Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures

N. Komninos, *Member, IEEE,* E. Philippou and A. Pitsillides, *Senior Member, IEEE*

Abstract— **The electricity industry is now at the verge of a new era. An era that promises, through the evolution of the existing electrical grids to Smart Grids, more efficient and effective power management, better reliability, reduced production costs and more environmentally friendly energy generation. Numerous initiatives across the globe, led by both industry and academia, reflect the mounting interest around the enormous benefits but also the great risks introduced by this evolution. This paper focuses on issues related to the security of the Smart Grid and the Smart Home, which we present as an integral part of the Smart Grid. Based on several scenarios we aim to present some of the most representative threats to the Smart Home / Smart Grid environment. The threats detected are categorized according to specific security goals set for the Smart Home/Smart Grid environment and their impact on the overall system security is evaluated. A review of contemporary literature is then conducted with the aim of presenting promising security countermeasures with respect to the identified specific security goals for each presented scenario. An effort to shed light on open issues and future research directions concludes the paper.**

Index Terms— **Smart Grids, Smart Homes, Security, Countermeasures, Challenges**

I. Introduction

The electric power infrastructure as we know it today has managed to serve our needs successfully, almost unchanged, for nearly a century; revolutionizing almost every aspect of our lives. However, as this infrastructure is inevitably aging it becomes increasingly less efficient, repeatedly running up against its limitations and constantly straining to keep up with our ever-increasing requirements. Needs for reliability, scalability, manageability, environmentally friendly energy generation, interoperability and cost effectiveness, bring forward the necessity for a modernized and intelligent grid for tomorrow; a new, reliable, efficient, flexible and secure energy infrastructure, known as the Smart Grid [1].

Through the incorporation of advanced power system electronics, networking and communication technologies the Smart Grid is envisioned to significantly enhance the existing electric grid. Allowing for more accurate real-time monitoring, ensuring the optimization of power flows and enabling for two-way communication between the utility and customer sides while pointing the way to a more environmentally friendly energy generation via the incorporation of renewable energy sources into the grid (both at the utility and the consumer sides) [2][3].

An indispensable part of this evolution, residential smart metering, brings the Smart Grid into our homes, transforming them into the Smart Homes of the future and allowing for more effective household energy monitoring and control.

Recent studies suggest that 40% of total energy consumption and 36% of total carbon dioxide emissions in the European Union can be attributed to homes and buildings [4]. The corresponding rates in the U.S and China range at similar levels making the need for home evolution imperative. The households of the future, need not only be significantly smarter but also more energy aware. We will refer to these, as energy aware Smart Homes; i.e. homes that leverage sensor and networking technologies to ensure communication amongst their appliances and a smart meter that constantly reports recorded energy consumption to the grid, whilst also allowing the Smart Grid to push information, such as dynamic pricing, back to the house. Such homes are expected to dynamically adjust their energy profile according to Smart Grid capabilities, while also providing their owners with the opportunity for remote device monitoring [5].

Smart Grid's success heavily relies upon communication. Every single entity part of this complex, heterogeneous network has to be able to communicate with any other entity in it and in the Smart Home, at any time, in an efficient but also secure manner. With this communication being greatly reliant on information technology though, concerns regarding security and privacy aspects inevitably creep in. Vulnerabilities inherent to communication and networking systems can clearly affect the Smart Grid, with consequences often more severe than what we are accustomed to face in ordinary information systems. In fact, if exploited successfully these vulnerabilities can severely harm the entire infrastructure, causing economies to collapse, societies to fall apart and people to lose their lives. Security thus becomes a primary concern for this critical infrastructure.

Despite its criticality however, the research on Smart Home and Smart Grid security issues is still in its early stages [6]. As a result, we are motivated to further investigate them. Our aim is to contribute to the already existing literature by providing a more comprehensive view of security in the Smart Grid environment, taking into account its persistent interaction with the Smart Home and focusing on the entire network, not only some specific subsystems which are often the focus of current security related literature. For this reason, our adopted approach involves the identification of threats that can arise, under some of the most typical scenarios of interaction between various entities of the Smart Grid environment, from

N. Komninos is with the Departments of Computer Science, City University London and University of Cyprus email: {Nikos.Komninos.1@city.ac.uk}.

