IOSUD - Universitatea Politehnica Timişoara
Şcoala Doctorală de Studii Inginereşti

RESEARCH AND SOLUTIONS FOR SMART METERING NETWORKS

PhD Thesis - Abstract

for obtaining the scientific title of doctor at

the Polytechnic University of Timișoara

in the PhD field of Systems Engineering

author: ing. Paul-Onuț NEGÎRLA

scientific supervisor Prof.univ.dr.ing. Ioan SILEA

September 2022

Table of contents

1. Introduction

In the current context, following the COVID-19 health crisis and the rising cost of energy, the energy sector plays a particularly key role both economically and politically. The production of electricity from renewable sources makes the widespread use of smart meters essential due to the flexibility and performance provided by a smart grid. Such a network can transmit real-time information from each consumption point and can also receive remote schedule updates without the need for field operators. The ability to be able to update smart grid equipment in an efficient and robust way underpins the continued development of the technological capabilities and cyber security of the entire energy network. Another vital component of the modern energy system is also smart meter-specific communication technologies, capable of communicating with suppliers' grid nodes in real time despite poor transmission environments that are heavily affected by interference.

This present paper, entitled "RESEARCH AND SOLUTIONS FOR SMART METERING NETWORKS", analyzes a current problem, which will be of great interest in the future as well, which concerns the problem of remotely updating smart energy meters. In the information technology industry, the likelihood of security vulnerabilities is considered at an early stage of the development of a new project. Therefore, system architects ensure that these programs can be updated in the future through a process that does not require manual operator interaction. This process is called an OTA upgrade or "Over the Air" upgrade and it is the only way that updates can reach millions of devices in a timely manner and at minimal cost. If this process does not work, it means that company operators would have to travel to each point of consumption for a manual upgrade of each piece of equipment. With tens of millions of smart meters installed across a country [1], the cost and time required to manually update these devices does not make such an approach feasible.

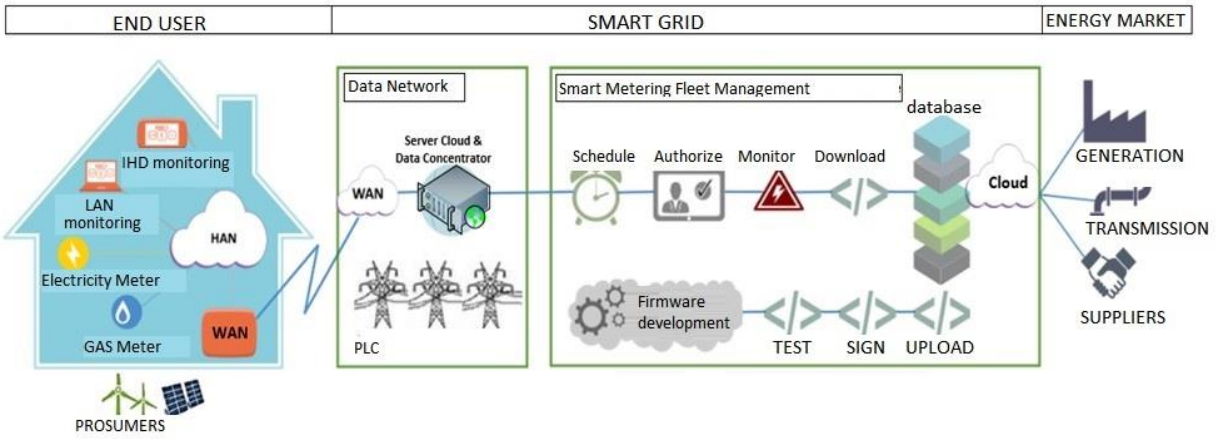

Fig. 1. - Overview of the smart metering system

Figure 1 shows an overview of the entire energy metering system from producer to end-user. The energy market is composed of three entities: producers, distributors and suppliers. The metering infrastructure is provided by distributors and suppliers in collaboration with smart metering companies, which are responsible for maintaining and updating the metering equipment and ensuring the flow of data from end-users to their contracted suppliers.

The strong interconnection between power system components makes managing the risk of smart meter malfunction (in the event of an attack or major failure) a particularly important task. The coordinated shutdown, due to a cyber-attack or fault, of significant portions of the grid will have major repercussions on the stability of the entire national grid and beyond.

Based on the analysis of smart meter problems, the motivation of the research is to find solutions for fast, secure mass upgrades using the current infrastructure to protect embedded systems in case of failures or security issues. The research topic addresses ways in which the reliability and security of embedded systems used in smart meters can be improved through techniques for updating, validating and protecting the programs loaded into their internal memories.

1.1 Aim and objectives of the research

The main goal of this work is to develop a reliable and secure update system, in distribution networks with limited data communications coverage, by investigating the following elements of its structure:

• software and hardware components required locally within each integrated system to ensure the reliability and security of smart metering programmes.

• methods of transporting software updates through weak radio signal environments or via voltage lines subject to interference.

• optimizing transport and performing local updates between adjacent nodes depending on signal quality.

Since an attacker is more likely to compromise a weak point in a computer system at the expense of well-fortified components [2], and the security of the whole network is given by these points, the study undertaken is focused on vulnerable metering equipment. Therefore, the objectives of the research are to find feasible solutions that can also be applied to equipment with limited technical capabilities, thus aiming to periodically remotely update the elements of the whole energy system.

1.2 Structure of the research work

The thesis is structured in four parts with a total of seven chapters (Fig. 2) distributed according to the figure below:

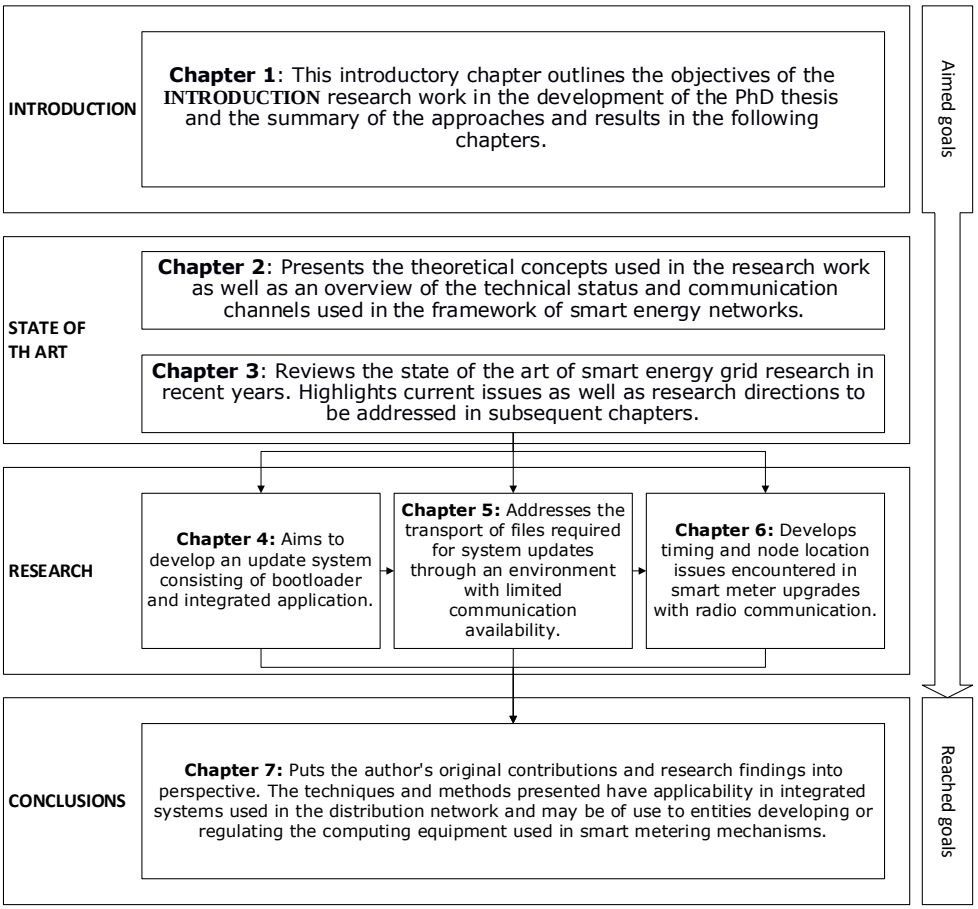

Fig. 2. - PhD thesis structure

The following part briefly outlines the issues covered in each of the seven chapters.

