Energy-aware Security Adaptation in Ubiquitous Mobile Network

Tewfiq El Maliki
Information Technology department hepia, HES-SO
University of Applied Sciences Western Switzerland
Geneva - Switzerland
email:Tewfiq.Elmaliki@hesge.ch

Aïcha Rizzotti-Kaddouri
Haute Ecole Arc Ingénierie he-arc, HES-SO
University of Applied Sciences Western Switzerland
St-Imier – Switzerland
email:Aicha.Rizzotti@he-arc.ch

***Abstract* — Data privacy and security are a major concern in any field mainly mobile commerce, Internet of Thing (IoT), and wireless data communication. Classical security is particularly based on encryption to protect data confidentiality, integrity, non repudiation and availability. However, mobile devices are limited in processing, battery life and communication bit rate. Therefore, many security protections are not used in order to save battery life. A new paradigm must be carried out to establish a framework capable to be energy aware when applying a security mechanism. In this paper, we present our Security Adaptation Reference Monitor (SARM). It is based on an autonomic computing security looped system, which fine-tunes security means based on the monitoring of the context including the user environment and energy consumption aspects. Thereafter, we investigate the cost of security and wireless communication related to battery consumption.**

Keywords-framework; autonomic; security adaptation; energy awareness; mobile network

I. INTRODUCTION

As mobile and wireless networks have become increasingly heterogeneous and particularly dynamic, the requirements in terms of security and performance must be addressed in a flexible manner but also in a dynamic way to deal with the evolution of the system in real time according to its context. In addition, the evolution of using smart phones privately and professionally highlights the urgent need of improving security of communication and data.

Currently, mobile phones have become real computers, but unfortunately, with less security. Hence, the existence of multiple flaws such as ease of misuse of resources, total control of communications, especially Short Message, etc.

The increasing number of applications and devices make security more relevant in this field. However, providing security faces challenges because of the severe limitation of CPU utilization related to communications, memory and resources. In fact, security is resources consuming, particularly in wireless Sensor Networks.

We propose a generic Security Adaptation Reference Monitor (SARM) as a compelling solution for this problem. Implementing SARM at each application level is not feasible because the change will interfere in each communication program in each device. The best way to overcome this constraint is to implement SARM in the kernel and consequently having an overall security control. Our work is inspired by the concept of Reference Monitor (RM) that was developed for data access [1].

Thereafter, the basic idea is to integrate SARM, which is an adaptive Security Framework in phones to deal with extremely dynamic security conditions while maximizing performance based on policies, preferences and risks associated with different contexts.

We describe a methodology intended for the use of users or system developers to determine *ab initio* the most suitable adaptive security and access means for different categories of wireless networks. We will also describe some principal resource costs for security and some applications of SARM.

The overall objective of our work is the exploration of SARM to secure transmissions, voice, data of mobiles phone such as Android devices. The principal objective is to use external cryptographic tamper-proof system based on Smart Card (SC) SD, which supports data encryption mechanisms and protected memory.

In Section 2, we survey other related work. Section 3 gives the problem statement, highlighting the motivation of our work then introduces SARM and explains its components and functionalities. Section 4 gives analysis of resource costs for security and explains our experiments. Section 5 addressed simulation implementation to validate SARM. Our simulation results and performance analysis are presented in Section 6 and Section 7 concludes our paper.

II. RELATED WORK

The concept of adaptation security in wireless network is used to mitigate the consequences of a substantial number of runtime threats, when it does not completely eliminate them. Many systems rated at the higher levels of security for data are implemented according to the reference monitor concept. A reference monitor is a concept that has proven to be a useful tool for computer security experts. It is the only effective tool known for describing the abstract requirements of secure system design and implementation.

Reference [2] has proposed an adaptive security application in mobile ad-hoc networks, where network conditions play a role in choosing relevant security mechanisms at runtime.