E.Philippou and A.Pitsillides are with the Department of Computer Science, University of Cyprus, P.O. Box 20537, 1678 Nicosia, Cyprus, email :{ephili01,andreas.pitsillides}@cs.ucy.ac.cy

customer side to utility side and vice versa. Our approach can be summarized in three key points.

- Firstly, there is the identification of the main scenarios of interaction between entities in Smart Home and Smart Grid environments. The classification of the risks that threaten these interactions and an evaluation of their impact on overall system security.
- Secondly, a review of current literature concerning security countermeasures that could potentially defend us against the detected threats is carried out. It presents promising security countermeasures with respect to the identified specific security goals for each presented interaction scenario.
- And thirdly, open issues are presented and future directions for research are proposed.

To the best of our knowledge, this is the first survey concerning Smart Grid cyber security issues that places such a strong emphasis on the Smart Home environment and its interaction with the Smart Grid environment. The reason for this focus lies in the recognition that with the dawn of the Smart Grid the role of the consumer and his Smart Home becomes of increasing importance to the Grid. Of course, the bulk transmission system at the utility side is still considered to be the primary focus of cyber security efforts. However, in the Smart Grid era the protection of network connections to the customers' homes becomes vital as it can also jeopardize the Grid's robustness and stability.

The remainder of this paper is organized as follows. In Section II, we briefly introduce the architectures of the Smart Grid and the Smart Home, underlining the benefits of their interactions. In Section III, we present the security goals that are expected to be met and identify threats that occur under representative scenarios of interaction between Smart Home/Smart Grid entities. The impact of these threats is also evaluated in this section. In Section IV, we review contemporary literature to discuss promising countermeasures against the different attacks identified in section III. Section V, provides an overview of ongoing standardisation efforts in the industry regarding Smart Grid Cyber Security. In Section VI, future research directions are proposed. Section VII, concludes our paper.

II. Smart Grid & Smart Home Overview

A. *Smart Grid Architecture*

To date, various frameworks describing the architecture of the Smart Grid have been proposed by both industry and academia with the most widely adopted and adapted model by far, being the reference model proposed by the U.S National Institute of Standards and Technology (NIST) [3].This model conceptualizes the Smart Grid as a set of seven interconnected domains. The first four domains (Bulk Generation, Transmission, Distribution and Customers) are responsible for the generation, transmission and distribution of energy but also for ensuring the two way communication between the customer side and the Advanced Metering Infrastructure (AMI) utility head end. The remaining three entities (Markets, Operations and Service Providers) are responsible for energy market management, energy distribution management and service provision.

