On the Security of Smart Grid Communications: Vulnerabilities and Countermeasures

By

Jorge Perea

A thesis submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCES
In
COMPUTER ENGINEERING

UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS
2015

Approved by:

________________________________ ________________
Kejie Lu, Ph.D Date
Graduate Committee Chair

________________________________ ________________
Fernando Vega, PhD Date
Committee Member

________________________________ ________________
Wilson Rivera, PhD Date
Committee Member

________________________________ ________________
Pedro Torres, PhD Date
Graduate School Representative

________________________________ ________________
Raúl E. Torres Muñiz, PhD Date
Department Director

ABSTRACT

Smart grid is an advanced power grid which has been developed to improve the efficiency and reliability of the electricity network. However, because of the complexity of the smart grid, it introduces many security issues. This thesis investigates the security weakness and countermeasures of the smart grid to improve the understanding of the threats that this system faces, which is crucial from a security risk management perspective and allows the addressing of these vulnerabilities which contribute to the improvement the smart grid security. To achieve this goal, we divide the problem in the investigation of the security of two smart grid elements: (1) we study the use cases security of the Advance Metering Infrastructure (AMI) which is one of the smart grid's most important components; (2) we evaluate the security of the ANSIC12.22 network protocol which is the most adopted solution for supporting the operation of AMI.

RESUMEN

Smart grid es una avanzada red eléctrica la cual está siendo desarrollada para mejorar la eficiencia y la confiabilidad de la red eléctrica clásica. Sin embargo, dada su complejidad *smart grid* introduce muchos problemas de seguridad informática. Esta tesis investiga las debilidades de seguridad y mecanismos de defensa de *smart grid* para mejorar el entendimiento de las amenazas que enfrenta este sistema, lo cual es crucial desde la perspectiva de manejo de riesgo en seguridad informática, a la vez que permite abordar dichas vulnerabilidades contribuyendo así al mejoramiento de la seguridad del *smart grid*. Para lograr este objetivo, se dividió el problema en la investigación de la seguridad de dos elementos del *smart grid*. Por un lado, se estudia la seguridad de los casos de uso de la infraestructura de medición avanzada (AMI por su sigla en inglés) la cual es una de los componentes más importantes del *smart grid*. Por otro lado, se evalúa la seguridad del protocolo de red ANSIC12.22 el cual es la solución más ampliamente adoptada para soportar la operación de la AMI.

.

ACKNOWLEDGEMENT

Thanks to the almighty God who gave me light when I was in darkness, for his immensurable mercy.

I want to express my sincere gratitude to my adviser Prof. Kejie Lu, for the instruction he has given me and his invaluable support in this journey. Thanks for your patience, thanks for your immense help. Additionally, I express my sincere gratitude to the professors serving on my graduate committee. Prof. Wilson Rivera, for his advice and constant willingness to help me and support me, my gratitude for your collaboration. Prof. Fernando Vega, for his life example, his advice, his attention and many helpful comments, thanks you.

Finally, I want to say thanks to my wife and baby, for their unconditional support and love. Thanks also to my family for their patience, thanks to my parents because this work is also a result of their efforts; thanks to my friends for their help and disposition in difficult times.

TABLE OF CONTENTS

LIST OF ACRONYMS

AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
DER	Distributed Energy Resource
DoS	Denial of Services
DDoS	Distributed Denial of Service
DR	Demand Response
HAN	Home Area network
IDS	Intrusion Detection System
IP	Internet Protocol
ISP	Internet Service Provider
MITM	Man in The Middle
NAN	Neighbor Area Network
PLC	Power Line Communication
QoS	Quality of Service
RCD	Remote Connect Disconnect
RF	Radio Frequency
UC	Use Case
WAN	Wide Area Network

LIST of TABLES

LIST of FIGURES

CHAPTER 1. INTRODUCTION

Smart Grid[1] is a modern electrical power grid infrastructure that was first introduced in the U.S. to improve the traditional power grid electricity system. The Smart grid consists of an advanced two-way communication infrastructure for improved efficiency, reliability and safety. It is expected that, with the introduction of the smart grid, the production and consumption of the energy will be more effective and sustainable because smart grid can provide both the customers and the utility with real time information about the demands and consumption of energy.

Because of the expected benefits of the smart grid, governments around the world have been promoting the transition from the classic power grid to the smart grid in order to accelerate the design and deployment of smart grid. For instance, in the United States, the Energy Independence and Security Act 2007 mandates the deployment of a smart grid, and the Obama administration is investing 4.5 billion U.S. dollars in smart grid deployment [2]. Similarly, the European Union approved a law requiring all members to install smart meters with an adoption rate of 80% by 2020 and 100% by 2022 [3]. Besides these efforts, many private companies have also invested intensively in smart grid.

Clearly, the smart grid promises enormous benefits in terms of efficiency and reliability of energy generation, distribution and consumption. However, due to its fast development and complexity, many security issues arise [4]. Additionally, due to its critical role, it is important to protect the smart grid from a wide range of potential attackers, such as organized crime, hostile governments [5], or even emotional-driven persons [6] with a variety of motivations. Therefore, considering these threats and their potential impact, and the fact that smart grid is still in an early stage of development and deployment, it is crucial to identify its potential vulnerabilities in order to create mitigation strategies for improving the security of the systems, which is the goal of this work.

In this thesis, to achieve the aforementioned goal, we investigate the security problems in smart grid from two perspectives. First, we study the security use cases of the Advanced Metering Infrastructure (AMI), which is one of the most important components in smart grid. Secondly, we evaluate the security of the ANSIC12.22 network protocol, which is the most adopted solution for supporting the operation of AMI.

1.1 Motivation

With the emergence of new communication technology and the need for a more efficient power grid infrastructure, the concept of smart grid has been proposed. The smart grid is expected to provide both customers and utilities with real-time information about the demands of energy. Consequently, the production and consumption of energy can be more effective and sustainable. Such a salient feature has motivated the industry and academic sector, in the research, analysis, design and deployment of the smart grid. Many governments all around the world have invested a huge amount of money in the development of this technology. This stimuli has caused a fast development of the communication technology necessary to support the smart grid as well as a huge deployment of the smart grid components in many countries [7]. For example, in the U.S. alone, more than 43 million smart meters have been installed according to the U.S. Energy Information Administration [8] , with a peak rate of installation as high as 12,000 meters a day [9].

Despite the increasing interests in smart grid and its fast development, there are many concerns related to the security issues, which can exist in this advanced power grid [10]. Therefore, there is a strong need for in-depth understanding of its potential security weaknesses. To this end, this work conducts an evaluation of the security of one of the most important components of the smart grid, known as the Advanced Metering Infrastructure (AMI), with the objective to identify potential vulnerabilities and to create mitigation strategies to reduce the risks, to which the system is exposed.

1.2 Contributions

The deployment of the smart grid is expected to address the efficiency and reliability issues of the electrical grid. However the deployment of this advanced grid infrastructure brings new challenges from the cyber security perspective; having a good understanding of the risks that the system faces is one of them. This thesis investigates security issues in smart grid to contribute to improving that understanding.

First, we present a use case centric assessment of the AMI. We conduct an analysis of the security weakness of each one of the AMI use cases as well as a discussion of potential attacker's motivations and attack interface. We also present a survey of existing AMI attacks and show our own findings in this regard. Additionally, we introduce a classification of AMI attacks.

Second, we present a security analysis of the ANSI C12.22 protocol. We identified vulnerabilities on the protocol services and potential attacks. Additionally, we present mitigation strategies for the identified vulnerabilities.

1.3 Organization of the Thesis

This thesis is organized as follows: Chapter 2 presents a background of the smart grid, AMI and ANSIC12.22, discussing their components, infrastructure, standards and services. Chapter 3 deals with related works. The fourth chapter presents a detailed analysis of vulnerabilities in AMI. Chapter 5 shows Denial-of-Service issues on ANSIC12.22. Finally Chapter 6 presents Conclusion and Future Directions.

CHAPTER 2. BACKGROUND

In this chapter, we first discuss the fundamentals of smart grid communications, including the smart grid infrastructure, requirements and challenges. Second, we introduced AMI, its system architecture, protocols, use cases and actors. At the end of the chapter, we present the ANSIC12.22 protocol; we define its basic concepts, topology and services.

2.1 Smart grid communications

Smart Grid is an advanced electrical power grid infrastructure which was proposed first in the U.S. to upgrade the traditional electricity system, known as the power grid, which was created many decades ago for the purpose of supplying energy for homes and business all around the country. Despite the importance of the power grid, it is supported by aging technologies that have increasing risk of failure and efficiency issues. Therefore, due to the evolution of the technologies, and the changes in the way that energy is generated, the traditional power grid is no longer able to satisfy the current and future requirements. To face the many new challenges and satisfy the actual needs of energy generation, management and consumption, governments all around the world are promoting the implementation of the smart grid, which is considered as the next generation of power grid with much better efficiency, reliability and safety, which can be achieved by introducing an advanced two-way communications infrastructure [1][11].

2.1.1 Smart grid infrastructure

The Smart grid distributes energy from electricity sources to power consumer using power and communication infrastructure, in this section we discuss such infrastructures [12][1][13].

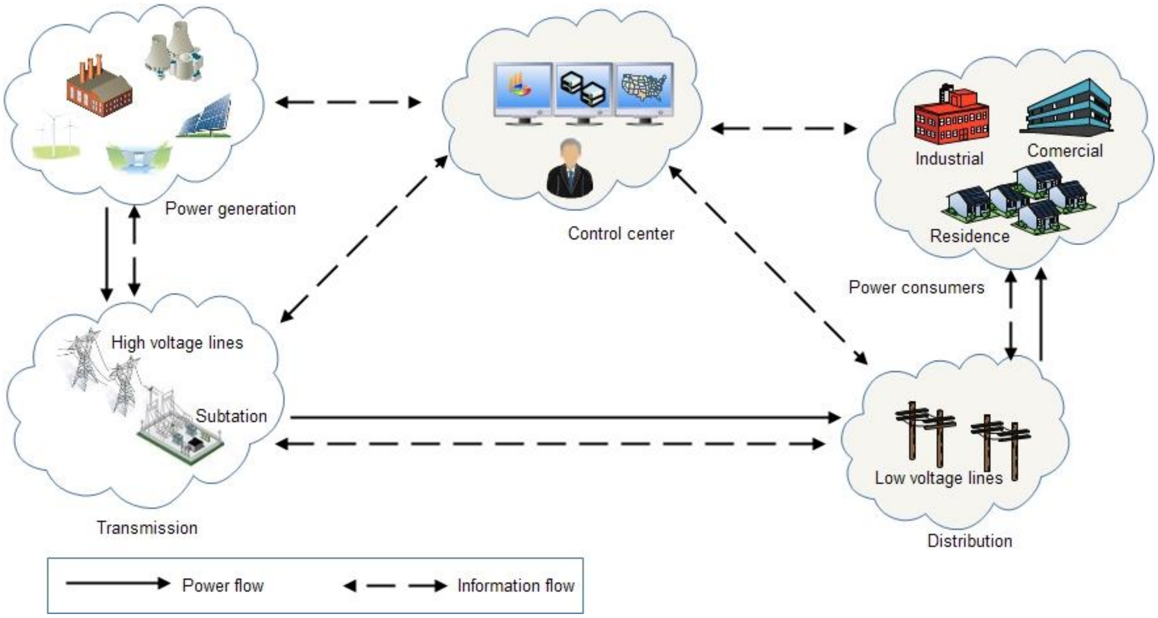

Figure 1. Smart grid infrastructure

Figure 1 shows one of the most common smart grid architecture with the following components:

- Power generation: This component includes traditional power generation plus distributed energy sources such as solar, wind, hydropower, etc.
- Transmission: consists in the transfer of energy from the power generation component to electrical substations using high voltage power lines.
- Distribution: delivers energy from electrical substations to customers

- Power consumers: smart meters in commercial, residential and industrial customers' facilities receive the electricity for consumption.

In addition to the electric infrastructure, smart grid is supported by a communication infrastructure which intercommunicate the previously mentioned components. The portion of this infrastructure which is placed in between the utility and the customer is called the Advanced Metering Infrastructure (AMI), which provides many functions such as meter reading, remote interaction with customers in home smart devices, outage detection, smart meter keying and emergency control. The AMI will be discussed in more details in the next section.

2.1.2 Smart grid requirements

Due to the current changes in energy generation and the introduction of an advanced communication technology, the smart grid has to address a set of new requirements. **Reliability** is one of such requirements because the smart grid has to handle an increasing energy consumption and peak demands supported by the aging power infrastructure[14]. Another important requirement is the **scalability** for supporting an increasing number of devices and services joining the communication network, as well as more and more customers interactions for energy monitoring[11]. Additionally, **security** is crucial to prevent cyber-attacks, whose potential impacts can cause the destabilization of the system. Another need that should be addressed is related to the **interoperability** of the system, which enables effective interaction among its components. **Standardization** is another requirement and should be achieved through all different subsystems of the smart grid. Finally, **Quality-of-Services** (QoS) is needed to support the communications among different components of the smart grid infrastructure [1].

2.1.3 Smart grid challenges

Due to the large-scale nature of the smart grid and its importance, smart grid infrastructure faces a lot of challenges[1]. In first place, considering the fact that smart grid is a highly complex system, modeling, analysis and design an appropriate communication infrastructure is very difficult. Moreover, very large scale problems have to be solved and uncertainty has to be managed. Additionally, due to the needs of grid-wide monitoring and control capabilities, the communication infrastructure has to manage a huge volume of traffic. Another challenge is how to manage a variety of new energy generation methods, because many of them are based on renewable energy, which are affected by both the weather conditions and the variation of the demands of the energy by customer in periods when its price is high. Finally, because of the system importance, its components and their interconnections through a two-way communication network, a large number of potential vulnerabilities may exist[15][16], which can be exploited by different attackers[5][17] with various motivations[18], causing many security issues[19][20][21]. Therefore, it is very challenging to manage the cyber security risk of the system.

2.2 AMI definitions

In this Section, we first discuss the AMI system. We then present the main AMI protocols, as well as AMI use cases and actors.

2.2.1. The System Architecture

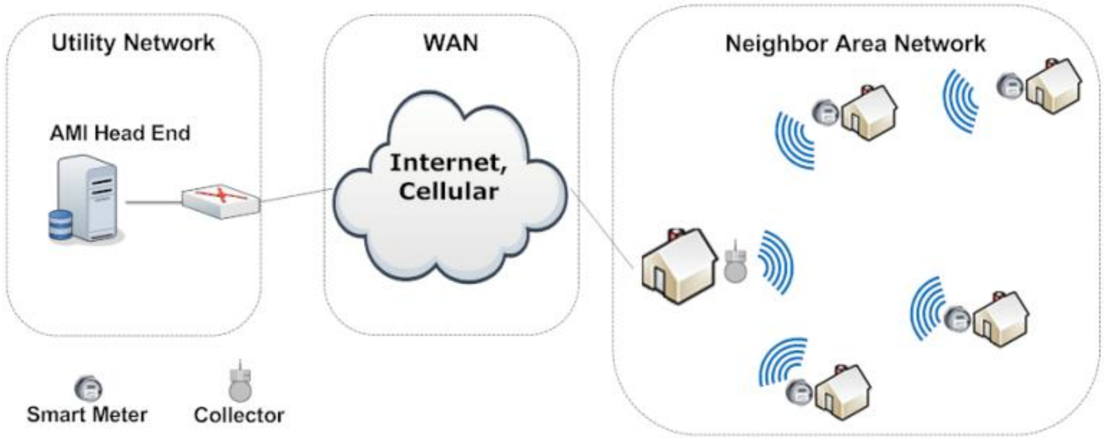

Figure 2. The system model for AMI.

In the literature, various AMI configurations have been proposed and deployed [1][10][22][23]. To facilitate the security analysis, we choose a dominating system architecture used in many existing studies, as illustrated in Figure 2, which consists of three network domains.

The **utility network** consists of servers and network devices at the utility premise. The key component in the utility network is called the **AMI Head End**, which can communicate with smart meters and perform a set of important functions. First, the AMI Head End can collect metering information, evaluate its quality and determine errors using the **AMI Meter Data Management System (MDMS),** and then deliver the processed metering data to billing systems [24]. Secondly, the AMI Head End can also send configuration and pricing information to smart meters, as well as manage and perform firmware upgrades remotely. Thirdly, the AMI Head End can receive alerts such as outage information for control and diagnostics, which may trigger other functions of the smart grid. To support these functions, several modules have been defined, including **AMI Network Management System, Demand Response Analysis and Control System** (DRACS), as shown in[25].

The **wide area network** (WAN) provides connectivity between the utility network and the neighborhood area network (NAN). Typically, WAN can be any networking technologies that provide long range communications, including cellular network, power-line communication (PLC) system, public switched telephone network (PSTN), and the Internet.

Finally, the **neighborhood area network** NAN is responsible for enabling the communications between smart meters in a neighborhood. To realize NAN, a number of technologies have been proposed to create a mesh network, such as IEEE802.11 (Wi-Fi), PLC, direct cellular communication, and other proprietary radio frequency (RF) communication technologies.

In NAN, two important types of components have been used: **collector** and **smart meter**. The **collector** is also known as aggregator, or **data collection unit** (DCU). This device acts as a gateway between the WAN and the smart meters. In practice, the collector may or may not have smart meter capabilities.

Smart meter is the device that has two-way communications capabilities to exchange data with the utility. Its main purpose is to measure, record and transmit energy usage data and event logs. Note that the energy usage can include both energy consumption and generation.

Besides the three major network domains, some in-home customer appliances can also be included in AMI, if they have the capabilities to communicate with smart meters. In such a case, the fourth type of network can be formed, which is known as the **home area network** (HAN).

2.2.2 . AMI protocols

Several standard protocols have been published in order to provide interoperability among AMI systems. In this section we describe the most relevant ones.

First, the ANSI C12 family[26] is one of the most adopted protocols for supporting AMI in the United States[27]. Its purpose is to transfer data units (known as tables) through different interfaces. This family of protocols is integrated by: ANSI C12.18 which provide point-to-point communication between smart meters (C12.18 devices) and a C12.18 client through optical ports; ANSIC12.19 specifies the data structure used to transport metering data between AMI devices; ANSIC12.21 is an extension of C12.18 that can be used over dial-up; ANSIC12.22 extends the ANSIC12.18 and ANSIC12.21 for data transfer over reliable networks.