The first chapter covers the chosen theme, the author's motivation and its setting in the current social and economic context. This introductory chapter outlines the objectives of the research work in the development of the PhD thesis and the summary of the approaches and results in the following chapters. It also focuses on the topicality of the chosen theme and the research perspectives opened by dealing with the chosen topic.

The second chapter presents the theoretical concepts used in the research work, as well as an overview of the technical status and communication channels used in smart energy networks. The initial analysis concludes the limitations of the equipment installed in the field and outlines the technological lifetime of at least 30 years of operation that they must fulfil after installation [3]. Also in the same chapter, the analysis of the current state of the art of technology standards used in the industry for upgrading remote integrated systems begins. The chapter describes the process of storing, downloading and installing updates using currently known methods. Two categories of problems are mentioned:

- The first category discusses the issue of running update programs locally within embedded systems, as well as the reliability and authenticity checks required in running smart metering applications.

- The second category discusses the problem of secure and optimal transport of update files in binary format over low-availability transport environments, noting the low performance offered by common methods.

Chapter 3 reviews the literature published over the last decade in the field of smart energy networks. It highlights the shortcomings of the industry and research areas described in the recent literature, and notes that there are still major challenges related to the management and upgrade of smart meters installed in the field as well as challenges related to the data communications infrastructure for both wired and wireless technologies.

Chapter 4 aims to study the impact of the update process on smart meters and to develop an update system consisting of a bootloader and integrated application. The application covers both reliability and security needs using a combination of common methods optimized for the current power grid environment, while fitting the usual system requirements of a smart meter.

Chapter 5 addresses the problem of transporting files required for system updates through an environment with limited communication availability by methods of sectioning files to sizes equal to the maximum transmission unit accepted by communication networks over power lines or radio communication media [4][5].

Chapter 6 elaborates on the node location issues encountered in smart meter upgrades with radio communication. The location of radio meters and the distance estimation algorithms have as starting points different information provided by the embedded transmit/receive equipment. In this chapter, a system for the acquisition of the Received Signal Strength Indicator (RSSI) has been designed and implemented. Emphasis has been put on the variation of the Received Signal Strength Indicator (RSSI) as a function of distance and geometric orientation of nodes and environment, both in indoor and outdoor spaces [6].

The closing chapter, **Chapter 7**, puts the author's original contributions and research conclusions into perspective. The techniques and methods presented have applicability in integrated systems used in the distribution network and may be of use to entities developing or regulating the computing equipment used in smart metering mechanisms. The chapter concludes with prospects for further research and final conclusions.

2. State of the art – methods and systems used in smart metering networks

To ensure improvements in efficiency, reliability, flexibility and return on investment for all producers, operators and customers involved in a smart energy grid, modern IT solutions need to be developed for all its components. Such a communication infrastructure must be robust, feasible and fast enough to ensure the timely exchange of data from supplier to end-customer and vice versa. This chapter reviews the current state of research in smart grid architectures, highlighting research into the process of upgrading the embedded software and communications capabilities required to ensure the performance, reliability and economy of the smart metering network.

The smart grid is designed to solve the problems of the energy network, including low reliability, frequent interruptions, high greenhouse gas emissions, energy security and safety [7]. One of the definitions for the smart grid, is that the smart grid is a communications network over the energy grid that collects and analyses data from different components of a grid to predict energy supply and demand. Ultimately, this information can be used to manage and control energy distribution [8].

The problems and solutions studied in the recent literature cover both the advantages and disadvantages of smart meters as well as unsolved problems. Through a stable process of software updates embedded in smart meters, users and suppliers will be able to gain access to a wealth of functionality and enhancements as they are implemented by industry [9].

Figure 3 below provides an overview of the research topics within smart metering networks and the links between them. It can be seen that new functionalities and technological improvements are being developed in the energy system that can be implemented as software by smart meter developers. Through the data network, the functionalities and changes arrive in the form of software or configuration updates to the smart meters, and the smart meters send back data and consumption parameters that can be used in future research by replaying the whole process.

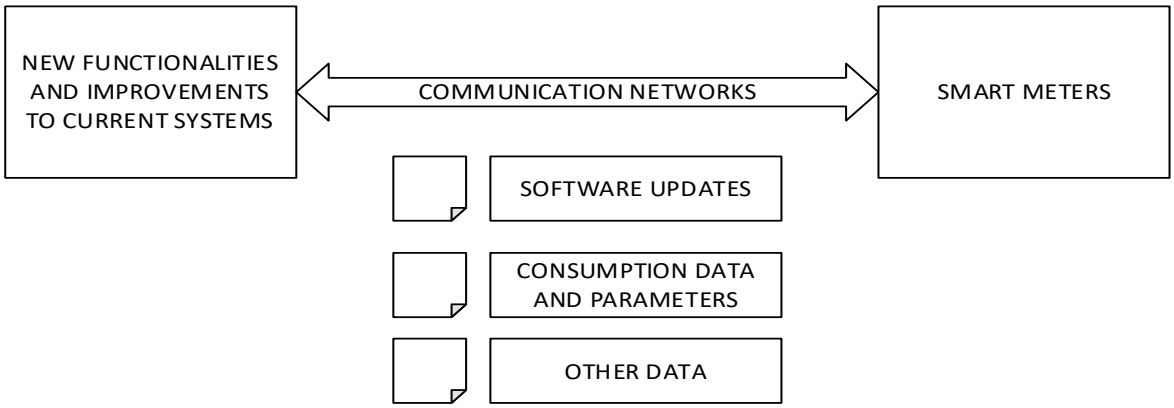

Fig. 3. - Overview of research topics in smart metering networks as well as the links between them

At the end of Chapter 3, "State of the art - methods and systems used in smart metering networks", the current methods of updating meters installed in national systems were listed and the requirements of these methods were analyzed both from technological considerations related to security, ease of implementation and hardware constraints and from other points of view that may highlight the feasibility or shortcomings that the industry is currently facing.

2.1 Challenges in the update process

As embedded systems undergo remote upgrades, device safety and security are the two key factors taken into consideration. The device's working condition must be maintained before and after the upgrade and the proper functioning of the device cannot be jeopardized. Physical access to devices already installed in the field is rarely a feasible approach for performing firmware updates, and therefore reliability and robustness of the device are design concepts that must not be compromised under any circumstances during software development. On the other hand, manufacturers need to ensure that the device will only be used for the purpose for which it was built, and repurposing it for other, often malicious, purposes must be prevented, and the internal logic of the device must not allow this. The security of update files and other software leaving the manufacturer's server must also be considered as intellectual property that must be protected with the same security and safety principles.

The theoretical notions listed in Chapter 2, "Theoretical notions", emphasize that a suitable software update mechanism for low availability systems must ensure the following requirements:

- It must be tolerant to system errors and be able to resume the update process from where it was previously stopped. The integrity of the system must not be affected by sudden interruptions of power.