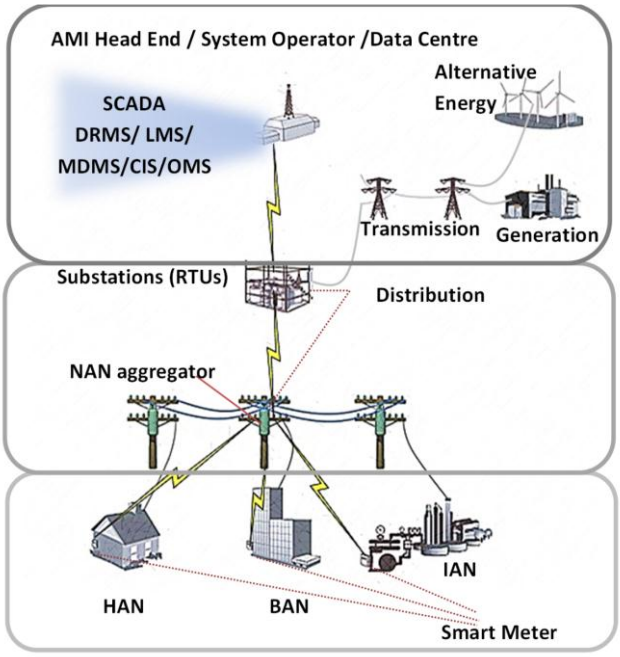


Fig. 1 A multi-layered conceptual model of the Smart Grid's architecture. Smart Homes at the lower layer are in continuous two-way communication with the AMI-Head End at the top layer, via the AMI-network entities of the second layer. A more detailed view of a Smart Home's internal environment and the way it interfaces to the external environment, illustrated here as the middle and top layers, is given in Fig.2

A slightly different architecture, merely inspired by NIST's conceptual model as described above, but also by [7][8] and [9], is adopted for the purposes of this study. This architecture conceptualizes the Smart Grid following a multi-layered approach. As shown in Fig.1, at the bottom layer of this model, one can find Home Area Networks (HANs), Building Area Networks (BANs) and Industrial Area Networks (IANs) i.e. wired or wireless networks in customer premises (homes, buildings or industrial areas) that interconnect appliances with smart meters and energy management devices, responsible for reporting the premise's consumption to the grid at any given time while also carrying messages from the grid back to the premise [10].
At the middle layer, one can find Neighborhood Area Networks (NANs) i.e. networks that cover small geographic areas, responsible for the interconnection of the smart meters of different kinds of premises with a distribution access point that aggregates the data collected by them forwarding them to the upper layer. Remote Terminal Units (RTUs) i.e. electronic devices responsible for the transmission of telemetry data to the SCADA system (at the top layer) and Phasor Measurement Units (PMUs) i.e. synchronized devices that measure electrical waves on the grid, are also considered to be part of the NAN [11]. At the top layer of this conceptual model, one can find Wide Area Networks (WANs) interconnecting multiple NANs. All the data collected by NANs (be it information that describes the grid's current state or the aggregate consumption of a neighborhood or any other kind of information) is delivered at this top layer. The Utility's head end, the Supervisory Control and Data Acquisition System (SCADA) responsible for the acquisition, processing, presentation and management of the data received, the Meter Data Management Systems (MDMS) responsible for billing customers according to their

