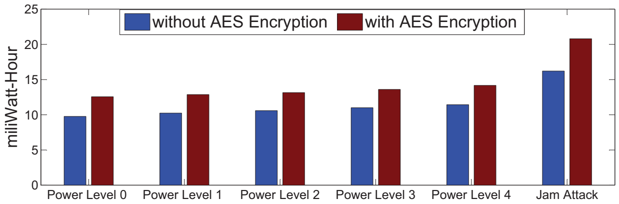

Fig. 6: Energy Consumption in miliWatt-Hour from the Described Experiments

E. Evaluation of the Experiments and Future Work

The experimental evaluation of this study has shown many valuable conclusions. First of all, the impact on energy consumption is important owing to different parameters such as the power level, channel assignment and encryption. Secondly the limited capabilities of smart devices severely affect the performance of the evaluation. One example is the maximum packet size and the transmission power. These are parameters which confine the effect of energy consumption. Furthermore, 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. Finally, the development of such a test-bed will give the potential for further investigation, experiments and automation of the procedures.

V. Conclusion

In this paper an experimental investigation on the energy consumption for secure life-logging in smart environments was described. The potential of smart objects and their interconnection with the Internet of Things has gained great attention in the research community because of the rising interest in Future Networks. 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] N. E. Petroulakis, I. Askoxylakis, and T. Tryfonas. Life-logging in Smart Environments: Challenges and Security Threats. In *the 2012 ICC ConWire*, Ottava, Canada, June 2012.

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

[3] IOS/IEO Commission. Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model. *ISO/IEC*, 1994.

[4] K. Stammberger, M. Semp, M. B. Anand, and D. Culler. Introduction to Security for Smart Object Networks. *IPSO Alliance*, 2010.

[5] A. Antonopoulos and C. Verikoukis. Network-Coding-Based Cooperative ARQ Medium Access Control Protocol for Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, 2012.

[6] J. Alonso-Zarate, E. Stavrou, a. Stamou, P. Angelidis, L. Alonso, and C. Verikoukis. Energy-Efficiency Evaluation of a Medium Access Control Protocol for Cooperative ARQ. *IEEE International Conference on Communications (ICC)*, June 2011.

[7] A. Fragkiadakis, V. Siris, and N. Petroulakis. Anomaly-based intrusion detection algorithms for wireless networks. In *the 8th WWIC 2010*, June 2010.

[8] 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.

[9] Digi XBee Pro. www.digi.com.

[10] Ettus Research. www.ettus.org.

[11] GNU Radio. http://gnuradio.org.

[12] T. Schmid. Gnu radio 802.15. 4 En-and decoding. *UCLA NESL, Los Angeles, CA*, 2005.

[13] 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.