- The device will be able to revert to a previous correct version when required by the faulty state of the upgraded equipment. Recovery modes are acceptable in certain situations, but not on low-maintenance devices or devices with difficult physical access.

- The equipment will be protected against malicious programs that have not been signed by a trusted source or the manufacturer.

- The integrated system will be protected against software piracy and software attacks. Implementation of cryptographic protection mechanisms and disabling of all physical hardware memory read interfaces are required.

- Resource requirements should be kept to a minimum on embedded devices, and where available, use the resources of an external server as much as possible.

- Update systems must ensure that the process does not get stuck in an intermediate state. The update process must use an atomic architecture.

2.2 Features and opportunities in the future of smart meters

In recent years, technological developments and the economic and social context have led to the emergence of a multitude of new technologies embedded in smart metering equipment. A brief history of smart meters and their progress to date has been presented in Figure 4.

The US National Institute of Standards and Technology (NIST) proposed in 2014 [10] a list of key functionalities to be implemented as soon as possible by the energy industry. Subsequently, these were also taken up at European and national level [11].

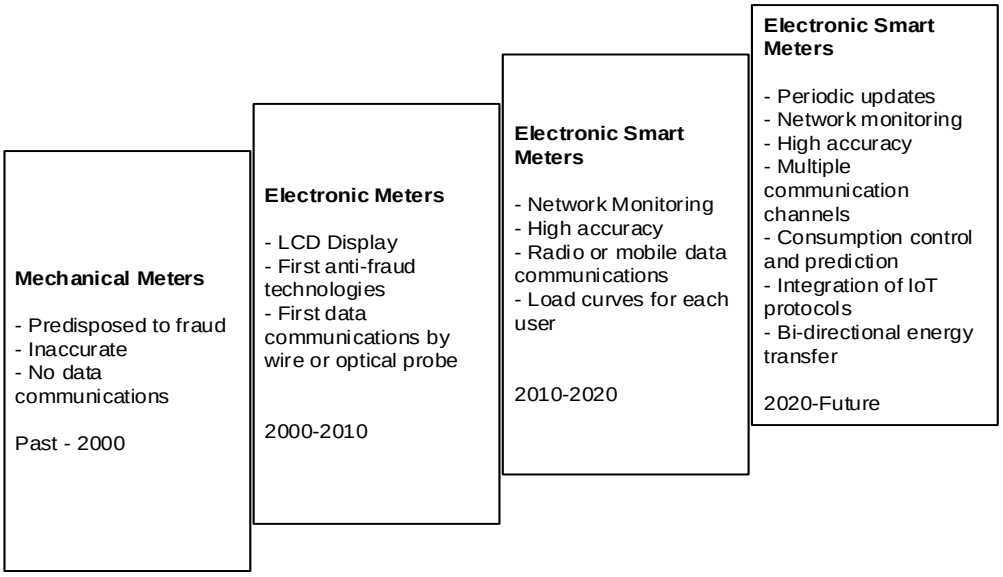

Fig. 4 - Evolution over time of smart meter network functionalities

2.2 Research directions

This chapter has presented papers and methods from the literature published between 2010-2021 on the future of smart metering networks and the challenges that need to be overcome for large-scale implementation of new functionalities proposed by industry.

Smart grids can solve the problems of two-way flow of information and energy, reliability and security issues of traditional energy grids. Using and producing energy in a smart way at both national and residential levels can put an end to energy waste and solve the problems caused by growing energy demand. This is made possible by the monitoring, analysis and control techniques outlined at the beginning of the chapter. It can therefore be concluded that smart meters play a key role in energy management and saving, and by the end of 2022, it is expected that two hundred million new smart meters will be installed during the implementation of more than 50 projects across Europe.

For data transmission, two popular technologies are used in the implementation of these projects: radio technologies under the ZigBee protocol and power line communication technologies under the NB-PLC protocol. Both technologies use data concentrators serving a specific area, and the connection from the concentrator to the central servers is done via mobile data technologies. These choices are based on low implementation costs and high flexibility of the chosen protocols, but they face challenges of coexistence in an already crowded frequency domain, challenges related to communication channel security, and challenges related to data congestion and lack of a real-time communication method.

A new area of research that has recently emerged considers both the problems encountered in smart metering networks and the problems encountered in Internet of Things (IoT) equipment used in smart home automation projects. The general proposals are to standardize and embed the two technologies in an IoT-assisted smart grid system that addresses interoperability and integration issues of new devices, distributed use of processing power for analyzing the huge volume of data, and the use of a hybrid communication topology that can address data congestion and data security issues. Smart

metering systems assisted by IoT equipment represent an integration of two emerging and promising worlds.

Metering and control applications running in smart meter software require a fast, reliable and secure network. The literature reviewed notes that network node location can provide additional support to optimization algorithms but can improve both the decisions made in routing packets through the network and reduce the time to resolve a physical fault by quickly identifying it in geographic space. In physical environments that do not allow the installation of GPS equipment, localization is based on radio signal indicators, and although the authors propose several methods for locating smart meters, they face high computational complexity and often rely only on the RSSI signal indicator, which can change significantly depending on environmental factors.

As the technologies involved in smart energy grids are evolving at an accelerating rate, it is important that each piece of equipment installed in the field subsequently has access to software updates that can bring additional functionality or improve the security of the meters and therefore the entire grid. Multiple standardized techniques and frameworks for remote updating of embedded systems have been analyzed and the main challenges and limitations that stem from hardware or communication network constraints have been highlighted. In addition, schemes for securing the whole update process through encryption, signature and other processes to verify the integrity and authenticity of the programs run by smart meters were discussed. Also, in this chapter, analysis tools and data transmission optimization methods that can play a key role in updating smart meters installed in areas with low access to data networks have been analyzed and research directions in this area have been suggested.

In conclusion, there are still major challenges that require further investigation of important open research issues in smart metering networks and in the management of smart meters already installed.

3. Research on the impact of remote updating methods of smart meters

Based on the current state of the art of smart metering networks, together with the conclusions of the theoretical concepts described above, the chapter entitled "Research on the impact of remote update methods for smart meters" proposes and analyses methods by which the update process can be implemented at the software level without compromising functionality or security due to the constraints of the type of hardware used. The cryptographic methods used in this chapter use dispersion functions to implement the firmware integrity checking algorithm, encrypting storage memories using the Advanced Encryption Standard (AES) with keys up to 128 bits to protect intellectual property, and security for file transport will be provided by communication channels based on symmetric keys and the HTTPS protocol.

The implementation of the proposed update system has been divided into two basic components as follows: The first component of the smart meter remote update system is covered by a secondary bootloader solution with image decryption, digital authentication and installation of the new software. The second software component has been integrated into the smart meter application and it takes care of authentication with the manufacturer's server in order to securely download a software image, then store it and at the same time will take care not to influence the metered sizes in any way throughout the update process. For the development of the integrated system compatible with the requirements of the SUIT

standard [10][11], a system based on the STM32L475 microcontroller with 128 KB RAM and 256 KB Flash memory was chosen.

As SUIT requirements do not allow the transport of a software image in unsecured modes, the firmware package will be stored in a 3rd memory area, intended for encrypted and signed image downloads. The transfer of the updated image to the idle sector will be done by the application when all verification and validation steps have been completed.

Smart metering equipment has in addition to the usual reliability and security requirements also strict requirements on the time needed for the bootloader to complete all the steps and run the corresponding metering application [12]. Therefore, once the firmware image containing the update is downloaded, the image integrity check, author signature check and decryption to an inactive partition will be done at the application level and not at the bootloader level in order not to delay the start of the metering application. The bootloader will only be responsible for choosing the active partition and checking the integrity of the application to be run.