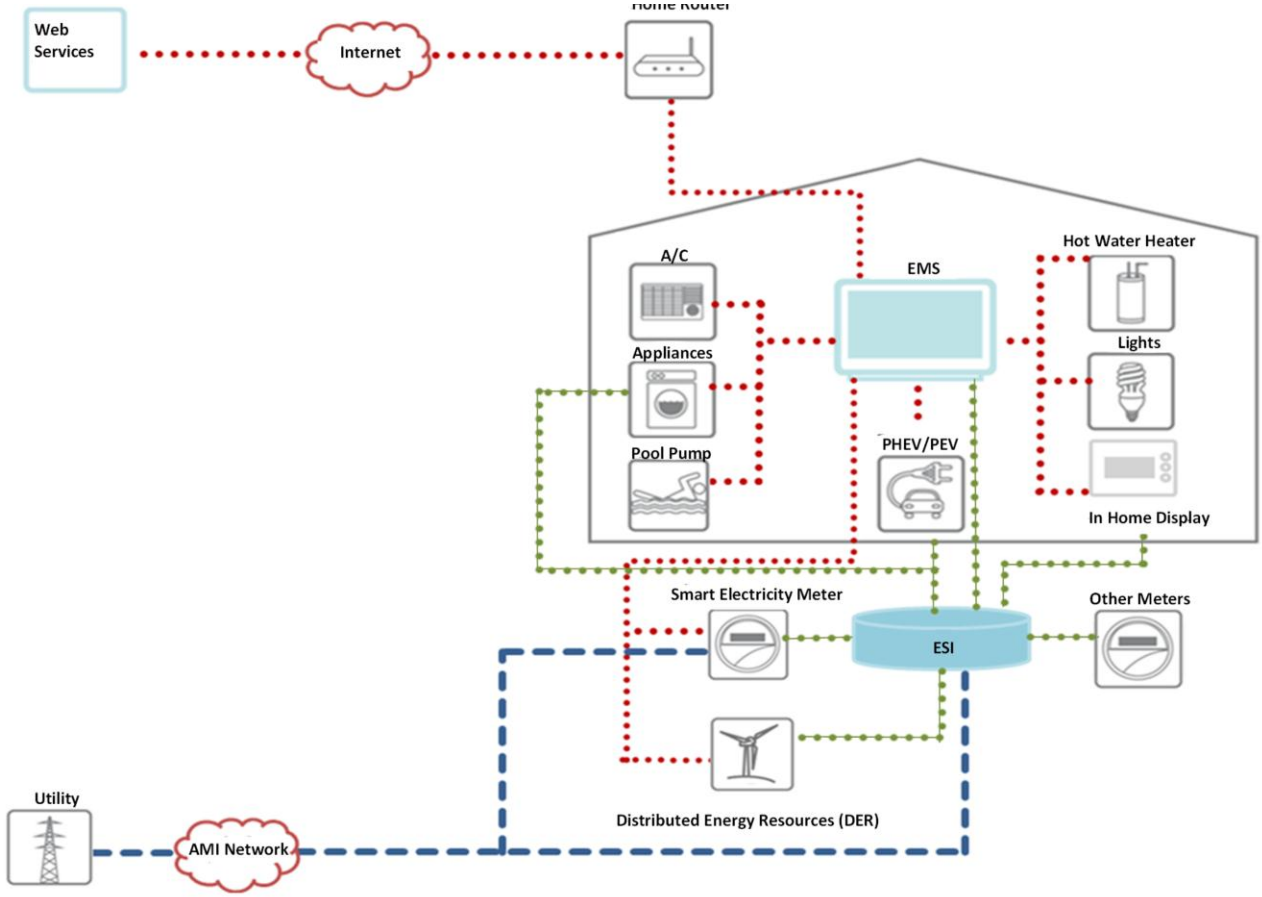


Fig2. An overview of a Smart Home's architecture, internal and external environments.

consumption, the Demand Response Management Systems (DRMS) and the Load Management Systems (LMS), the Outage Management Systems (OMS) and the Customer Information Systems (CIS), can all be found at this layer [3]. In addition, bulk generation, distributed generation, transmission networks, distribution networks, energy markets and service providers are also considered part of this upper layer.

B. Smart Home Architecture

The Energy Aware Smart Home is expected to be in constant interaction with its internal and external environments. The external environment of a Smart Home consists of all the entities belonging to the Smart Grid and the single entity responsible for the interconnection of the Smart Home with the Smart Grid. The internal environment on the other hand, consists of all appliances and devices belonging to the Smart Home, which are centrally managed by an entity in it. Both the internal and external environments are represented by specific entities within the Smart Home network [12]. An entity known as the Energy Services Interface (ESI) represents the "external environment" whereas an entity known as the Energy Management System (EMS) represents the "internal environment". The ESI (Fig.2) is the interface between the Smart Home and the Smart Grid. It enables the remote control of devices, the support of Demand Response programs, the monitoring of Distributed Energy Resources such as wind turbines belonging to premises, the forwarding of consumption data to the neighborhood collection points (if it acts as a meter), Plug in Electric Vehicles/ Plug in Electric Hybrid Vehicles (PEV/PHEV) charging etc.

Despite their logical separation the ESI and Smart Meter functionalities can be integrated in one physical device due to cost considerations. The EMS (Fig.2), on the contrary, is the system that enables the management of various appliances and systems within the Smart Home, so as to help the Smart Home adapt its energy profile to suit the grid's capabilities. Of special interest to us, are the appliances controlled by the EMS that are part of the category of Large Controlled Loads [13] such as washing machines and air-conditioning systems whose operation significantly burdens the grid, but can be postponed to a later time when the grid's resources are less constrained. Also controlled by the EMS are thermostats, light switches, pool pumps and PEVs.

