Delft University of Technology
Master's Thesis in Embedded Systems

Power Modulation based Device-Socket Association

Nikolaos Larisis

embedded software

TU Delft Delft University of Technology

Power Modulation based Device-Socket Association

Master's Thesis in Embedded Systems

Embedded Software Section
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
Mekelweg 4, 2628 CD Delft, The Netherlands

Nikolaos Larisis
N.LARISIS@student.tudelft.nl

20th September 2013

Author
Nikolaos Larisis (N.LARISIS@student.tudelft.nl)
Title
Power Modulation based Device-Socket Association
MSc presentation
27th September 2013

Graduation Committee

Prof.Dr. Koen Langendoen (Chair)	Delft University of Technology
Assistant Prof.Dr. Przemyslaw Pawelczak	Delft University of Technology
Associate Prof.Dr. Jos Weber	Delft University of Technology

Abstract

Smart metering can be entitled as a pivotal research area empowering the provision of enhanced energy conservation services. Academic research focuses mainly on upper context aspects such as smart grids or smart homes. Relatively lower interest is drawn to user awareness for reducing energy usage. Every individual can achieve a greener footprint when provided with detailed information about the appliances' consumption that he uses.

To that extent, a direct association between the user/device, and the corresponding wall socket must be established, especially when the latter is publicly accessible. The objective of this thesis is to examine and present a novel ***Power Modulation Association*** protocol. The proposed protocol is deployable for the pair of a smart wall socket and a smart device. Information is exchanged over the AC power cable via modulating either the power demand of the device, or the power supply provided by the socket. Via this technique, when shareable sockets are present, individual pricing policies for domestic or vocational habitats may be introduced that can influence the building power consumption. Ultimately, a socket is paired with the attached device and thus, the latter is then granted with electrical power.

The evaluation of the system is performed by extensive experimentation in actual running conditions. The aim was to select the optimal association modality and above all, confirm the feasibility of the developed communication schemes. Results demonstrate that the proposed system is capable of establishing a half-duplex serial communication mechanism that can effectively facilitate the pairing between a smart socket and a smart device.

Preface

This Master of Science thesis presents the fruits of my research efforts within the Embedded Software Group during the last eight months. My interest in the specific topic was stimulated by Yunus Durmus's initial inspiration, that was further cultivated due to my enthusiasm for algorithmic and systems design. Whilst conducting my internship, I had the chance of being confronted with similar research area challenges. This enabled me to gradually formulate a profound passion in smart metering aspects and thus realize the initial thesis topic into an actual deployable implementation.

This project has been successfully accomplished due to the supportive intervention of various people throughout its design and implementation stages. First of all, I would like to thank Nick Ray from Priva BV for providing me the actual apparatus on which this work was based on. Further, I would like to thank Ertan Onur for his motivation with respect to the thesis topic itself. Moreover, I would like to thank Prof. Koen Langendoen for accepting me as a master student in the Embedded Software Group, and Yunus Durmus for his continuous guidance and support. Finally, I would like to thank Niels Brouwers, Kishor Chandra, and dr. Venkatesha Prasad for their feedback and the great insight that they have given me.

Nikolaos Larisis

Delft, The Netherlands
20th September 2013

Contents

Chapter 1

Introduction

Global societal and economic prosperity is inextricably related to contemporary approaches concerning energy management issues. A basic aspect of this problem is undeniably energy conservation at vocational and domestic environments. According to the European Commission [1], in The Netherlands 39.25% of the total energy consumption is attributed to the household and services sectors combined together (Table 1.1). The Smart grid was introduced as a promising $C0_2$ emissions reduction policy aiming at real-time demand response, custom-tailored pricing, and reducing the cost of generation, distribution and consumption of energy [21]. The global shift for a greener planet, evident in central governmental directives both at US [2] and EU [3] level, intends to stimulate smart metering's mass introduction at a fully deployable home energy management systems (HEMS) extent.

Within this context, "embedded sensor networks and actuating systems are expected to play a key role in monitoring and reducing building's overall energy consumption" according to [37]. Home automation systems can aggregate power usage information either from smart meters deployed onto the circuit breaker panel, or from smart wall sockets connected to specific appliances. An entire Home Area Network (HAN) is formulated consisting of a number of sensors and actuators, which can significantly reduce the energy footprint. Moreover, the relevant research fields of smart homes and smart metering are of great importance if we consider the amount of energy that is generally wasted by devices. This is significant and can be caused by stand-by mode operation (approximately 10% of total domestic consumption [36],[24]), or by inefficient operation during high-peak load hours. Although research is also conducted on the non-macroscopic level of appliance detection, monitoring, and control, little has been accomplished with respect to empowering consumers with intuitive hints for increasing their energy awareness.

Utilizing smart metering solutions on an appliance level is a major step towards the aforementioned aspect of user's awareness. Besides providing

Economy Sector	Power Consumption (TWh)	% of total
Transport	15	27.77
Industry	14.3	26.48
Households	11.5	**21.29**
Services	9.7	**17.96**
Agriculture	3.4	6.29
Other	0.1	0.21
Total	54	100

Table 1.1: Annual energy consumption statistics per sector, NL, 2010, [1].

feedback on the overall power consumption, users are also capable of distinguishing from which devices –and thus activities– most of the power is consumed. According to studies, the monthly-based charging scheme deters user's proactiveness since, "it is generally expected that by providing detailed and immediate feedback, between 5% and 15% of the electrical household energy consumption can be saved", [42]. To that extent, it is imperative that each individual is promoted to an active participant within a HEMS. This should be achieved not only by facilitating him with power monitoring and control capabilities, but mostly via correlating each appliance's real-time power consumption to the appropriate owner and user. Furthermore, active monitoring of individual devices enables the introduction of personal billing policies as long as the smart socket and the device can be securely paired. The need for security is vital since undesired situations such as *Man-in-the-Middle* attacks must be prevented (see Section 2.1.3).

Today, the association of a device and its connected socket is being done manually in most of existing HEMS. However, for a system that is scalable and practical, the association should be performed without human intervention. Some solutions to secure autonomous pairing require the use of RFID tags such as Sony's Authentication Outlet [4]. According to its operating principle, each socket must have an RFID reader embedded on it, and each user must be provided with an RFID card. In order to acquire power the user must scan his card over the socket, and then enter manually to the HEMS the specifications of the appliance he will connect (Figure 1.1). Although a user can be easily associated with the socket, the deprecation of the device as an integral part of the pairing scheme undermines its overall applicability. Furthermore, conventional wall sockets and especially legacy devices need new hardware in order to support RFID. But above all, instead of the device, in fact it is the plug that is being authenticated. The attached device can be indirectly associated via user intervention, making the overall proposed solution more complex. These deficiencies stimulated further investigation for alternate association protocols.

What arose as a necessity was indeed the inclusion of the device into the

Figure 1.1: Sony's Authentication Outlet employing RFID technology, [4].

pairing protocol, but on top, the selection of a secure auxiliary communication link other than of wireless nature. Choosing a wired medium as the link benefits from the fact that the wireless variant is susceptible to interception, more prone to connectivity failures, and its leading relative solutions such as the WPS [8], luck significant applicability (see Section 2.2.3). This novel approach in comparison to most common pairing methods that are summarized in [41], utilized the AC power cord as the communication channel. Typically, secure device pairing protocols aim at bootstrapping a secure channel between two previously unassociated entities. The procedure is unfolded over a secondary link by the exchange of a few bits of information (commonly referred to as "tokens") according to various methods. The novelty of the thesis proposition lies not only in the form of the medium, but also in the manner that tokens are exchanged over it. Similar to the Power Line Communication (PLC) [22], fluctuating the power demand or supply on one end will cause a corresponding modular signal to be sent over the power cord.

This operating principle directly poses a number of challenges for the two entities. Initially, the socket must be capable of constantly monitoring the power consumption of the attached device with an high granularity and sampling rate. At the same time, the socket must also be able to abruptly switch on/off electricity supplied to the device. On the contrary, the device should be equipped with a computation unit capable of controlling its power demand in a software manner. Finally, the device must also be able to detect and indicate at all times the status of its power supply.

1.1 Problem Statement

Smart metering is a wide research area with a prime interest in promoting power consumption reduction. Within this research spectrum HEMS are

existing solutions that enable ***users*** to remotely monitor and control their ***devices***. Nevertheless, in order to further increase users' energy awareness first, the exact power footprint at an appliance level must be deduced. Second, individually pricing policies must be introduced for public energy resources such as at enterprises, train stations or shared apartments. To that extent, a more direct association between ***sockets*** and the attached appliances must be provided. Most of the available HEMS do not offer advanced appliance level functionalities, whereas existing pairing protocols can be utilized in order to associate different entities. The question is, can a HEMS-related solution that would rely on a user-device-socket pairing mechanism and that would facilitate a power footprint cutback be proposed?

The main objective of this thesis is the proposition of a secure pairing protocol which can be incorporated in any existing HEMS and that would adhere to the following set of requirements:

- **Feasibility**: Secure pairing must be achieved without imposing any extra hardware requirements on the entities to be associated. The protocol should be based on smart wall sockets and should not require any modifications on the appliance side. Instead, the appliance needs only to be equipped with a computation and communication unit. To that extent, a common laptop and a smartphone were used during implementation and experimentation since they can both serve these prerequisites well.
- **User-friendliness**: The protocol should be designed so as user intervention is unnecessary. Users are usually unwilling to actively participate into a pairing procedure, and thus indirect approaches must be followed.
- **Reliability**: The protocol should successfully associate any common laptop or smatphone, in noisy environments, and within a predefined and decent bootstrapping time interval even in the worst case scenario.

1.2 Solution and Contributions

All the above requirements and their ramifications formulated the course of the proposed solution's design and implementation. A literature survey was conducted in order to locate research attempts or products adhering to the above functionality. Inspiration was also taken from common wireless communication modulation techniques [40] and signal processing tools. Overall, the ***Power Modulation Association*** (*PMA*) protocol is proposed as a solution to the aforementioned problem that was meticulously designed, implemented, and experimentally evaluated.

PMA is a secure device pairing protocol for establishing an association between a user, the appliances he uses, and a wall socket, via the assistive

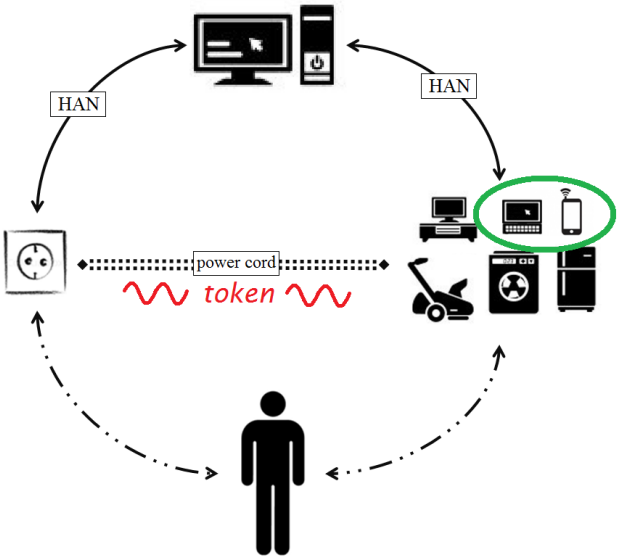


Figure 1.2: PMA's application domain entities. In current implementation only smart devices (laptops and smartphones) are taken into consideration.

intervention of a HAN server (Figure 1.2). Nevertheless, the exact protocol definition is simplified without affecting its overall applicability in two ways. Firstly, only a laptop and a smartphone are examined as the devices to be paired (marked with a green circle in Figure 1.2) whereas legacy appliances are left as part of the future work. Secondly, the association is employed only onto the pair of the smart wall socket and the smart device, whereas the user is indirectly incorporated into the pairing scheme. The central server is assigned with the initialization of the association over the auxiliary HAN infrastructure. The underlying algorithm is launched by the user when the device is plugged into the socket via notifying the server. Then, relevant pairing information (*tokens*) are exchanged via power modulation techniques. Depending on the channel's transmission direction, two distinct pairing *communication schemes* are introduced; ***device-to-socket*** (*D2S*) and ***socket-to-device*** (*S2D*).

PMA's experimental verification outlined the following contributions:

- A novel, non-invasive, and with no extent hardware modifications solution is proposed, that is capable of correlating appliances connected to wall sockets and their users.
- A robust power modulation association between a smart socket and a smart device is established, with a 21% (D2S) and 28% (S2D) Bit Error Rate for the two proposed communication schemes in optimal case. The validity of the protocol was algorithmically assessed and

experimentally verified for both laptops and smartphone devices.