Simplicity and keeping the processes taking place within the program loader to a minimum comes from the need to keep the program as robust as possible since bootloaders of this type cannot be updated and are only written once during the lifetime of the smart meter. A second reason is closely related to the speed with which these steps need to be executed in order to run the meter program as fast as possible, avoiding losses and gaps in the consumption load profile.

End-to-end experimental tests were run, whereby the basic application of the STM32L475 microcontroller was repeatedly updated, and execution times for each step of the processes described in the process diagram of the program loader and in the process diagram of the software mode responsible for the firmware updates of the smart meter were measured using the oscilloscope and digital signals.

The download times of the updates do not impact the operation of the smart meters, these measurements are only for control purposes and can give a higher degree of confidence in the interpretation of the results. On the other hand, boot up timings are periods during which the smart meter cannot perform other operations and energy consumption may not be recorded during this process.

The results presented show that it is possible to implement a remote update system even for low-power systems with limited hardware resources such as those found in equipment installed in the smart grid. A microcontroller with a minimum of 128 KB RAM and a minimum of 256 KB Flash is required to meet the minimum level of security and to cover all fault protection mechanisms. The presented system based on the STM32L475 microcontroller met all functionality and security requirements required by the SUIT standard and is a suitable solution for smart meters connected in smart grid networks.

The impact on smart metering operations in the upgrade process was reduced using the methods presented, and the average time to install new firmware under laboratory conditions was 7.0148 seconds.

The methods presented in this chapter highlight the importance of standardizing the update process in smart metering networks. The coexistence of metering equipment in the energy system data network can be strongly affected by the solutions chosen by smart meter manufacturers. Synchronization of the technologies chosen by developers can have a major

impact on the whole network, and the interconnection of these meters into the energy system in a coherent way can improve both transmission speed and reachability of hard-to-reach areas, topics that will be covered in the next chapter.

4. Improving availability through data segmentation in PLC networks

Power grids vary in size, from covering a single building to national grids covering entire countries or even transnational grids that can cross continents. With the roll-out of smart meters around the world, there are use cases where common solutions fail and network availability of some meters is very low due to poor communication conditions. This chapter proposes a data segmentation model for large data files that need to travel securely and reliably through the smart grid. In particular, the proposed method addresses PRIME PLC network availability improvements through the appropriate use of application-level data segmentation algorithms and their calibration for transmission rates according to the noise levels present in the power grid.

Throughout the development of the chapter, experiments have been carried out on a low power electrical network to evaluate the availability improvements by the proposed method as well as the feasibility of remote firmware upgrades for equipment communicating over high noise networks. Experimental results show that the presented method of remote firmware update is dependable and practical in areas where the availability of smart equipment to data networks is low.

PLC systems have a divided market between PLC G3 and PLC PRIME Narrow Band protocols [13]. These technologies, while having the great advantage of not requiring the installation of new infrastructure communicating over the power grid, have the disadvantage that the success rate in data transmission is affected by interference from consumers or the distance of transmission nodes between adjacent households. The equipment requirements chosen by the ERBD and the National Energy Regulatory Authority are suitable for densely populated areas, but the limitations of power line communications are seen when dealing with very large volumes of data, and although the nationwide installation of equipment is not yet nearing completion we already have countless situations where the initial requirements are now proving insufficient.

The global DLMS / COSEM standard (IEC 62056, EN13757-1) for smart energy metering requires certain data structures, such as tariffs that can change dynamically every two minutes or contract choice by meter from multiple energy suppliers or even load profiling for supported contract tariffs at one minute resolution for all energy types (active, reactive, imported/exported). Such complex structures usually overwhelm the chosen protocols and can easily reach sizes of several megabytes. On the other hand, performance evaluations of the two bands in PLC systems (PRIME and G3) show that this transmission can be performed at a higher speed on PRIME, but performs worse in the presence of interference or network noise [14, 15].

The packet error rate in PRIME networks increases with packet size [16]. PRIME meters are experiencing increasingly low availability as the size of packets transmitted has increased significantly, and hardware solutions proposed in the literature cannot improve an already installed meter that has significant packet loss. Therefore, the current chapter aims to improve the error rate of packets transmitted over PRIME networks, which could subsequently lead to improving the success rate of remote firmware updates in smart meters.

Segmenting the data to an appropriate size in a dynamic way, each communication channel, could lead to improvements in current protocols, and smart meters, which rarely maintain a reliable connection with the energy supplier, will then be able to get software updates in a practical way.

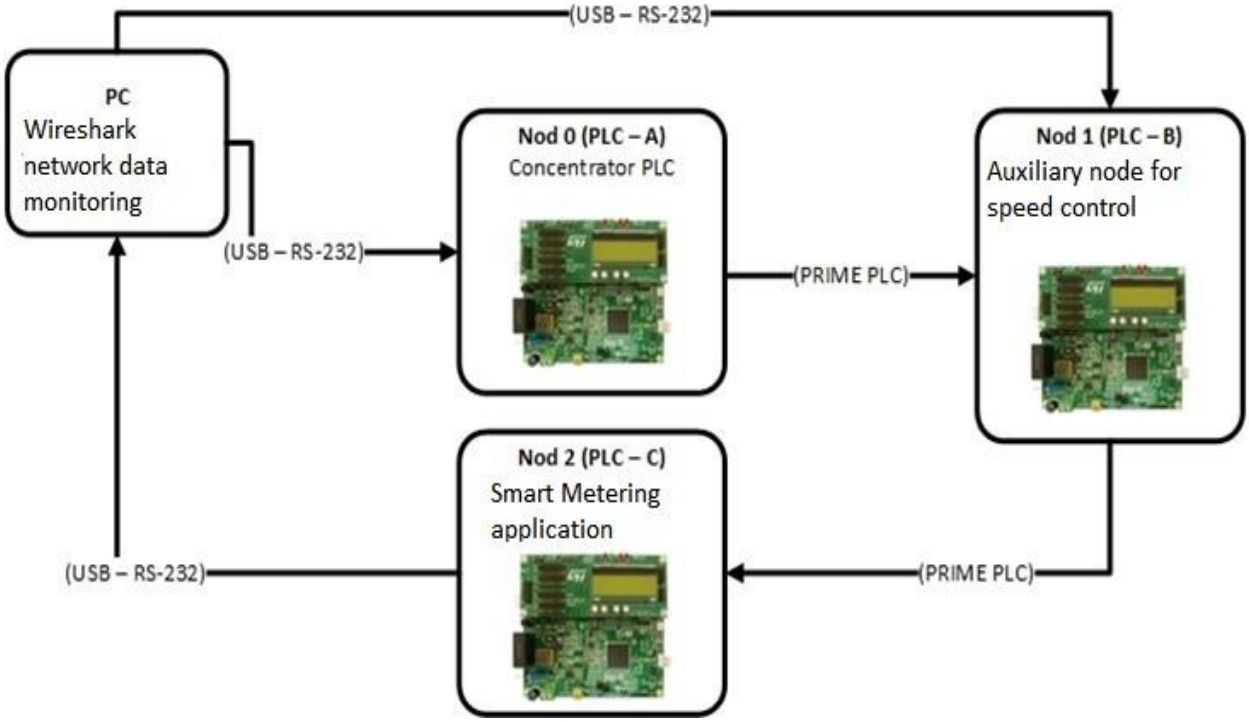

Fig. 5. - Topology of the PoweRline Intelligent Metering Evolution data segmentation method evaluation network (PRIME).