Second, Zigbee Smart Energy Profile (SEP)[28][29][30] is a communication standard for supporting HAN and NAN. This protocol supports many AMI functionalities such as real time pricing, demand response and billing. Regarding security, the protocol proposes the use of AES-based encryption, SHA functions for hashing and public key mechanisms. Additionally, it supports TLS, IPSEC and AES-CCM for securing the transport, network and data link layer of the OSI model respectively. In terms of the application layer, the protocol communication is based on RESTful services over HTTP.

2.2.3 AMI Actors and Use Cases

In this subsection, we first specify the actors in the AMI system. We then discuss typical use cases.

2.2.3.1 *AMI Actors*

Utility: The utility is a company or agency that provides utility services to its customers. In the AMI system, the utility maintains its utility network that includes different management systems, as shown in Figure 2.

Customer: In the AMI system, a customer is an entity that obtains utility services. Customers can be categorized into residential (e.g., home owners), commercial (e.g., office buildings, apartment complexes), industrial (e.g., manufacturing plants), and municipals (e.g., street lights, traffic lights, subways, etc.).

Third party: A third party can be any entity other than the utility and its customers, such as Internet service provider (ISP), billing companies, other utilities, etc. In some cases, a customer may subscribe services from a third party company to manage the devices in its premise (i.e., HAN).

2.2.3.2 AMI Use Cases

With the definitions above, we now consider the following 13 important use cases [31][26]. To enumerate them, we use the abbreviation UC (standing for use case) plus a number.

- UC0. WAN/NAN Communications: The WAN/NAN communications enables information exchange in AMI.
- UC1. Meter Reading: The AMI Head End reads metering data periodically or on-demand remotely so that customers will be billed on their energy usage.
- UC2. Time-of-use (TOU) pricing: The cost of energy varies depending on the energy demand, which changes along the day. The AMI Head End sends the TOU pricing to customers in different moments in the day. Thus, based on this

information, customers can adjust their energy usage to increase the energy consumption when it is cheaper, and decrease the consumption when the energy is more expensive.

- UC3. Prepayment notification: Utility can offer customers a lower rate if they can prepay energy usage. For a customer who chooses this option, the AMI head end sends a notification to the smart meter when the available balance reaches a threshold. Alternatively, the smart meter can stop the energy consumption if the fund is insufficient.
- UC4. Remote HAN interaction: A customer can use the AMI system to interact with devices at customer's premise via the Internet.
- UC5. Third party metering data access: A customer can query his or her energy usage data through a third party platform.
- UC6. Remote Connect/Disconnect: AMI allows utilities customer to remotely connect or disconnect (remote meter disconnect (RCD)) the utility service, which eliminates the need for utility personnel to visit the customer premise.
- UC7. Outage Detection: Smart meter can provide to the utility up-to-date information about the status of customer's service.
- UC8. Power Quality Analysis: AMI can obtain data from smart meters, such as harmonics, voltage, variations, etc., and then perform power quality analysis. By analyzing the quality, the AMI can trigger other actions in power distribution networks to improve power quality.

- UC9. Firmware upgrade: When a new firmware of smart meter is available, the utility can send the new firmware to smart meters and upgrade them using the AMI communication infrastructure.
- UC10. Program update: A utility can use AMI to remotely install programs in the smart meters.
- UC11. Smart meter keying/rekeying: When a smart meter is installed, the utility can set a cryptographic key. If a smart meter is compromised, the utility may have to send new keys to other smart meters via the AMI communication infrastructure.
- UC12. Emergency control: To get a special energy rate, a customer may agree a temporal suspension of the energy supply in case of emergency. In this case, the utility may send an RCD command to smart meters to satisfy the peak energy demand or improve the grid reliability in some AMI segments.

2.3 ANSIC12.22

In this section we describe the protocol ANSIC12.22. We start discussing the protocol background; second we present ANSIC12.22 basic concepts, and finally we introduce the protocol topology and services.

2.3.1 ANSIC12 family

In this section we describe the protocols of the ANSI C12 family which support AMI communications. These standards where co-published by IEEE as IEEE 1377 and IEEE 1703, and by Measurement Canada as MC12.19 and MC12.22 [32].

ANSI C12.22[33][34] defines an application layer protocol used for transmitting messages over any underlying transport networks, to provide end-to-end communication between the utility data management system and the AMI end devices (i.e. smart metes and collectors) across heterogeneous network segments. The messages transmitted by this protocols include the data table elements defined in ANSI C12.19[35], IEEE P1377/D1, and MC1219. ANSI C12.22 uses the Advanced Encryption Standard (AES) as the encryption mechanism, which supports three security modes: none, authentication only and cipher text with authentication.

ANSI C12.19[35] specifies the data structure used to transport metering data between AMI devices. ANSI C12.18[36] defines a protocol to provide point-to-point communication between smart meters (C12.18 devices) and a C12.18 client through optical ports. This protocol is used by field crews to maintain or read metering data directly from smart meters using the optical port interface in front of them. ANSI C12.21[37] is an extension of C12.18 that can be used over dial-up modems and can be used to replace the ANSI C12.22 in some AMI deployments.

A concrete set of requirements for implementing ANSI C12.22 over IP networks has been defined by IEFT in [32], where TCP, UDP and IGMP are proposed to forward C12.22 messages.

2.3.2 C12.22 basic concept [34]

C12.22 application: Application that implements a set of C12.22 services to successfully interact in a C12.22 network.

C12.22 node: An element in the network that attaches a network segment, it should run at least one C12.22 application. A node can act as a client or a server. In the first case, the node sends a logon service request to initialize a session. In the last one the node receives a logon request. Smart meters acts as C12.22 nodes in AMI.

C12.22 relay: It is a node that provides datagram segmentation, address resolution and optionally data forwarding to other C12.22 nodes.

C12.22 master relay: It is a C12.22 relay operating in the top of the relays hierarchy. Its main function is to provide registration and deregistration services to C12.22 node to join or leave a network segment. It also notifies to the authentication or notification host in the network, when these services take place.

C12.22 host: It is a C12.22 node that performs authentication services to other C12.22 nodes, or need to be notified when such event occurs. A C12.22 host typically runs on a server instead of an embedded device. It is located in the utility network.

C12.22 gateway: Represents a C12.22 Node that translates other protocols to ANSIC12.22 or vice versa. The AMI collector is the ideal element to perform C12.22 gateway functions due to its position in the network.

C12.22 message: It represents any service request, service response, notice, or device status sent from one C12.22 node to another across the C12.22 network.

C12.22 network: Communication infrastructure that has at least one C12.22 master relay and one or more C12.22 nodes.

C12.22 network segment: A set of nodes that can communicate among themselves without any C12.22 relay. C12.22 network segments are interconnected through C12.22 relays.

Called ApTitle: It is used as the 7 layer source address of a C12.22 message.

Calling ApTitle: It is used as the 7 layer destination address of a C12.22 message.

2.3.3 C12.22 topology[38]

An ANSIC12.22 network topology is illustrated in Figure 3.

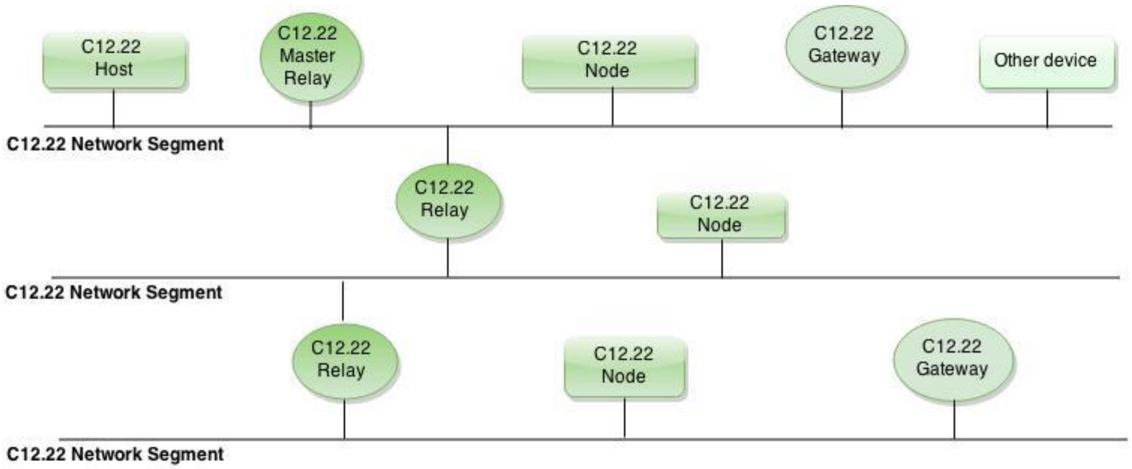

Figure 3. ANSIC12.22 topology

As illustrated in the figure above, the ANSIC12.22 topology is organized as follow: at the top of the hierarchy there is a master relay, which provides registration services for devices under its domain. Second, there are relays, which provide message forwarding, data segmentation and address resolution services. Third, there are gateways, which translate ANSIC12.22 messages to and from other protocols. In the fourth place, there are C12.22 nodes which send and receive data but do not have forwarding capabilities. Fifth, special nodes known as “host” may be present in an ANSIC12.22 topology; these hosts may authorize the registration of nodes in a master relay domain or subscribe for notification when a C12.22 node is registered. Finally, there may be other devices which do not implement the ANSIC12.22 protocol.

2.3.4. C12.22 Services

ANSI C12.22 describes 13 services for supporting the programming, configuration, and information retrieval of C12.22 nodes through the network[38]. In this section we provide a description of these services:

Identification service: this service is useful to obtain the functionality of a node. As response, the service returns the standard, version and revision supported by a particular node along with a optional list of features.

Read service: this service allows the partial or complete transfer of tables from a node to another. As response, the service returns the length of the request data and the data itself. The write service is very similar to the read service but writing information in node´s tables instead of reading it.

Logon service: it is used to establish a session between two nodes. Between the parameter used to request this service we can find <req-session-idle-timeout>, which is used to indicate to the C12.22 server the desired time that a session can be idle, before the server may terminate it. A value of zero means that the requested session should be open forever.

Security service: This service is useful for setting access permission to C12.19 tables while not provide any security mechanism to the message itself. In this service, a node sends a request to another sending its identity and a password, then the destination node validates if that password belongs to its security table and grant the access permissions established for that particular password.

Logoff service: This service allows the termination of a session previously established using the logon service. As result, the service responds with and ok message, then all the resources associated to the session should be free. The termination service is similar to the logoff service except that the former one should be used only for certain reasons such as security issues, excessive errors, among others. The disconnect service has the functionality of the termination service plus a transition to the offline state, that is to say, after the termination of the session the disconnected node will not be able to receive any communication from the network.

Wait service: This service is used to prevent a session from terminating because of time out reasons. When a node is interested in keeping an idle session alive, it can send a wait request specifying the amount of time it desires the session to be extended. As result, the node which received the request can send an ok message accepting the extension of the session for the requested time.

Registration service: This service is used by C12.22 nodes to be part of a C12.22 network segment. The C12.22 node sends a request to the master relays indicating some identification information. Once the master relay accepts the registration, it sends notifications to those hosts that are registered to receive it, and sends a registration service response to the node with the ApTitle that the node should use, this ApTitle can be established by the master relay or by a C12.22 relays, the last one in the moment that forwards the message. In this step every C12.22 relay that forwards that message will add the new node to its routing table. On the other hand, this service can also be used for a node to auto-assign a master relay, putting a blank value in the called ApTitle field.

Deregistration service: This service is used to remove a C12.22 node from the routing tables of relays and master relays. To use this service it is necessary to send the address of the node which is desired to be deregistered from the network. As response, the service can return an ok message indicating that the node was deleted from the routing tables.

Resolve service: This service is used to translate ApTitles to lower layer addresses. A resolve service request has as calling and called ApTitle, the ApTitle of the node that needs to resolve a direction and the ApTitle of the node whose direction is intended to retrieve respectively. This request is forwarded through the network until a C12.22 responds it with the native network address of the intended C12.22 node. In network segments with broadcast, this service can be used to get the list of C12.22 relays, by putting the ApTitle of the messages in 0 or setting the master relays. In the former, every node with auto-assigned master relay capability will respond putting its own ApTitle and native address. In the last one, every node able to forward packets to the master relays whose address is in the request will respond with its own ApTitle and native address.

Trace services: This service is used to retrieve the list of all C12.22 relays that forward a message to a particular destination. When a node needs to know the relays in the path to another node, it can send a trace service request to the destination node, then each relay which receives it appends its own address and forwards it to the next relays, then, when the message arrives to a relay which is adjacent to the destination node, this relay sends a response to the requester node appending its own address.

CHAPTER 3. RELATED WORK

In this chapter, we discuss related work in three areas, i.e., smart grid security, AMI security, and ANSIC12.22 security.

3.1 Smart grid security

In this section, we present a literature survey regarding smart grid security issues and countermeasures.

In the first place, [15] presents an analysis of attack vector and threats related to the data metering component of the smart grid. Some of the presented threats are system-level threats which are related to the operation of the grid such as network intrusions and denial of services. Other groups of threats are driven by theft of services consisting of the substitution, swapping or manipulation of meters to report wrong usage data. A final kind of threats is related with privacy and confidentiality affected mainly by message interception techniques. With regards to the attack vectors, the paper divides the AMI in different tiers to ease the analysis. As a result, the authors reported a variety of attack vectors, including traffic sniffing, configuration manipulation, social engineering, backend services in charge of receiving metering data inside the utility network, as well as the web application front-end which accesses that data.

In [39], the authors investigated the *blackout attack* against the smart grid and proposed countermeasures to prevent it. Specifically, they considered that an attack can be performed by abusing smart grid characteristics using cyber physical system malware, with the following five phases. Phase 1 consists of the initial penetration of the system and installation of malware for data colleting purposes. Phase 2 uses the installed malware to gather information about the smart grid structure and configuration. Phases 3 and 4 are the development of the malware for the blackout attack and the launching of the attack, respectively. The last phase consists of cleaning up any log of the malware from the system as well as erasing any malware sample to complicate computer forensic activities. Additionally, to the aforementioned steps, the authors presented a set of countermeasures to mitigate the blackout attack, which consist of application and network white listening, file and memory integrity monitoring, system refinement and multifactor authentication. Finally, the paper explains the implementation of a smart grid prototype powered by virtual machines and Arduino kits to demonstrate the effectiveness of the attack and the proposed countermeasures.

[5] discusses potential high impact attacks such as remote commands to interrupt the energy supply in a huge number of smart meters, malicious software updates and upgrades to block the meters and the modification of cryptographic keys to deny the access to smart meters configuration and monitoring. The sending of remote commands to interrupt energy supply (off-switch command), is also used in [40] to achieve a more complex attack. In the paper, the authors introduced the use of the off-switch to cause a

destabilization of the energy generation process, and put the voltage and frequency of the network outside of its tolerance limits to cause total blackouts. To mitigate the off-switch attack, [41] proposes the use of a random time delay. In this approach, when a smart meter receives a remote disconnect command, it waits for a certain period of time before effectively interrupting the energy supply. The authors demonstrated how this scheme is useful to prevent rapid changes in the system load, as well as to provide time for the utility to detect and stop the attack in progress. An interesting result of this work is that a delay distribution from 0 to 2 hours can reduce the percentage of the energy interruptions of the targeted smart meters below 1%.

In other directions, [42] presents the assessment of vulnerabilities in the electricity pricing transmission in AMI as well as countermeasure techniques. To conduct this research, the authors simulated two cyber-attacks to manipulate the guideline electricity price received by smart meters. By using simulation experiments, the authors showed that an attacker can reduce his electricity bill by 34% while increasing other's bill in about 8%. Additionally, the attacker can unbalance the energy load of a power system in local communities, which shows the effects in the power system due to cyber-attacks on the communication system. Regarding the countermeasures, the authors used support vector regression in order to detect pricing manipulation and they demonstrated by simulation that this technique is effective. Finally, several defensive strategies for preventing smart grid cyber-attacks can be found in [43][44][45][46][47][48].

Similarly, [20] presents a survey of representative threats against smart home/smart grid environment. The authors started by showing the smart grid and smart home architecture and benefits. Then, they discussed several security issues in smart homes such as eavesdropping, traffic analysis, message modification, illegal software installation, and device impersonation which can be used to launch attacks against the reporting of right energy consumption, energy import and export signals, physical metering tampering, remote home monitoring and control, and the gathering of user's energy usages data. Additionally, researchers presented some potential attacks against some smart grid elements like utility servers, Wide Area Measurement Equipment, demand response signals, outage reporting and network aggregators. Furthermore, the paper presents a survey of countermeasures for the discussed attacks. These defensive measures include: data obfuscation, encryption algorithms, anonymization, trusted aggregators, intrusion detection system, digital watermarking, and alternate frequency channels among others.

Cyber security testing is also an important topic for smart grid security. In [49], the researchers approached the problem of cyber security testing in smart grid; and they proposed a solution for the problem, where the solution includes three main components: a methodology to define appropriate places to evaluate security, a scheme to measure the security of the system and the creation of tools to carry out the tests. For the testing methodology, they proposed the use of a generic approach, which is also valid for Smart Grid. Some of the steps are: gathering system information, identifying system components, gathering protocol specification, assessing the system under several inputs and outputs, identifying threats and evaluation of security controls. Regarding the approach to facilitate the identification of metrics for security evaluation and comparison, the authors evaluated several strategies in the literature and decided to use a formal model along with the development of a theorem and its proof. In order to carry out the tests, they used a cyber-physical Testbed with emulation, simulation and integration of real equipment capabilities. Finally, the authors created a multi-platform packet dissector library to analyze network traffic and an AMI visualization framework for management purposes.

In the same direction, [50] presents the integration of the emulation framework OpenVZ with network simulator S3F in order to achieve a high fidelity Testbed for the analysis of large scale systems, where they showed the solution of important challenges in the conversion from emulated time to virtual time and vice versa to make the integration possible between OpenVZ and S3F possible. Additionally, the authors present a case-study of a cyber-attack in the Smart Grid consisting in a DDoS against the AMI abusing the ANSIC12.22 Trace Service, demonstrating the utility in their approach. Finally, [6][51][52][53][54] describes another simulation frameworks for smart grid security evaluation.