- A user is indirectly –via his device– paired, since his identification can be extracted during initialization, and thus his power footprint can be deduced and tracked.
- Ultimately, by leveraging the PMA a building occupant can be individually charged and his behaviour can be induced towards a more parsimonious energy footprint.

1.3 Organization

This document is organized as follows. Chapter 2 briefly describes the theoretical background as well the related work with respect to the thesis proposition. Chapter 3 overviews the design considerations of the protocol, its operating principle, and the overall architectural design. Chapter 4 highlights intrinsic protocol issues and describes various implementation aspects. Chapter 5 reports about experimental results, and Chapter 6 concludes with general remarks and discusses about the potential for future expansion.

Chapter 2

Background and Related Work

In this chapter the background theory and the related work are presented. Both the theoretical aspects and the selected related work are further classified into three categories. First, HEMSs that the PMA protocol could be used for. Second, power metering solutions that utilize similar hardware. Third, association protocols which PMA belongs to.

2.1 Theoretical Aspects

This section discusses the aspects which are relative to the PMA's background theory. A HEMS is undoubtedly the main application domain with such intrinsic characteristics that need to be investigated beforehand. Moreover, the HEMS categorization is performed according to the power metering solution that is employed and to that extent, more light needs to be shed in that perspective. Nevertheless, a complete definition of the secure pairing protocols must be provided since PMA is such in essence.

2.1.1 Home Energy Management System

The research problem lies within the field of energy awareness and conservation. As previously stated in Chapter 1, nowadays there is a global inclination towards a smarter, greener planet. Such a challenging domain is an application objective that concerns a wide scope of societal and private activities. These may start from reducing automotive/industry emissions, up to developing new building materials, and the proliferation of renewable energy sources. Going one step further, there are also more sophisticated visions such as a future smart home (Figure 2.1). In the latter application domain, commonly cited as Home Energy Management System (HEMS), a deployment scenario of the PMA protocol can be mostly beneficiary.

Figure 2.1: A HEMS deployment example, [29].

A HEMS is typically a system that is based on a smart metering solution and an underlying Home Area Network (HAN). It is responsible for collecting the household's overall power consumption data, and remotely controlling the deployed electrical appliances. Its aim is to optimize in real-time the energy supply and distribution according to users' demands and power utilities' pricing policies. Throughout academic literature and enterprise activities there can be encountered an abundance of existing HEMS products and relevant research perspectives. The prior can be further classified with respect to the deployed metering modality into two main categories:

- **Smart meters**: The power monitoring and control is performed by a smart meter which is attached to the main power line or circuit breaker panel. Initially, one subcategory are solutions that monitor the power consumption at a ***household level*** such as Microsoft Hohm [5] and Google Power Meter [6], which are *commercial* products, or *custom* based ones like PMWCM [32]. They rely on existing smart meters and cannot provide information at an ***appliance level***. On the contrary, *commercial* based solutions like RECAP [37] and E750 [42], or *custom* based ones like in Smart Box [31] and EPM [39] can provide such information. They augment the smart meter's capabilities in order to achieve appliance recognition. By introducing complex algorithms that resort to pattern recognition techniques or similar methods, they can indirectly detect and classify the appliances by analysing their energy footprint.

- **Smart sockets**: At the same time, there are also solutions that focus even more at the appliance level utilizing sophisticated hardware circuitry. The actual wall socket is replaced or circumvented by smart sockets in order to measure and control the power supply. Analogously, there exist *commercial* products such as Plogg [26] and AVEC A999 [33], as well as *custom* based attempts such as IPM-WSN[24], *Ito et al.* [25], ACme [27], Ubi-PMeter [28], and SmartMeter [35].

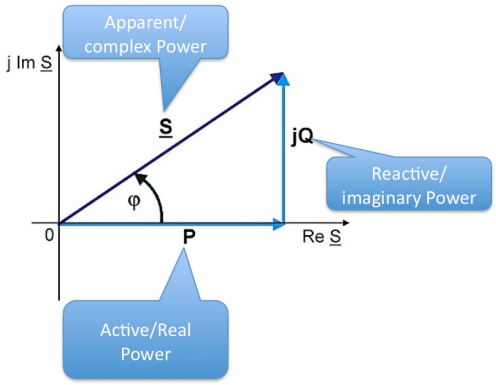


Figure 2.2: Power notions in an AC circuit, [37].

In each of the above cases, what is aimed for is the provisioning of power consumption and control information to the end user. The ultimate objective is to increase user's energy awareness, but none of the aforementioned achieves it at the same extent as the thesis proposition may achieve.

2.1.2 Power Metering

With respect to power metering, there is a variety of existing commercial products and academic custom implementations that provide real-time energy measuring. Depending on the metering modality they are divided into the categories previously explained in Scetion 2.1.1.

As a common and basic feature, any smart socket or meter ought to be able to monitor the power consumption of the attached device. According to Electrical Engineering (EE) theory, power (P) in every DC circuit is computed as the product of the amperage (I) and the voltage (V). On the contrary, in an AC circuit matters are more complicated. Reactive components that are present cause a phase difference between V and I since power is temporarily stored in them. This power is labelled as *reactive* (Q), whereas the power that is transferred as net energy as *real* or *active* (P). These two notions formulate the overall *complex* power (S) abiding to the following formula,

$$S = P + j \cdot Q$$

that may be also illustrated in the form of a complex number on the Cartesian Field (Figure 2.2). Usually, smart sockets measure all of the above forms of power but mostly they indicate the amount of *apparent* ($|S| = \sqrt{P^2 + Q^2}$) power.

2.1.3 Secure Pairing Protocols

The main contribution of our research encompasses the proposition of a novel association scheme. The terms *pairing*, or *association* protocol, or more elaborately, *secure device pairing* refer all to the same theoretical notion. That is a mechanism that is defined as the process of establishing a secure channel between two unassociated entities over a communication link. The procedure is relying on various auxiliary out-of-band (OOB) methods all aiming at eliminating the so-called *Man-in-The-Middle* attacks, that is, when an attacker eavesdrops on the channel and impersonates one of the two entities. The objective is then to exchange a handful of bits of secure information (commonly cited as *tokens*) over the OOB link which is imperceivable by the attacker. This procedure bootstraps a mutual association and thus a proper communication over the primary link can be proceeded.

In [41], a comparative overview of the most common methods is presented, which provided great inspiration whilst designing PMA's operating principle. These methods often differentiate depending upon the application domain, but above all, in the manner in which the tokens are exchanged. For example, in "Blinking Lights" [38] one device is equipped with an LED and the other one with a light detector. The LED-enabled device transmits OOB data via blinking while the other counterpart receives it by detecting ambient light fluctuations. Besides this visual form of OOB communication, the link can also be of IR nature, wireless, physical contact, audio, or a simple AC power cord as in our case.

2.2 Related Work

2.2.1 Home Energy Management Systems

Besides the categorization given in Section 2.1.1, the various HEMS solutions can be further evaluated with respect to a number of extra features. These include the underlying HAN wireless communication protocol, appliance recognition, localization and control capabilities, and above all, the level of stimulating user involvement and thus increasing energy awareness. In Table 2.1, a comparative overview of the studied HEMS solutions is presented adhering to the aforementioned features. As manifested from the results, only six cases have been identified to achieve an extensive user involvement via various forms of proposed APIs. At the same time, only two out of the previous six cases ([42] and [26]) offer well enough appliance-level capabilities. Nevertheless, after relevant investigation it was found that the "Energy Smart Home" system (ESH) presented in [26] is based on a commercial smart socket labelled "Plogg" that is no longer available on the market.

To that extent, any further research with respect to identifying an optimal HEMS focused entirely on "Handy feedback" system cited in [42]. Handy

Name	Ref.	Metering	Propriety	Appliance			HAN	User
				Recognition	Localization	Control	protocol	Awareness
Hohm	[5]	meter	commercial	-	-	-	custom[1]	limited
Meter	[6]	meter	commercial	-	-	-	custom	limited
PMWCM	[32]	meter	academic	-	-	-	WiFi	extensive
RECAP	[37]	meter	commercial	✓	-	-	ZigBee	extensive
Handy Feed.	[42]	meter	commercial	✓	✓	-	GPRS/DSL	extensive
Smart Box	[31]	meter	academic	✓	-	✓	ZigBee	limited
EPM	[39]	meter	academic	✓	-	✓	RF/PLC	limited
ESH	[26]	socket	commercial	✓	✓	✓	ZigBee	extensive
AVECA999	[33]	socket	commercial	-	-	✓	6LoWPAN	extensive
IPM-WSN	[24]	socket	academic	✓	✓	-	ZigBee	limited
Ito et al.	[25]	socket	academic	✓	✓	✓	LAN	limited
ACme	[27]	socket	academic	✓	✓	✓	6LoWPAN	limited
Ubi-PMeter	[28]	socket	academic	✓	✓	-	ZigBee	extensive
SmartMeter	[35]	socket	academic	✓	✓	✓	802.15.4	limited

Table 2.1: Comparative overview of studied HEMS solutions.

feedback is a research attempt to provide an enhanced HEMS based on an existing E750 smart meter from the Landis+Gyr corporation [7]. It is based on the E750 meter so as to aggregate power consumption data both on household and appliance level. Except of advanced monitoring interoperability, "Handy feedback" exhibits more competitive features. The appliance recognition is not achieved via the use of elaborate ([37]) or simple ([31],[39]) classification algorithms that rely on power footprint profiling. Moreover, it does not require additional sensors towards the same objective. Instead, it takes advantage of the E750's offered capabilities. Regardless the above, its unrivalled characteristic is the extent in which the user is facilitated with energy feedback. An advanced web-API is developed that enables consumers to login remotely and monitor the power consumption of single appliances via web services. The latter, and specifically its user-friendly GUI, is what attributes the most towards increasing the user's energy awareness.

Nevertheless, although the smart meter solution is easier to deploy in comparison to multiple smart sockets, still as a centralized architecture it is more prone to various malfunctions. First of all, it is a single-point failure system and inflexible to deployment alternations. In addition, an important drawback is the fact that it does not offer appliance control. Moreover, the actual HEMS does not exhibit wireless communication features since the power consumption data are measured centrally by the meter. To that

[1] custom refers to a HAN protocol selection that depends upon the utilized smart metering solution.

extent, the notion of HAN cannot be directly attributed to it. Finally, neither Handy feedback nor any other solutions from Table 2.1 promote the user to an integral entity of the HEMS. Despite their auxiliary API functionalities the user still remains an observer that may be willing to adjust or not his power footprint. Instead, PMA can sit on top of any smart meter/socket based HEMS with appliance monitoring and power supply control. From thereon, it can increase energy conservation by promoting the user to an actual participant of the HEMS.

2.2.2 Power Metering

Between a smart meter or a smart socket solution, the latter was preferred since as an approach it would potentially end up with a more scalable implementation. In Appendix 6.1, a complete overview of custom and commercial smart sockets is provided. These specific products were encountered whilst conducting a literature survey. Initially, the PMA's design approach required the development from scratch of a custom socket. Nevertheless, it was concluded that profound EE knowledge and guidance was required and to that extent, the design stage relied to three specific commercial solutions, presented later on in Chapter 3.

Amongst the various metering approaches there was one particular research that suits the PMA protocol best. Nemo [43] is a power metering solution specifically designed for Wireless Sensor Networks (WSN). According to its operation layout, a special hardware circuit board is developed for WSN deployments that can be attached to a host sensor node. This platform uses the power cabling between Nemo itself and the host in order to exchange power measurements in real-time. The energy information is transmitted solely through the power line by modulating the current load and the supply voltage. To that extent, Nemo resembles a lot the thesis's proposition. In the PMA protocol, information is also exchanged over a power cord. In particular, both thesis's proposed communication schemes have exactly the same operating principle as Nemo's modulation techniques. When the socket/Nemo needs to send data to the device/host node, it modulates the power supply. On the reverse link, the device/host node modulates its power demand to carry data. Although Nemo was published in April 2013 it was long after PMA's design methodology had been formulated. Yet, its contribution was tremendous since it proved that similar concept deployments can be successful.