Figure 5 illustrates the network topology used to evaluate the data segmentation solution. This topology consists of three communication nodes connected to power lines based on PRIME communication protocol evaluation platforms. The nodes are also connected to a system that can monitor the entire system through an embedded diagnostic interface. The interface uses a custom application developed specifically for this test and has commands that can simulate a given network quality or analyze the success rates of PRIME transmissions between experimental nodes. Node two, PLC-C, was examined as the primary device while the other two nodes have an auxiliary role. Node zero runs a generic PLC-PRIME data concentrator application while maintaining the functions corresponding to a mesh network, and node 1 has in addition to its basic functions the capability to simulate a packet transmission success rate thus being able to simulate conditions in a low performance network.

To avoid segmentation and reassembly through the PRIME layer, we need to look at its common part convergence substrate, CPCS. The functionality of CPCS is responsible for splitting the output data into constant ClMTU segments of 256 bytes each. PRIME 1.3.6 supports up to sixty-four segments of ClMTUSize. This results in a maximum transmission length of 16,384 bytes, after which the upper layers must manage further segmentation and reassembly. Segmentation at the application layer will follow the same structure as that at the physical PRIME layer, and the common part convergence substrate (CPCS) follows the same format as described in Table 1:

Table 1. - PRIME segmentation header fields and structure.

Name	*Length*	*Description*
Type	2 bits	Segment type. 0b00: first segment. 0b01: intermediate segment. 0b10: last segment. 0b11: reserved
NSegs	N bits	Total number of segments – 1.
SEQ	N bits	Sequence number of the current segment.

In the system described, using the parameters described above and by resizing the segments according to the PRIME MTU sizes, the following tests were performed:

- Test one. Initial speed, focusing on the speed at which segments needed retransmission during a normal transmission of a daily load profile reading that has LoadProfileDaySize = 1,327,104 bytes.
- Test two. Test with data segmentation using daily load profile readings configured for a data segment of size = 256 bytes. This approach divides the formatted data into 5184 segments.

The experimental results show the number of retransmitted packets in Figure 6a for the system without data segmentation and Figure 6b for the system with segmentation.

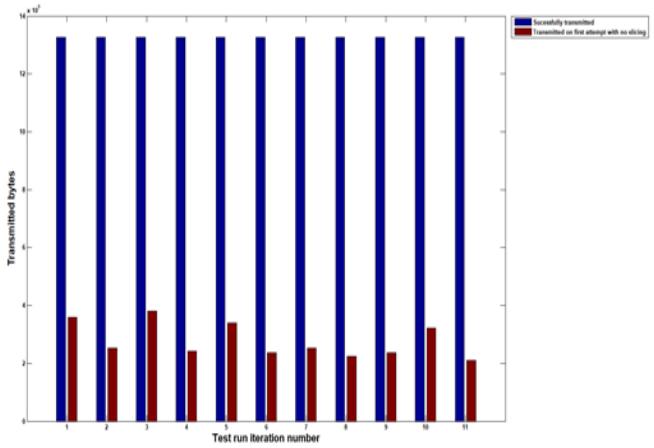

Fig. 6a - Initial results of the daily load profile reading via PLC-PRIME from PLC-A to PLC-C.

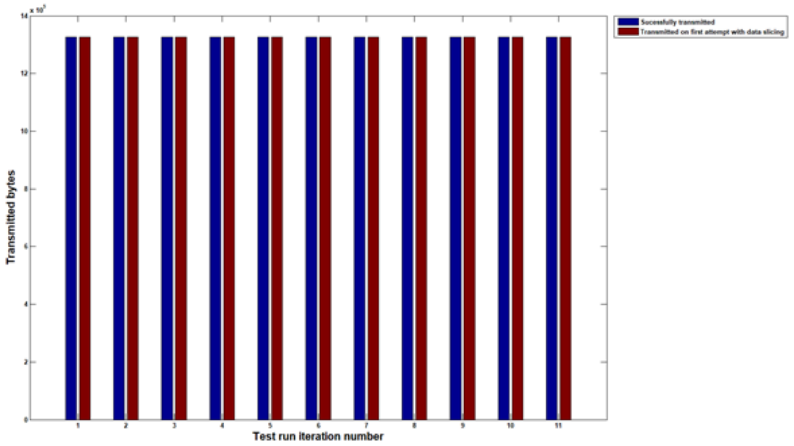

Fig. 6b - Transmission of daily load profile readings through application-level limited segments.

The data showed that during the application-level segmentation-based test the load profile readings successfully reached the intended destination without packet loss and, moreover, each segment was properly transmitted in a single transmission window without the need for retries or retransmissions. However, the transmission rate decreased significantly during the experimental analysis, therefore, this issue was analyzed in the next steps.

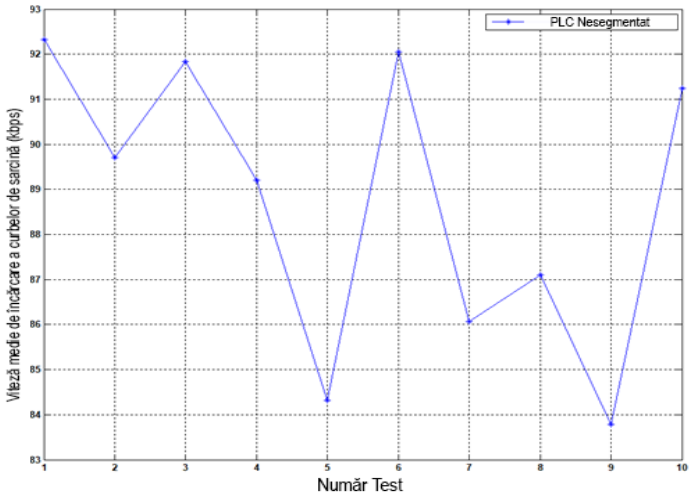

Fig. 6c - Observed baud rates on a PLC communication channel not using application-level data segmentation.

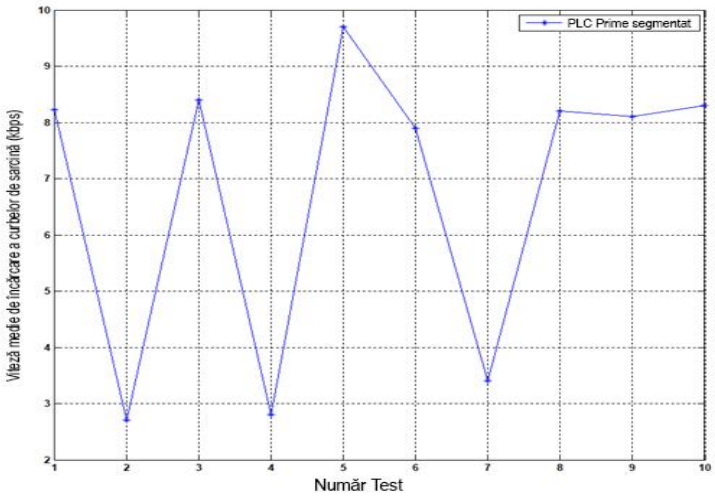

Fig. 6d - Transmission speeds observed on the communication channel from PLC-A to PLC-C using application-level data segmentation.

Initially (Fig. 6c) the transmission speed was in the range [83 kbps, 93 kbps], which is not unusual for a low voltage line network that does not suffer from interference or other network quality problems.

Aiming for a network that requires packet retransmission as infrequently as possible and communication as close as possible to what data communication looks like in an interference-free environment, the impact of a data segment solution that significantly improves network availability but at a visibly lower speed compared to standard protocols was analyzed. In the case of devices that would remain for a longer period of time at 0% availability, transmission speed is not an immediate issue, as these devices would be inaccessible for a long period of time anyway.

Finally, tests show (Fig 6d) the cost paid to increase network availability, the transmission speed dropped from an average of 88,761 kbps to 6,763 kbps, allowing a load profile, in the most complex format, to be transmitted for the entire period of a day in about 20 minutes.