The following table summarizes the presented studies. The security aspect is composed by availability (A), integrity (I) and confidentiality (C).

Reference	Security aspect	Attacks	Countermeasures
[15]	A,C,I	Attacks against each one of the security aspects in all the AMI tiers.	Encryption, strong passwords, integrity checks, physical resilience of smart meters
[39]	A	Smart grid Black out attack	Multifactor authentication, integrity monitoring, while listening
[5]	A	Interrupt electricity supply	Implementation of cryptographic controls
[40]	A	Destabilization of energy generation process	N/A
[41][43][44][45][46][47] [48]	A, C, I	N/A	Random delays for meter shutdown when receiving RCD commands, cross-layer security, agent-based protections.
[42]	I	Manipulate electricity prices	Detection: Support vector regression to detect pricing manipulation
[20]	C,I	Traffic analysis, message modification, device impersonation	Encryption algorithms, IDS, data obfuscation.
[6][49][50] [51][52][53] [54]	A, C, I	N/A	Creation of a cyber- physical test bed for vulnerability validation purposes.

Table 1. Summary of smart grid studies on security

3.2 AMI security

Many papers have been published related the security in the Advanced Metering Infrastructure (AMI). [18] Investigates whether or not it is possible to steal energy in the new smart grid, and documents the methods that the adversaries may use to commit energy fraud. Additionally, the researchers validated their findings through penetration testing. As a result, this work shows different vectors for conducting energy fraud, which demonstrates the feasibility of this issue in the smart grid. Similarly, [55] studies the issues and challenges in detection of energy theft for AMI in the smart grid. First, the authors explained the techniques for energy theft detection as well as a comparison among them using detection rate, false positives, methodology and implementation cost as comparison parameters. The discussed techniques are: classification which uses machine learning and artificial intelligence showing a medium level in terms of detection rate, false positives and cost; state monitoring which has a high detection rate and cost and low false positive; game theoretical approach that has a medium detection rate and false positive at a low cost. Regarding the challenges for energy theft detection, the authors pointed out privacy issues, secure data collection and data storage and processing capabilities.

In [56], the authors discussed the integration and security aspects of AMI. The paper presented several attacks which constitute AMI security issues, including: eavesdropping, data modification, DoS, identity or service spoofing and compromised keys. Additionally, the paper presents security recommendations for AMI consisting of identity base encryption, asymmetric encryption, digital signature, and sharing secret keys in legacy infrastructures.

More potential attacks as well as security controls for AMI are introduced in [57], where the use of a worm to infect smart meters and send malformed authentication packets to another smart meters is described, along with an early warning system for smart grid intended to detect attacks before they take place in the network. This warning system can forewarn the DDoS attacks beforehand. Presumable attacks related with abnormal voltages and fluctuation can also be detected.

In terms of privacy, it has been proved that potential violation of privacy may occur in the AMI, because the energy usage information stored in the meters can expose customer habits and behaviors due to some activities. For example, typical activities such as watching TV have detectable power consumption signatures [58]. In addition, the presence of people in a particular home can be inferred from the energy consumption, which can be exploited by thieves to determine when to target a particular home [23]. Additionally, [59][60][61][62] present more studies about inferring user lifestyle from their energy usage, which is collected and transmitted almost in real-time for the smart meters. Moreover, [63][64] propose countermeasures to mitigate this problem found on an escrow-based anonymization scheme and data aggregation for all smart meters using a spanning tree topology rooted in the collector engine.

In other direction, some authors have researched the attack methodology and penetration testing techniques in the AMI. In [65], the authors presented an archetypal attack tree approach for penetration testing across multivendor implementations of AMI systems. The authors then applied their approach to model attacker goals, which allows them to find real attack scenarios. The attacks discussed in this paper can be accomplished in different ways following different paths in the archetypal trees. An AMI penetration testing plan was also presented in [23]. This plan is intended to help electric utility security teams to conduct their penetration testing activities and the plan consists of a set of penetration testing tasks that can be completed in a systematic way. These tasks are the following: penetration testing planning; target system set up; testing of embedded devices, network communication, server OS, and server application; end-to-end penetration testing; and result interpretation and reporting.

In the same sense, [66] proposes an AMI attack methodology, which is based on the assumptions of some vulnerabilities that may be presented in an AMI deployment and the subsequent set of attacks used to find and exploit them. This attack methodology is divided into the following stages: reconnaissance for gathering information about the system; initial analysis, which consist in the use of techniques to identify vulnerabilities and new attack vectors; deep analysis to further determine potential vulnerability areas; and finally the exploitation phase which consists in the execution of attacks to validate the existence of vulnerabilities in the system. It is important to note that, unlike the previous methodology, which evaluates all the aspects of an AMI, this attack methodology is limited to physical components, which are located outside the physical premise of utility companies and therefore cannot be protected by their physical security controls. Similarly, [25] presents a set of guidance and security controls for securing the smart grid, and it shows the security concerns related to AMI. The approach used in this work consisted of the examination of the AMI use cases, followed by the evaluation of risk for the infrastructure; then the conduction of AMI security service domain analysis and finally the recommendation of security controls.

Several studies have addressed the problem of effective Intrusion Detection Systems (IDS) for AMI. For instance, [67] shows the need for monitoring and intrusion detection solutions in the AMI. To conduct their study, the authors presented a model of the likely threats that this infrastructure could face. Additionally, they surveyed the literature to understand appropriate detection technologies and analyzed IDS common components, types and challenges. Next, the authors proposed the architecture of an infrastructure for a comprehensive AMI monitoring solution. In the same way, [22] presents a study of intrusion detection requirements. The authors of this work conducted a survey of various threats faced by AMI as well as common attacks. The attacks discussed were: distributed denial-of-service (DDoS) attack against the Data Collection Unit (DCU), stealing customer information and sending remote disconnect commands to the smart meters, among others. In addition, they analyzed the threats and attacks objectives of AMI looking to tie them to individual attack steps. The type of information that would be required to detect attacks was also gathered. These steps are necessary in order to understand the requirements for an intrusion detection solution. As a conclusion, the authors' analysis suggests a hybrid sensing infrastructure consisting of a centralized IDS collaborating with sensors embedded in the meters to provide the best coverage for monitoring attacks. Finally, authors in [68][69][70] presented different strategies for intrusion detection in AMI including: noninvasive approaches, collaborative mechanisms and detection of compromised smart meters through cumulative analysis.

The approach of constraints definition to detect security violations was also used in [71]. In this paper, the authors studied configuration invariants and security constraints and they proposed a formal modeling of AMI components' configuration using Prolog declarative logic to verify its compliance with security guidelines. Among the modeled components' configuration, the authors presented the AMI physical components and AMI data delivery modes. Additionally, this work presents an AMI threat model analysis consisting of schedule misconfiguration and denial-of-service (DoS) attacks. Following the research line of intrusion detection on AMI and based on [22][27], [72] presents a complete design of an IDS called Amilyzer. This design is based on the study of realistic failure scenarios. Additionally, the paper presents a comprehensive security policy for AMI and lessons learned from the IDS evaluation after being deployed during several months in a real AMI.

The following table summarizes the presented studies.

Reference	**Security aspect**	**Attacks**	**Countermeasures**
[18][55][68][69][70]	I	Physical tampering, eavesdropping, meter spoofing	IDS techniques based on machine learning, artificial intelligence, state monitoring and game theory.
[57]	A	DDoS using malformed authentication packets	Early warning system
[59][60][61][62][63] [64]	C	inferring user lifestyle from their energy usage	Anonymization schemes, data aggregation.
[23][25][65][66]	A,C,I	Penetration testing methodology	Integrity protection, multifactor authentication, use of key management schemes
[22][67][71][72]	A,C,I	MITM, packet flood, jamming, drop packets, node impersonation	Implementation of IDS

Table 2. Summary of AMI studies on security

3.3 ANSI C12.22 security

In the previous section, we presented a review for the AMI security. In this section, we will discuss those works which are related specifically with the ANSIC12.22 protocol. In [73], the authors discussed three vulnerabilities in ANSIC12.22 services. First, they presented the trace service vulnerability, which is due to the lack of validation of the size of the trace service response and the lack of mechanisms to prevent identity spoofing. Because of this vulnerability, an attacker can spoof the address of a victim node and start many trace service request impersonating it. As a result, all relays in the path of the attacker request will append their own addresses to a message that will be send to the victim address; so, this message can get considerably big as more relays forward it. Once the victim receives all the messages its network resources will be exhausted because of the number and size of the packets, which results in a DDoS attack. In the second place, the authors presented the resolve service vulnerability, which relies on the same principle of spoofing the victim's address to cause that unsolicited services responses exhaust the victim's resources. Additionally, the paper presents the urgent traffic vulnerability which allows an attacker to set an URGENT bit in his traffic to receive a priority treatment. Then, if the attacker sends a huge amount of traffic, the legitimate traffic in the network will be delayed or dropped because the network resources are being wasted processing the attacker traffic. Finally, the paper presents countermeasures to these attacks, which includes the implementation of watchdogs in the network. With this defensive measure, the relays can act as watchdogs and monitor the outgoing traffic from the neighbors. In this way, when a node originates a huge amount of traffic, it is detected and other nodes can drop the packets or downgrade their treatment.

In [74], the authors studied the impact of a DDoS attack against the AMI. For this, the network behavior was simulated using a stochastic activity network (SAN) model. Then the paper presents a recreation of a DDoS attack by exploiting the trace service vulnerability of the ANSIC12.22 protocol. After simulating different AMI topologies and varying the number of attackers between 1 and 2, the results show an increment in the percentage of time that the egress node is busy or with a full queue in more than 20% in the best case and about 70% in the worse case.

Finally, [27] proposes a specification-based intrusion detector sensor based on the development of a set of constraints to ensure the compliance with a defined security policy. The authors' approach was to create constraints in the ANSIC12.22 transmission in such a way that a constraint violation implies a security violation. The defined constraints are divided in three categories: network-based, device-based and application-based and are defined based on the analysis of a system model, potential threats and network traces captured from different use cases. In the study, the network traffic was generated by an emulator called Table TstBench. Additionally, the authors defined a formal framework and a proved a theorem to validate that the defined constrains successfully detected security violations. Finally, these constraints were implemented on an intrusion detection sensor and evaluated under different conditions in order to measure its efficiency.

The following table summarizes the presented studies.

Reference	**Security aspect**	**Attacks**	**Countermeasures**
[73]	A	DDoS against three vulnerabilities in the standard.	In network detection sensors
[74]	A	DDoS against vulnerability in the trace service.	N/A
[27]	A	Meter reading attack, service switch attack,	Formal framework to detect security violations

Table 3. Summary of studies on ANSIC12.22 security

CHAPTER 4. VULNERABILITIES OF ADVANCED METERING INFRASTRUCTURE

The Advanced Metering Infrastructure (AMI) is a core component of the smart grid which facilitates the two-way communications between the utility and the smart meters for metering, monitoring, and control purposes. Because of the fundamental importance of AMI, its security risks have attracted significant attention in the literature [68][75][76][77][78]. However, despite these studies, the security weaknesses and threats of the AMI have not been fully understood yet. To contribute with the understanding of the AMI security, in this chapter, we present a comprehensive security analysis on the vulnerabilities in AMI for service availability. In particular, we apply a use-case-centric approach to investigate the service availability issues. This new approach can improve the understanding of the vulnerabilities associated with specific use cases, which provides a better classification of attacks and facilitates the design of countermeasures. Based on such an approach, we systematically evaluate existing AMI attacks and identify potential new attacks. Therefore, the security analysis presented in this chapter is important to improve the existing knowledge regarding the risk that AMI faces, which is crucial from a security risk management perspective.

The organization of this chapter is as follows. First, we present the AMI attack interface. Second, we discuss potential attacker motivations. Third, we present a use case centric approach for AMI security assessment. This approach is used to conduct the analysis of the security weakness of each one of the AMI use cases. Additionally, as part of the aforementioned approach, we present a survey of existing AMI attacks, as well as new potential attacks that we discovered. Finally, we introduce a taxonomy of AMI attacks.

4.1 Attack interface

There are different points in the AMI infrastructure that can be used to start an attack. In this section, we discuss the more relevant ones[15].

WAN: Depending on the WAN technology in use for a utility, an attacker will have different attack vectors. In the case that a DSL technology is in place, the attacker can perform a network scanning in the entire utility network segment with the goal of identifying collector´s well-known open ports. Then the attacker can try to penetrate and change the DNS configuration on the collector to accomplish a DoS or MITM attack over the Internet. If the utility uses a cellular based technology for wide area communication, the attacker can setup a rouge base station near a collector to force it to connect to the WAN using the fake base station, thus, the attacker will be able to intercept the collector's traffic, and violate its confidentiality.

Utility local network: An attacker can penetrate the internal utility LAN using a conventional attack. Once inside the LAN the attacker could try to infect other machines until reaching the utility server which runs the Meter Data Management System (MDMS) to steal or manipulate customer's metering data. Additionally, from inside the LAN the attacker may try to target the internal network to obstruct the communication between the utility and the smart meters, making it very difficult for the utility to control and monitor the system. Furthermore, a utility insider can also use the utility local network to attack the AMI.

Utility server: Using techniques like social engineering, an attacker can penetrate the utility management server, in order to steal sensitive information such as customer's energy consumption data, system configuration and architecture, installing backdoors in the system, etc.

Service provider: An attacker could gather information regarding third-companies such as an Internet Service Provider (ISP), retail energy provider, and account management provider which receive information from the AMI system. Then, the attacker may try to penetrate these providers to attack the utility network from these third-party companies, taking advantages of possible trust relationship between systems.

Collector: Using techniques like jamming, an attacker can provoke a DoS attack against a collector. Also the physical access or front optical port could give the attacker the possibility to tamper or install malicious firmware/software in the device, allowing him to launch many types of attacks (i.e. DoS against smart meters, dropping of utility packets, spreading malware to other collectors, etc.). It is important to note that the collector is the most critical point in the AMI system, because it is the only bridge between the utility management software and the smart meters.

Smart meter: The same attacks that are possible against collector are likely to happen again the smart meter with a smaller impact. Additionally, the communication between these devices and the home appliances is another attack vector.

NAN: Attackers can try to eavesdrop the traffic between smart meters and between the smart meters and the collector. The goal in this scenario could be the gathering of cryptographic keys when they are being changed remotely in the rekeying process, as well as customer's information.

HAN: Attackers can try to eavesdrop the communication between the smart meter and the in-home appliance with malicious purposes.

4.2 Attacker's motivations

Attacks against the smart grid and the AMI can be motivated for different reasons, in this section, we discuss the most relevant ones[6][15][55][79][23]:

Causing disorder or chaos: Terrorist groups, hostile governments and criminal organizations may try to force the government to satisfy their demands by causing blackouts by attacking the AMI system, as a medium of pressure. Also, the political sector may try to pursue the same goal for their interests.

Activism: Activist groups may want to manifest their differences with the utilities for environmental or health damages issues. Recently, some strikes took place due to customer inconformity with the RF radiation of smart meters[80][81][82].

Economical reasons: Economical criminals may be willing to get money extorting the utility; a cyber attacker may steal customer habits information for selling and marketing purposes; criminals may sell software to customers for committing energy fraud; a customer may be looking to reduce electricity bills; and utility employees may look for money by committing energy fraud or teaching how to do so to customers. Additionally, industrial competitors may pay cyber attackers to cause black outs in the competitors systems in order to harm them.

Emotionally driven individuals: A disgruntled employee or contractor can attack the AMI for revenge purposes. This same motivation may become the incentive for a customer to penetrate the system and inject fake energy consumption data so that a target victim has to pay a very high electricity bill.

Recreational purposes: Hackers looking for acceptance or recognition may attack the system to show off their abilities and techniques. Additionally, customers interested in neighbors activities or looking for learning about the system can cause harm.

No motivation: Careless or not well trained employees may make mistakes in configuring the system, making it vulnerable or unstable.

4.3 Use-Case-Centric Analysis for AMI security

In this section, we present a security analysis of AMI. First, we present important assumptions for our study. Second, we introduce the notation that will be followed to classify the AMI attacks. Finally, we conduct a security assessment of each one of the AMI use cases presented in section 2.2.3.2. For this security analysis we focus on two types of attacks, i.e., the denial-of-energy-service (DoES) attack and the denial-of-communications-service (DoCS) attack. It is important to note that because of the abstract nature of the AMI use cases, which represent high level requirements we conducted our security analysis by performing a detailed analysis of each use case and asking ourselves for each one the use cases the following question: how can this functionality be abused for malicious purposes? This is the rationale that real attackers use to identify potential attack vectors. Thus, by answering this question we adopted the position of an attacker which allowed us to discover relevant vulnerabilities in different AMI use cases.

4.3.1. Assumptions

In our discussion, we assume that the attacker can inject information in NAN even if cryptographic mechanisms are applied, which has been demonstrated in [18]. We assume that the attacker can control at least one smart meter, which has been demonstrated in [83]. We also assume that all the smart meters are deployed with the same symmetric cryptographic key in the AMI implementation. Therefore, when a smart meter is compromised, the utility must send a new key over the AMI networks.

To facility further discussions, we now briefly present two man-in-the-middle (MITM) attack scenarios. The first attack is based on the condition that the cellular network is adopted as the WAN technology. In such a case, an attacker can set-up a rogue base station (e.g., a femtocell station) near the collector so that the collector connects to the utility network via the rogue base station, as shown in Figure 4.

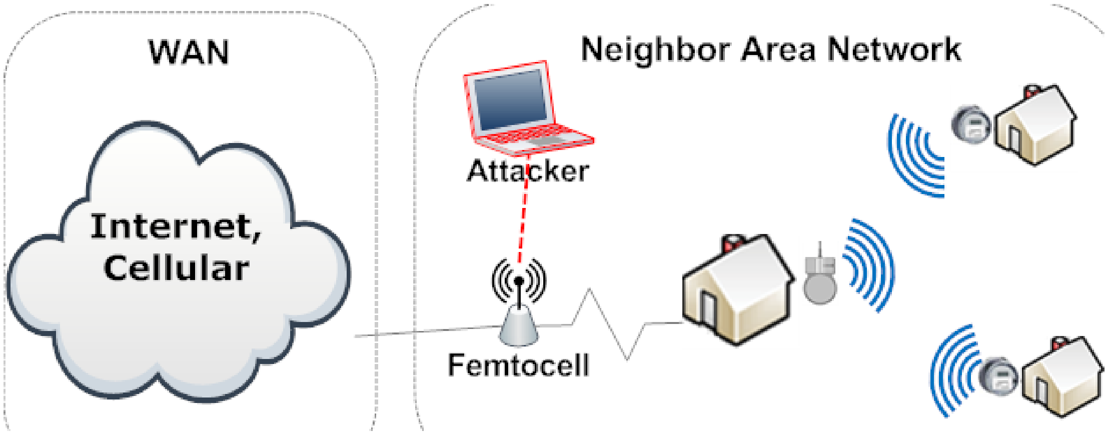

Figure 4. An example of the man-in-the-middle attack.