Figure 2 illustrates the ESI and EMS along with the entities connected to them. The green dashed-dotted lines represent the entities connected to the ESI whereas the red-dotted lines represent the entities connected to the EMS. The blue dashed line represents the communication between the Smart Home and its external environment.

The ESI and EMS are in continuous two way communication ensuring that the internal environment is acting in accordance with the external environment's requirements and capabilities.

C. Benefits arising from Smart Home – Smart Grid interaction

As illustrated in Fig.2 (blue dashed lines) the Smart Home can communicate with its external environment in two ways. Either through the Smart Meter or through the ESI. In the former case the Smart Meter communicates with the NAN aggregator to report household consumption. In the latter, the ESI is responsible to enable various other interactions between the Smart Home and the Utility such as remote load

control. Through the EMS, Web Services are made available to the Smart Home, enabling among other things the remote configuration of HAN devices.

The integration of the Energy Aware Smart Home to the Smart Grid assuredly leads towards the successful meeting of some of the Smart Grid's major goals. Some of the most illustrative benefits resulting from this interaction are: demand response programs; load shedding programs; effective feedback; peak shaving capabilities; and energy exchanges.

1) Demand Response Programs

A Demand Response Program is essentially an agreement between the utility and its customers, promising the customer reduced tariffs or discounts in the end-of-month electricity bill, provided that he agrees to reduce his electricity consumption in response to signals received by the grid. The underlying concept is that when all customers each conserve a little, there will be enough power for everyone [14]. Today, there exists a plethora of different Demand Response programs, each of which has its own policies in terms of rewards, penalties, consumer notification policies (eg. day-ahead, day-of) and consumer cooperation bases (voluntary /mandatory). Whatever their specific characteristics however, the benefits of these programs, are still the same in principle and include a better matching of supply and demand that leads to a more reliable grid operation.

2) Load Shedding Programs

As in [15], Load Shedding is the terminology we use to describe the intentionally engineered switching off of electrical supply to parts of an electricity grid that happens under emergency situations as a last resort to protect the grid from suffering permanent damage. Emergency situations that could trigger Load Shedding regimes mostly include shortfalls in supply that require an immediate drop in demand before the demand-supply imbalance jeopardizes the stability of the grid.

Load Shedding usually happens in two ways, either automatically or selectively [16]. Automatic load shedding usually occurs as a result of concurrent failures of vital elements in the electrical grid and aims at isolating the part of the grid that faces the failure from the rest of the grid, to avoid a cascading event. Selective load shedding on the other hand, occurs when time is available to make selective choices on which customers can be shed. In such cases, priorities assigned to different feeders along the grid help minimize the impact of load shedding. Usually areas that have a residential, commercial or industrial customer mix and no specific critical infrastructures, are assigned a lower priority whereas feeders that supply infrastructures of critical importance such as hospitals, airports, sewerage and water pumping stations are assigned higher priorities. Higher priority areas are always the last to be affected and the first to regain power supply for apparent reasons.

3) More effective feedback

According to [17], "The effectiveness of feedback on energy consumption", a substantial percentage of domestic energy wastage of every household can be attributed to the lack of proper feedback. Through this survey it becomes apparent that the reason why consumers cannot actively participate in the effort for energy conservation lies in the fact that they only have a vague idea of the amounts of energy they are using for different purposes in their daily lives. As the author's study suggests effective feedback can change this as it can render energy more visible and therefore easier to manage and control. However, not all sorts of feedback are considered effective. As Kempton et.al. mention in [18] the end-of-month bill is such an example. Although it mentions our overall consumption and how much we are charged for it, it seems that the electricity bill alone cannot help us conserve energy, because it does not reveal where the majority of energy was spent. On the other hand, "Social Electricity" [19] a Facebook energy-awareness through-social-comparisons application which allows electricity footprint (provided through bimonthly electricity bills) comparisons with friends / neighborhood / town / country was shown to have been beneficial in reducing electricity consumption, with suggestions of much greater reduction if real time information were available.