Nemo is an innovative implementation of a smart metering solution that employs power modulation techniques for data communication. Nevertheless, the same features are also exhibited in PMA but the application domain and the nature of electrification are entirely different. Nemo and its host are powered on DC, whereas in PMA the power cord runs on AC. Moreover, in spite of WSN inherent drawbacks (such as duty cycle related operation

and communication initialization only by a host) Nemo is described by its developers as a non-invasive implementation. Still, this assumption cannot hold in a non-WSN deployment. In case a laptop is acting as the host, then dedicated cabling are needed to commute data from and towards Nemo. Then Nemo's non-invasiveness feature is negated whereas PMA retains its own. The reason is because the PMA does not imply the use of any extra hardware neither for the device nor for the communication link.

2.2.3 Secure Pairing Protocols

Except of the association schemes listed in [41], there are many other alternatives since device pairing is an ongoing research topic especially in the wireless security spectrum. For example, more elaborate schemes are the Bluetooth pairing [30] and the Wi-Fi Protected Setup (WPS) [8]. The latter, in its Push Button Configuration variant, achieves minimal user intervention. In order to associate a device with the wireless network, the user has to press a button on the access point and then initiate the WPS from the client device within a 2 minutes deadline. Although WPS could be employed in order to pair the socket and the device, the probability of collisions is high if another device also starts pairing during the same time interval. To that extent, WPS served only as a stimuli in identifying a more robust OOB link.

Sony's Authentication Outlet [4] is exactly such a kind of association protocol. As a solution it does not only offer a secure method of pairing, but above all, it pushes forward the boundaries in user's active participation and power footprint correlation within a HEMS. The association is done by the use of RFID tags. Every user has to scan his RFID card over the socket's RFID reader in order to achieve pairing. Although, it is very innovative, straight-forward in use, and does not require extensive human intervention, it introduces new problems. Firstly, the device is not considered as an integral part of the pairing scheme. Furthermore, both sockets and appliances need new RFID hardware. Most important of all, instead of the device, in fact it is the plug that is being authenticated. The user must manually enter into the provided overlying GUI the specifications of the device in order to relate them with the connected socket. Finally, there is also the need for a mass supply and adoption from end-users of such RFID cards, and mass deployment of RFID sockets in common and private habitats. In PMA such implications are avoided since it comfortably sits on top of existing hardware equipment. Moreover, PMA's implementation can both associate the socket with the device and ultimately its user.

Ultimately, the PMA protocol inherits the best features from Sony's solution. First, it employs an pairing method for correlating a smart device with a smart socket. Moreover, it retains the device's user as an integral part of the HEMS by indirectly pairing his credentials with the used

socket. According to [41], the user must not be directly involved in the pairing due to potential *rushing user* phenomena. To that extent, the focus was mainly driven on the device-socket pair instead of the user-socket as in Sony's product.

Chapter 3

Protocol Overview

In this chapter the PMA's operating principle is explained in detail. Further, the design considerations are presented, detailing the various constituents of the PMA protocol and their intrinsic characteristics and finally, PMA's architectural design is unfolded.

3.1 Protocol Definition

The proposed association protocol inherits the intrinsic methodology of most pairing algorithms. The association procedure is achieved via the exchange of tokens through the OOB channel –the AC power cable in our case– between the two counterparts (device and socket). A server is also present and assists the procedure over an auxiliary HAN link (wireless or wired). Depending on the transmission direction (who is the sender and the receiver of each token) two distinct communication schemes are defined (Section 4.1). When the sender is the device the scheme is labelled as ***Device-to-Socket (D2S)***, and in the reverse direction, as ***Socket-to-Device (S2D)***.

The protocol is launched every time a device is plugged into a smart wall socket by its user. The user then uses the auxiliary HAN link and requests from the server to be granted with electrical power by initializing the underlying PMA algorithm. As a response, the server allocates a configuration setup message including i.a. the actual token, and forwards it again over the auxiliary link to the appropriate scheme's sender.

Each token is transmitted by the sender as a series of binary signals of varying pulse length and amplitude sent over the power cable. Typically, the communication frame (Section 4.2) consists of a training/synchronization sequence followed by the token. The token's bits are encoded by modulating the amplitude (high/low in Fig. 3.1) of the power consumption in the D2S scheme, and by modulating the status of electrical supply (on/off in Fig. 3.1) in the S2D scheme. On the whole, modulation is performed in a manner that resembles common communication modulation techniques (Section 4.3.3).

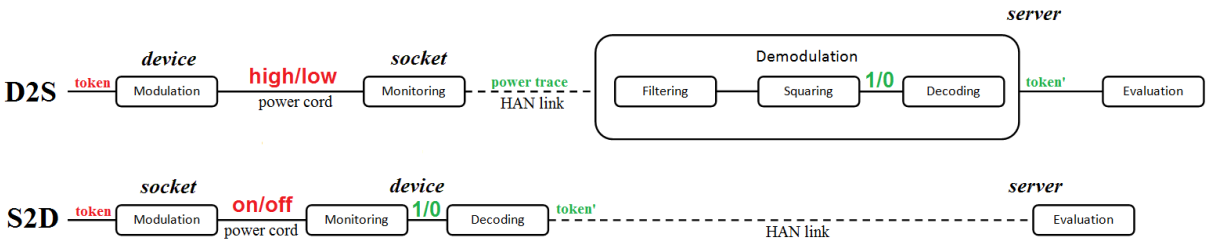


Figure 3.1: Communication schemes' information flow.

The receiver collects the raw binary signals and forwards them to server in the S2D case, or reformulates them via demodulation into a token and forwards this decoded token back to the server in the D2S case. The server, in S2D case only, will demodulate itself the raw data into a token. The demodulation procedure (Section 4.3.4) in the D2S case is consisted of a filtering routine which denoises the power trace, a squaring routine that transforms the filtered trace into a square wave of binary amplitude, and finally a decoding process that reformulates the squared trace into a token. In the S2D case demodulation contains only the decoding routine.

Finally, in both cases the server evaluates the two versions and upon a match the association is considered complete and the device is granted with electrical power. Otherwise, the procedure is repeated for a predefined number of attempts. In case of persistent failure, the socket is directed to switch off its relay and the device is denied access to electrical power. In Figure 3.1 the information flow for both schemes is presented, whereas the employed methodology will be described in Section 5.2.

3.2 Requirements

Using power modulation to create signals for the employed association protocol sets some specific requirements for both the device and the socket. The pairing protocol is designed for smart devices such as laptops and smartphones. Similarly, smart wall sockets are used as the other counterpart to be paired. Both entities must be qualified with the ensuing characteristics in order to facilitate proper operation.

1. ***Computation capabilities:*** Both entities must be equipped with a processing unit and memory. These features are essential for executing complex numerical and algorithmic instructions and thus, supporting PMA's hosting. To that extent, reprogrammability to custom needs is a vital feature for research, especially for the smart socket side.

2. ***Communication capabilities:*** Both entities need to be equipped with an antenna or LAN adapter for wireless/wired intercommunic-

Figure 3.2: Smart socket solutions: GoGreen's Energy Meter, iHome's Power Switch, and NXP's OM13006 Kit (EM773 Plug Meter and USB Dongle).

ation, since the PMA protocol directs that auxiliary information is exchanged via a wireless/wired channel.

3. ***Advanced powering features:*** For each distinct communication scheme different prerequisites need to be taken into consideration.

   - **Device-to-Socket**: From one side, the ***socket*** must be able to monitor the power consumption of the attached device at high resolution and sampling rate rates. The collected power trace can be either stored and processed locally, or transmitted to a server for further data manipulation. On the contrary, the ***device*** must be capable of controlling its power draw in a modular and software directed manner.
   - **Socket-to-Device**: In the same vein, the ***socket*** needs to be equipped with a relay in order to modulate the power supply by switching on/off the electricity. Concurrently, the ***device*** must be capable of constantly monitoring and indicating the status of its power supply provided by the wall socket.

Unless the aforementioned requirements are not fulfilled, the association protocol cannot be successfully implemented and applied. Fortunately, as far as the ***device*** counterpart is concerned, any common laptop computer or smartphone can very well satisfy the above description.

Regarding the ***socket*** module, the above requirements can be satisfied by various off-the-shelf smart sockets. Three different products presented in Figure 3.2 are used in our testbed. After evaluation (see Section 5.1), the third solution was promoted as the optimal one. The OM13006 metrology engine from NXP[9] consists of two components; the actual socket power meter and a USB Dongle, which serves as the power trace sink. The power meter is based on an EM773 energy metering IC accompanied with an ARM Cortex-M0 (50 MHz, 8kB SRAM, 32kB Flash, FreeRTOS) and a wireless M-Bus 868MHz OL2381-based communication antenna. The USB sink is a wireless transceiver with an LPC1343 MCU and the same OL2381-based

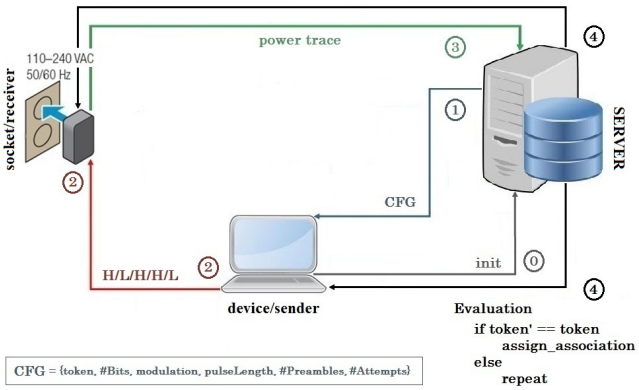


Figure 3.3: ***Device-to-Socket (D2S)*** communication scheme and association protocol stages. (H/L: High/Low power consumption footprint).

communication antenna. The power meter measures along with other electricity features the voltage, the amperage, and the active power in Watts within 1% accuracy and at a sampling rate of 1 Hz. Then it transmits the information to the USB Dongle that is attached to a server. Nevertheless, in the end solution the server can be easily skipped and its software responsibilities can be appointed to the socket thanks to the latter's advanced operability (see Section 6.1).

3.3 Architectural Design

PMA's novel pairing mechanism is based on a multi-tier architectural design. As stated before, the protocol can operate in a more simplified peer-to-peer version in which the socket will act as the server. Nevertheless, the current implementation includes a server that coordinates the overall pairing process. The protocol is unfolded in five stages, partially differentiating for the two communication schemes whenever applicable (Figures 3.3 and 3.4):

- **Initialization (Step** 0**)**: In the first step, the server and the device discover each other when the latter is attached to a socket. A secure auxiliary wireless or wired[1] channel is established between the server and the device via the exchange of identification information. The user/device's credentials are sent to the server otherwise the PMA algorithm cannot be launched. This information can be later on added to the final socket-device association pair in case of successful pairing[2].

[1]Depending on the deployed underlying HAN infrastructure.

[2]In future implementation expansions, the user's intervention can be fully omitted if automatic profiling tools can extract his identification indirectly from his device ID. For more information please refer to Section 6.1.

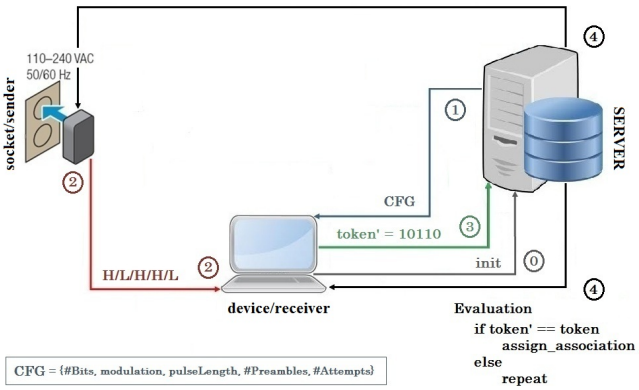


Figure 3.4: ***Socket-to-Device (S2D)*** communication scheme and association protocol stages. (H/L: On/Off electrical supply).

- **Configuration Setup (Step** 1**)**: The server forms the configuration of the communication frame (*CFG* in both figures) which consists of the token, the token's number of bits, the modulation technique, the signal pulse length, the number of synchronization preambles, the number of attempts, and sends it to the device.

- **Modulation and Monitoring (Step** 2**)**: According to the communication scheme, the sender forms and transmits a communication frame. Concurrently, the receiver initializes the monitoring routine.

  - ***D2S***: In the D2S scheme, the token is formulated as a series of high and low power consumption levels. The *device* is modulating its power demand and at the same time, the *socket* is recording the power footprint of the attached device.
  - ***S2D***: In the S2D scheme, the token is formulated as a series of on and off electrical supply status. The *socket* is modulating the power supplied to the attached *device*, which from its side is able to indicate whether it is powered or not.