In Chigan Chunxioo et al.'s paper [3], the authors report that often a highly secure mechanism inevitably consumes a large amount of system resources, which in turn may unintentionally cause a security attack. Consequently, a suitable security service is provisioned in a progressive way

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

to achieve the maximum overall security services against network-performance services throughout the course of Wireless Local Area Network (WLAN) and Sensor networks operation.

Some solutions have already been implemented but they are based on a fixed security scheme and may not be adequate for systems exposed to diverse operating contexts [4] as found in wireless environments and Internet of Things networks.

We can state that current systems either suffer from a number of drawbacks in terms of their overall security capacity and dynamism, or else they are highly specific, addressing a single security issue. Hence with the current setup, total security is far from achievable. We propose a security adaptation Framework for wireless environments, which we call a SARM.

III. MOTIVATION FOR OUR FRAMEWORK

We argue that the spare processing and transmission resources are wasted in mobile environments if security is over-provisioned. Hence, the trade-off between security and performance is essential in the choice of security services. Adaptive security mechanisms are also found in flexible protocol stacks for wireless networks [5], context-aware access control systems [6] and security architectures [7]. This has motivated us for the implementation of a completely reconfigurable architecture [8], which is fundamental to adapt the architecture to the terminal and network variability of the context and particularly in the security field [9]. Seigneur [10] has introduced autonomic security pattern in his security design but only at the authentication level. So, we will use autonomic system to design our framework and take advantage of all the power of it architecture.

A. The system

Three principal components of the autonomic system have been identified in the design of our Framework [11], [12]. These have been extended based on adaptation security architecture.

For the Management unit, we add policies and logs for short- and long-term security or Quality of Service security analysis and monitoring. The block risk, vulnerabilities and performances are based on the risk management module. Risk is in general analyzed as a function of threats and their likelihood, which represents the frequency of hazard [13]. Also, hazard can be broken down into threat and vulnerability components. Each vulnerable element is coupled with an associated safeguard. Finally, risk management is formulated as the maintenance of a set of requirements framed as constraints on the aforementioned factors. If the level of risk falls below a threshold then no action will be taken other than a re-sampling of risk; otherwise, some predefined action will be launched in order to protect assets, and the safeguards related to vulnerabilities will be reviewed. [14]

Policy should be deployed and maintained so as to save time and complexity and make centralized system management more feasible. In addition, risk, performance and vulnerability analysis is a key issue in the Framework because it is responsible for detecting potentially insecure contexts, environments that are potentially wasteful of energy, and/or particularly vulnerable applications. Thus, the analysis could attempt a trade-off between all of these constraints in order to choose an efficient action in the adaptation action to tune the functional unit.

In the end, the functional unit is responsible for selecting adequate security means, like efficient network access. The device will then adapt its security so as to have the most efficient mechanisms. In doing so, the loop will make the communication system more self-managing in terms of security and more accurate in coping with any dynamic changes in context.

This autonomous security Framework is thus well-adapted to react dynamically during runtime, depending on the security parameters and context. In fact, a trade-off between security and performance is also carried out.

We have depicted our generic Framework in Figure 1. It is comprised of two units, which are based on the concept of the reference monitor so as to ensure the security of any network.