Subsequently, the feasibility of the application-level segmentation method for remote firmware updates was investigated. The update process via data segments was compared to the manual update process via the optical probe interface.

During the experimental tests, the average download speed of the firmware update via the optical interface was 15016.3 bps (14.66 kbps), while an average speed of 7769.4 bps (7.59 kbps) was achieved by the PLC approach with data segmentation.

A visual comparison of speeds is shown in Figure 7. While this shows that the optical interface operates at slightly better speeds, we have shown that the data segmentation approach is still a viable solution, with speeds in a similar range of values.

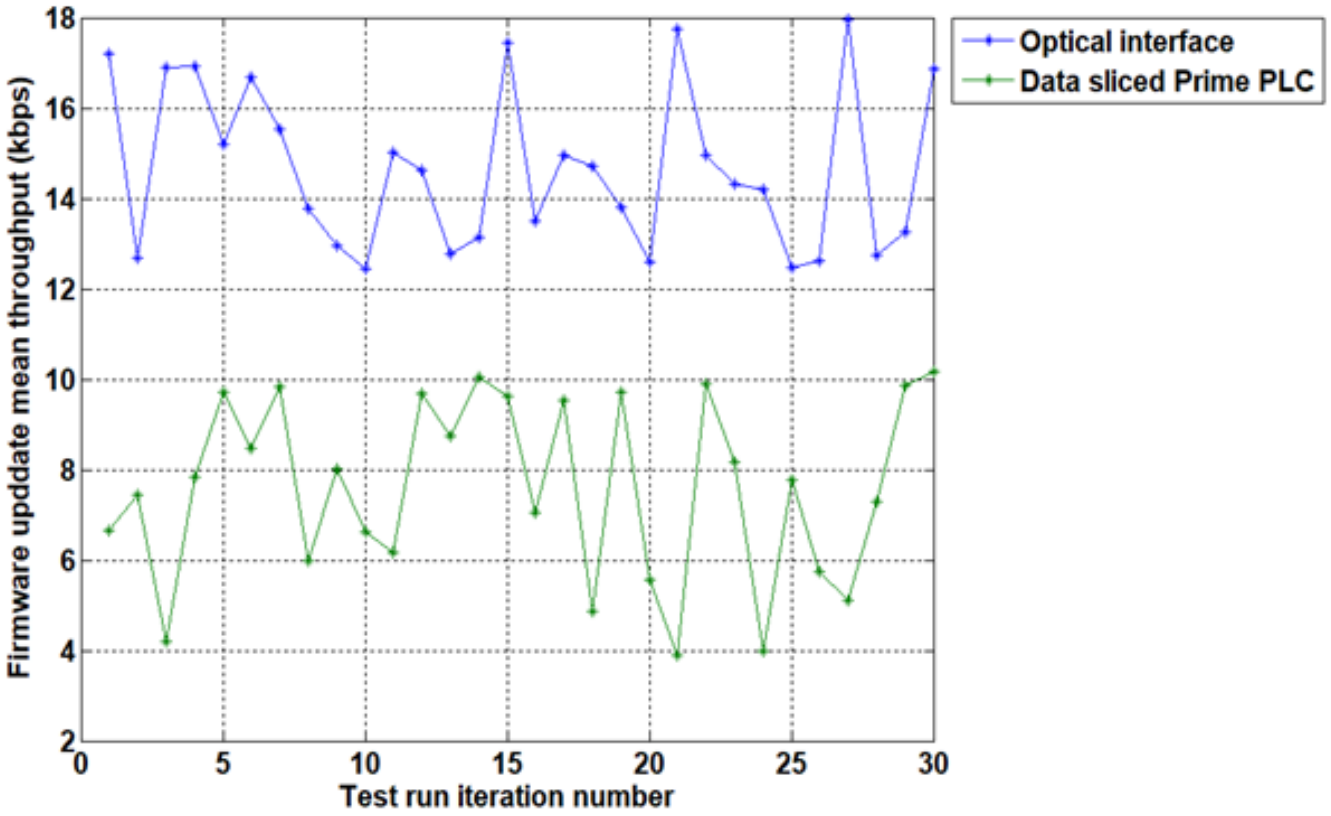

Fig. 7 - Visual representation of update rate test results

As the results presented above show, by reducing the segments transmitted within a given time window, it was shown that the retransmission rate was significantly reduced, and PLC communication with data segments can improve availability by transmitting at least one segment from the targeted smart meter whenever there is a short availability window. In addition, the firmware update process can still achieve speeds comparable to the same operation performed manually by an operator in the field, without the logistical costs involved. This means that nodes that are at the network end in a PRIME network can be upgraded and are no longer left unsecured due to the inability to get a full upgrade in the same availability window.

5. Considerations for measuring signal levels in wireless metering for node position estimation

Wireless sensor networks (WSNs) are widely used in various monitoring systems including energy metering and monitoring systems. Given the distributed nature of these networks, a growing number of research studies focus on important issues such as: maximizing network autonomy, node location and data access security. Algorithms for node location and distance estimation take as a starting point different information provided by nodes, and signal strength level is often such a starting point. In this chapter a system for acquiring the received signal strength indicator (RSSI) has been designed, implemented and tested.

Through the research conducted, it is recommended to carry out signal measurements, on site, when considering extending the network area. The paper presents issues related to signal level measurements (using RSSI) when the supply voltage to the nodes and the orientation of the sensors (in the same location) do not always remain the same.

The results and experiments presented in the paper are useful for the realization of the at least two applications as follows:

- a system to identify the position of smart meters in the field or domestic consumers in a home with smart sensors/smart sockets.
- a system for reading the energy consumption of each of the apartments on the staircase of a multi-story building.

In this chapter, an RSSI acquisition system was designed, implemented and tested to use this measure as an input dataset for future development of smart meter distance and location estimation algorithms. The goal of the system is to allow the user to measure RSSI levels between active nodes in the system and in both transmission directions.

The total current consumption is given by (5.1):

$$\mathbf{C_{Total}}\,(\mathrm{mA}) = \mathbf{C_{CPU}} + \mathbf{C_{Outputs}} + \mathbf{C_{Transceiver}},\ \langle \mathrm{mA} \rangle. \quad (5.1)$$

The value of interest is the total current consumption of the node when it is in active TX mode, as this is the only value that could be dynamically changed by an energy efficient data transmission algorithm.

The communication protocol provides two control commands, which can be used to measure and control current consumption during a transmission. The variation of current consumption with respect to the values written via these commands can be seen in Fig. 8a and 8b respectively for the linearized value.

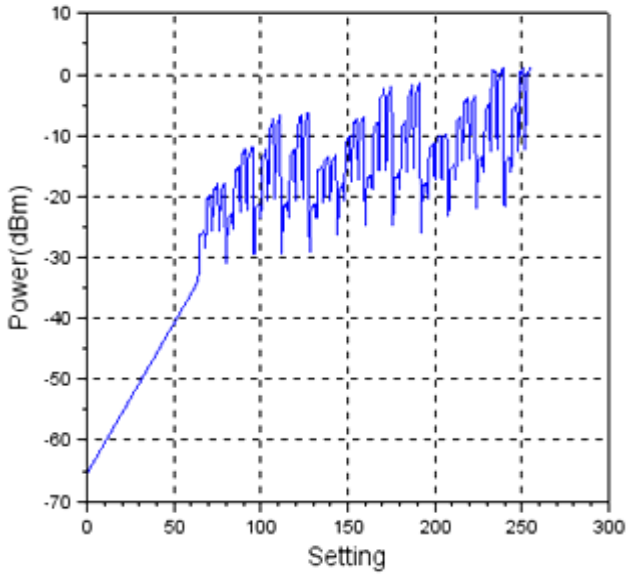

Fig. 8a - Nonlinear variation of transmission power level as a function of register setting.