- **Demodulation (Step** 3**)**: The receiver processes the raw data and decodes them into a token according to the configuration message.

  - ***D2S***: In D2S's current implementation[3], the socket is not capable of executing the demodulation procedure. Instead, it simply forwards the raw measurements to the central server. Then the server completes the stage by itself.

[3]Once again, in future implementation expansions the server's participation can be fully omitted if the corresponding software functionality is transferred to the socket. For more information you are referred to Section 6.1.

  - ***S2D***: In the S2D scheme, the token received by the device is then conveyed back to the server.

- **Tokens' evaluation (Step** 4**)**: The server evaluates the received token by comparing it with the initially allocated one. He then notifies the device about the outcome and acts accordingly to the result. In case of success, the associated pair of device and socket is stored in local records. Furthermore, as previously mentioned, the record can be augmented with the user's credentials as they were extracted during initialization stage. Thus, the user is also considered as a part of the formerly established association. Ultimately, the user/device is granted with power and individual billing is commenced. On the contrary, in case of unsuccessful association the process is repeated for a number of predefined attempts. In case of persistent failures, the socket is directed by the server to cut off the energy supply to the device/user.

Chapter 4

Implementation Analysis

In this chapter, the two communication schemes are further elaborated by focusing on the implementation features that differentiate them. Moreover, the actual communication frame is presented, and the implementation of the various protocol phases is explained in detail.

4.1 Communication Schemes

As previously stated, in both the D2S and S2D schemes a token is transmitted in digital format, as a series of high and low level signals. The difference resides in the way these levels are constructed from the binary bit stream, and realized in each scheme. The token is formulated in a mutually defined –and thus recognized– modular manner, which the receiver only needs to reverse engineer so as to elicit the conveyed information. All these directives on how to accomplish the prior is embedded into the configuration message sent initially from the server to both pairing counterparts.

4.1.1 Device-to-Socket (D2S)

In the D2S scheme the token is conceived as a series of high and low power consumption levels. Every bit of the token is produced by an abrupt increase or decrease in the power consumption level on the *device* side. At the same time, since the NXP's *socket* can measure (1Hz sampling rate) the device's energy footprint it will be able to *a posteriori* detect these variations in wattage within the actual power trace. After experimentation (see Section 5.3) it was proven that the D2S scheme is applicable only in laptops.

In order to transfer a **'1' bit** of the binary token, the laptop adjusts its power consumption to the highest achievable level by absorbing as much power as possible. This can be achieved by increasing the screen's brightness to 100% and/or stressing the CPU load to 100%. Both tactics are administered for a maximum energy consumption. In addition, elaborate methods

have been developed all aiming at exerting nearly a 100% CPU load, ranging from benchmarking techniques, invoking large iterations, computing complex numerical problems (such as prime numbers calculation), and in multi-threaded operation whenever the laptop's CPU was multicore.

In order to transfer a **'0' bit**, the laptop adjusts its energy consumption to the lowest attainable level by consuming as less power as possible. This may be accomplished by decreasing the screen's brightness to 0% and/or suppressing the CPU's frequency to a minimum operational status. Analogously, both strategies are utilized for a minimal consumption. Furthermore, OS's inherent kernel features are being exploited for such a deliberate CPU performance degradation. Contemporary laptops support multiple CPU power management schemes i.a., powersave, on-demand, performance, which are regulated via kernel utilities named *powercfg* in Windows OS [10] and *cpufrequtils* in Linux-based machines [11]. Moreover, via these utilities the CPU frequency can be manually set even down to 1% of its capability.

The idea of switching to powersave mode and suppressing CPU performance ('0' bit), or algorithmically exerting 100% CPU load ('1' bit) relies on a fundamental notion; the correlation between CPU frequency (f) and power consumption (P) in any CMOS circuit abiding to the following formula:

$$P = C_L \cdot V_{DD}^2 \cdot f$$

where C_L is the gate load capacitance, V_{DD} is the supply voltage, and f the clock frequency[34]. Obviously, by simply altering the f while both C_L and V_{DD} remain constant, different power consumption levels can be achieved.

4.1.2 Socket-to-Device (S2D)

In the S2D scheme the token is formulated as a series of high (ON) and low (OFF) powering status levels. Every bit of the token is formatted by abruptly switching ON and OFF the electricity via the socket's relay. Thus, the power supply towards the device (laptop or smartphone) can be deliberately fluctuated. Concurrently, the device is able to continuously detect and indicate its electrical supply status, at a rate of 1Hz (1 power state per one second) according to PMA's implementation.

In order to transfer a **'1' bit** of the token, the socket's relay is switched ON. Equivalently to D2S case, this operation is algorithmically directed; the server sends a specific and predefined –by OM13006's default configuration– signal code in order to switch ON or OFF the relay. In order to transfer a **'0' bit**, the socket is directed to switch its relay OFF. Therefore, these pulses corresponding to varying powering status are identified by the device and can be stored locally for the proceeding demodulation process.

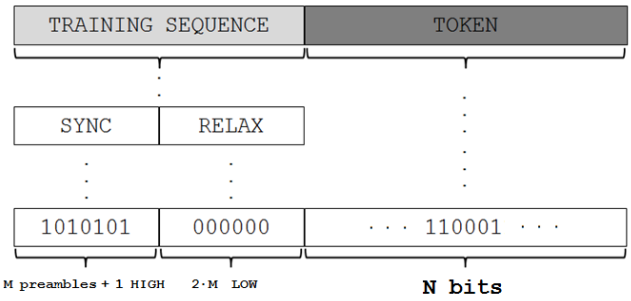


Figure 4.1: Communication frame format.

4.2 Communication Frame

The communication frame is a sequence of raw samples captured by the receiver. Each sample in the D2S case is a power measurement in Watts which lasts 1 second in duration. In the S2D case, each sample is an electrical status indication again of 1 second in duration. A set of several samples forms one pulse, which is the building block of the frame. In the D2S case, we need 4 samples whereas in the S2D case only 2. The overall frame's format is depicted in Figure 4.1. The `TRAINING SEQUENCE` is partitioned into a `SYNC` period and a `RELAX` one. The `SYNC` field (by default interpreted as 101010101, 0x55) is comprised of M number of preambles[1], plus one high pulse. Its role is to mark the start of the communication frame and provide information about the level of the high pulse in the D2S scheme. The `RELAX` period is a set of $2 \times M$ low pulses. It serves the identification of the noise level for the D2S scheme and in general, it facilitates further the synchronization with respect to the beginning of the `TOKEN` section. Finally, the `TOKEN` is N bits in length with each bit constituted by a number of high or low pulses depending on the selected modulation technique.

4.3 Protocol Stages

The PMA protocol is unfolded in four distinct phases which were previously introduced in Section 3.3. In the current section, the implementation aspects of the various stages will be explained in detail.

4.3.1 Initialization

According to implementation, the corresponding communication during initialization is facilitated by web-socket programming API and a minimal UI.

[1]We abusively define as a preamble, a pair of a high and a low pulse.

4.3.2 Configuration Setup

As previously described in Section 3.3, the configuration message allocated by the server is comprised of the following set of information:

1. ***Number of token bits*** : A length of **10 bits** was chosen for the token. Different lengths can be supported since it is set as a variable.
2. ***Token*** : A user may select any decimal number from **0 up to 1023**. Its binary representation is then used for all subsequent PMA's stages.
3. ***Modulation technique*** : Five modulation methods were developed, implemented, and experimentally evaluated (see next section).
4. ***Pulse length*** : According to subsection 4.2, the communication frame consists of a set of high and low level pulses. Every pulse lasts **4 seconds** in duration for the D2S scheme and **2 seconds** in the S2D case. This relatively high number in the D2S case is chosen to facilitate a proper deployment for all the modulation methods (see next section).
5. ***Number of `SYNC` preambles*** : Since the `SYNC` period is chosen to be valued **10101010**1, the number of preambles (pairs of one high plus one low pulse) must be then set to **4**.
6. ***Number of attempts*** : Every association procedure can be repeated up to **2** number of attempts according to the current implementation.

4.3.3 Modulation

The modulation routine directs the manner according to which the various token bits are formulated. This adheres to explicitly defining the number of high and low pulses each bit in the `TOKEN` period will be comprised of. To this extent, the actual implementation was inspired by typical modulation techniques used is digital communication theory [40]. In our protocol five methods are developed and experimentally verified, which are labelled: *Pulse Code Modulation* (**PCM**), *Non-Return Zero Level* (**NRZL**), *Amplitude Shift Keying* (**ASK**), *Binary Frequency Shift Keying* (**BFSK**), and *Binary Phase Shift Keying* (**BPSK**). These methods resemble only in notion and should not be identified as identical to the actual homonym techniques.

Assuming that we want to transmit the token $710_{(10)} = 1011000110_{(2)}$, the token's formulation for each method respectively will comply to the format exhibited in Table 4.1. For example, in the PCM variant every '1' bit of the token's binary representation is conveyed as one high pulse, and every '0' bit as one low pulse. In more elaborate schemes such as the BFSK, every '1' bit is transmitted as a series of a high, a low, a high, and a low pulse, whereas every '0' bit as a series of two high pulses accompanied with two consecutive low ones. To that extent, having relatively small pulse lengths would have hindered the proper deployment of all the previous transitions.

Table 4.1: Modulation techniques representation example.

Method	Token : $710_{(10)} = 1011000110_{(2)}$
PCM	H - L - H - H - L - L - L - H - H - L
NRZL	HH - LL - HH - HH - LL - LL - LL - HH - HH - LL
ASK	HL - LL - HL - HL - LL - LL - LL - HL - HL - LL
BFSK	HLHL - HHLL - HLHL - HLHL - HHLL - HHLL - HHLL - HLHL - HLHL - HHLL
BPSK	HLHL - LHLH - HLHL - HLHL - LHLH - LHLH - LHLH - HLHL - HLHL - LHLH

4.3.4 Demodulation

While the sender is in modulation phase, the receiver simultaneously commences the monitoring procedure in order to collect the raw communication frame data. The objective of the demodulation is to process the raw data and reformulate them into a token conforming to the configuration message directives. This procedure is different for the two communication schemes.

- In the **S2D scheme**, the outcome of the monitoring routine is a sequence of ones and zeros corresponding to the output of the employed power supply polling mechanism (*WMIC Win32_Battery* utility in Windows OS [12], and *acpi* in Linux-based machines [13]). At a sampling rate of 1Hz, a 'one' is recorded if the device is electrified and a 'zero' if not. This binary sequence is traversed until the `SYNC` preambles are detected. Then, based on the pulse length, the number of token bits, and the modulation scheme, the binary sequence is decomposed into a number of symbols. Depending on the prevalence of ones over zeros and versa, each symbol is promoted to '1' or '0' bit respectively. Thus, the whole communication frame information is deduced, and the `TOKEN` transmitted over the channel can be validated.

- In the **D2S scheme**, the outcome of the monitoring routine is the power trace composed of measurements in Watts that may be inherently noisy. In order to extract and discard the noise from within the trace, a `filtering` subroutine is used. In particular, a moving average filter [14] with a window size of two samples is applied (see Section 5.3), and any fluctuations of insignificant amplitude are then eliminated. The denoised power trace must be then dispatched to `squaring` subroutine which classifies every filtered sample to '1' or '0' level according to a threshold value. The threshold is defined (see Section 5.2) after the `SYNC`'s maximum high (P_H) and low (P_L) pulse power level preambles, abiding to the following formula:

$$threshold = \frac{max(P_H) + max(P_L)}{2}$$

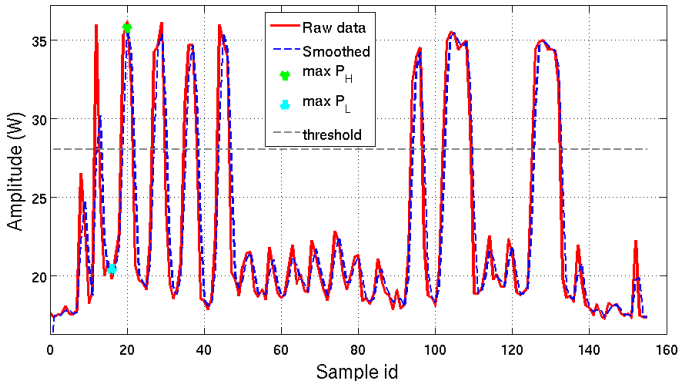


Figure 4.2: Filtered power trace indicating threshold value.