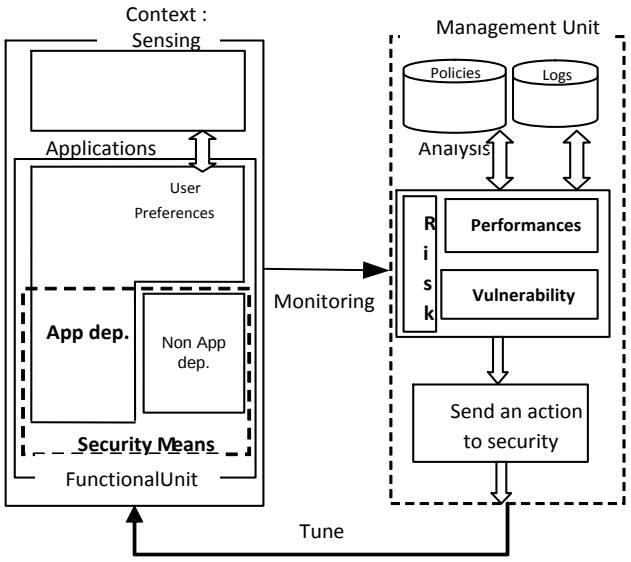

Figure 1. Foundations of our adaptive security Framework

B. Discussion of SARM

The key challenge for SARM is to adapt the Reference Monitor (RM) and autonomic system concepts to wireless communication and beyond, including data access control. The goal of a RM is to enforce security by preventing all processes and users from accessing any data except through the reference itself. The security kernel is managed by security policies.

We have also chosen to apply the autonomic computing security pattern [15] in the design of SARM by dividing it into a functional unit and a monitoring unit. The Framework is adapted to a cross-layer security approach. As a result, the Framework will reduce overheads even at very high levels.

To reduce the system's complexity and to make the system incremental, we propose a feedback loop Framework

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

as introduced in [10] at the authentication level, that is, the system will automatically tune to its best configuration based on its particular monitored context, thus avoiding any static decision making. Hence, the SARM is split into two units looped in a servo control system model in order to fine tune the adequate security measures/means, which we will discuss later. One unit, called the management or monitoring unit, monitors the context by evaluating and analyzing risks, performance, and energy consumption, which are significant for detecting attacks, and tunes the adequate security means using the second module, which is called the functional unit.

C. Security Means

As depicted in Figure 2, security means are defined as any algorithm or mechanism that could ensure security but that also has the capacity not to take security action unless it is actually necessary. It also includes the choice of adequate network access, because some network communication technologies are more secure, with higher levels of energy consumption, while others are less secure, with lower levels of energy consumption. Security means can be application-dependent, as in the case of localized trust [16] or distributed trust [17], or application-independent, as with cryptographic protocols. Indeed, localized and distributed forms of trust are good paths to explore because they generate low-computing charges (less energy consumption) and in some cases give better results. Thus they fit the context of Wireless Sensor Network, for example, perfectly.

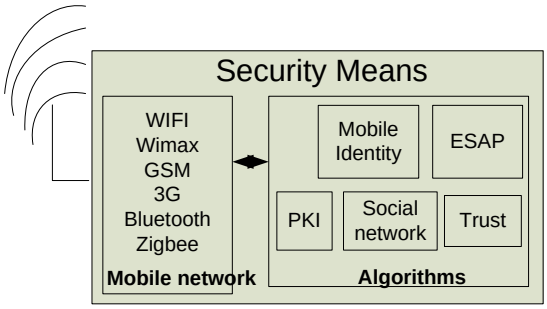

Figure 2. Security Means details

Thus, the analysis could delve into a trade-off between all these constraints to choose an efficient action to tune the functional unit.

IV. Analysis of Resource Costs for Security

A. Motivation

For a long time, security has been treated as a static component in system design, with static security assessment assumed to protect the system throughout its lifetime and assuming that energy is unlimited. However, this assumption does not hold anymore because devices are disconnected from power line and they are in battery mode that has limited live time. Reference [18] declares that Wi-Fi devices consume 30% more energy than normal mode. In [19], we find a complete study of energy consumption in mobile phones and it is proved that a 3G connection consumes from 5 to 10 times more energy than Wi-Fi. In addition, the problem of energy is a key issue in sensor networks and IoT. Therefore, the security cannot be considered without other context aspects especially energy awareness.