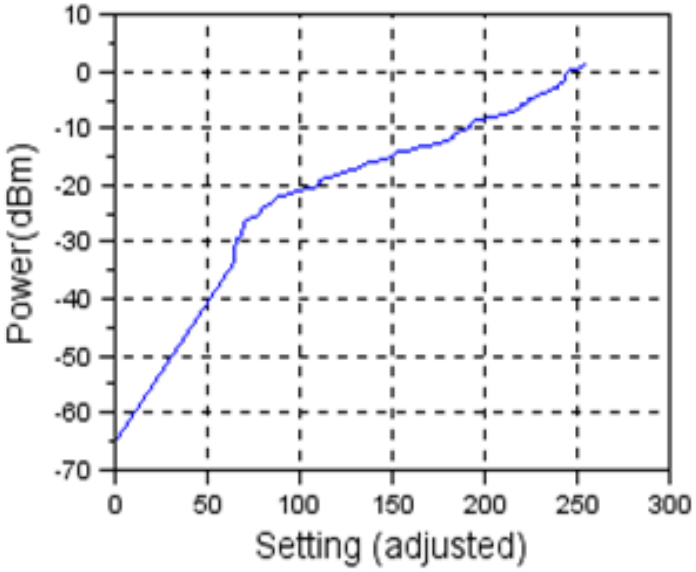

Fig. 8b - Transmission power level linearization according to the transmitter power register setting.

In the case of a node, the current measurements made according to the transmit power differ depending on the level of battery charge used, therefore the range of such a sensor, estimated by measuring the battery voltage, influences the accuracy of the distance estimation based on the RSSI measurement.

Figure 9 shows the difference in current consumption when there is a 0.48 volt drop in the power supply.

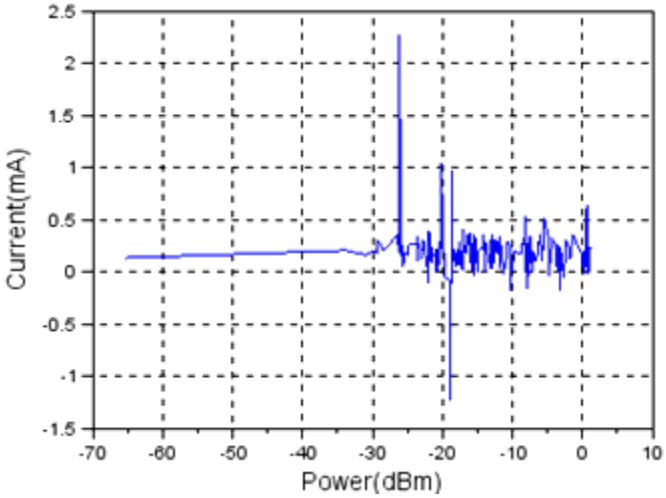

Fig. 9 - Current consumption as a function of transmission power.

Several sets of measurements were also carried out in the experimental framework to assess the level of RSSI under different spatial orientation conditions. Figures 10a and 10b show the variation of RSSI level with distance measured outdoors and indoors, respectively. Figures 11a and 11b show the variation of RSSI level with vertical positioning, respectively in the horizontal plane.

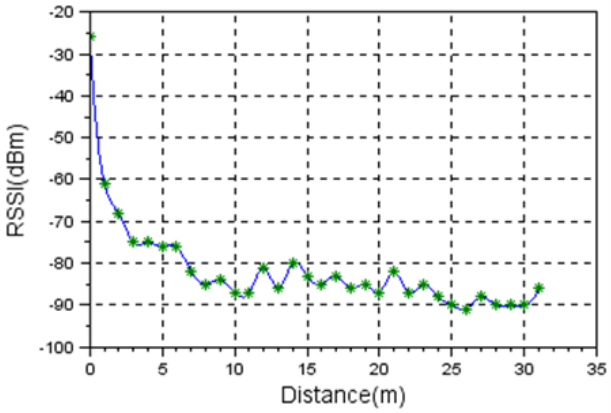

Fig. 10a. - RSSI level as a function of distance. Measurements in open field.

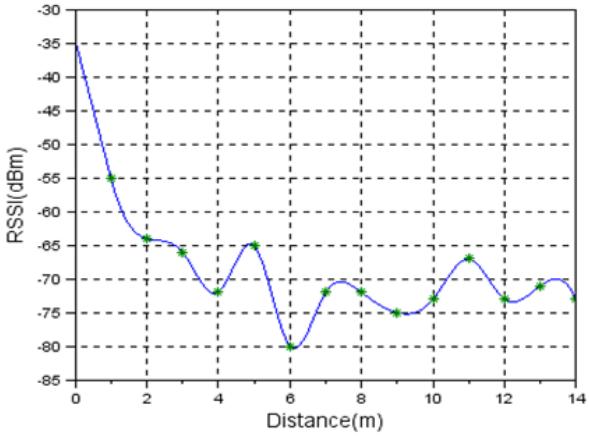

Fig. 10b. - RSSI level as a function of distance. Indoor measurements on a 14 m long and 1.5 m wide corridor.

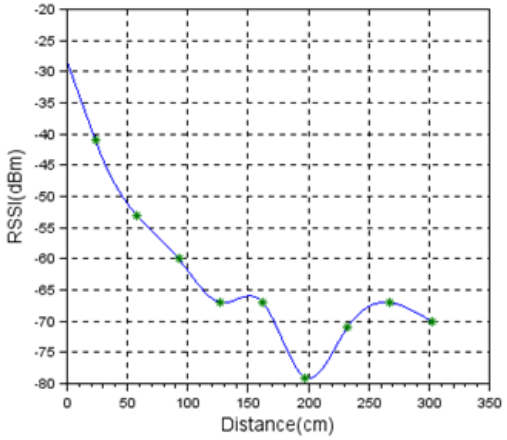

Fig. 11a. - RSSI level as a function of node orientation in a vertical measurement configuration with nodes positioned face to face.

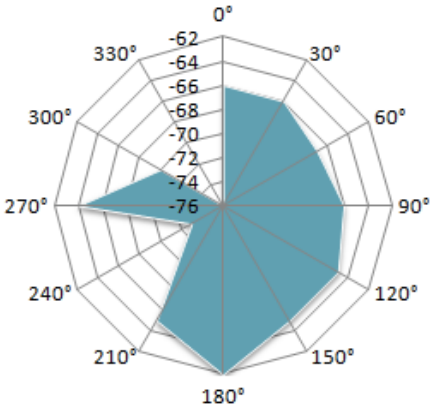

Fig. 11b. - RSSI level according to the horizontal orientation of the node in a measurement configuration with the nodes back-to-back at a distance of 1m.

The aim of this chapter was to highlight the extent to which the results of scientific experiments may differ in wireless smart metering networks depending on the orientation of one node relative to other nodes. As a result, in an application where wireless node networks are used, depending on the radio module used, there are implications for autonomy issues and localization issues especially in cases where the position and orientation of nodes are not known.

The RSSI metering system described in this paper, based on the proposed wired and wireless communication protocol, has proven its reliability and compatibility with wireless metering networks. In order to use RSSI values as input data for distance or location sensing algorithms, RSSI values cannot be used without intermediate processing steps to mitigate the non-linearity of the measured values. The measurement results confirmed that the RSSI level varies with distance, sensor geometric orientation and environmental characteristics.

In networks that use energy-efficient wireless equipment (e.g.: smart gas meters), the RSSI factor is expected to be a solution for detecting the distance between nodes and then adjusting the transmission power to a specific value corresponding to the measured distance. By reducing the transmission power, the current consumption of the transceiver is reduced and therefore the node autonomy is increased.