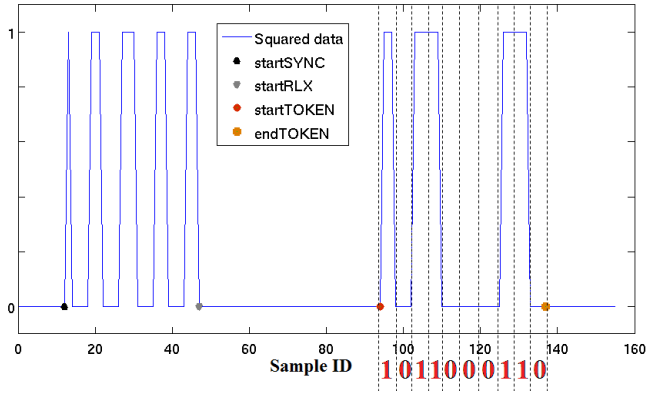


Figure 4.3: Squared power trace indicating `SYNC`, `RELAX` and `TOKEN` boundaries. Both `filtering` and `squaring` processes are applied to same trace with PCM modulation and with $710_{(10)}$ as the transmitted token.

As an output, a square wave is produced that can be fetched into the `decoding` subroutine, which is identical to the procedure described in the S2D's case. In Figure 4.2 the output of the `filtering` subroutine is presented. Although the denoised waveform almost coincides with raw one, the `filtering` subroutine is important for the protocol deployment as the experimental results proved (see Section 5.5.2). For the same initial trace, the `squared` form is given in Figure 4.3 along with the outcome of the `decoding` phase.

4.3.5 Token Evaluation

Token evaluation is implemented as a simple binary comparator between the initially allocated token and the demodulated one.

Chapter 5

Experimental Evaluation

In this chapter, the experimental setup is presented including a detailed description of the parameters that were evaluated, and the experimental results obtained after actual running conditions deployments.

5.1 Experimental Setup

The experimentation testbed is constituted of the ensuing components. Regarding the ***socket*** side, after a literature survey three off-the-shelf smart sockets were evaluated, see Table 5.1. The response of each socket was measured individually and NXP's product was determined as the best solution. Moreover, a plethora of smart hardware systems was utilized as the ***device*** side counterpart. In Table 5.2 the technical specifications of each device are presented as well as their role in the pairing protocol. In most of the experiments, the Dell laptop served as the device side, whereas the HP laptop operated as the ***server***. An actual deployment of the testbed including all the aforementioned components is depicted in Figure 5.1.

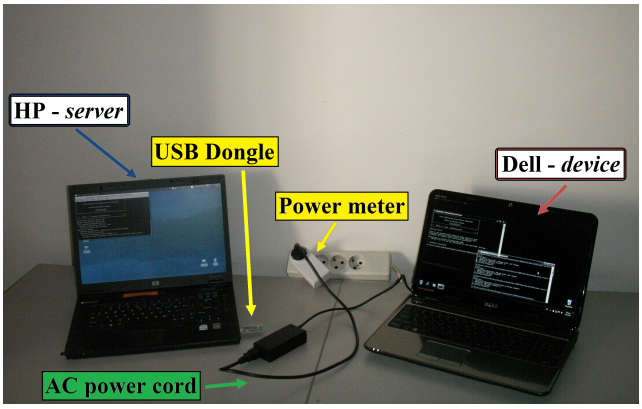


Figure 5.1: Experimentation testbed in actual running conditions.

Table 5.1: Socket Power Meter Comparison

Product name	Energy Meter[15]	Power Switch[16]	OM13006
Manufacturer	GoGreen	iHome	NXP
Accuracy	10%	>5W	1%
Sampling rate	0.5Hz	0.1Hz	1Hz
Transmission rate	–	0.1Hz	<1KHz
Wireless protocol	–	Z-Wave	M-Bus
Relay	–	✓	✓
Reprogrammability	–	limited	extensive

Table 5.2: Deployed Hardware Systems Specifications

Brand	Model	CPU	OS	Role
Dell	Inspiron 5070	4x Intel i3 M370 @ 2.39GHZ	Windows 7	Device
Lenovo	ThinkPad	4x Intel i3 M330 @ 2.13GHZ	Ubuntu 13.04	Device
HP	Compaq nx 740	2x Intel T5500 @ 1.66GHZ	Ubuntu 12.04	Device/Server
Packard Bell	Netbook-ZE6	Intel N570 @ 1.66GHZ	Windows 7	Device
Samsung	i5800	Samsung S5P6422 @ 667MHz	Android 2.1	Device
Raspberry Pi	B	ARM1176JZF-S @ 700MHz	Raspbian	Device/Server

In addition to the prior, both for the previous and the results to follow, the number of $710_{(10)}$ as the token to be transmitted was always selected. This specific number was deliberately chosen due to its "challenging" binary representation. For example, selecting $512_{(10)} = 1000000000_{(2)}$ would not have facilitated at all PMA's overall implementation procedure since the noise effect would have been difficult to identify.

5.2 Evaluation Procedure

Different experimental parameters were considered during the evaluation procedure in order to assess the validity of the PMA association protocol. These parameters refer to the different implementation phases given below.

1. ***Communication schemes deployment***. Initially, each scheme's applicability had to be verified for both the laptop and the smartphone. The protocol was deployed for both devices and with respect to S2D and D2S cases, at different battery levels for the latter. Moreover, all the developed modulation methods had to be tested. For brevity reasons, the output trace for only the D2S case is shown in Figure 5.2.

2. P_H ***realization***. As a next step, the various means of conducting the modulation had to be implemented for only the D2S scheme, since producing high and/or low pulses for the S2D case was relatively easier.

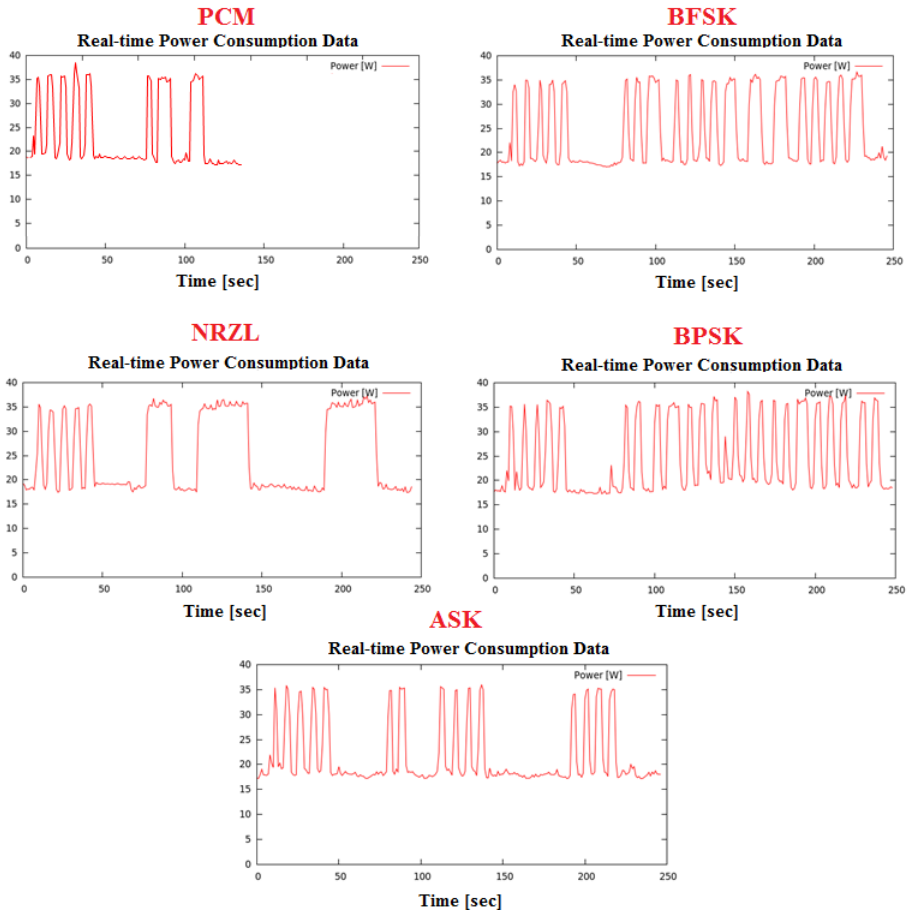


Figure 5.2: Power trace of D2S's modulations in non-noise conditions, with disabled kernel's power management, and with detached laptop's battery.

To that extent, two different parameters for pulse signalling were evaluated; adjusting the display brightness and exerting a high CPU load.

3. P_L ***realization***. During low pulses, the presence of *noise* was exhibited in the communication channel for the D2S case. In general, noise is interpreted as undesired distortion of the power trace. According to experimentation, noise may be attributed to either unexpected CPU scheduling tasks (preemptive CPU utilization) and deliberate malicious user's interventions (irrelevant applications' launch whilst in association procedure). In order to avoid noise interference, the influence of intrinsic OSs' CPU degradation utilities (previously explained in Section 4.1.1) was experimentally assessed.

4. ***Demodulation filtering***. Despite of CPU *underclocking*, noise could still be reported in some device cases (such as the Netbook-ZE6) or

generally, when a laptop's battery was not fully charged. The noise level can significantly affect the overall communication and to that extent, various filtering and threshold formulae were employed. During implementation two different filtering algorithms (*noving average* and *median*) were examined that were invoked with various window sizes (from to 2 up to 5). Moreover and regarding the threshold level, it can be alternately defined according to `SYNC`'s period local maxima as:

$$
\begin{aligned}
(A): &\quad min(P_H) \\
(B): &\quad \frac{min(P_H) + max(P_H)}{2} \\
(C): &\quad \frac{min(P_H) + max(P_L)}{2} \\
(D): &\quad \frac{max(P_L) + max(P_H)}{2}
\end{aligned}
$$

Nonetheless, in order to evaluate the robustness of the prior –since CPU's intrinsic noise cannot be deliberately enforced– independent stressing routines were also developed and run in parallel when needed[1]

5. ***Total BER evaluation***. Finally, extensive experimentation was conducted regarding the overall evaluation and correctness of the proposed protocol. Since it is in fact a half-duplex communication mechanism, its validity is explicitly defined with respect to the **Bit Error Rate** (BER) notion. BER can be elicited from the Hamming distance [23] between the initially allocated token by the server, and the token that is reformulated via demodulation by the receiver.

5.3 Experimental Results

In the ensuing text, the experimental results for each phase of the aforementioned evaluation procedure are explained in detail.

Communication schemes deployment. The initial experimental setup referred to both a smartphone and a laptop deployment, in noisy conditions for the latter. Furthermore, experimenting with different battery levels provided with two major conclusions. Initially, it was found that the output power trace behaves similarly for the cases above and below approximately 85% of Dell's battery status. In Figure 5.3, the relative difference between the high and the low pulse level is illustrated. Apparently, the amplitude of $P_H - P_L$ is influencing the modulation process since if it is considerably low then there is not sufficient margin for creating the two signal levels.

[1]When employed during modulation the stressing routines will produce noise since their implementation is similar to the very same algorithm that is responsible for exerting a 100% CPU load whilst formulating a P_H. Thus PMA's consistency is further solidified.

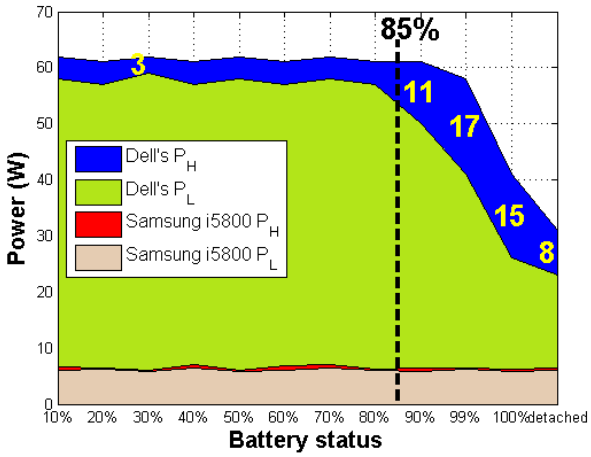


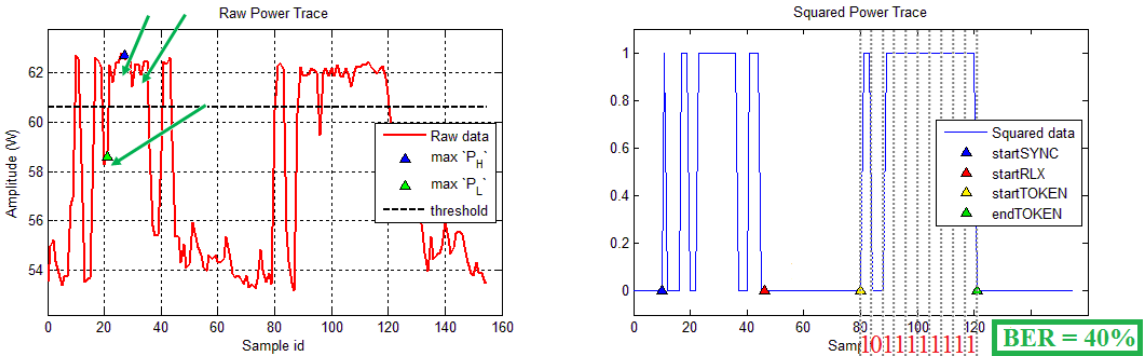
Figure 5.3: $P_H - P_L$ relative difference (purple in Dell, red in Samsung) for D2S and various battery levels. 85% margin was reported only in Dell case.