B. Data and telephony

Data security has become a major concern for all users, particularly for applications in Self-Organization Network field, because they require many security features adapted to their wireless transmission. Different kinds of security mechanisms and strong cryptographic algorithms are available to prevent any violation of data security. Unfortunately, these security capabilities are time and energy consuming. Indeed, certain algorithms and mechanisms are strong enough to protect largely the data but at the same time reduce severely battery lifespan. That is why an adaptable platform for mobile device will save energy and reduce the delay to fit to the limits of a real time range; mainly for telephony application. In this respect, to deploy Voice over IP (VoIP) so that users receive an acceptable level of voice quality, VoIP traffic must be guaranteed certain compensating bandwidth, jitter, and packet loss.

According to G.729 [20], codec requires packet loss far less than **1%** to avoid audible errors. G.114 of International Telecommunication Union [20] specification recommends less than **150 ms** one-way end-to-end delay for high-quality real-time traffic, such as voice; and for Jitter buffers, varying delay, further add to the end-to-end delay, and are usually effective only on delay variations of less than **100 ms**.

Thereby, the delay must be less than 100 ms, which is a significant constraint for mobile device.

C. *Smart Cart*-Secure Digital *(SC-SD) Card*

SC is a card that securely manages and stores information separately from the rest of the device's components. In a SC-SD, man can find security platform delivered through a secure microSD processor. Architecture details are described in Fig. 3. The main objective is to integrate SARM in this smart card to protect voice and data infrastructure, preventing loss or theft of sensible data, vital information and proprietary assets. Another objective aims to increase the awareness of the costs using encryption and access networks.

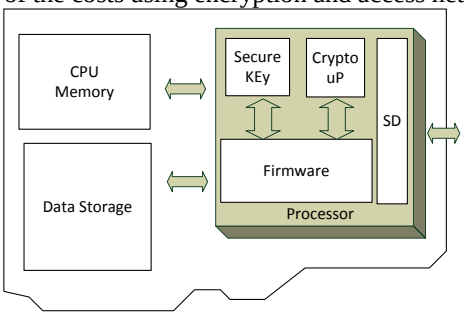

Figure 3. Architecture of SC-SD

D. Goal of analysis

The goal of our analysis is to integrate cryptographic algorithms and security mechanisms in SARM in order to implement them in a SC-SD memory card. Thereby, our

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

SARM means will be chosen perfectly according to context. This will help designers and developers to fit timely the users' preferences and policy in order to have efficiency application and security system. That is why we have carried out experimental measures to compare energy consumption of different algorithms and access networks. Based on the results, we could adapt timely our SARM means to policy and user's preferences. In this respect, we increase the efficiency and validation of the Framework.

Our main goal is to establish a model for the power consumption of phones in many cases to know how to mitigate between security and power consumption in our Framework.

V. ASSUMPTIONS AND EXPERIMENTS

There are three techniques for performance evaluation:

a) Analytical

b) Simulation

c) Measurement

Simulations offer less accuracy than measurements. For this matter, we have previously developed hardware and software to measure energy consumption. That is why we have privileged the measurement instead of analytical or simulation methods. Analytical technique is complicated due to the fact that this method needs more precision and requires more time. We have made several assumptions to limit the scope of the study and also to keep the implementation and complexity reasonable.

TABLE 1. MAIN CHARACTERISTICS OF EXPERIMENTS

Phone	**Networks**
Galaxy S3; GT9300	WLAN or Cellular network
Android version 4.1.2	803.11g; GSM/UMTS/G4
Battery: 3.8 V; 2100 mAh	Protocols: Data channel (Session Initiation Protocol SIP/RTP); SMS; switched channel, voice PCM G.711 (64 kbit/s)

Further studies are needed to consider an overall evaluation. We use commercially available mobile phones with a SC-SD for the SARM.

A. Metrics and Measurements Methods

Our focus is to determine the impact of cryptographic algorithms and use of different access networks on battery resources. We will explain the methodology of the measurements.

1) Encryption Latency

We will evaluate the latency of some means in SARM, such as identity. The latency is the time to encrypt a block cipher or a file calculated based on a time function.