Another scenario is based on the condition that the Internet is used as the WAN technology. In this case, an attacker can first perform a network scanning in the entire utility network segment (or related segments based in previous information gathering) with the goal to identify predefined open ports in collectors. Then the attacker can try to compromise the collector and change the gateway configuration to point to a server under the control of the attacker. In the way, the messages towards the AMI Head End from the collector will be redirected to the attacker's server, which will forward the messages to AMI Head End. In the next step, the attacker can send an init message[65] to the utility and spoof the collector's ID, so the AMI Head End will send future messages to the attacker instead of the collector.

In either one of the above scenarios, the attacker is able to read and modify the traffic between the AMI Head End and the collector.

4.3.2. Notations

To facilitate further discussions, we define an attack by using the style of UCx.Ty. In this notation, UCx represents the use case; T represents the final target. T can take the values of either C or E, representing communications and energy, respectively. Finally y is an index.

In some scenarios, an attack can be based on another one. In such case, we use UCx.Ty[UCu.Tv] to specify that attack UCx.Ty is due to UCu.Tv.

4.3.3. Denial of Communication Service (DoCS) Attacks

In this subsection, we present existing and new discovered DoS attacks against the communication service, to differentiate this from the attack against the energy service, we use the terms Denial of Communication Service (DoCS) and Denial of Energy service (DoES), respectively.

4.3.3.1 Existing DoSC Attacks

UC0.C1 - Jamming attack: Since many NANs are based on wireless communications systems, they are vulnerable to jamming attacks. For instance, an attacker can easily transmit radio signals in the 2.4GHz frequency bands so that AMI devices using this frequency cannot communicate with each other[27].

UC0.C2 – Spoofed ID attack: In [65], the authors presented a group of possible communication attacks against the AMI. In one of these attacks, the attacker may identifies the ID of a collector, and then tries to associate with the utility by spoofing the collector’s ID just identified. As a result, messages from the utility Head End will be sent to the attacker instead of the collector, which may drop or tamper them.

UC0.C3 – Port attack: In the second attack presented in [65], the attacker can identify the listening ports of a smart meter, and then sends several messages to that port to overwhelm the smart meter.

UC0.C4 – Disconnect attack: In [65], the authors also identified that it is possible for an attacker to physically disconnect smart meters, as well as, disable them by using a remote control command.

UC0.C5 – Trace attack: In [73], the authors presented several attacks on ANSI C12.22 protocol. The first one is to use the trace service provided by C12.22. In particular, the attacker can send trace messages to a large number of smart meters, using the address of a victim node as the source for the trace requests. Consequently, the smart meters which receive the malicious messages will send responses to the victim. Then, due to the amount of responses received by the victim, its computational resources may be exhausted quickly. A similar attack has also been identified in [74].

UC0.C6 – Address resolution attack: The second attack identified in [73] is to exploit the address resolution service defined in C12.22. The idea of the attack is similar to UC0.C5.

UC0.C7 – URGENT message attack: Finally, the authors in [73] presented an attack in which one or more compromised smart meters can send messages with the URGENT flag activated, which is defined in C12.22. In this way, messages from other smart meters may be delayed.

4.3.3.2 Potential DoCS Attacks

UC9.C1 – Firmware upgrade attack: If an attacker can launch a MITM attack, it can further compromise the AMI system by initiating the firmware upgrade procedure in collectors or smart meters. In this case, the legitimate communications functions can be partially or completely disabled. For example, one smart meter may stop forwarding message for others in NAN, as shown in Figure 5.

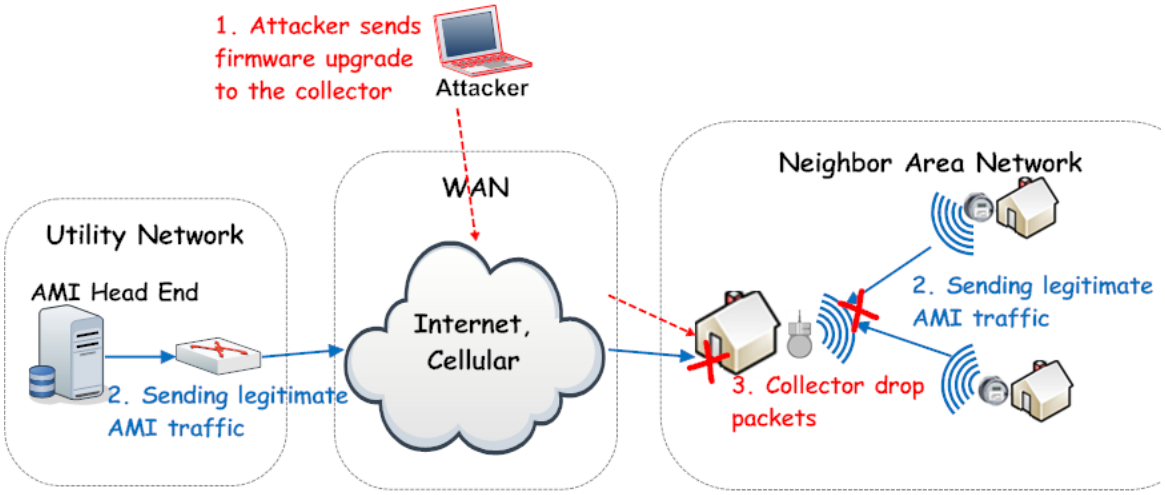
1. Attacker sends firmware upgrade to the collector
Attacker
Utility Network
AMI Head End
2. Sending legitimate AMI traffic
WAN
Internet, Cellular
Neighbor Area Network
2. Sending legitimate AMI traffic
3. Collector drop packets

Figure 5. The firmware/program upgrade attack.

UC10.C1 – Program update attack: Similar to UC9.C1, the attacker can also upgrade programs running in smart meter, which can affect the availability of communications services.

UC11.C1 – Metering keying/rekeying attack: In AMI system, the AMI Head End will initiate a rekeying procedure if one or more smart meters are compromised. The process can be affected if one or more nodes in NAN drop the rekeying messages.

UC7.C1 – Outage detection attack: Similar to UC11.C1, compromised smart meters or collectors can drop the outage detection message, which may prevent the AMI Head End to start the outage recovery process.

4.3.4. Denial of Energy Service (DoES) Attacks

In this section we present existing and new attacks against the availability of the energy service.

4.3.4.1 DoES Existing attacks

UC6.E1 and UC10.E1 – Switch-off attack: These attacks were discussed in [5], in which the main idea is to cut off a customer' energy supply either by sending RCD commands (UC6.E1) or by sending malicious program updates (UC10.E1) to make smart meters crash. In [40], the authors proposed to further exploit the switch-off attack such that voltage in a region can be out of the acceptable range, causing a cascaded problem with unforeseen consequences.

UC6.E2 – Power-off by malware attack: In [83], the authors proposed a possible attack by spreading a self-propagating malware in smart meters. In particular, by creating an in-flash root kit, the authors were able to have full control over all exposed smart meter capabilities, including remote power on, power off, usage reporting, and communication configurations.

4.3.4.2 Potential DoES Attacks

UC1.E1 – Meter reading attack: In this attack, an attacker can modify the meter reading data after it has launched the MITM attack. Specifically, the attacker can send fake messages to the AMI Head End that indicate significantly reduced energy consumption. In response to the small demand, the DRACS may decrease the power generation, which may cause massive power outage in certain regions. An example of this attack is shown in Figure 6.

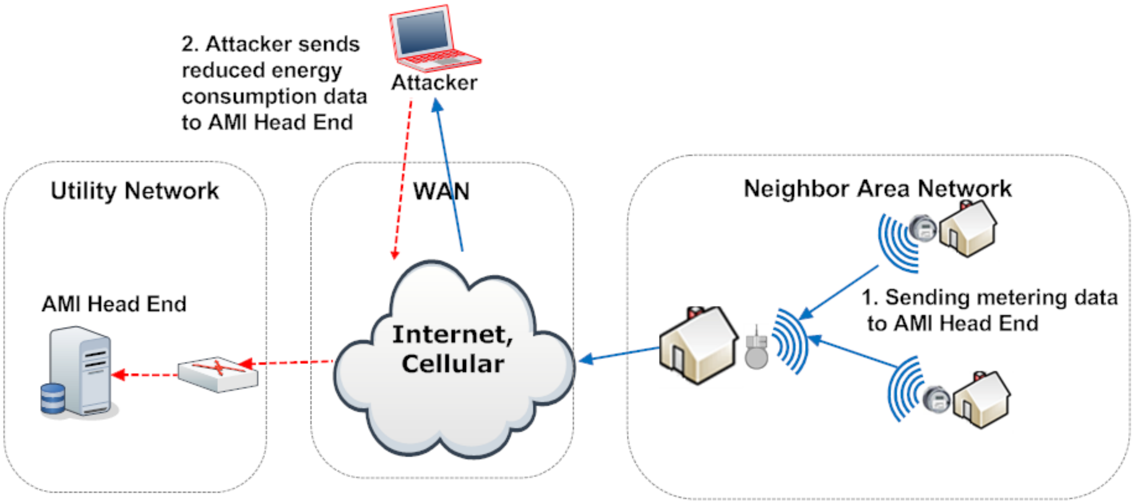
2. Attacker sends reduced energy consumption data to AMI Head End
Attacker
Utility Network
WAN
Neighbor Area Network
AMI Head End
Internet, Cellular
1. Sending metering data to AMI Head End

Figure 6. The meter reading attack.

UC2.E1 – Time-of-Usage (TOU) attack: In this attack, we consider that the attacker can send faked TOU pricing messages to smart meters. As illustrated in Figure 7, if the smart meters receive a lowered price, the customers may decide to increase the power consumption, which can cause power outage in certain regions.

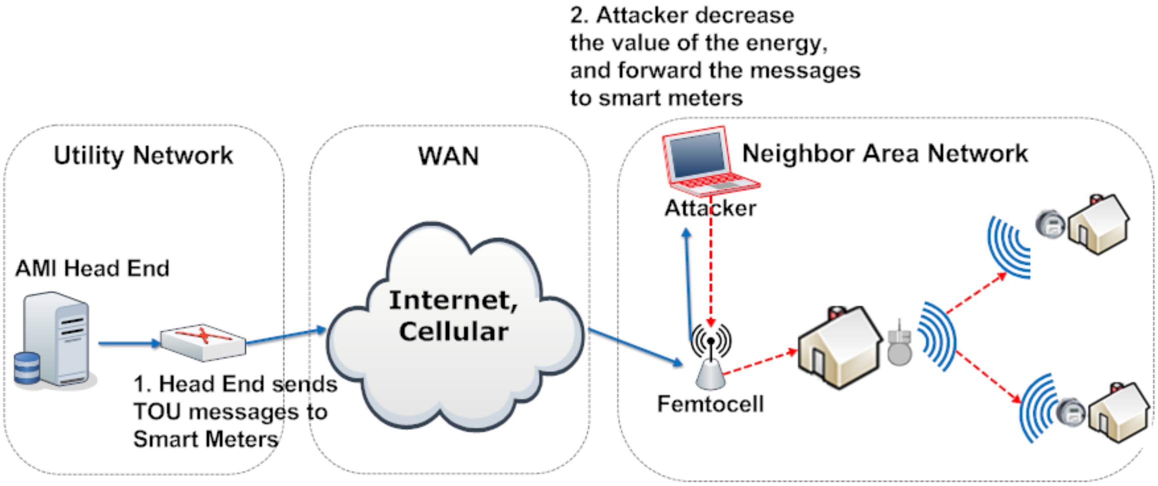
2. Attacker decrease the value of the energy, and forward the messages to smart meters
Utility Network
WAN
Neighbor Area Network
Attacker
AMI Head End
Internet, Cellular
1. Head End sends TOU messages to Smart Meters
Femtocell

Figure 7. The TOU attack.

UC12.E1 [UC1.E1] and UC12.E1 [UC2.E1] – Emergency Control attack: As mentioned previously, some customers may choose to suspend their energy supply in case of emergency. If an attacker successfully launched either UC1.E1 or UC2.E1, the AMI Head End will send RCD to the smart meters of these customers, which will disconnect the power supply.

UC6.E3 [UC12.E1] – Remote Connect attack: After UC12.E1, the AMI Head End may eventually mitigate the outage after a certain amount of time. In this case, it will send remote connect command to affected smart meters. In this situation, the attacker can drop the remote connect message to force the group of customers to continue the disconnection of their power supply.

UC3.E1 [UC1.E2] and UC3.E1 [UC2.E2] – Prepayment attack: In this attack, an attacker can send faked metering data (UC1.E1) such that the AMI Head End will overestimate the energy consumption of a customer, or can send faked pricing message (UC2.E2) so that the smart meter will calculate the cost of energy using a higher rate. In both cases, a customer may be denied further energy supply due to insufficient balance.

4.4 Chapter conclusions

In this chapter, we have presented an analysis of the AMI security with the aim to contribute to the understanding of the risks that AMI faces. Given that AMI is a key component for smart grid, it is crucial to protect the availability, specially the communication and energy services availability. To improve the understanding of service availability in an AMI system, in this chapter, we have systematically analyzed the vulnerabilities of AMI use cases. Specifically, we proposed to apply a use-case-centric approach for the security analysis, which has not been used in the literature. Through extensive discussions, we demonstrated that the proposed approach can help to classify existing attacks and identify new potential attacks.

CHAPTER 5. DENIAL-OF-SERVICES ISSUES ON ANSI C12.22

In last decades, the collection of metering data was a challenge for utilities because this activity was performed manually by crews in customer facilities. To improve the efficiency and reduce the cost of this process, industry patterns created the ANSIC12.18 and ANSIC12.21 protocols to carry metering date over optical port and telephone lines respectively. While these new standards facilitate the collection of large amount of meter data and the configuration of vast number of meter devices, they only provide a one way communication from meters to utilities[26]. This limited communication was not able to support the new demands in the metering area, such as demand response and load control. Then, the protocol ANSIC12.22 was created as a solution for the aforementioned limitations and requirements. This protocol is able to transport metering data over reliable networks and provides a two-way communication between meters and utilities, which make it a competing option to support the AMI. However, despite the high adoption of this protocol, there is a lack of understanding of its inherent security issues. In this chapter we present a study of the ANSIC12.22 protocol. We also focus on the analysis of the security of each one of the services, which support the protocol operation. As a result of this analysis, we found potential vulnerabilities and evaluate their impact using the CVSS and simulation. Additionally, we propose countermeasures to facilitate the mitigation of the identified security issues.

The rest of this chapter is organized as follows: section 5.1 presents the description of the system model. Section 5.2 introduces the discovered security issues in the ANSIC12.22 protocol. Section 5.3 presents the computation of the vulnerabilities' severity. Section 5.4 presents a validation of the impact of the discovered vulnerabilities using simulation. In section 5.5 we discuss the proposed countermeasures. Finally, section 5.6 presents the chapter conclusions.

5.1 System model

In this section we consider an ANSIC12.22 network segment which is equivalent to the NAN of the AMI infrastructure discussed in section 2.2.1. However, some AMI components may play the role of many ANSIC12.22 elements at the same time. For our study we consider the following correspondence between AMI and ANSIC12.22 components. First, the collector unit in the AMI should have modules for supporting master relay, gateway and authentication host functionalities. Second, we assume that each smart meter act as relay and terminal nodes and some of them may have notification host capabilities.

5.2 Security analysis of ANSIC12.22

In this section we present our findings regarding the security issues of the ANSIC12.22 protocol. We approach the analysis of the ANSIC12.22 security in the study of the security of each one of its services, and then we will present the discussion in terms of service security issues. We conducted this study based on the following assumptions. First we assume that the neighbors that are part of the AMI use RF communications instead of power line or any other. We also assume that the network segments have broadcast capabilities and then the number of node discovered when using a resolve service request may be high. Additionally, we also assumed the compromise of at least one smart meter as well as the possibility of obtaining cryptographic keys from it. Finally we assume that the C12.22 network uses a lower layer communication method in preference of the application layer routing functionality as described in the standard, then the network needs to translate ApTitle to lower layer addresses each time a message is transmitted.

In addition to the above mentioned assumptions, it is important to highlight that we designed a specification-based approach to identify vulnerabilities in ANSIC12.22, which consist in the following: based in the ANSIC122.22 specification, we gathered the description of each one of the services provided by this standard. Next, for each one of the services we created diagrams of their message exchange sequence. Then, we investigated each sequence to identify implicit assumptions; after that we introduced conditions that may invalidate the identified assumption and finally we validated whether the break of that assumption represents a security issue. To illustrate the above mentioned approach consider a scenario with two nodes A and B represented in Figure 8.