Secondly, the initial idea directed the unilateral development of the D2S scheme. Nonetheless, deploying it in smartphones is proven to be unsuccessful since the corresponding relative difference in Figure 5.3 is nearly zero[2]. Finally, Raspberry Pi's case was the most cumbersome of all. From one hand, the S2D scheme cannot implemented at all since there is no auxiliary power source and thus, if the socket is switched off the Pi shuts down instantly. On the other hand, the D2S's deployment was also unsuccessful. Available Raspberry Pi models do not offer any kind of CPU power management utilities nor any other means for power demand fluctuation.

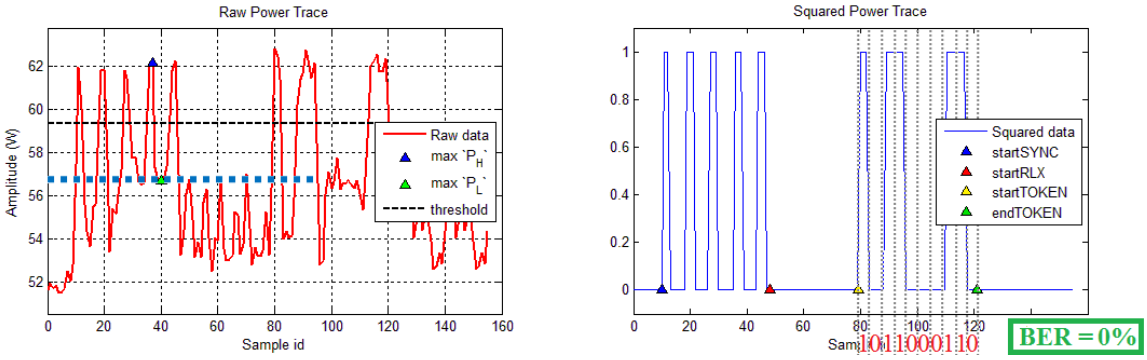
P_H ***realization***. The initial idea with respect to modulating the power footprint signature was by means of adjusting the display brightness. Nevertheless, experiments indicated that even at drastic transitions (from 0% to 100% and versa) the relative difference in recorded power amplitude was not significantly comparable with the overall waveform (less than 3W). For brevity reasons, the related figure is provided in the PMA's support website, [17]. To that extent, various *stressing* algorithms were developed (Section 4.1.1) in order to exert a high CPU load, and thus increase the overall power consumption in conjunction with the brightness fluctuations. Empirically, the prime numbers calculation variant was the one selected for the experiments since it could inflict almost a 100% load for both Dell laptop's cores.

P_L ***realization***. The noise effect is especially precarious when transmitting low pulses. The 'zero' level if augmented with noise can reach or surpass the 'one' level (indicated with green arrows in Figure 5.4a), thus increasing the overall BER. As a safety countermeasure, the laptop is algorithmically

[2]Modulating the power demand in smartphones could not be achieved at a desirable level. Therefore, S2D was introduced and experimentally verified for both devices.



(a) Disabled OSs' kernel power management features for PCM case.



(b) Enabled OSs' kernel power management features for PCM case.

Figure 5.4: Effect of CPU performance degradation with similar noise.

switched to *powersave* mode, thus behaving as if it is "sedated"; whatever a user's application or a CPU scheduler's task will attempt to execute will be significantly delayed in processing[3]. Therefore, since CPU performance is procrastinated, the laptop's power trace retains at mediocre levels when sending low pulses, at least comparatively lower than the high pulse level (indicated with blue line in Figure 5.4b). The utilization of OSs' intrinsic power management features was chosen for extra robustness. In fact, the protocol can operate without switching to *powersave* mode but then it will be susceptible to noise related hazards. In Figure 5.4 the influence of the above features' application is exhibited onto the actual power trace. Without power management (Fig.5.4a) the BER is 40%, whereas with (Fig.5.4b) it is 0%. Nevertheless, the actual gain attributed by the introduction of power management features cannot be calculated. The reason is because noise is an inherently unpredictable factor and thus the imposed BER decrease remains unidentifiable. Moreover, the noise influences differently the various modulation schemes. For example, in PCM case a 100% BER can be reported only with 0 tokens, whereas BFSK and BPSK are more error-prone.

[3]since in *powersave* CPU's frequency can be manually set even to 0% of its capability.

Table 5.3: A posteriori evaluation of best 8/32 filter, threshold combos.

	Moving Average				*Median*			
Threshold \ window	2	3	4	5	2	3	4	5
A : $min(P_H)$	-	46.17	-	-	-	-	43.82	-
B : $\frac{min(P_H)+max(P_H)}{2}$	-	-	-	45.29	-	-	-	47.35
C : $\frac{min(P_H)+max(P_L)}{2}$	-	45.29	-	-	-	-	46.47	-
D : $\frac{max(P_L)+max(P_H)}{2}$	*43.82*	-	-	-	-	**43.23**	-	-

Demodulation filtering. Regarding the demodulation process, various filtering and threshold formulae were employed. In Table 5.3 the *a posteriori* evaluation of 8 different combinations of 2 filters, 4 window sizes, and 4 thresholds for the same input traces is depicted. A posteriori refers to the fact that during `squaring` implementation, the final evaluation tool of "BER calculation" had not been already developed. Instead, these combinations were chosen from the rest 26 since their output was closer to the expected behaviour, a fact that was later on verified. In most cases, the traces exhibit higher input noise than normal scenarios, and referred to various deployment devices such as the Dell and the Lenovo laptop as well as the Netbook-ZE6.

According to the results, the optimal combination is the *median* filter for a window size of *3* and with (D) as threshold formula, indicated with bold in Table 5.3. This set of rules reports a minimum 43.23% BER. Nevertheless, the difference in BER compared to the combination that was employed in most of the experimentation (*moving average*/2/(D)) is almost marginal, with 43.82% BER in the latter case indicated with italics. Relatively small differences apply also for the other combinations. The reason is because the specific experimentation environment was deliberately defined at the extremes in order to facilitate a robust `squaring` implementation. Moreover, these 8 cases spread equally in between the two filters, thus not providing a concrete conclusion about which one should be preferred. Regarding the window sizes, it is also hard to reach a decision whether small sizes lead to a lower BER rather than larger ones. Finally, the only succinct conclusion is the (D) formula's prevalence. Both its related results exhibit the two lowest BERs, a feature which was expected by definition. The threshold should not be too high in the trace as in case (B) or too low as in (C), neither should it rely entirely on a single level value as $min(P_H)$.

Total BER evaluation. The final conducted experiments involve the deployment of all PMA's operational stages. In Figure 5.5, the BER of the two communication schemes (D2S and S2D) for the five modulation methods and for 10 random tokens is presented. In particular for the D2S case only, different battery and noise levels also needed to be tested. Error bars (depicted with purple and only in S2D for clarity reasons) indicate the 95% confidence intervals calculated according to the standard deviation ($\pm 2\sigma$)

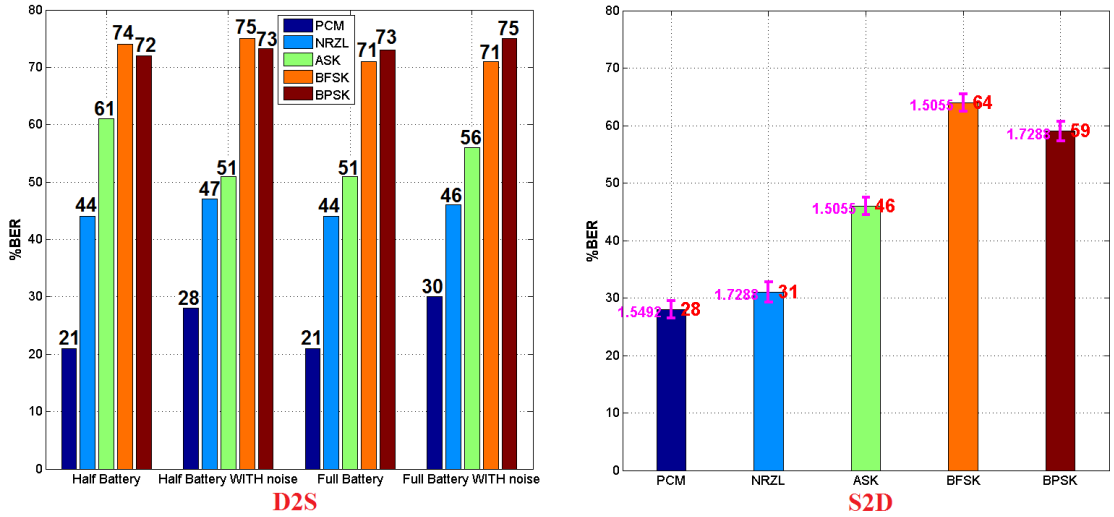


Figure 5.5: Modulation methods' BER for D2S (left) and S2D (right), and corresponding confidence interval. The results refer to 10 random tokens.

for the corresponding experiment. More information on the aforementioned and non-verification procedure steps as well as the raw results can be found on the PMA's support website [18].

According to the results, PCM can be attributed as the best modulation method since it achieves the lowest BER for all setups. Such an outcome was expected to be derived since PCM has the smallest pulse length and thus there are fewer *delays* whilst token formulation for both D2S and S2D schemes (see Section 6.1). A related important remark is the fact that in the end noise does not influence the BER behaviour in the D2S case. For example, BFSK reports the same BER when the battery is full whereas ASK with noise has lower BER than the non-noisy one for a half-full battery. This is because the *threshold* reassures that no noise is interpreted as a '1' symbol. Further, due to power management features the P_L level with noise raises only a few Watts. However, the BER can be reported even lower in noisy conditions. In such cases, shifts in the power trace are what further increases the overall BER (see Section 6.1). On the whole, the optimal communication modality for the PMA in general would include; D2S as the communication scheme, PCM as the modulation method, moving average with a window size of 2 as the filtering technique, and the (D) formula amongst threshold definitions. Ultimately, D2S's BER is reported at **21%** and S2D's at **28%** in the optimal above scenario.

5.4 Discussion

The main aim of a pairing protocol is to associate multiple devices that may simultaneously try to connect to different sockets in the same deployment. The number of devices that the server is capable of administering depends on the number of the concurrent pairing requests and it also determines the ***token's size***. An N-bit token with no bit errors can differentiate up to 2^N devices at the same time, although such extreme cases may not be encountered in actual deployments. In a home environment the token's size can be smaller, while lengthier tokens may be required in a campus/corporation site, or when low BERs are being exhibited. In the presence of bit errors, the server can still accomplish pairing by checking the Hamming distances between the tokens' versions. This is achieved since the PMA protocol is implemented so as to lessen the effect of noise. Furthermore, NXP's underlying HAN offers increased robustness with respect to multiple ***synchronously*** monitored devices. Nevertheless, the conducted experiments did not involve a parallel devices' deployment since only one OM13006 kit was available.

Finally, there are minor ***security*** issues regarding protocol's operation. The OOB link (AC power cord) is physically resilient to any interception since the intruder needs to be physically attached to a smart socket. Still, the auxiliary wireless/wired channel is prone to *Man-in-The-Middle* attacks but their overall negative effect can be tackled. Secure Sockets Layer (SSL) cryptographic techniques [19] can be employed specifically for the HAN medium. To that extent, the overall protocol can be considered as well secured.