2) Energy Consumption

To measure the current level, we have developed an electronic card capable to measure a low current level via low precision resistor (r=50mΩ) in series between battery and the mobile phone. The electronic card uses many low noise amplifiers (gain =200) and has an USB interface in order that data will be directly accessed from a PC. The equivalent circuit scheme is shown in Figure 4.

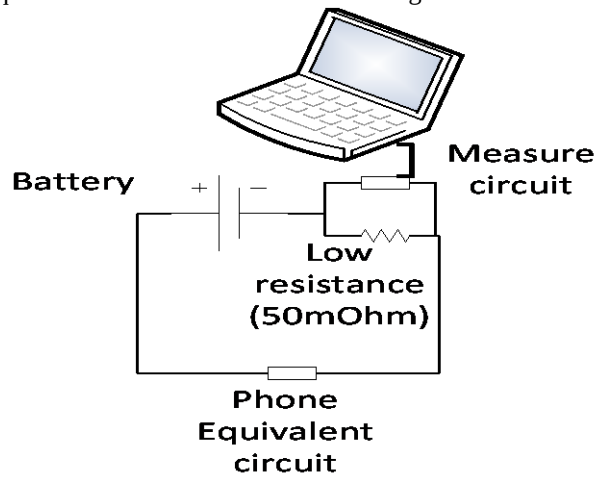

Figure 4- Scheme of experimental energy consumption circuit

The most known problem of battery detection mechanisms was bypassed by using all four battery's connectors; otherwise there will be no power. At the same time, to avoid battery fluctuations we have connected the battery to DC adapter. The time of a single measure is 2500 times by a second. Figure 4 illustrates the details of the experiments. The formulas are only applying Kirchhoff's circuit laws to our circuit. To calculate the power via our method we must: Take the measured voltage via the PC Vpc(t) and divide it by the amplifier gain 200 to have V(t):

$$\mathbf{V(t) = Vpc(t)/200} \quad (1)$$

then apply the equation with V(battery = 3.8)

$$\mathbf{P(t)=U(t).I(t) \approx V.V(t)/r(50m\,\Omega)} \quad (2)$$

Finally, we use (1) and (2) to calculate the power:

$$\mathbf{P(t)= Vpc(t)*0.38} \quad (3)$$

VI. RESULTS AND DISCUSSION

B. Identity management

We have studied all Identity management platforms [21] and we have had a good background in this field as a means in our Framework. We have implemented a test-bed based on WLAN network and mobile phones. The main goal is to know the time consuming difference between a secure and non-secure connection. The results are shown in Figure 5. The requirements of this experience are:

a) E65 telephone

b) WLAN 802.11b, D-link Access Point

c) Tomcat server

d) Security assertion markup language (SAML) [2] Token and Secure Sockets Layer (SSL) connection

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

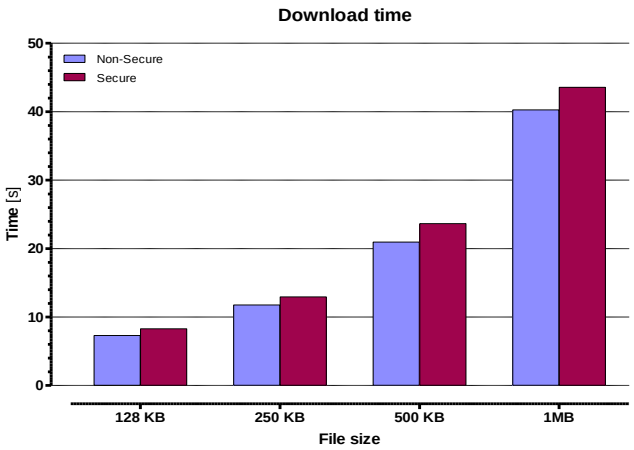

Figure 5. Download time of different files

Figure 5 shows the download time average difference between secure and non-secure for different file sizes. In all cases, the difference between secure and non-secure ranges from 10% to 15%. For each measure, the specific file download is done 30 times. The standard deviation is less than 1.7%.