Undoubtedly, the constant interaction between the Smart Grid and our Energy Aware Smart Home, will allow for a more effective feedback. Pricing signals indicating the electricity tariff at any given time will arrive at our homes, allowing our devices to inform us instantly about the amount of energy (in terms of money) that will be spent if a certain device gets switched on at a specific moment. Such detailed view of energy consumption is expected to give the consumer a better understanding of his energy usage patterns and the impact his decisions have on his end-of-month electricity bill, thus helping him make better informed decisions that will benefit not only his pocket but also the grid.

4) Peak Shaving Capabilities

An equally valuable benefit that the Smart Home and Smart Grid interaction has to offer is the introduction of dynamic pricing schemes that enable charging energy according to the time of use and current demand. Such schemes allow customers to benefit from lower rates when using energy during off-peak hours and result in a better distribution of demand due to shifting part of it from peak to non-peak hours, a process known as peak shaving [20].

5) "Energy exchanges"

Yet another benefit resulting from the two way communication between the Smart Home and the Smart Grid is the fact that the Smart Grid consumer has the option to become an energy producer too. By installing distributed energy resources at his premises, the customer can generate, store and sell energy back to the Grid. Such a prospect, promises to open up the energy market allowing for "energy exchanges" to be created, where energy will be bought and sold in prices governed by the forces of supply and demand [21].

III. SECURITY ISSUES IN THE SMART HOME AND THE SMART GRID

Having just exposed some of the most vital benefits arising from the interaction of Smart Home and Smart Grid entities, we can now further appreciate the importance of communication amongst the entities of this critical infrastructure. What we should notice however, is that as the connectivity amongst the different entities of the Smart Grid and/or the Smart Home increases, the challenges also increase; especially those challenges relative to system security. Thanks to its critical nature, the Smart Grid can

easily become a prime target for terrorists, hackers and vandals aiming to cause anything from a simple discomfort to havoc. Therefore, it is imperative that we start focusing on ways to safeguard its reliable operation and fulfill its security goals.

A. Smart Home/Smart Grid security objectives

Clearly describing the security goals the Smart Home/Smart Grid environment is expected to meet, serves as our first step in the effort for ensuring unfailing and consistent Smart Grid operation. For the purposes of this paper, we consider the six commonly adopted goals described below [13] [22-23] as the most important for Smart Home/Smart Grid security. These goals are:

Confidentiality: *the assurance that data will be disclosed only to authorized individuals or systems.*

Integrity: *the assurance that the accuracy and consistency of data will be maintained. No unauthorized modifications, destruction or losses of data will go undetected.*

Availability: *the assurance that any network resource (data/ bandwidth/equipment) will always be available for any authorized entity. Such resources are also protected against any incident that threatens their availability.*

Authenticity: *the validation that communicating parties are who they claim they are, and that messages supposedly sent by them are indeed sent by them.*

Authorization: *the assurance that the access rights of every entity in the system are defined for the purposes of access control*

.

Non repudiation: *the assurance that undeniable proof will exist to verify the truthfulness of any claim of an entity.*

B. Security Attacks

Security threats within the Smart Home/Smart Grid environment usually attempt to compromise one or more of the security goals we just described. These threats can be classified into two broad categories.

In the first category, namely "passive attacks", we place attacks attempting to learn or make use of information from the system without affecting system resources. In other words, in passive attacks the adversary intends to obtain information being transmitted not to modify it but to learn something from it. Passive attacks can take the form of eavesdropping or traffic analysis. By eavesdropping we refer to the unauthorized interception of an on-going communication without the consent of the communicating parties. By traffic analysis we refer to something subtler. Instead of trying to get hold of message contents, like in an eavesdropping attack, in traffic analysis the adversary monitors traffic patterns in order to deduce useful information from them. Both of these attacks are considered difficult to detect since they do not alter data. Thus, in dealing with them our focus is on prevention rather than detection.