5.5 Lessons Learned

The experimentation procedure revealed some obscure aspects of the protocol's implementation such as the bandwidth that the PMA can support as well as, its behaviour with respect to ambient noise conditions.

5.5.1 Channel Capacity

According to the experimentation's testbed, tokens are conveyed at a relatively low bandwidth due to the socket's fixed sampling rate, which cannot be set over 1Hz. In fact, NXP's product offered the maximum sampling frequency and reprogrammability of all commercial metering solutions encountered. As stated in Section 4.3.2, each pulse consists of 4 samples and lasts 4 seconds in duration in the D2S scheme, and 2 samples and 2 seconds in duration in the S2D case. Moreover, as shown in Section 4.3.3, depending on the modulation scheme a bit may be comprised of 1 up to 4 pulses (or symbols). Therefore, in the worst case (D2S's BFSK and BPSK) the

Table 5.4: Bandwidths of different modulation schemes in bps

Modulation	Pulse length (in symbols)	Bandwidth (in bps)	
		D2S	**S2D**
PCM	1	0.25	0.5
NRZL	2	0.125	0.25
ASK	2	0.125	0.25
BFSK	4	0.0625	0.125
BPSK	4	0.0625	0.125

channel bandwidth is 0.0625bps. In Table 5.4 the bandwidths of all modulation techniques for the two communication schemes are listed. In the experiments conducted, the optimal token (S2D/PCM) transmission takes $27 \times 2 = \mathbf{54\ seconds}$, with 10 bits of the `TOKEN` plus 9 pulses as the `TRAINING SEQUENCE` and 8 pulses in the `RELAX` period. To that extent, the overall duration is still within acceptable margins if considering that for instance the WPS requires 2 minutes to complete [8]. What can be deduced is that, with higher sampling rates higher bandwidths are expected to be achieved. However, then more elaborate experiments are required to detect the effect of the battery's rectifier (see Sections 5.5.2 and 6.1) as a bottleneck to the channel's bandwidth.

5.5.2 SNR Behaviour

Both communication schemes are designed in a noise-resilient manner. In ***S2D***, no noise can appear since symbols are by default of binary nature. On the contrary, in the ***D2S*** scheme enabling *powersave* mode accompanied with `filtering` and `squaring` suppresses the effect of noise. Although small window sizes[4] were reported to have the lowest BERs, it was experimentally verified that with an unfiltered power trace, the BER for the cases presented in Table 5.3 is 47.05%, 50.58%, 53.23%, and 46.47% for the A, B, C, and D threshold formulae respectively. To that extent, applying a filter cannot be discarded since it achieves lower BERs. Nevertheless, it was observed during experimentation that the battery has a significant impact on the modulation process. In particular, delays are incurred by the battery's rectifier since it is an inductive element (see Section 6.1). Assuming that an X amount of power responds to a high pulse level, the rectifier absorbs a relative small portion but large enough to delay the actual display of X within the monitoring routing, and thus affects the modulation speed.

[4] A *moving average* with window size of 2 and a *median* filter with a window size of 3 (as presented in Section 5.3) are approximating the input trace, thus implying that the `filtering` routine might have been unnecessary.

Chapter 6

Conclusion

The field of energy awareness and conservation was chosen as the thesis research domain. The proposed protocol's major contribution lies in that it can be well incorporated into an existing Home Energy Management System (HEMS). In the latter, identification of individual devices facilitates energy consumption reduction. Ultimately, by leveraging on PMA the individuals behaviour can be induced towards a more parsimonious energy footprint. The user is indirectly participating in the association scheme and thus individual pricing policies may be introduced.

The objective of this thesis was to develope an innovative pairing protocol that utilizes power modulation for data communication. In particular, inspiration was taken from Sony's RFID solution and existing HEMS relative solutions. Similarly to other pairing protocols, an authentication token is used for association. As a novel solution, the AC power cable constitutes the transmission medium with power modulation as the means of intercommunication. The token can be sent according to two different schemes (Section 4.1); *device-to-socket* (D2S) and *socket-to-device* (S2D). In D2S, the device is directed to fluctuate its power demand in order to transmit symbols. In S2D, symbols are sent by switching on and off the socket's power relay.

According to the experimental results (Section 5.3), the D2S is applicable only in laptops whereas the S2D can operate well for both laptops and smartphones. Moreover, the PCM modulation method is the optimal one since it achieves a 21% BER in the D2S case, and a 28% in the S2D. Although PMA's implementation is merely mature, the results are promising for future research. Still, there are a number of issues to be further investigated.

6.1 Future Work

- **Delays in Symbol Transfer**: The exhibited BER in both communication schemes may also be attributed to delays whilst the tokens are being formulated. In the ***D2S*** scheme, delays are produced in

between the kernel's mode switches, as well as when increasing or decreasing the exerted CPU load. For example, even if we switch to *on demand* mode and concurrently stress the CPU to 100%, a non-trivial amount of time is required by the CPU to complete the execution of these operations. In the ***S2D*** scheme, it is the very nature of the polling mechanism that may cause delays during token formulation. A '1' or '0' symbol is recorded by querying the AC powering status via indirectly invoking relevant kernel APIs. To that extent, the same nature of delays is also manifested as in the D2S case. Overall, the delays can considerably influence the `decoding` routing since shifts in the recorded trace might be exhibited. Further investigation needs to be conducted in order to identify the actual influence of the delays in the overall BER calculation.

- **Implementation revision**: The previous remark about the delays as well as the Lesson 5.5.2 indicate that both the *decoding* routine for the S2D and the *modulation* stage for the D2S need to revised in their implementation so as to achieve a better BER. For example, an interrupt-based solution for the S2D's *decoding* can be proposed. Currently, the AC powering status is indirectly polled via kernel utilities. An interrupt routine would significantly increase the speed of the polling mechanism and thus the modulation speed. Moreover, the whole protocol is subject to various other improvements such as the end-user's full incorporation into the association procedure, and deprecating the server's algorithmic assistance. The former, as initially mentioned in Section 3.3, can be achieved if automatic profiling tools can extract the user's identification indirectly from his device ID and during the *initialization* stage. The latter, also firstly mentioned in Section 3.3, can be accomplished if the corresponding server's software functionality is transferred entirely to the socket. The specific NXP's product and current server's programming APIs are fully compatible, thus facilitating an easy final transition.

- **Channel theoretical enhancement**: The current communication frame format is designed in a plain manner. In more advanced designs, CRC checksums may be added in order to increase the protocol's robustness. Moreover, the use of an auxiliary channel can be totally deprecated if the whole configuration message (including pulse length, number of attempts, etc.) is embedded within the frame. Finally, more investigation is required into the channel's SNR behaviour and so as to concisely formulate the delays during symbols' transmission.

- **Custom meter development**: Lesson 5.5.1 highlighted the protocol's major deficiency. The NXP's relatively low sampling rate results in a very low channel bandwidth. Further, in comparison to con-

temporary communication protocols, PMA can be characterized as an obsolete technology in terms of speed. To that extent, resorting to a custom-made smart socket implementation is the only solution as long as relevant corporate activities do not concern about increasing the sampling rate of commercial smart metering solutions.

- **Legacy appliances**: As an ultimate goal, any kind of everyday appliance must be able to actively participate under the PMA protocol. Currently, only smart devices such as laptops, smartphones or PDAs can be paired. Nevertheless, PMA can be expanded if the following considerations are satisfied regarding the two communication schemes.

  The ***S2D*** scheme is operational on the condition that the device has a backup energy source. Batteries in laptops or smartphones serve exactly this role. To that extent, they can easily detect the fluctuating power supply caused by the smart socket. In a future scenario, appliances may all be equipped with a simple MCU for monitoring and an auxiliary power module in order to support a fully S2D deployment.

  On the contrary, expansion in the ***D2S*** case is less demanding. Appliances need only to control their power demand in a software directed manner. Considering the appliances' manufacturing trend for more and more clever machines, the scenario in which each appliance can remotely communicate within a HAN and fluctuate its power trace does not seem improbable. Indeed, General Electric is the first enterprise to have already announced from July 2010 the introduction of the next generation HEMS. Nucleus [20], does not only provide the underlying HAN infrastructure, but it is an elaborate attempt to equip all GE's machines with advanced and common embedded systems for enhanced functionalities. On the same grounds, few modifications need to be performed in order that the PMA protocol finds its place in a full-scale and real-life deployment. Such envisions are not foreseen as precarious as long as attention may be driven into PMA's existence and relative importance.

Bibliography

[1] Directorate-General for Energy Unit, European Commission. Market observatory & Statistics: http://ec.europa.eu/energy/observatory/countries/doc/2012-country-factsheets.pdf. 2012.

[2] Office of Electricity Delivery & Energy Reliability, U.S. Department of Energy. Smart Grid R&D Multi-Year Program Plan (2010-2014). September 2011.

[3] Directorate-General for Research Information and Communication Unit, European Commission. European smart grids technology platform - vision and strategy for Europes electricity networks of the future. 2006.

[4] Sony's Authentication Outlet. http://www.sony.net/SonyInfo/News/Press/201202/12-023E/. 14 February 2012.

[5] Microsoft Hohm, http://www.microsofthohm.com.

[6] Google Power Meter, http://www.google.com/powermeter.

[7] Landis+Gyr Smart Meter product, http://www.landisgyr.co.uk/webfoo/wp-content/uploads/2012/12/Landis+Gyr-E750-Brochure-English.pdf

[8] https://www.wi-fi.org/sites/default/files/downloads-registered/wp_20101216_Wi-Fi_Protected_Setup.pdf

[9] http://ics.nxp.com/support/design/microcontrollers/smart.metering/

[10] http://technet.microsoft.com/en-us/library/cc748940%28WS.10%29.aspx

[11] http://doc.opensuse.org/products/draft/SLES/SLES-tuning_sd_draft/cha.tuning.power.html#sec.tuning.power.tools.cpufrequtils

[12] http://msdn.microsoft.com/en-us/library/windows/desktop/aa394074%28v=vs.85%29.aspx

[13] https://wiki.archlinux.org/index.php/ACPI_modules

[14] http://www.analog.com/static/imported-files/tech_docs/dsp_book_Ch15.pdf

[15] http://www.go-green.nl/index.php?lang=en&category=power&id=gsm00812

[16] http://www.ihome.eu/static/manual/powerswitch.pdf

[17] https://sites.google.com/site/nlarisis/techstuff/mscthesis/experimentation/brightness_CPU_running.png?attredirects=0

[18] https://sites.google.com/site/nlarisis/techstuff/mscthesis

[19] http://tools.ietf.org/pdf/rfc6101.pdf

[20] http://www.ecomagination.com/portfolio/nucleus

[21] Zhong Fan, Parag Kulkarni, Sedat Gormus, Costas Efthymiou, Georgios Kalogridis, Mahesh Sooriyabandara, Ziming Zhu, Sangarapillai Lambotharan, and Woon Hau Chin. Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. In *Communications Surveys & Tutorials, IEEE*, vol.15, no.1, pp.21,38, First Quarter 2013.

[22] S. Galli, A. Scaglione, and Zhifang Wang. Power Line Communications and the Smart Grid. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference*, pp.303,308, 4-6 October 2010.

[23] R.W. Hamming. Error detecting and error correcting codes. In *Bell System Technical Journal*, vol.29, no.2, pp.147-160. April 1950.

[24] Joon Heo, Choong Seon Hong, Seok Bong Kang, and Sang Soo Jeon. Design and Implementation of Control Mechanism for Standby Power Reduction. In *Consumer Electronics, IEEE Transactions*, vol.54, no.1, pp.179,185, February 2008.

[25] Masahito Ito, Ryuya Uda, Satoshi Ichimura, Kazuya Tago, Tohru Hoshi and Yutaka Matsushita. A Method of Appliance Detection Based on Features of PowerWaveform. In *Applications and the Internet, Proceedings 2004 International Symposium*, pp.291,294, 2004.

[26] Marco Jahn, Marc Jentsch, Christian R. Prause, Ferry Pramudianto, Amro Al-Akkad, and Rene Reiners. The Energy Aware Smart Home. In *Future Information Technology (FutureTech), 2010 5th International Conference*, pp.1,8, 21-23 May 2010.

[27] Xiaofan Jiang, Stephen Dawson-Haggerty, Prabal Dutta, and David Culler. Design and Implementation of a High-Fidelity AC MEtering Network. In *IPSN09*, San Francisco, California, USA, 15-18 April 2009.