C. Energy Evaluation

1) Voice Communication energy cost

We have carried out an end to end voice encryption, which is very important to secure in mobile network mainly that any telephony call is not protected at all inside the Global System for Mobile (GSM) network. In Figure 6 we find the network level of our experiment, which contains these elements:

a) Commercially smart card SD for encryption,
b) SIP protocol for signaling,
c) Real Time Protocol RTP for ToIP, and
e) Data channel.

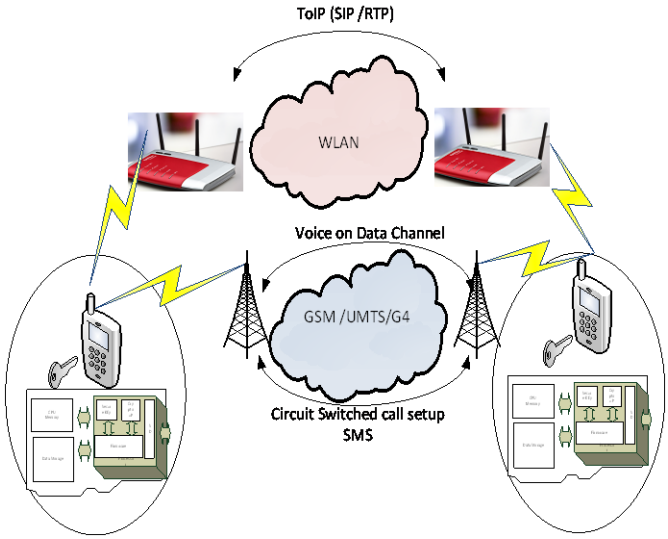

Figure 6: Configuration of SARM experiments

2) Analysis of Results

All energy metrics are based on experiments with Samsung S3 Galaxy. The experiments show power consumption for a voice transmission without and with encryption (Padding and non-Padding). A voice packet is based on 20ms and 64kbit/s, which gives a 160bytes size.
Blowfish cipher has the highest encryption energy consuming for 20ms encryption block, which seems to be less efficiently with a small block, because it uses one function to process the entire buffer of plaintext. Figure 7 illustrates that for larger files, Blowfish is more efficient, which is more adequate for voice encryption. Advanced Encryption Standard (AES) is the more energy consuming for long block. However, it is the strongest in terms of cryptographic properties. In all cases, the difference between secure and non-secure ranges from 12% to 20%. Moreover, for each measure, the specific measures are done 30 times. The standard deviation is less than 1%. Therefore, we can state that almost 70% of energy is consumed by transmission and 15% by encryption.