6. Final conclusions and personal contributions

The final chapter summarizes a series of conclusions regarding the objectives of the PhD thesis, the topicality of the topic and the personal contributions presented in the previous chapters. The chapter is also intended to present the ways of exploiting the results and some technical elements proposed in the research work in the field addressed. The chapter concludes by listing the identified future directions of study and the published work resulting from the doctoral research.

The main objectives pursued in the PhD thesis led to the following personal contributions:

A comprehensive analysis of the technologies used, globally, in energy networks has been developed both in terms of the technologies used by metering systems and in terms of the communication technologies chosen for the digitization of energy networks.

An upgrade system for embedded systems has been developed and is compatible with the technical features of smart meters in production. The system consists of a bootloader and a process application and aims to meet all the requirements of the SUIT standard [10]. The development of the system emphasized high reliability and a high degree of IT security both at the network node level and at the update distribution process level. The software design process was aimed at achieving an update system with minimal impact on the energy metering process.

A complete client (smart meter) - server (cloud) architecture has been created to validate the above system, and the file distribution system required for software updates can convert binary applications into encrypted and signed files to current security standards. The programs and the distribution process were then used in experimental work carried out in the publication of some papers and in the development of subsequent chapters.

The second research objective led to the development of a critical analysis of the frequency and volume of data transported from smart meters to the supplier via power lines.

An experimental system for simulating PRIME network nodes has been developed to objectively evaluate further proposed optimization methods for transporting data over this type of networks and a metering application-level data segmentation algorithm has been developed. The algorithm optimizes the transport of large files over PRIME networks, and the most common cases in which it can be used are the transport of files required for updates or the transport of data packets containing load profiles of each consumption site. The algorithm aims to increase the rate of successful transmissions to reduce communication errors in areas where the quality of the PRIME network is heavily affected by disturbances. By using application-level data segmentation using the proposed model, data transfers became more stable without the need for retransmission

attempts. In addition, devices deployed in a network affected by interference experienced a notable increase in the rate of successful load profile transmissions, as well as an increase in the success rates for remote firmware updates. The results have been published in peer-reviewed journals, and the algorithm and details of the network node simulation stand have been part of the content of Web of Science articles.

Research and analysis of the RSSI signal indicator emitted by smart meters based on radio technologies have established that it can be used to estimate the distance between network nodes.

A system for the analysis of signal parameter-based localization algorithms, RSSI, has been designed and experimentally implemented. Details of its implementation, as well as experimental measurements and final observations, were published in a "Web of Science" journal, and the experimental stands and methods led to the facilitation of laboratory support at the Polytechnic University of Timisoara [17][18].

The validation of the research developed as a result of the present PhD thesis was achieved through the publication of 10 scientific papers. The publications on the chosen field of research have been presented at prestigious international journals and conferences, and 4 papers have been indexed in the "Web of Science" database.

6.1 Research perspectives

Through the results obtained and through the theoretical and practical analysis of the research developed in the PhD thesis, several directions and perspectives of study in the field of PhD thesis were observed.

A first direction of research is towards extending the proposed update system to further reduce the impact of this process on smart metering applications. Updates through operating systems designated to embedded equipment will be considered.

A particularly complex new research horizon is the problem of embedding Internet of Things technologies within smart grids. Energy meter software updates could benefit from broadband connectivity of closely connected household equipment by standardizing the coexistence of the two families of equipment.

The research in the PhD thesis also showed that there is an opportunity for some optimizations of data transport depending on network topology and signal quality. Also, research on sensor fusion algorithms [19][20] could be applied to smart metering data transport optimization or in system fault localization algorithms.

Finally, securing and digitizing the entire distribution network is a vast area, and the topic of updating remote smart meters in a robust and secure way needs further research work.

Bibliography

[1] Alaton Clément, Tounquet Frédéric, Benchmarking smart metering deployment in the EU-28 with a focus on electricity, Publications Office of the European Union, 2020

[2] Viega, John, and Gary R. McGraw. *Building secure software: How to avoid security problems the right way, portable documents*. Pearson Education, 2001.

[3] **Negirla, P.**, Nanu, S., Silea, I. and Stefan, O. "Another Approach Regarding the Balance Between Natural and Manufactured Ecosystems". In International Symposium in Management Innovation for Sustainable Management and Entrepreneurship (pp. 171-181). Springer, Cham. 2019.

[4] **Paul Negirla**, Romina Druță, and Ioan Silea. "Availability improvements through data slicing in PLC smart grid networks." Sensors 20.24 (2020): 7256.

[5] **Paul Negirla** and Ioan Silea. "Data Slicing Model Proposals for Low-availability Smart Metering Equipment". Conference: 6th International Conference on Sensors and Electronic Instrumentation Advances, Porto, Portugal, Proceedings of the 2nd IFSA 2020.

[6] Dolha Stelian, **Paul Negirla**, Florin Alexa, and Ioan Silea. "Considerations about the signal level measurement in wireless sensor networks for node position estimation." Sensors 19, no. 19 (2019): 4179.

[7] Ghasempour, Alireza. "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges." *Inventions* 4.1 (2019): 22.

[8] Ghasempour, Alireza. "Optimum number of aggregators based on power consumption, cost, and network lifetime in advanced metering infrastructure architecture for Smart Grid Internet of Things." *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2016.

[9] Barai, Gouri R., Sridhar Krishnan, and Bala Venkatesh. "Smart metering and functionalities of smart meters in smart grid-a review." *2015 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE, 2015.

[10] Moran, Brendan, et al. A Firmware Update Architecture for Internet of Things. RFC 9019. IETF, 2021.

[11] Moran, Brendan, et al., A Concise Binary Object Representation (CBOR)-based Serialization Format for the Software Updates for Internet of Things (SUIT) Manifest, IETF, 2021

[12] SR EN 50470-1:2007 EN 50470-1:2006 Echipamente de măsurare a energiei electrice (c.a.). Standard european, 2007

[13] Kearney, A.T. Smart Metering in Romania, 3 September 2012. Romanian Authority for Energy Regulation: Bucharest, Romania, 2012.

[14] Hoch, M. Comparison of PLC G3 and PRIME. In Proceedings of the 2011 IEEE International Symposium on Power Line Communications and Its Applications, IEEE, Udine, Italy, 3–6 April 2011; pp. 165–169.

[15] Matanza, J.; Alexandres, S.; Rodriguez-Morcillo, C. Performance evaluation of two narrowband PLC systems: PRIME and G3. Comput. Stand. Interfaces 2013, 36, 198–208.

[16] A Da Rocha Farias, L.; Monteiro, L.F.; Leme, M.O.; Stevan, S.L., Jr. Empirical Analysis of the Communication in Industrial Environment Based on G3-Power Line Communication and Influences from Electrical Grid. Electronics 2018, 7, 194.f

[17] Druta, R., Druta, C., **Negirla, P.** and Silea, I., "A review on methods and systems for remote collaboration". Applied Sciences, 11(21), p.10035., 2021.

[18] Silea, I., **Negirla, P.**, "Students Training Through Applied Activities at Department of Automation and Applied Informatics, University Politehnica Timisoara". European Journal of Engineering and Formal Sciences, 3(2), pp.1-9. 2020.

[19] **Paul Negirla** and Mariana Nagy. "Mobile Robot Platform for Studying Sensor Fusion Localization Algorithms." In International Workshop Soft Computing Applications, pp. 317-326. Springer, Cham, 2018.

[20] **Negirla, P.**, et al., "Sensor fusion for accurate human body temperature measurement at a distance" Conference: 6th International Conference on Sensors and Electronic Instrumentation Advances, Porto, Portugal, Proceedings of the 2nd IFSA, 2020.