[28] Yi-chao Jin, Ru-chuan Wang, Hai-ping Huang, and Li-juan Sun. UbiPowerMeter: A Novel Paradigm to Reduce Energy Consumption. In *International Journal of Smart Home*, vol.4, no.2, April, 2010.

[29] Hwantae Kim, Suk Kyu Lee, Hyunsoon Kim, and Hwangnam Kim. Implementing Home Energy Management System with UPnP and Mobile Applications. In *Computer Communications*, vol.36, no.1, pp.51-62, ISSN 0140-3664, 1 December 2012.

[30] Cynthia Kuo, Jesse Walker, and Adrian Perrig. Low-cost Manufacturing, Usability, and Security: An Analysis of Bluetooth Simple Pairing and Wi-Fi Protected Setup. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security* (FC'07/USEC'07), Springer-Verlag Berlin Heidelberg, pp.325-340, 2007.

[31] Ying-Xun Lai, J.J. Rodrigues, Yueh-Min Huang, Hong-GangWang, Chin-Feng Lai. An Intercommunication Home Energy Management System with Appliance Recognition in Home Network. In *Mobile Networks and Applications*, vol.17, no.1, pp.132-142, 1 February 2012.

[32] Li Li , Xiaoguang Hu, and Weicun Zhang. Design of an ARM-Based Power Meter Having WIFI Wireless Communication Module. In *Industrial Electronics and Applications, 2009. ICIEA 2009. 4th IEEE Conference*, pp.403,407, 25-27 May 2009.

[33] Timo Ojala, Pauli Nrhi, Teemu Leppnen, Jani Ylioja, Szymon Sasin, and Zach Shelby. UBI-AMI: Real-Time Metering of Energy Consumption at Homes Using Multi-Hop IP-based Wireless Sensor Networks. In *Proceedings of the 6th international conference on Advances in grid and pervasive computing* (GPC'11), Springer-Verlag Berlin Heidelberg, pp.274284, 2011.

[34] Ala' Qadi, Steve Goddard, and Shane Farritor. A Dynamic Voltage Scaling Algorithm for Sporadic Tasks. In *Proceedings of the 24th IEEE International Real-Time Systems Symposium* (RTSS '03). IEEE Computer Society, Washington, DC, USA, pp.52, 2003.

[35] Andreas Reinhardt, Dominic Burkhardt, Parag S. Mogre, Manzil Zaheer, and Ralf Steinmetz. SmartMeter.KOM: A Low-cost Wireless Sensor for Distributed Power Metering. In *Local Computer Networks (LCN), 2011 IEEE 36th Conference*, pp.1032,1039, 4-7 October 2011.

[36] J.P. Ross and A. Meier. Measurements of whole-house standby power consumption in California homes. In *Energy*, vol.27, pp.861-868, September 2000.

[37] A.G. Ruzzelli, C. Nicolas, A. Schoofs, and G.M.P. O'Hare. Real-Time Recognition and Profiling of Appliances through a Single Electricity Sensor. In *Sensor Mesh and Ad Hoc Communications and Networks (SECON)*, 7th Annual IEEE Communications Society Conference, pp.1,9, 21-25 June 2010.

[38] N. Saxena, J.-E. Ekberg, K. Kostiainen, and N. Asokan. Secure device pairing based on a visual channel. In *Security and Privacy, 2006 IEEE Symposium*, pp.6,313, 21-24 May 2006.

[39] H. Serra, J. Correia, A.J. Gano, A.M. de Campos, and I. Teixeira, .Domestic power consumption measurement and automatic home appliance detection. In *Intelligent Signal Processing, 2005 IEEE International Workshop*, pp.128,132, 1-3 September 2005.

[40] William Stallings, *Wireless Communications & Networking*, chapter 6: Signal Encoding Techniques. Prentice Hall, New Jersey, 2nd Edition, 2004.

[41] Yi Wang, Bhaskar Krishnamachari, Qing Zhao, and Murali Annavaram. Markov-optimal sensing policy for user state estimation in mobile devices. In *IPSN10, April 1216, Stockholm, Sweden*, pp.268-278, 2010.

[42] Markus Weiss, Friedemann Mattern, Tobias Graml, Thorsten Staake, and Elgar Fleisch. Handy feedback: connecting smart meters with mobile phones. In *Proceedings of the 8th International Conference on Mobile and Ubiquitous Multimedia*, (MUM '09). ACM, New York, NY, USA, Article 15, 4 pages, 2009.

[43] Ruogu Zhou and Guoliang Xing. Nemo: A High-fidelity Noninvasive Power Meter System for Wireless Sensor Networks. In *Proceedings of the 12th international conference on Information processing in sensor networks* (IPSN '13). ACM, New York, NY, USA, pp.141-152, April 2013.

Appendix A

In this appendix, a complete overview of custom and commercial smart sockets is provided. These specific power metering solutions were encountered whilst conducting the literature survey.

In Table 6.1, 26 different commercial products are presented that are further divided according to their fundamental functionality. Besides the operating voltage, control is also reported referring to the ability or not of the socket to control the power supply of the attached device. Furthermore, the socket's cost is indicated whenever relative information was available. **Category 1** exhibits full-scale solutions that include both a smart socket and a power trace sink module. It is the most attractive category since it consists of products that could be easily incorporated into PMA's design. Nevertheless, the most important attribute not listed here was the extent of reprogrammability, a feature that eventually only NXP's solution fully provides. **Categories 2** and **3** can be utilized after being modified in order to either sniff their wireless data packet with custom-made receivers (cat.2) or to wirelessly transmit what is displayed on their on-board screen (cat.3). **Category 4** solutions cannot be used without an European adapter. Although relevant transformers can assure compatibility, the overall scheme would only further complicate the protocol's setup without any significant gain.

In Table 6.2, 13 different custom solutions and their major functional features are presented. The latter include the V, I, and P metering modalities, the remote power supply control capability, the on-board MCU, and the communication protocol that can be supported. All indicated solutions provide great insight and sufficient knowledge with respect to implementing a custom socket. In the support website [18], a document labelled "AC Power Measurement EE Theory" has been compiled aggregating all this knowledge acquired in the aforementioned process. Moreover, a cost-estimation is provided with respect to a potential custom socket implementation and its selected technical features. Nevertheless, the task was proven cumbersome and instead, NXP's product was utilized during PMA's design.

Table 6.1: ***Commercial*** smart metering solutions encountered in literature and market.

Ref.	Product	Producer	Communication	Voltage	Control	Origin	Cost
Category 1 – Fully deployable products							
[9]	OM13006	NXP	M-Bus	220	✓	NL	280€
1	Home Start	Plugwise	ZigBee	220	✓	NL	102€
2	EGM-PWM	EnerGenie	USB	220	-	NL	-
3	EGM-PWML		USB	220	-	NL	-
4	EGM-PWM-LAN		Ethernet	220	-	NL	-
[16]	Power Switch	iHome	Z-Wave	220	✓	NL	133€
5	SG3010	Billion	ZigBee	100-240	-	TW	-
6	SG2097	Billion	PLC	100-240	✓	TW	-
7	SmartPlug	AlertMe	ZigBee	220	✓	UK	45£
8	MyPlug	Orange	ZigBee/GSM	220	✓	FR	80€
9	MonostripT	VisiblEnergy	WiFi	110-240	-	US	100$
10	Smart Outlet	Oblo	ZigBee	220	✓	RS	100€
11	ZHWR202	Develco Product	ZigBee	100-240	✓	DK	-
12	Smart Plug	GEO	ZigBee	220	✓	UK	20£
13	SPM111	SensingTek	ZigBee	90-264	✓	TW	-
14	Smart Socket	PowerTech	WiFi	100-240	✓	TW	-
15	EnergyAudit	PowerTracker	ZigBee	220	✓	AU	120AUD
16	Z808A	Netvox	ZigBee	220	✓	TW	-
17	PicoWatt	Tenrehte	WiFi/Ethernet	110-240	✓	US	300$
18	MeterPlug	StickNFind Technologies	Bluetooth	100-240	✓	US	60$
Category 2 – Wireless display products							
19	EC11	Elro	433MHz	220	-	NL	50€
20	IAMS	CurrentCost	433MHz	220	-	UK	12£
Category 3 – Display products							
21	EC12	Elro	NA	220	-	NL	10€
[15]	Energy Meter	GoGreen	NA	220	-	NL	17.5€
Category 4 – US power line standard (110V/50Hz) products							
22	Power Meter	Ryobi	None/Display	110	-	US	25$
23	Kill-A-Watt	P3 International	916MHz	110	-	US	35$

Table 6.2: ***Custom*** smart metering solutions encountered in literature.

Ref.	V	I	P	Control	MCU	Communication
[31]	voltage divider	current converter	ADE7763	✓	*undef*	PLC/ZigBee
[25]	voltage divider	shunt resistor	MCU via ADC	✓	*undef*	*undef*
[39]	voltage divider	shunt resistor	ADE7757	-	PIC-based	RS232/I2C
[36]	diode bridge	current coupling	8bit SAR-ADC	✓	MCS-51	RS232/I2C
[27]	direct input	shunt resistor	ADE7753	✓	Epic	6LowPAN
[27]	direct input	inline Hall-effect	MCU via ADC	✓	Epic	6LowPAN
[28]	voltage divider	inline current transformer	ADE7755	-	ARM-based	ZigBee
24	NA	Clamp-on current transformer	MCU via ADC	-	Arduino	433MHz
25	voltage divider	shunt resistor	ADE7753	-	ATMega1281	IEEE 802.15.4
26	voltage divider	AMR sensor	ADE7753	-	NA	Serial port
27	voltage divider	Rogowski coils	ADE7753	-	PIC18F242	RS232
[35]	NA	inline Hall-effect	MCU via ADC	✓	ATtiny44	IEEE 802.15.4
28	voltage divider	current sense resistor	ADE7757	✓	MSP430	IEEE 802.15.4

Appendix References

1. http://www.plugwise.com/idplugtype-f/home/home-start
2. http://energenie.com/item.aspx?id=6853
3. http://energenie.com/item.aspx?id=6735
4. http://energenie.com/item.aspx?id=6736
5. http://smartgrid.billion.com/datasheet/SG3010-Meter.pdf
6. http://www.billion.com/product/BillionSG2097-PLC-Adapter.html
7. https://www.alertme.com/products/smartplug-1622.html
8. http://www.my-plug.fr/fonctionnalites/description/
9. http://www.visiblenergy.com/products/monostrip.html
10. http://oblo.rt-rk.com/products/smart-outlet
11. http://develcoproducts.com/ZigBee_Relays/Wall_mounting.aspx
12. http://www.greenenergyoptions.co.uk/what-we-do/smart-plugs/
13. http://www.sensingtek.com/product_detail.php?s=11
14. http://www.power-tech.com.tw/01_energy/03_detail.php?pdid=14
15. http://powertracker.com.au/product/sg3010-t1-smart-appliance
16. http://www.netvox.com.tw/z808a.asp
17. http://www.tenrehte.com/products/
18. http://meterplug.com/
19. http://www.elro.eu/en/products/cat/products-out-the-range/out/assortment/wireless-energy-meter-set
20. http://www.currentcost.com/product-iams.html
21. http://elro.eu/en/products/searches_new/search&keywords=EC12/
22. http://www.ryobitools.com/catalog/electronic_hand_tools/E49CM01
23. http://p3international.com/products/p4200.html
24. T.A. Geumpana, J. Koentjoro, N.D. Widjaja, and B. Nusantara. Developing cloud energy consumption monitoring system for home electronic appliances: Indonesian case. In *International Journal of Information Technology and Business Management*, vol.6, no.1. 2012.
25. http://www.ti5.tuhh.de/events/fgsn09/proceedings/fgsn_095.pdf
26. D.R. Munoz, D.M. Perez, J.S. Moreno, and E.C. Montero. Design and experimental verification of a smart sensor to measure the energy and power consumption in a one-phase AC line, In *Measurement*, vol.42, no.3, pp.412-419. April 2009.
27. P.M. Jansson, J. Tisa, and W. Kim. Instrument and measurement technology education – A case study: Inexpensive student-designed power monitoring instrument for campus submetering. In *Instrumentation and Measurement, IEEE Transactions*, vol.56, no.5, pp.1744,1752, October 2007.
28. N.B. Priyantha, A. Kansal, M. Goraczko, and F. Zhao. Tiny web services: design and implementation of interoperable and evolvable sensor networks. In *Proceedings of the 6th ACM conference on Embedded network sensor systems*. ACM, New York, USA, pp.253-266. 2008.