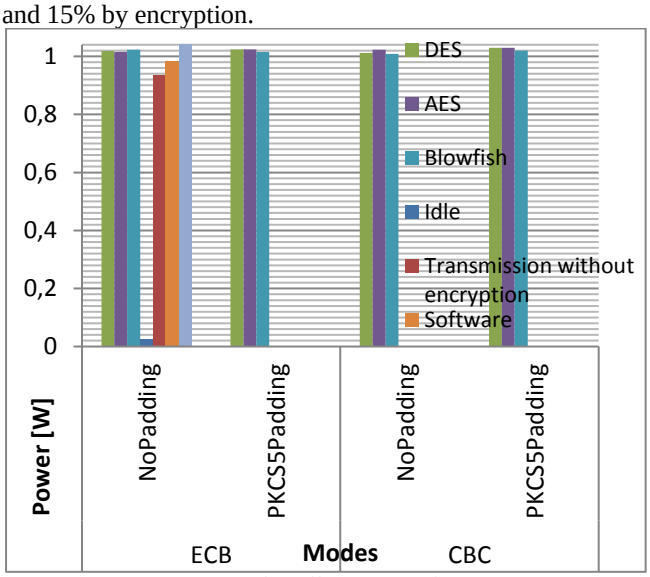

Figure 7. Power for different cases of encryption

3) Access network energy consumption

We must have an overall view about the energy consumption of security utilization in order to tune the best security means and also to choose the best access network depending on the context, user preferences and policies in SARM. That is why we have carried out measurements of energy consumption for Wi-Fi and Bluetooth. The graphs in Fig.8 and Fig.9 show energy consumption (µjoules/Byte). One can see the energy consumption for a file transmission of respectively 100Mbytes over Wi-Fi and 10Mbytes over Bluetooth connections. We have depicted for different distances the average energy consumption, standard deviations (std-dev) and average +2*std-dev -represents 95% of statistical cases-. For short distance -2m line-of-sight-, Wi-Fi energy consumption is higher than Bluetooth. But for higher distances Bluetooth is more energy consuming than Wi-Fi. Please note: The average was carried out over 10 different experiments.

Copyright (c) IARIA, 2016. ISBN: 978-1-61208-493-0

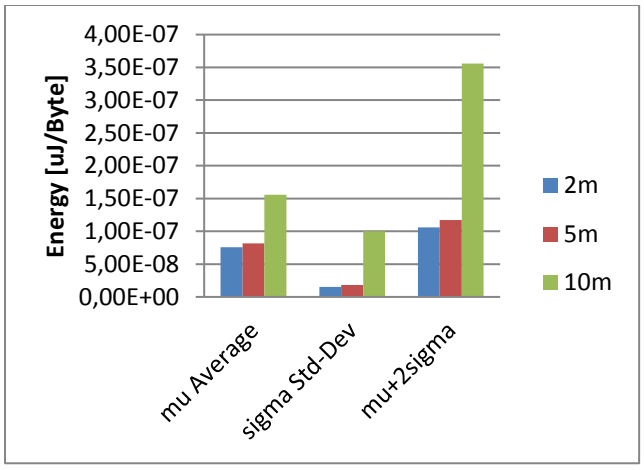

Figure 8. Energy consumption for Wi-Fi 100Mbytes

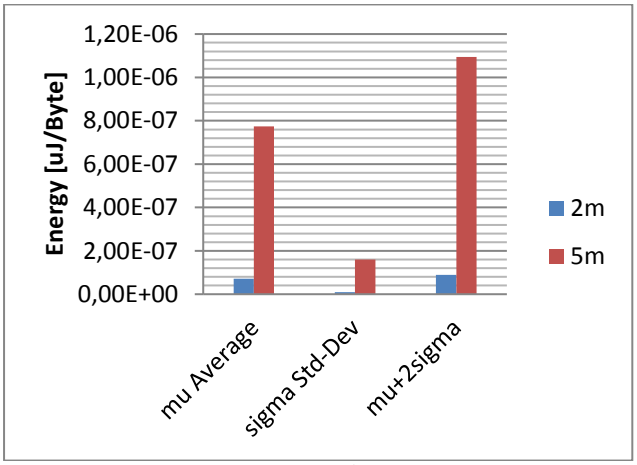

Figure 9. Energy consumption for Bluetooth 10Mbytes

These conclusive and accurate results have been used in one of research projects called iNUIT -Internet of Things and Urban Innovation- [22].

VII. Conclusion and Future Work

The energy consumption is accurately evaluated and is mainly consumed within wireless transmission. These experiments are a foundation for all simulations and evaluations in the future to explore the efficiency of our Framework. Indeed, it gives us a solid background to launch the simulations, of our Framework SARM based on the tuning of the security means related to the accurate energy and access network consumption tradeoffs. Besides, the experiments have given us the opportunity to study a full end-to-end secure telephony connection based also on SARM and SC-SD. Nevertheless, we need further studies of the Framework for real applications, different contexts, and diverse access networks and energy consumption. In short, the proof of concept of SARM was based on implementing it in a tamper resistant security module based on a Secure Digital Card. The results are conclusive and accurate to continue research on efficient energy security adaptation.