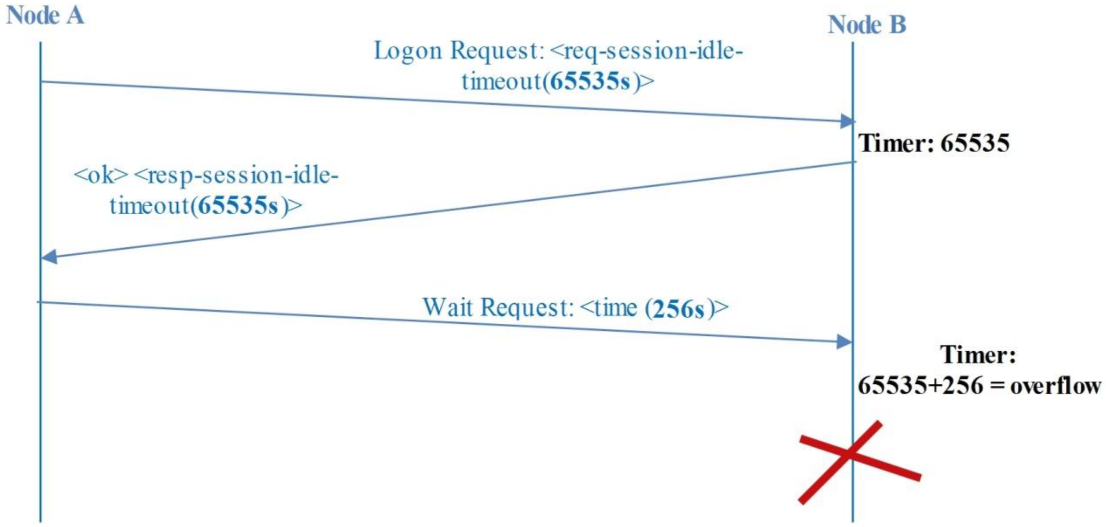
Node A
Node B
Logon Request: <req-session-idle-timeout(65535s)>
Timer: 65535
<ok> <resp-session-idle-timeout(65535s)>
Wait Request: <time (256s)>
Timer:
65535+256 = overflow

Figure 8. Wait Service Attack.

In first place A sends a logon request to B setting the req-session-idle-timeout value to 65535, which means that A is willing to establish a session with B that can be in the idle state for 65535 seconds. Then, after receiving that message B replay with an OK message, containing the time a session may be in the idle state. Now, considering the message exchange sequence of the wait service, it is possible to realize that a node may ask for an extension of a session in the idle state. Thus, the amount of time which is requested in the wait service petition will be added to the current value of the session timer. Consequently, after conducting a detailed analysis of this behavior and knowing the maximum value that can be allocated into the timer variable (65535 according to the specification), it is possible to identify an implicit assumption in the service specification, which consist in assuming that a node will not issue wait service request at least that it has a session that it is about to finish for being too long in the idle state and have to be extended. At this point, following our specification-based approach, we should consider a situation when that assumption may be invalidated. In this case, such a situation occurs when a node ask for a session's extension when the session is not about to finish but it has the idle session timer in its maximum value (65535 seconds); consequently if node A asks for a session extension by issuing a wait request and a extension value T, the value T has to be add to the current idle session timer which is in its maximum value, therefore the extension operation will cause a overflow in the timer variable. Then, following our approach, we have to determinate whether the introduced condition represents a security issue or not. Thus, because the consequence of the introduced condition is the overflow of the timer variable, and the fact that buffer overflow situations frequently provoke denial of service, we can determinate that indeed the condition that we introduce occasioned a security issue in the wait service. Thus, after applying our specification-based approach in this illustrative scenario we identified a new vulnerability in the ANSIC12.22 protocol. Finally, we applied the described approach for each one of the services detailed in the specification and we were able to identify 21 vulnerabilities which are described in the next section.

5.2.1 Identification service security

Identification manipulation vulnerability

Assumption: an identification response will only be received as a result of an identification request.

Potential vulnerability: when receiving unsolicited identification responses, a node may overwrite existing legitimate information related to other node in the network.

Potential attack: An attacker may send an unsolicited identification response message to a victim node spoofing the identity of a relay. As a result, the victim node overwrites previous known information about that relay. Then, depending on the information provided by the attacker in the identification message, different scenarios may happen. First, if the attacker changes the supported standard field, the victim node will not be able to communicate with the relay because of protocol incompatibility issues. Second, if the attacker sets the security mechanism to be clear text without authentication, then the victim may be forced to sends messages without the security protections to the network. In case that other policy is being used, the victim may reject to communicate with the relay because of the lack of security guarantees. Thus, in the first case, the privacy and integrity of the message is at risk, while in the second case, the victim node suffers a DoS.

5.2.2 Read service security

Excessive data size vulnerability

Assumption: The size of the data contained in a read response message is manageable.

Potential vulnerability: When a node receives a message whose size after reassembling is bigger than its memory capacity, a buffer overflow conditions may occur.

Potential attack: an attacker may send data with an excessive large size a as part of a read response message to cause DoS against a victim node.

Incomplete data vulnerability

Assumption: the data received as part of a read response message will be a finite chain of segments.

Potential vulnerability: when a segment of data arrives to a node as part of a reading response, it will open a thread to wait for the arrival of the rest of the data. Then, in the case that the remaining data never arrives, the thread may be open for an indeterminate time consuming computational resources in the victim's node.

Potential attack: an attacker may send many unsolicited read responses to a victim node, then the attacker may set the count field value to 65535 to indicate that the data is incomplete. As a result, the victim node will open a thread for every connection established by the attacker under these same circumstances. Consequently, this pool of threads will quickly consume the victim's resources for a non specified amount of time, causing a DoS condition.

Unbound index vulnerability

Assumption: the index plus element-count value will not exceed the size of a table.

Potential vulnerability: when the index of the elements intended to be retrieved plus the element-count amount is bigger than the table size, retrieving of data in adjacent tables may happen.

Potential attack: an attacker may try to read privileged data in a victim's node by setting the index and element-count fields big enough to go out of a table boundary and get unauthorized access to reserved information. The attacker may try to read the table zero at the index zero plus an arbitrary big element-count to retrieve the information stored in all the victim's tables. This information may include: security keys, passwords, configuration parameters, etc. Additionally, a negative element-count or index may cause a similar result.

5.2.3 Write service security

Information overwriting vulnerability

Assumptions 1 and 3 of the read services also apply for the write service. Therefore, similar vulnerabilities and attacks may occur. However, given the nature of the write service, assumption number 3 has a bigger impact which is beyond the information leak in the read service. For instance, writing information in an unauthorized table of a victim node may cause the overwriting of the data which was previously located in that table. Because of this, many attack scenarios may occur. First, if the overwritten data are configuration parameters, the victim will not be operable because of arbitrary configuration changes. Second, if the data is related to stored passwords or cipher keys, the overwriting of them may cause the rejection of the victim's traffic because of incorrect cryptography values. Third, if the data correspond to energy pricing, the node may underreport the energy consumption if the new price is lower than the legitimate one, or may shutdown itself in the case that the price is too high. Fourth, routing information data may also be corrupted causing communication interruptions. Finally, if the victim is a collector or a master relay, the impact of the attack increases considerably because the network segment may lose its capacity to send or receive traffic from external networks, including the utility network.

5.2.4 Logon service security

Timeless session vulnerability

Assumption: The duration of a session is limited.

Potential vulnerability: when establishing a session using the logon service, the node which started the petition may request the desired duration time of the session using the req-session-idle-timeout field; if this field is set to zero, the session will be open without any time limit. This situation may cause sessions to be open indefinitely, which may exhaust a node's resources.

Potential attack: an attacker may establish multiple sessions in a victim's node with the req-session-idle-timeout field set to zero. This will exhaust the victim's resources due to the computational cost of keeping sessions open. Additionally, if the victim node is a collector or master relay, its collapse may interrupt the communications of the network segment.

Log overflow vulnerability

Assumption: there will be enough space to store event and history logs.

Potential vulnerability: each time a node receives a logon request, the user-id information of the request may be saved in the event and history logs. However, if the logged information grows beyond the node storage capacity, an overflow condition may occur.

Potential attack: an attacker may send several logon requests to multiple targets in a network segment to overflow their event and history log, causing DoS against the victim nodes. This attack may have a bigger impact if the affected nodes are relays, collectors or master relays.

5.2.5 Security service security

Authorization vulnerability

Assumption: A node will only access the information which is authorized to its own user-id.

Potential vulnerability: when access permissions over a particular table are granted to a user-id, the spoofing of that user-id may cause unauthorized access to information.

Potential attack: through eavesdropping on the channel, an attacker can detect when a node starts a security service request. Then the attacker may spoof the user-id information contained in the request, to access the information that is only accessible to the victim node. Additionally, the attacker may collect the passwords transmitted in the service request for future unauthorized accesses.

5.2.6 Logon service security

Session termination vulnerability

Assumption: the logoff request may only be sent by a node participating in a session.

Potential vulnerability: when a node receives a logoff request with appropriate session sequence, the node will terminate the session without validating the origin of the request.

Potential attack: an attacker may eavesdrop the communication channel to detect open sessions, then the attacker may issue logoff request targeting each one of the discovered sessions in order to interrupt ongoing communication. This attack requires the prediction of session sequence numbers (known as calling AP invocation id) which are generating by monotonically incrementing a initial chosen number. It is important to note that the impact of this attack can be maximized if the attacker targets sessions in which a collector is involved because it will interrupt the communication of a network segment and any external network.

Session expiration vulnerability

Assumption: the logoff response is only sent by a node participating in a session.

Potential vulnerability: when a node receives an unsolicited logoff response with the error code isss (invalid session state sequence), the receptor node will not be able to issue logoff request because that is not allowed when receiving an isss response code. Then, the session may be open until reaching the timeout.

Potential attack: an attacker may send an unsolicited logoff response with the error code isss to force a particular session to last until the timeout. If the attacker issues logoff responses to every ongoing session, there will be a waste of resources in the network given the cost of keeping sessions open. As a result, the network performance will decrease and some nodes may exhaust all their computational resources.

5.2.7 Termination service security

The security analysis of this service is equivalent to the logoff service because they share a very similar functionality.

5.2.8 Disconnect service security

Illegitimate disconnection vulnerability

Assumption: this service is used only for legitimate purposes.

Potential vulnerability: when a node receives an illegitimate disconnection request, it will abort all its ongoing sessions and will enter into the offline state. In such state, the node is not longer able to communicate with the network.

Potential attack: an attacker may send disconnect request messages to several nodes to prevent them to communicate in the network. The impact of this attack may increase if the number of victims is high or the target is a master relay, collector or relay.

5.2.9 Wait service security

Extended session vulnerability

Assumption: there will be only one wait request per session idle period.

Potential vulnerability: receiving multiple wait service requests for the same session will force the adding of time units to the session timeout counter, which may cause an overflow if the mentioned variable goes out of its maximum value.

Potential attack: an attacker may sends wait request to extent a session to its maximum possible value (4.2 minutes approximately); if the attacker sends multiple requests, the victim's node will add the requested times. Then, after adding too many time values, the variable keeping track of the total requested time may be overflowed, which may cause DoS in the victim's node. Additionally, a high rate of requests may exhaust the network or processing resources of the victim node. Also, keeping sessions open for long periods may exhaust victim's resources.

5.2.10 Registration service security

ApTitle reutilization vulnerability

Assumption: an ApTitle is only registered for a node

Potential vulnerability: when a master relay registers the same ApTitle to different nodes, inconsistency in route entries may occurs.

Potential attack: an attacker may issue a registration request setting the native address field to be its own native address, and the ApTitle field to be the ApTitle of a victim node. As a result, the master relay will create an association between the attacker's native address and the victim's ApTitle. This will cause that all traffic destined to the ApTitle of the victim's node will be rerouted to the native address of the attacker. Then, the victim will not be able to receive any messages from the network. This situation constitutes a DoS attack.

ApTitle assignment vulnerability

Assumptions: authoritative proxy relays only assign unused ApTitles

Potential vulnerability: when ApTitles in use are assigned to a node, network inconsistencies may occur.

Potential attack: an attacker may register in the network as an authoritative proxy relay by activating the RELAY flag in the node-type field of the registration request. Then, when a node issues a registration request asking for an ApTitle, the attacker may assign an ApTitles which is being used for other node to create routing errors. In such a situation, at most one of the nodes sharing the same ApTitle will have access to the network, but for the rest of victims it will be a DoS attack.

Subscription vulnerability

Assumption: the number of nodes subscribed for receiving notification will be small.

Potential vulnerability: when the number of notification subscriber is high, the master relay notification mechanism may flood the network segment with notification messages.

Potential attack: an attacker may spoof the address of each node in a network segment, then the attacker may sends subscription request to the master relay using each one of the spoofed addresses. Consequently, when a registration request occurs, this causes the master relay to send notifications to every node in the network segment. In this scenario, the attacker may sends several fake registration request using fake addresses, which will cause the master relay to flood the network segment by sending a notification to every node in the segment for each one of the messages sent by the attacker. Then DoS may happen.

Registration period vulnerability

Assumption: only the master relay or delegated relays may send registration responses.

Potential vulnerability: when a small registration period is granted to a node, it may reissue a registration request, which will consume resources in the network and in the master relay.

Potential attack: an attacker may send unsolicited registration response directed to a group of victim nodes spoofing the master relay address. In these messages, the attacker may set the registration period to a very small value, causing that every victim node reissues a registration request when that period finishes. Then, due to all periods finishing almost at the same time, the master relay will receive many simultaneous registration requests which may exhaust its computational resources, which constitutes a DoS attack.

Routing table overflow vulnerability

Assumption: the number of nodes in a network segment will be smaller than the maximum possible size of the routing tables.

Potential vulnerability: when several nodes are registered in the network the routing table may overflow.

Potential attack: an attacker may register fake ApTitles in a network segment, then each registration adds an entry to the routing tables of the network relays. Once that routing tables reach their maximum size, overflow conditions may occurs. In such a situation, the relay may adopt one of the following behaviors. First, not to implement any mechanism to handle overflow, this may cause the crash of the node. Second, the node may overwrite old entries. In this case, if the number of fake nodes is high enough, all the legitimate entries will be overwritten. Third, the node may discard any new entry after full its routing table, in this case, registration of new legitimate nodes will not be possible. It is important to note that in all these scenarios the DoS attack is successful.

5.2.11 Deregistration service security

Illegitimated deregistration vulnerability

Assumption: only legitimate nodes will serve deregistration requests.

Potential vulnerability: when an illegitimate deregistration service request is issued, the ApTitle which is set in the request message may be removed from the routing tables of the relays.

Potential attack: an attacker may use this service to deregister nodes from the network. Thus, the attacker may have the possibility to deregister multiple nodes simultaneously or to target crucial nodes such as relays or collectors to increase the impact of the attack. Additionally, the re-registration request that the victim nodes may issue after being removed from the network may exhaust resources in the network or in the master relay.

5.2.12 Resolve service security

Unbound resolution vulnerability

Assumption: the number of relays responding to resolve request is small.

Potential vulnerability: when many relays respond to a resolve request, the node which originated the petition may exhaust its resources trying to process all the incoming data.

Potential attack: an attack for this vulnerability was discussed in [73]. The attack consists in spoofing a victim address in a resolve request, and then the victim resource is exhausted because of the multiple responses. This is clearly a DoS situation.

5.2.13 Trace service security

Unbound trace vulnerability

Assumption: the size of the trace service response is manageable.

Potential vulnerability: when receiving trace responses bigger than the memory capacity of a node, overflow may occur.

Potential attack: an attacker may spoof a victim address and start a trace service request. Then, if the number of nodes forwarding the message is big enough, the trace response will cause a DoS condition on the victim node upon receiving it. This situation was discussed in [73].

Inaccurate topology vulnerability

Assumption: only accurate information will be provided in the trace response message.

Potential vulnerability: when inaccurate information is provided regarding the relays between a source and a destination, diagnosis activities may be obscure.

Potential attack: an attacker may register as a relay in the network and provide fake responses to trace service requests. This will cause the reception of wrong topology information in the victim node.

5.3.1 Attack scenarios

To further explain the identified security issues, in this subsection we illustrate some attack scenarios.

ApTitle reutilization attack

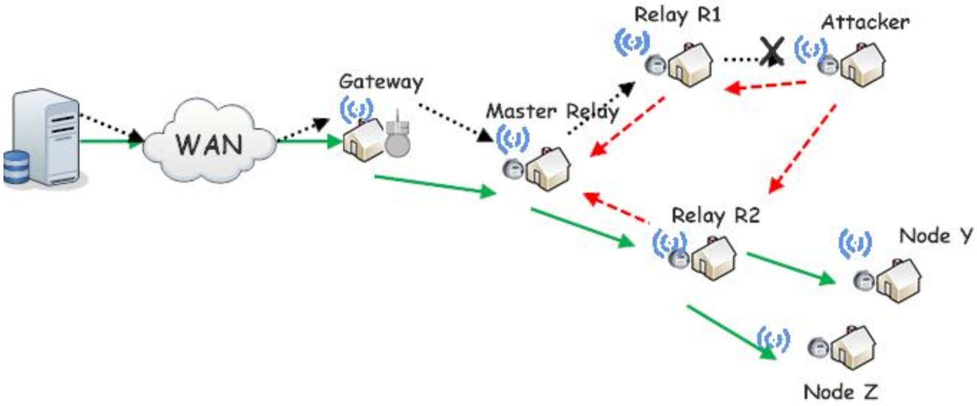

Figure 9. Isolation attack

This attack relies on a vulnerability of the registration service consisting in the lack of mechanisms to prevent that two or more nodes request a registration service with the same calling-ApTitle. Figure 9 illustrate this situation. In normal conditions, nodes Y and Z receive messages from the AMI Head End following the route represented by solid lines. At any time, an attacker can start monitoring the channel to detect neighbor nodes. In the considered scenario, the attacker will detect nodes Y and Z which will be his victims. Once the attacker collects the list of neighbor nodes, he starts sending registration service requests establishing the detected ApTitle in the field calling-ApTitle and his native address in the field native-local-address of the request message (dashed lines in Figure 9). These messages are directed to the master relay via normal relays. Once the master relay responds with an <ok> code, every relay that forwarded the request message (R1 and R2 in Figure 9) will update an entry in its routing table, establishing a mapping between the ApTitle of nodes Y and Z, and the native address of the attacker. At this point, every message from the AMI Head end to the nodes Y or Z will be directed to the attacker (dotted lines in Figure 9), who can drop the packets causing the isolation of nodes Y and Z.

It is important to realize that this attack can be combined with the resolve and trace services to expand the set of discovered nodes and cause DoS with a bigger impact. Finally it is also important to note that if the victim of the attack is a gateway, the impact of the attack grows significantly because every message sent from the AMI NAN to the AMI Head end will be directed to the attacker´s node instead of the legitimate gateway. Thus, the attacker may drop the out-going communication of the whole network under this particular gateway.

Timeless session attack

This attack relies on the timeless session vulnerability of the logon service, consisting in the possibility of establishing session without a time limit by setting the field <req-session-idle-timeout> to zero. To leverage this attack, the trace and resolve service are used.