References

[1] J. Anderson, “Computer Security Technology Planning,” http://seclab.cs.ucdavis.edu/, June, 2016.

[2] C. Chigan, L. Li, and Y. Ye, “Resource-aware Self-adaptive Security Provisioning in Mobile Ad-Hoc Networks,” Proc. IEEE Wireless Communications and Networking Conference, 2005, pp.2118–2124.

[3] C. Chigan, Y. Ye and L. Li, “Balancing security against performance in wireless ad-hoc and sensor networks,” 60 IEEE Vehicular Technology Conference, USA, 2004, pp.4735-4739.

[4] L. Yuan and G. Qu, “Design Space Exploration for Energy-Efficient Secure Sensor Network,” ASAP 2002, pp.88-97.

[5] C. Hager, “Context Aware and Adaptive Security for Wireless Networks,” PhD thesis, Virginia Polytechnic Institute and State University, 2004.

[6] M. Lacoste, G. Privat, and F. Ramparany. “Evaluating Confidence in Context for Context-Aware Security,” European Conference on Ambient Intelligence (AmI'07), 2007, pp.88-97.

[7] J. Al-Muhtadi, D. Mickunas, and R. Campbell. “A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile Devices,” IEEE Wireless Communications, 9(2):60–65, 2002.

[8] E2R Deliverable D2.2. “Equipment Management Framework for Reconfiguration: Architecture, Interfaces, and Functions,” December 2005.

[9] T. Jarboui, M. Lacoste, and P. Wadier, “A Component-Based Policy-Neutral Authorization Architecture,” French Conference on Operating Systems (CFSE), 2006.

[10] J.-M. Seigneur, “Trust, Security and Privacy in Global Computing,” PhD Thesis, 2005.

[11] T. El Maliki, “Security Adaptation in Highly dynamic wireless”, PhD Thesis, Geneva, 2013.

[12] E. D. Sontag, “Mathematical Control Theory: Deterministic Finite Dimensional Systems”, Ed. Springer, Jul. 1998.

[13] F. den Braber, T. Dimitrakos, B. A. Gran, K. Stølen, and J. Ø. Aagedal, “Model-based risk management using UML and UP”, Issues and Trends of Information Technology Management in Contemporary Organizations, 2002.

[14] A. Gehani, “Performance-sensitive Real-time Risk Management is NP-Hard”, Workshop on Foundations of Computer Security affiliated with the 19th IEEE Symposium on Logic in Computer Science (LICS), 2004.

[15] D. M. Chess, C. C. Palmer, and S. R. White, “Security in an autonomic computing environment”, IBM Systems Journal, vol. 42, no. 1, pp. 107–118, 2003.

[16] Davis, “A localized trust management scheme for Ad-Hoc networks,” in Proceedings of the 3rd International Conference on Networking (ICN '04), March 2004.

[17] X. Titi, T. El Maliki, and J.-M. Seigneur,"Trust-based Hotspot Selection", IADIS International Conference e-Society2010, Portugal. Best Quantitative paper award.

[18] White Paper, “Power Consumption and Energy Efficiency Comparisons of WLAN,” Products Atheros Communications, (acceded at: http://www.atheros.com/pt/papers.html), 6/2016.

[19] N. Balasubramanian, A Balasubramanian, and A. Venkataramani, “Energy Consumption in Mobile Phones”, IMC’09, 2009.

[20] ITU-T recommendations to find at http://www.itu.int. 6/2016.

[21] T. El Maliki and J.-M. Seigneur: “A Survey of User-centric Identity Management Technologies”, Secureware , 2007.

[22] HES-SO, Project iNUIT, to find at http://www.hes-so.ch/data/documents/Brochure-iNuit-web-en-6518. 6/2016.