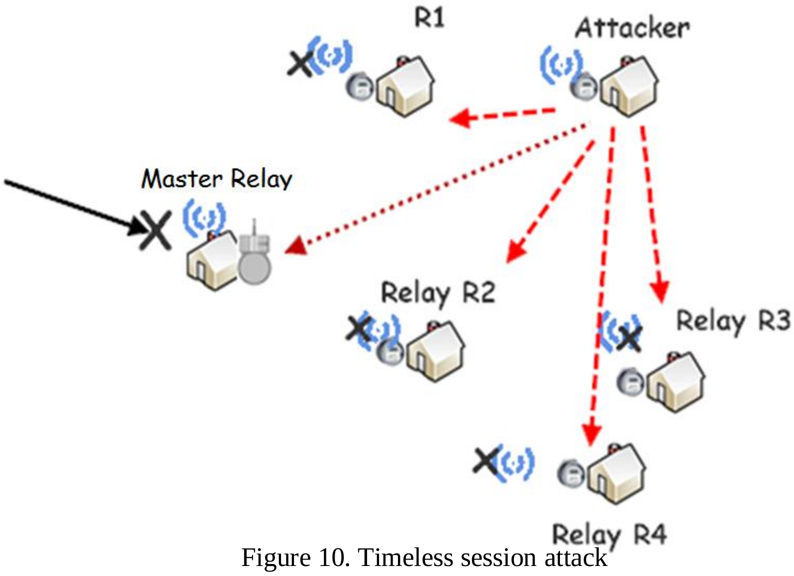

Figure 10. Timeless session attack

Figure 10 illustrates this attack. First the attacker sends resolve request service messages using two formats. In the former one, the attacker sets a preconfigured master relay ApTitle in the called-ApTitle field of the message; by doing this, it is possible to discover every relay with capabilities to forward messages to that specific master relay. In the second format, the attacker sets the called-ApTitle to zero, causing that every relay with auto-assigned master relay capabilities respond putting with their own ApTitle and native address in the response message. At this point, the attacker has collected a list of active relays in the network; to gather even more information about the network topology, the attacker could send trace service request to every discovered relay to find relays that did not respond his previous resolve request. Then, the attacker start sending logon service requests to each one of the discovered relays setting the <req-session-idle-timeout> field in zero and setting fake information in the field called-ApTitle in order to establish many session without time limit in the victim's nodes (dashed lines in Figure

10). The target of this attack is to cause a resource exhaustion (X symbol in Figure 10) due to the computational cost of keeping session alive (in terms of timers, buffer, etc); this attack will also cause a DoS in the network due to the inability of the relays to forward or segment messages and resolve addresses.

A variant of this attack can be launched consuming fewer resources in the attacker side. It consists in launching the timeless session attack against the network gateway (dotted lines in Figure 10). Once the gateway collapses as a result of the attack, all ongoing and future communications between the AMI head end and the smart meters will be dropped (solid line in Figure 10).

Illegitimate deregistration attack

Figure 11 illustrates this attack. In this scenario, an attacker starts sending deregistration service requests (dashed lines in Figure 11) to the master relay spoofing the ApTitle of a group of nodes. Once the master relay receives the malicious message, the spoofed nodes will be disconnected from the network segment. Eventually, these disconnected nodes will try to register again in the network by sending registration service request to the master relay (solid lines in Figure 11) in a concurrent fashion; this amount of traffic arriving at the master relay can cause it to collapse constituting a DDoS against it (X symbol in Figure 11). Furthermore, because of the collapse of the master relay, the network will lose the capacity to register the victim’s nodes, making it impossible to route message to them. It is important to note that the bigger the number of victim's nodes, more likely the attack will be successfully.

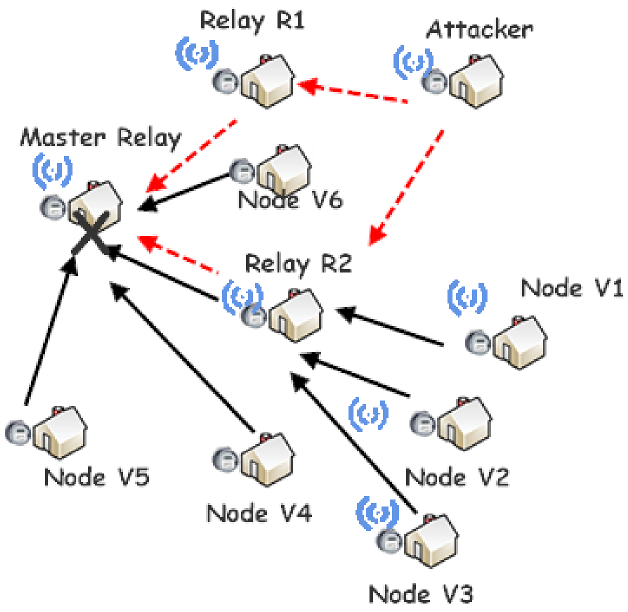

Figure 11. Disconnect attack

5.3 Vulnerabilities' severity measurement

The process of measuring the impact of software vulnerabilities has been approached through different methods by many different vendors. Thus, CVSS was created to address the lack of standardization in the process of scoring software vulnerabilities, providing standardized vulnerability scores, contextual scoring and an open framework [84]. The latter allows us to have access to the individual characteristics used to calculate a severity score. CVSS consists of three metric groups: base, temporal and environmental and is useful to calculate the severity of a particular vulnerability in a numeric scale (from 0 to 10). Additionally, CVSS is widely used for security bulletins, vulnerability management organizations, software application vendors and researchers to establish the severity of security weakness in a standardized way and categorize them accordingly.

In this section we present the application of the CVSS version 2 to the vulnerabilities presented in the previously. We consider that CVSS is appropriated for our research because it provides a set of metrics that enables evaluation, comparison and classification of the ANSIC12.22 vulnerabilities as a function of their severity. It is important to clarify that we will use only the base metrics of the CVSS because these are the only metrics that represent intrinsic and fundamental characteristics of the vulnerabilities, which are invariant regardless of the user environment and the time.

5.3.1 Impact score of ANSIC12.22 vulnerabilities

Table 4 shows the severity rating convention of the CVSS.

Severity	**Range**
Low	0.0 – 3.9
Medium	4.0 - 6.9
High	7.0 – 10.0

Table 4. Severity rating convention

Table 5 presents the impact score of each one of the discovered vulnerabilities. It is important to mention that we compute these scores by using the online calculator provided in the web site of the National Vulnerability Database (https://nvd.nist.gov/cvss.cfm?version=2). This calculator take parameters such as the access complexity, access vector, authentication and level of impact over the availability, integrity and confidentiality of each vulnerability; then based on that input the calculator computes the impact of the vulnerabilities applying the CVSS version 2 approach.

Vulnerability	**Score**	**Severity Rating**
Information overwriting vulnerability	7.1	High
Identification manipulation vulnerability	7	High
Excessive data size vulnerability	5.5	Medium
Incomplete data vulnerability	5.5	Medium
Unbound index vulnerability	5.5	Medium
Log overflow vulnerability	5.5	Medium
Registration period vulnerability	5.5	Medium
Routing table overflow vulnerability	5.5	Medium
Illegitimated deregistration vulnerability	5.5	Medium
Unbound resolution vulnerability	5.5	Medium
Unbound trace vulnerability	5.5	Medium
Illegitimate disconnection vulnerability	5.5	Medium
Subscription vulnerability	5.5	Medium
Timeless session vulnerability	5.2	Medium
Session expiration vulnerability	5.2	Medium
Extended session vulnerability	5.2	Medium
ApTitle reutilization vulnerability	4.1	Medium
ApTitle assignment vulnerability	3.8	Low
Inaccurate topology vulnerability	2.7	Low
Authorization vulnerability	2.3	Low
Session termination vulnerability	2.3	Low

Table 5. Impact score of ANSIC12.22 vulnerabilities

As a result of the application of the CVSS to the ANSIC12.22 vulnerabilities, we found that the 9.5% of them have a high severity, 71.4% have a medium severity, and the 19.04% have a low severity.

5.4 Simulation results

In this section we present a validation of the impact of the discovered vulnerabilities by conducting simulation.

5.4.1 Simulation description

For the simulation scenarios, we assume a master relay M1, a relay R1 and 100 meters sending periodic messages each 1 second (background traffic) to M1 through R1. Additionally, we consider a malicious node which lunch attacks against the network. Regarding to duration of the simulation, it ends when each one of the 100 meters have sent 10 messages to M1.

In relation with the computational environment, the simulations were executed in a machine with 8 cores of 2GHz each one, and 8 GB of RAM. Additionally, we developed a light weight version of the ANSIC12.22 protocol in Java. This prototype implements network services described in chapter 5 of ANSIC12.22 specification published by IEEE [38]. Consequently, we used a multithread approach to simulate nodes and TCP Java sockets to allow communication between them.

5.4.2 Simulation analysis

Illegitimate disconnect vulnerability

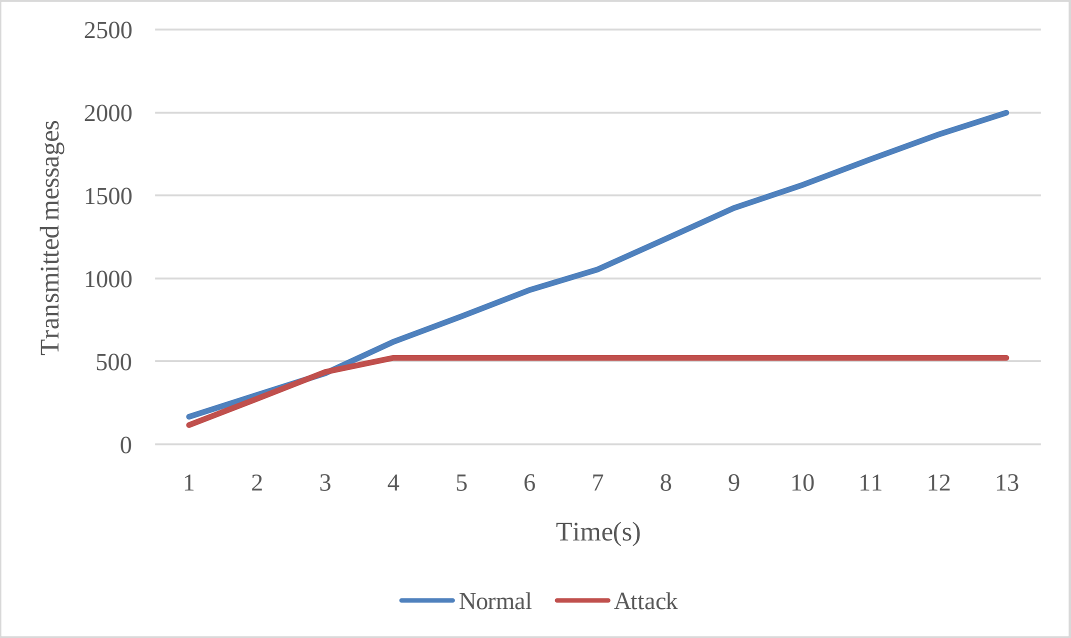

Figure 12. Illegitimate disconnect attack

Figure 12 shows the result of launching an illegitimate disconnect attack against a ANSIC12.22 network. At t=3s the attacker sends a disconnect request message to R1, as we explained before, the receiver of such a message will close all its sessions and go to a offline state, where it cannot receive or send data. Once R1 receives the message, it starts the procedure to disconnect from the network between t=3s and t=4s. Then, at t=4s, R1 has stopped all its communication with the network, as a result R1 is not able to forward more messages from the meters to M1. In figure 12, this can be appreciated by a sudden stop in the increment of the red line. It can be appreciate in the figure that at t=4s the aggregated number of transmitted messages remains constant at a value near 500 messages, which is the total number of messages transmitted before the attack. Consequently, at the end of the simulation, the total number of messages transmitted in this scenario is 538. However, in the normal scenario the total is 2000. Then, by sending only a message to R1, the attacker was able to reduce the entire network traffic in a 73.1%.

Excessive data vulnerability

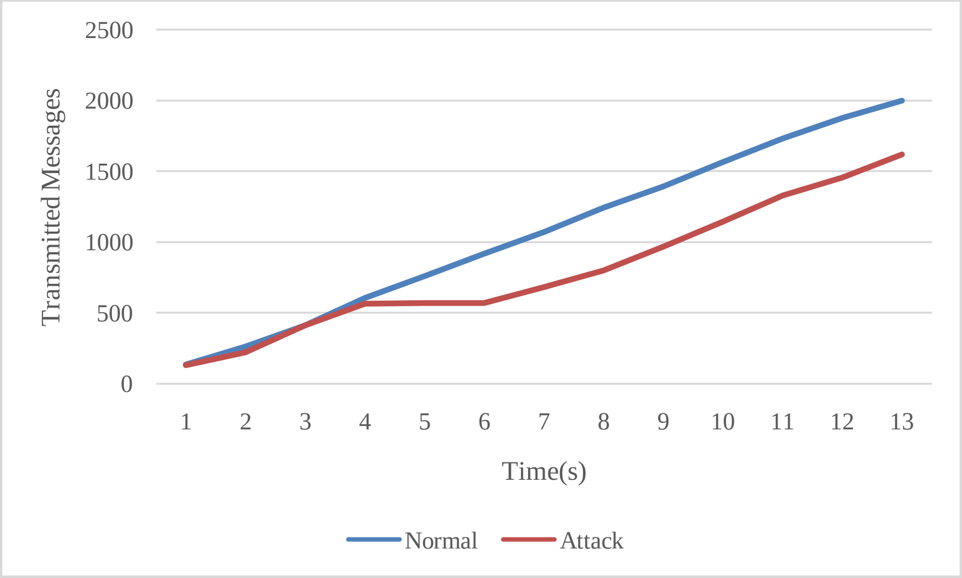

Figure 13. Excessive data attack

To abuse the excessive data vulnerability, we considered the transmission of a malicious message whose size exceeds the memory capacity of the victim´s node (R1). Then, given that the memory capacity of R1 is 144kb, we choose a 167458bytes (167.4kb) message to evaluate this vulnerability.

This simulation starts with the normal background traffic as described in the beginning of this section (read line between t=1s and t=3s). Thus, at t=3s the attacker sends a malicious message of 167.4kKb to R1, which receives it between t=3s and t=4s. Then, because the message size exceeds the memory of R1; it goes to a blocked state until some memory is released. Meanwhile, R1 is not able to process any incoming message. Next, at t=6s, R1 frees the memory and start processing messages. However, because of the attack, the number of transmitted packets do not increment between t=4s and t=6s (horizontal red line between t=4s and t=6s in figure 13). After t=6s R1 transmits messages at a normal rate. Finally, at the end of the simulation, the number of transmitted messages is 1608 which is a 19.6% less in comparison with the 2000 messages transmitted in the normal scenario.

Illegitimate deregistration vulnerability

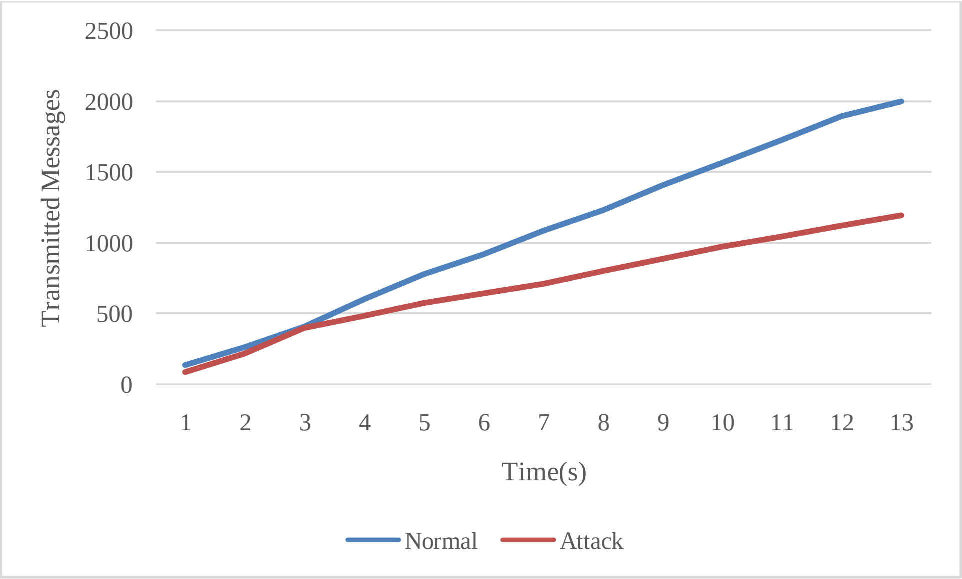

Figure 14. Illegitimate deregistration attack

To validate this vulnerability, we considered the transmission of a deregistration message from an attacker node to the master relay. This message contains the ApTitle of R1 as the source ApTitle, that is to say, the attacker sends the message to the master relay M1 spoofing the address of R1. Thus, once the master relay receives the malicious message, it will deregister the ApTitle of R1. Then, any subsequent message from the R1 to the master relay will be discarded.

The simulation starts with the normal background traffic as described in the beginning of this section (read line between t=1s and t=3s). Then, at t=3s the attacker sends a malicious deregistration request message to M1 spoofing the ApTitle of R1. Once upon receiving the message, M1 removes R1 from its registration table, and sends a response code back. As a result, any future message from R1 to M1 will be discarded by the last one. However, this situation does not stop the entire network traffic, because the meters continue sending messages to M1 using R1 as a proxy. But, because M1 discards all packets from R1, the meters never receive responses for their request. Thus, only half of the traffic is being transmitted through R1, which justifies the reduction of the slope of the red line between t=3s and t=4s in figure 14. Finally, at the end of the simulation, the total number of transmitted messages is 1200 which represents a reduction 39.2% in comparison with 1976 messages transmitted in the normal scenario.

ApTitle reutilization

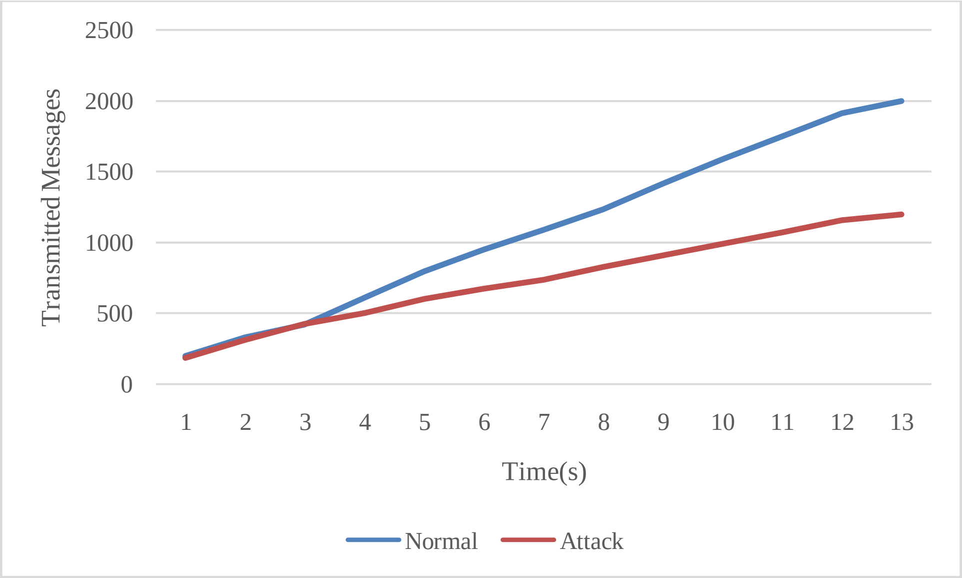

Figure15. ApTitle reutilization

To validate this vulnerability, we set up a scenario where an attacker sends a registration request to the master relay, containing the ApTitle of R1 and a native address of a no existing node. Consequently, once the master relay receives the malicious message, it will add the registering ApTitle to its registration table, creating an association between the received ApTitle and the native address contained in the request message. However, because the registering ApTitle is the address of a relay that was already registered, the master relay will update the native address associated to R1 with the address received in the registration message which does not belong to any node. As a result, the master relay will try to send message destined to R1 to the fake native address provided by the attacker. Thus the messages from the master relay to R1 will be discarded.

The simulation starts with the normal background traffic as described in the beginning of this section (read line between t=1s and t=3s). Thus, at t=3s the attacker sends a malicious registration request message to M1 setting the ApTitle of R1 as the registering ApTitle. As a result, M1 adds the ApTitle of R1 to its registration table, which already has an entry for this ApTitle. Then, as can be appreciate in figure 15, after t=4s M1 discards any message from R1, halving the network traffic. Finally, at the end of the simulation, the number of transmitted messages is 1200 which is a 38.2% less in comparison with the 1942 messages transmitted in the normal scenario.

Log overflow vulnerability

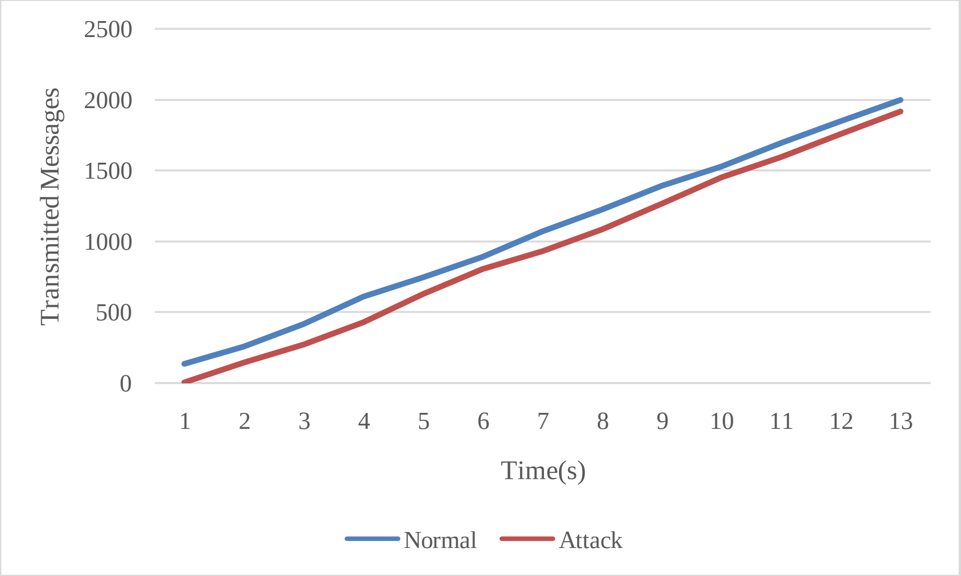

Figure 16. Log overflow attack

To validate this vulnerability, we simulated a scenario where an attacker starts several sessions with a relay in order to cause an overflow in its log file due to excessive number of entries (each session creates a log in the receiver side).

In this simulation, the attacker sends messages to M1 from t=0s to t=13s, with the intention of create a high number of sessions and overflow the event and history log in M1. Consequently, due to the attacker sending messages 4 times faster than a meter, the relay R1 delays the forwarding of legitimate meter traffic (gap between blue and red line in Figure 16). However, given that the memory storage of M1 is 1280001 bytes and each log entry takes 128bytes, the attacker has to send 1001 message to overflow the log file. Thus, at the current rate of 4 messages per second the attacker will need more than 250 seconds to achieve this goal. Now, considering that every second M1 receives background messages from metes, the size of the log file will increase as a function of time following the formula:

$$\mathrm{size(t)} = 128\frac{\mathrm{bytes}}{\mathrm{message}} * \mathrm{backGroundRateEffective}\frac{\mathrm{message}}{\mathrm{seconds}} * \mathrm{t\,seconds}$$

$$+\frac{\mathrm{128bytes}}{\mathrm{messages}} * \mathrm{attackerRate}\frac{\mathrm{messages}}{\mathrm{seconds}} * \mathrm{t\,seconds}$$

Simplifying:

$$\mathrm{size(t)} = 128\frac{\mathrm{bytes}}{\mathrm{seconds}} * (\mathrm{backGroundRateEffective} + \mathrm{attackerRate}) * \mathrm{t\,seconds}$$

Where backGroundRateEffective is the average number of message that R1 forwards every second out of the 100 messages transmitted by the meters per second (backGroundRate), which was determined to be 78 messages per second from the simulation data; and attackerRate has a value of 4. Then, the log file will be bigger than

128001 bytes at t=12.1s which is almost at the end of the simulation. This means that at a rate of 4 messages per second the attacker will achieve the goal of overflow the log file size, almost at the end of the simulation. This result can be appreciated in figure 16 because the end value of the total traffic in the normal scenario is bigger than the traffic in the attack scenario for a low margin. Specifically, in the attack scenario, R1 has transmitted 1899 message at t=13s, having 42 messages delayed and 59 loosed. It is important to note, that the delayed messages are caused by the extra time required by R1 to process the attacker's traffic, and the lost packets are caused by the abuse of the vulnerability. Given, that only the 0.97% of the messages were discarded, the attack has a low impact. However, using the formula derived from the simulation and assuming the attacker is able to send 40 messages per second instead of 4, the log file of R1 will be overflow by t=8.4s and R1 will not forward any more messages after that moment. Consequently, the total number of lost packet will be near 47%.

5.5 Mitigation strategies

The vulnerabilities presented in section 5.2 exist because a group of fundamental security flaws are common to many of them. Consequently, the solution of these flaws will mitigate the presented vulnerabilities. In this section, we propose mitigation strategies for the fundamental security flaws.

5.4.1 Fundamental security flaws

From analyzing the nature of the vulnerabilities presented in section 5.3, we realize that these vulnerabilities consist in the combination of low level security flaws. Then our approach for creating mitigation strategies for these vulnerabilities, consist in identifying and solving these fundamental security flaws. Table 6 shows the identified security flaws.

Low level flaw	**Vulnerability**
Acceptance of unsolicited response messages	Identification manipulation vulnerability(V1), Incomplete data vulnerability (V3), Session expiration vulnerability (V10), Registration period vulnerability (V15)
Identify spoofing	V1, Authorization vulnerability (V8), Session expiration vulnerability (V9), ApTitle reutilization vulnerability (V13), Subscription vulnerability(V14), V15, Routing table overflow vulnerability (V17), Unbound resolution vulnerability (V19), Unbound trace vulnerability (V20)
Lack of packet size validation in the reassembly process.	Excessive data size vulnerability (V2)
Keeping idle connection alive for too long.	V3, Timeless session vulnerability (V6), Extended session vulnerability (V12)
Lack of validation of the index plus element-count value.	Unbound index vulnerability (V4), Information overwriting vulnerability (V5)
Lack of validation of the log file size	Log overflow vulnerability (V7)
Lack of validation of source node authorization	V9, Illegitimate disconnection vulnerability (V11), ApTitle assignment vulnerability (V16), Illegitimated deregistration vulnerability (V18), Inaccurate topology vulnerability (V21)
Lack of validation for duplicated ApTitles	V13

Table 6. Security flaws for discovered vulnerabilities.

As can be observed in table 6, there are security flaws which are common to several vulnerabilities, then the solution of the common flaws will allow the mitigation of many vulnerabilities simultaneously. More specifically, we can create mitigation strategies for each one of the 21 discovered vulnerabilities, by designing security mechanisms for the 8 different security flaws presented in table 6. For instance, by solving the identity spoofing issue it is possible to mitigate vulnerabilities V1, V8, V10, V14, V15 and V20, because each one of them relies in the possibility of conducting a identity spoofing attack.

5.4.2 Security countermeasures

Following, we propose countermeasures for the fundamental security flaws presented in the previous section.

Limit the time of idle sessions and connections: The existence of the zero value in the logon service request message causes the establishment of session without time limit, which can be abused by an attacker as shown in the previous section (timeless session vulnerability – V6). A simple but effective way to mitigate this vulnerability is to establish a maximum time limit to the C12.22 sessions; this maximum limit should be used as default value when a zero set <req-session-idle-timeout> message is received. Then, when an attacker issues a request for a session without time limit, the victim node may set a timer to a maximum value T for closing the session if it enters the idle state. Thus the attacker will not be able to exhaust the victim's resources, because the sessions will not be open indefinitely. Additionally, if the attacker tries to keep the session alive by sending multiple wait service requests (extended session vulnerability – V12), which ask for an extension in the session timeout, the victim node will increase the session timer but only until reaching the value of T (which have to be chosen according to network needs). After that, any other message asking for more extensions of the session's time will be discarded. Consequently, it protects the victim node of suffering an overflow in the variable keeping track from the session timeout, because with this method the value of that timer will not have a value greater than T. Additionally, the possibility of having an open connection waiting for the reception of message segments for a indefinitely period of time provokes the incomplete data vulnerability (V1). A solution for this issue consists of setting a timer to the value of T (being T maximum timeout value for a session). Thus, each time a segment arrives, the receiver node will wait T seconds; if after this period the next message segment does not arrive, the node may close the connection and discard the received segments. Then, if an attacker tries to force an open session in a node by sending an incomplete message, the victim node will terminate such a session before significant resource consumption occurs, which will reduce significantly the impact of a potential attack.

Controls over duplicated ApTitles: As we discussed in the previous section, it is possible for a malicious node to request a registration service setting in the field calling-ApTitle, an ApTitle that can be in use by other node (ApTitle reutilization vulnerability – V13). Our proposal to mitigate this vulnerability consists in having a record of registered ApTitle and the native network address related to it. Under this approach, when a malicious node tries to register an ApTitle which is already in use by other node, the master relay may check the record for previous assigned ApTitles. Then the master relay will determine that the ApTitle which is trying to be registered by the attacker is already in use. Consequently, the master relay will reject the registration request.

Reassembly control: After reassembling a message which is divided in several small segments, the size of the final assembled packet may exceed the memory capacity of network nodes (excessive data size vulnerability – V2). To mitigate this issue, we propose an enhancement to the reassembly algorithm. This modification consists in the following: when a segmented message arrives to a node, the reassembly algorithm should validate that the size of the received segment plus the size of all segments received previously do not exceed the memory capacity of the node. Then, if the size of the new segment fits into the available memory, the reassembly algorithm may proceed as normal; otherwise all related segments have to be discarded.

Log size control: When receiving several logon request messages the storage capacity of a node may be exhausted (log overflow vulnerability – V7), because according to the protocol specification, every logon request has to be logged. To mitigate this flaw we propose a modification of the logger process, such that, each time a logon request arrives, the logger should validate whether or not the addition of a new log entry may exhaust the storage capacity. In affirmative case, the log entry should be discarded and the node has to send an alarm to the utility to report the situation; otherwise, the logger may proceed as normal. Thus, when an attacker tries to overflow the storage capacity of a node, the node will be able to block the attack by discarding log entries which may exhaust its storage capacity.

Control partial table access: When processing a read or write request, the index plus the element-count value may exceed a table boundary. This situation facilitates the abuse of the unbound index (V4) and information overwriting (V5) vulnerability respectively. To deal with this security flaw we propose the following mechanism: each time a node receives a partial reading or writing request it should be validated so that the resulting value of the intended index plus the element-count value is not greater than the table size. Then, an attacker will not be able to access or overwrite information beyond the limits of a table which mitigate the mentioned vulnerabilities.

Preventing identity spoofing: Due to the lack of mechanisms to prevent identity spoofing, many attack scenarios may succeed (V1, V8, V10, V13, V14, V15, V17, V19 and V20). To prevent this we propose the following. Each time a node receives a request message, it has to ask for a positive confirmation to the address of the sender node, if a non negative confirmation is received, the receiver node may assume that the sender is the legitimate owner of the source address contained in the request message, otherwise the receiver may determine that a spoofing attack is taking place. To further illustrate this countermeasure consider the following scenario: a malicious node A wants to spoof the identity of a given relay R1 in order to launch an identification manipulation attack against a victim node V. For this, the attacker will send an unsolicited identification response message to the victim node. This message is prepared setting the ApTitle of the relay R1 as the source address. Upon the reception of this message, the victim node V should issue a confirmation request to R1 to validate that it sent the identification request message. Consequently, because R1 did not send any request message previously, it will replay sending a negative confirmation to V. Once V receives the negative confirmation, it will discard the malicious message sent by the attacker. Thus, the spoofing will be prevented as well as the subsequent identification manipulation attack.

Prevent unsolicited responses: when receiving unsolicited service responses, a node may accept and process the received messages. This situation facilitates the abuse of some vulnerabilities (V1, V3, V10 and V15). To address this issue, we propose that each time a node receives an unsolicited response message, it should be discarded without further processing. Thus, when an attacker tries to abuse any of the vulnerabilities which depend of this security flaw, its messages will be dropped and the attack may be prevented.

Origin authority control: for vulnerabilities such as illegitimate disconnect (V11), illegitimate deregister (V18), ApTitle assignment (V16), session termination (V9) and inaccurate topology (V21) the lack of validation for determining the authority of a node which sends specific messages, allows the accomplishment of different attacks. To approach this issue, we propose security measures for each one of the vulnerabilities individually. First, with regard to the disconnect vulnerability, we purpose the creations of a list of nodes which are authorized to issue disconnect commands, and the implementation of the spoofing prevention mechanism discussed above. Then, if a disconnect request proceeds from a node which is not in the list of authorized nodes, the receiver node will discard it. Additionally, any attempt to spoof the identity of an authorized node should be prevented by the anti-spoofing mechanism. The same approach applies for the illegitimate deregistration vulnerability. Second, with regard to the session termination vulnerability, a mitigation consist in validating the source address of any logoff request, then if that address does not match the address of the node which established the session which is intended to be terminated, the logoff request should be ignored. Third, related to the ApTitle assignment vulnerability, we propose the following confirmation strategy: once a node receives an ApTitle as part of the registration process, it should query the master relay to determine that the ApTitle is not already in use. If the master relay confirms the availability of the ApTitle, then the node may use it, otherwise, it should ask the master relay for a different one. Finally, to abuse the inaccurate topology vulnerability, the attacker requires adding the addresses of relays which are not in the path from a sender node to a destination in the trace service response. Our proposed countermeasure consists in the implementation of a validation procedure in the relay which is adjacent to the victim's node. Thus, when a trace service response is received by this relay, it can validate the information contained in it, by matching the address of the nodes in the service response with those in its own routing table. Thus, if the attacker add nodes which are inexistent or that do not belongs to the path from the victim's node to the selected destination, the adjacent relay will detect that and will delete the trace service response.

5.5 Chapter conclusions

In this chapter, we have investigated the security of ANSI C12.22 standard. Specially, we utilized a specification-based approach to study the security of the ANSIC12.22 services. As a result, we discovered vulnerabilities in each one of the protocol services and we proposed countermeasures to mitigate them. Additionally, we presented the computation of a severity score for each one of the discovered security issues, which helps in the management and mitigation of vulnerabilities. With these results, we expect to contribute to the understanding of the security risks inherent to the ANSI C12.22 protocol, which is essential to improve the security of AMI and therefore the security of the Smart Grid.

CHAPTER 6. CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

The security of the smart grid is an important topic and a big challenge. In order to provide security solutions for the smart grid, it is required to first understand the security weaknesses and attacks that may threaten the system. With the goal to contributing to the understanding of the smart grid security, we have conducted a security assessment of two crucial smart grid technologies: the Advanced Metering Infrastructure (AMI) and the ANSIC12.22 standard.

First, we applied a use-case-centric approach to investigate security weakness of each one of the AMI use cases focusing on availability issues. We found that our security analysis can improve the understanding of the vulnerabilities associated with specific use cases, which provides a better classification of attacks and facilitates the design of countermeasures.

Second, we used a specification-based approach to conduct an evaluation of ANSIC12.22 security. As a result, we found 21 vulnerabilities in ANSIC12.22 services from which more than an 80% present a severity impact of medium or high degree. Furthermore, through simulation we show that in some scenarios, it is feasible to drop more than 73%

of transmitted messages by sending only one malicious message. Additionally, we proposed mitigation strategies for the identified security issues.

In summary, we can conclude that our research extends the understanding of the smart grid security which contributes to facilitating the management of the cyber security risk associated to the smart grid systems.

6.2 Future work

While we have presented multiple contributions for improving the security of the smart grid, there are still many important topics that have to be investigated in order to have a comprehensive solution for smart grid security. In the following, we describe these research needs.

First, a future work should be the validation of the security issues that we discovered in a real scenario, as well as the execution of the proposed attacks to determine their real impact and feasibility. Additionally, there should be an evaluation of the performance and effectively of our proposed countermeasures in real systems. Secondly, continuous research is needed to adapt the existing AMI IDS solutions for detecting new vulnerabilities, as well as, evaluation of their effective detection rate and performance. Finally, it is necessary to further investigate the security of different protocol standards for AMI and design appropriate countermeasures in order to facilitate the mitigation of vulnerabilities in smart grid deployments.

REFERENCES

[1] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges,” *IEEE Commun. Surv. Tutorials*, pp. 1–16, 2012.

[2] *M LaMonica, “Obama signs stimulus plan, touts clean energy”, CNN, Feb 7 2009, at http://news.cnet.com/8301-11128 3-10165605-54.html. .*

[3] *European Parliament and Council, “Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.”.*

[4] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, “Bad Data Injection in Smart Grid : Attack and Defense Mechanisms,” *Commun. Mag. IEEE,*, no. January, pp. 27–33, 2013.

[5] R. Anderson and S. Fuloria, “Who Controls the off Switch?,” *Smart Grid Commun. (SmartGridComm), 2010 First IEEE Int. Conf.*, 2010.

[6] J. Chinnow, K. Bsufka, A. Schmidt, R. Bye, A. Camtepe, and S. Albayrak, “A Simulation Framework for Smart Meter Security Evaluation,” *Smart Meas. Futur. Grids (SMFG), 2011 IEEE Int. Conf.*, 2011.

[7] M. Hashmi, S. Hänninen, and K. Mäki, “Survey of Smart Grid Concepts , Architectures , and Technological Demonstrations Worldwide,” *Innov. Smart Grid Technol. (ISGT Lat. Am. 2011 IEEE PES Conf.*, pp. 1–7, 2011.

[8] U. . E. I. Administration, “How many smart meters are installed in the U.S and who has them?,” *http://www.eia.gov/tools/faqs/faq.cfm?id=108&t=3*, 2014. .

[9] D. Hull, “PG&E Details Technical Problems with Smart Meters,” *http://www.mercurynews.com/search/ci_14963541?nclick_check=1 - 04/28/2010*, 2010.

[10] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A Survey on Cyber Security for Smart Grid Communications,” *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[11] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, “Smart Grid Technologies: Communication Technologies and Standards,” *IEEE Trans. Ind. Informatics*, vol. 7, no. 4, pp. 529–539, 2011.

[12] X. Li, I. Lille, and N. Europe, “Securing Smart Grid : Cyber Attacks , Countermeasures , and Challenges,” *Commun. Mag. IEEE*, vol. 50, no. 8, pp. 38–45, 2012.

[13] D. He, C. Chen, J. Bu, S. Chan, Y. Zhang, and M. Guizani, “Secure service provision in smart grid communications,” *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 53–61, 2012.

[14] K. Moslehi, R. Kumar, and S. Member, “A Reliability Perspective of the Smart Grid,” *Smart Grid, IEEE Trans.*, vol. 1, no. 1, pp. 57–64, 2010.

[15] F. Skopik and Z. Ma, “Attack Vectors to Metering Data in Smart Grids under Security Constraints,” *Comput. Softw. Appl. Conf. Work. (COMPSACW), 2012 IEEE 36th Annu.*, 2012.

[16] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, “A Denial of Service Attack in Advanced Metering Infrastructure Network,” in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 1029–1034.

[17] R. Vigo, E. Yüksel, C. Dewi, and P. Kencana, “Smart Grid Security A Smart Meter-Centric Perspective,” in *20th Telecommunications Forum*, 2012, pp. 127–130.

[18] S. Mclaughlin, D. Podkuiko, and P. Mcdaniel, “Energy Theft in the Advanced Metering Infrastructure,” *Crit. Inf. Infrastructures Secur. Springer Berlin Heidelb.*, vol. 6027, no. 2010, pp. 176–187, 2010.

[19] K. I. Sgouras, A. D. Birda, and D. P. Labridis, “Cyber Attack Impact on Critical Smart Grid Infrastructures,” *Innov. Smart Grid Technol. Conf. (ISGT), 2014 IEEE PES*, 2014.

[20] N. Komninos, E. Philippou, A. Pitsillides, and S. Member, “Survey in Smart Grid and Smart Home Security : Issues , Challenges and Countermeasures,” *Commun. Surv. Tutorials, IEEE*, vol. 16, no. 4, pp. 1933–1954, 2014.

[21] T. Goodspeed, S. Bratus, R. Melgares, R. Speers, and S. W. Smith, “Api-do : Tools for Exploring the Wireless Attack Surface in Smart Meters,” in *2012 45th Hawaii International Conference on System Science (HICSS)*, 2012.

[22] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. a. Cardenas, and J. G. Jetcheva, “AMI threats, intrusion detection requirements and deployment recommendations,” *2012 IEEE Third Int. Conf. Smart Grid Commun.*, pp. 395–400, 2012.

[23] S. D. Justin Searle, Galen Rasche, Andrew Wright, “AMI Penetration Test Plan.” [Online]. Available: http://www.smartgrid.epri.com/doc/AMI-Penetration-Test-Plan- 1-0-RC3.pdf.

[24] D. Bian, M. Kuzlu, M. Pipattanasomporn, and S. Rahman, “Analysis of Communication Schemes for Advanced Metering Infrastructure (AMI),” *PES Gen. Meet. Conf. Expo. 2014 IEEE*, pp. 14–18, 2014.

[25] C. T. Group, T. A. Security, A. Project, and E. Corporation, “Security Profile for Advanced Metering Infrastructure, v2.0,” no. 865, 2010.

[26] a. F. Snyder and M. T. G. Stuber, “The ANSI C12 protocol suite - updated and now with network capabilities,” *2007 Power Syst. Conf. Adv. Metering, Prot. Control. Commun. Distrib. Resour.*, pp. 1–6, 2007.

[27] R. Berthier and W. H. Sanders, “Specification-Based Intrusion Detection for Advanced Metering Infrastructures,” *2011 IEEE 17th Pacific Rim Int. Symp. Dependable Comput.*, pp. 184–193, Dec. 2011.

[28] A. Hahn and M. Govindarasu, “Cyber Attack Exposure Evaluation Framework for the Smart Grid,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 835–843, 2011.

[29] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart Grid — The New and Improved Power Grid: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[30] V. Kounev, “Advanced Metering and Demand Response Communication Performance in Zigbee based HANs,” *Comput. Commun. Work. (INFOCOM WKSHPS), 2013 IEEE Conf.*, pp. 3405–3410, 2013.

[31] *O. S. G. user group (OpenSGug) Smart Grid Network Task Force, “Smart grid network system requirements specifications v5.0-draft1,” http://osgug.ucaiug.org/UtiliComm, 2011.* .

[32] A. Moise and J. Brodkin, “ANSI C12.22, IEEE 1703, and MC12.22 Transport Over IP,” 2011. [Online]. Available: http://tools.ietf.org/html/rfc6142. [Accessed: 27-Mar-2014].

[33] *ANSI C12.22: Protocol specification for interfacing to data communi- cation networks. National Electrical Manufacturers Association, 2008.* .

[34] A. Moise, “ANSI C12.22 (c1222),” 2013. [Online]. Available: http://wiki.wireshark.org/C12.22. [Accessed: 27-Mar-2014].

[35] *ANSI C12.19: Utility industry end device data tables. National Electrical Manufacturers Association, 2008. .*

[36] *ANSI C12.18: Protocol Specification for ANSI Type 2 Optical Port. National Electrical Manufacturers Association, 2006. .*

[37] *ANSI C12.21: Protocol Specification for Telephone Modem Communication. National Electrical Manufacturers Association, 2006. .*

[38] IEEE, *IEEE Standard for Local Area Network / Wide Area Network (LAN / WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables*, no. June. 2012.

[39] B. Min and A. S. Grid, "Design and Analysis of Security Attacks against Critical Smart Grid Infrastructures," *Eng. Complex Comput. Syst. (ICECCS), 2014 19th Int. Conf.*, pp. 59–68, 2014.

[40] M. Costache, V. Tudor, M. Almgren, M. Papatriantafilou, and C. Saunders, "Remote control of smart meters : friend or foe ?," in *Computer Network Defense (EC2ND), 2011 Seventh European Conference on*, 2011, pp. 49–56.

[41] W. G. Temple, B. Chen, and N. O. Tippenhauer, "Delay Makes a Difference : Smart Grid Resilience Under Remote Meter Disconnect Attack," *Smart Grid Commun. (SmartGridComm), 2013 IEEE Int. Conf.*, pp. 462–467, 2013.

[42] Y. Liu, S. Hu, and T. Ho, "Vulnerability Assessment and Defense Technology for Smart Home Cybersecurity Considering Pricing Cyberattacks," *Proc. 2014 IEEE/ACM Int. Conf. Comput. Des.*, pp. 183–190, 2014.

[43] C. Fan, S. Huang, and Y. Lai, "Privacy-Enhanced Data Aggregation Scheme Against Internal Attackers in Smart Grid," *IEEE Trans. Ind. Informatics*, vol. 10, no. 1, pp. 666–675, 2014.

[44] V. Namboodiri, V. Aravinthan, and W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," *IEEE Syst. J.*, vol. 8, no. 2, pp. 509–520, 2014.

[45] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward Unified Security and Privacy Protection for Smart Meter Networks," *IEEE Syst. J.*, vol. 8, no. 2, pp. 641–654, 2014.

[46] K. J. Ross, K. M. Hopkinson, S. Member, and M. Pachter, “Using a Distributed Agent-Based Communication Enabled Special Protection System to Enhance Smart Grid Security,” *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 1216–1224, 2013.

[47] R. Q. Hu, S. K. Das, and H. Sharif, “An efficient security protocol for advanced metering infrastructure in smart grid,” *IEEE Netw.*, vol. 27, no. 4, pp. 64–71, 2013.

[48] M. M. Farag, M. Azab, and B. Mokhtar, “Cross-Layer Security Framework for Smart Grid : Physical Security Layer,” in *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2014, pp. 1–7.

[49] C. Testbeds, T. Yardley, R. Berthier, D. Nicol, and W. H. Sanders, “Smart Grid Protocol Testing Through Cyber-Physical Testbeds,” *Innov. Smart Grid Technol. (ISGT), 2013 IEEE PES*, 2013.

[50] D. Jin, Y. Zheng, H. Zhu, D. M. Nicol, and L. Winterrowd, “Virtual Time Integration of Emulation and Parallel Simulation,” in *ACM/IEEE/SCS 26th Workshop on Principles of Advanced and Distributed Simulation*, 2012, pp. 201–210.

[51] C. Siaterlis, “Developing Cyber-Physical Experimental Capabilities for the Security Analysis of the Future Smart Grid,” in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, pp. 1–7.

[52] N. Hadjsaid, “Vulnerability Analysis of Coupled Heterogeneous Critical Infrastructures : a Co-simulation Approach with a Testbed Validation,” in *2013 4th IEEE/PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*, 2013, pp. 1–5.

[53] B. Chen, S. Mashayekh, and K. L. Butler-purry, “Impact of Cyber Attacks on Transient Stability of Smart Grids with Voltage Support Devices,” in *IEEE Power and Energy Society General Meeting (PES)*, 2013.

[54] J. Yan, Y. Yang, W. Wang, H. He, and Y. Sun, “An Integrated Visualization Approach for Smart Grid Attacks,” in *Third International Conference on Intelligent Control and Information Processing (ICICIP)*, 2012, pp. 277–283.

[55] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, “Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid,” *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 105–120, 2014.

[56] M. S. Thomas, S. Member, I. Ali, and N. Gupta, “Integration and Security Analysis of Metering Infrastructure,” in *Power India Conference, 2012 IEEE Fifth*, 2012, pp. 1–6.

[57] Z. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, “An early warning system against malicious activities for smart grid communications,” *IEEE Netw.*, vol. 25, no. 5, pp. 50–55, 2011.

[58] P. McDaniel and S. McLaughlin, “Security and Privacy Challenges in the Smart Grid,” *IEEE Secur. Priv. Mag.*, vol. 7, no. 3, pp. 72–74, 2009.

[59] J. Liu, Y. Xiao, and S. Li, “Cyber security and privacy issues in smart grids,” *Commun. Surv. Tutorials, IEEE*, vol. 14, no. 4, pp. 981–997, 2012.

[60] U. S. NIST, “Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. Available at: http://csrc.nist.gov/ publications/PubsNISTIRs.html#NIST-IR-7628.,” 2010.

[61] P. L. Fengjun Li, Bo Luo, “Secure and privacy-preserving information aggregation for smart grids,” *Int. J. Secur. Networks (IJSN), Spec. issue Secur. Priv. smart grids,*, vol. 6, no. 1, p. 2839, 2011.

[62] A. Cavoukian, J. Polonetsky, and C. Wolf, “Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation,” *Identity Inf. Soc.*, no. November, 2010.

[63] C. Efthymiou and G. Kalogridis, “Smart Grid Privacy via Anonymization of Smart Metering Data,” *Smart Grid Commun. (SmartGridComm), 2010 First IEEE Int. Conf.*, pp. 238–243, 2010.

[64] F. Li, B. Luo, and P. Liu, “Secure Information Aggregation for Smart Grids Using Homomorphic Encryption,” *2010 First IEEE Int. Conf. Smart Grid Commun.*, pp. 327–332, Oct. 2010.

[65] S. Mclaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. Mcdaniel, “Multi-vendor Penetration Testing in the Advanced Metering Infrastructure,” *Proc. 26th Annu. Comput. Secur. Appl. Conf. ACM*, 2010.

[66] J. Carpenter, M., Goodspeed, T., Singletary, B., Skoudis, E., & Wright, “Advanced metering infrastructure attack methodology,” *InGuardians white paper*, 2009.

[67] R. Berthier, W. H. Sanders, and H. Khurana, “Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions,” *Smart Grid Commun. (SmartGridComm), 2010 First IEEE Int. Conf.*, pp. 350–355, 2010.

[68] M. A. Rahman, E. Al-Shaer, and P. Bera, “A Noninvasive Threat Analyzer for Advanced Metering Infrastructure in Smart Grid,” *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 273–287, 2013.

[69] X. Liu, S. Member, P. Zhu, S. Member, Y. Zhang, S. Member, and K. Chen, “A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure,” *IEEE Trans. Smart Grid*, pp. 1–9, 2015.

[70] Z. A. Baig, A. Al Amoudy, S. Science, S. Arabia, and K. Salah, “Detection of Compromised Smart Meters in the Advanced Metering Infrastructure,” *IEEE GCC Conf. Exhib.*, pp. 1–4, 2015.

[71] M. A. Rahman and E. Al-shaer, “AMIAnalyzer : Security Analysis of AMI Configurations,” in *Configuration Analytics and Automation (SAFECONFIG), 2011 4th Symposium on*, 2011, pp. 1–2.

[72] R. Berthier and W. H. Sanders, “Monitoring Advanced Metering Infrastructures with Amilyzer,” *Cyber-security SCADA Ind. Control Syst. C&ESAR*, 2013.

[73] S. Rana, H. Zhu, C. W. Lee, D. M. Nicol, and I. Shin, “The Not-So-Smart Grid : Preliminary Work on Identifying Vulnerabilities In ANSI C12.22,” *Globecom Work. (GC Wkshps), 2012 IEEE*, pp. 1514–1519, 2012.

[74] Z. Yordy, “Using SANs to Model DDoS Attacks in Simple AMI Networks.”

[75] M. S. Thomas, S. Member, I. Ali, S. Member, and N. Gupta, “A Secure Way of Exchanging the Secret Keys,” *Power Syst. Technol. (POWERCON), 2012 IEEE Int. Conf.*, 2012.

[76] E. For, “Communication Security for Smart Grid Distribution Networks,” *Commun. Mag. IEEE*, vol. 51, no. 1, pp. 42–49, 2013.

[77] T. Mehra, V. Dehalwar, A. S. Grid, and A. M. I. Communication, “Data Communication Security of Advanced Metering Infrastructure in Smart Grid,” *Comput. Intell. Commun. Networks (CICN), 2013 5th Int. Conf.*, pp. 394–399, 2013.

[78] E. Choo, Y. Park, and H. Siyamwala, “Identifying Malicious Metering Data in Advanced Metering Infrastructure,” *Serv. Oriented Syst. Eng. (SOSE), 2014 IEEE 8th Int. Symp.*, pp. 490–495, 2014.

[79] L. Garcia and S. Zonouz, “TMQ : Threat Model Quantification in Smart Grid Critical Infrastructures,” *Smart Grid Commun. (SmartGridComm), 2014 IEEE Int. Conf.*, pp. 584–589, 2014.

[80] F. Barringer, “New Electricity Meters Stir Fears,” *http://www.nytimes.com/2011/01/31/science/earth/31meters.html?pagewanted=all&_r=0*, 2011. .

[81] R. Lau, “Protests continue against Hydro-Quebec smart meters,” *http://globalnews.ca/news/1394087/protests-continue-against-hydro-quebec-smart-meters/*, 2014. .

[82] J. Schwartz, “Protest, petition urges Port Angeles to stop ‘smart’ meter project,” *http://www.peninsuladailynews.com/article/20140320/NEWS/303209989*, 2014. .

[83] *M. Davis, “Recoverable advanced metering infrastructure,” in Black Hat USA, 2009. .*

[84] P. Mell, K. Scarfone, S. Romanosky, I. Group, B. Brook, S. Hanford, S. Raviv, G. Reid, and G. Theall, “A Complete Guide to the Common Vulnerability Scoring System,” *Publ. by FIRST-Forum Incid. Response Secur. Teams,* pp. 1–23, 2007.

BIOGRAPHY

Jorge Perea received a bachelor degree in computer engineering from the University of Cartagena, Cartagena, Colombia, in 2012. During his bachelor, he worked in several research projects such as “Development of a guide for the identification and mitigation of security issues in IEEE 802.11 networks, through the design and implementation of a vulnerability validation scheme” and “Identification, assessment and mitigation of security issues in the data network and servers of University of Cartagena”. In the last year of his bachelor studies, he traveled to Spain for a research internship related to the simulation and security analysis of the integration of mobile IP protocols and QoS algorithms. After receiving his bachelor, he worked for about one year as a full time employee in the development, testing and maintenance of large scale financial software. Currently, he is working toward a Master degree in Computer Engineering at the University of Puerto Rico.