The second category, namely "active attacks", is the category where we place those attacks attempting to alter system resources or affect its operation. Active attacks can involve some modification to data or the introduction of fraudulent data into the system. The most common amongst these attacks are masquerading, replay, message modification, denial of service and malicious software. A masquerading attack takes place when an intruder pretends to be a legitimate entity to gain privileges. A replay attack involves the passive capture of messages in a communication and their retransmission to produce an unauthorized effect. A message modification attack, involves the alteration of the contents of a legitimate message or the delaying or reordering of a stream of messages, aiming to produce an unauthorized effect. A denial of service attack aims to either temporarily or permanently interrupt or suspend the availability of the communication resources of a system. Finally, malicious software attacks, are attacks aiming to exploit internal vulnerabilities to modify, destroy and steal information or gain unauthorized access to system resources.

All the above mentioned threats and many more subcategories of these will be identified for the Smart Home/Smart Grid environment in the sections to follow. The security requirements they violate as well as an impact evaluation will also be presented.

C. Impact evaluation

For the assessment of the criticality and sensitivity of certain interactions and the evaluation of the impact level of threats against those interactions within the Smart Home/Smart Grid environment, we adopt FIPS 199, impact level assessment criteria [24]. FIPS199 characterizes potential impact of threats as Low, Moderate or High. Where the potential impact is said to be:

Low (L), if the violation of one or more of the security goals described above can be expected to have a **limited** adverse effect on Smart Home's/Smart Grid's operations, assets or individuals. Limited adverse effect could mean degradation of an entity's capability to efficiently perform its primary functions, minor damage to assets, minor financial losses or minor harm to individuals.

Moderate (M), if the violation of one or more of the security goals described above can be expected to have a **significant** adverse effect on Smart Home's/Smart Grid's operations, assets or individuals. Significant adverse effect could mean significant degradation of an entity's capability to efficiently perform its primary functions, significant damage to assets, significant financial losses or significant harm to individuals (not including loss of life or life threatening injuries).

High (H), if the violation of one or more of the security goals described above can be expected to have a **severe or catastrophic** adverse effect on Smart Home's/Smart Grid's operations, assets or individuals. Severe or catastrophic adverse effect could mean severe degradation or loss of an entity's capability to perform its primary functions, major damage to assets, major financial losses or severe harm to individuals (that could even result in loss of life or life threatening injuries).

D. Smart Home Security Issues

Describing the Smart Home in section II we made a conceptual separation between its internal and external environments. The EMS was presented as the main entity of the internal environment on which appliances, DERs and PEVs get connected to, report their consumption and receive on/off signals. The ESI was also presented as the entity that links the Smart Home with its external environment. Various interactions amongst Smart Home entities could become targets for a cyber or physical attack by an adversary or even by a mischievous customer. Below we introduce some of the most basic scenarios of interaction between entities within the Smart Home and discuss potential threats and their possible consequences. The scenarios are numbered using the notation SH_number. Each scenario refers to the interaction of entities within Smart Home followed by scenario's serial number. Table I provides a more concise view of the threats presented in each scenario of this section, the security goals violated and an impact evaluation. The attacks identified for each scenario are classified as derived from the networking domain (N) or derived by a Smart Home-introduced concept (SH).

1) SH_1 : Attacks threatening successful device energy-consumption reporting

Smart Meters within the Smart Grid, are expected to be able to provide detailed consumption information about the home they are connected to in 15-minute intervals (compared to one month as is the case with the traditional grid) [25]. Such a development becomes synonymous to the collection and transmission of greater volumes of consumption data from Smart Home appliances and creates a major risk against customer privacy. During the transmission of this data from appliances to the EMS an eavesdropping attack [26] by an adversary for example, could result in valuable consumption data leaking to the adversary who can then process them to infer a lot about a customer's lifestyle. Such processing of the data collected could mean passing them through a load profiling algorithm or through a use mode detection algorithm for example. In the first case an adversary can infer what devices are on at any given time (since each device has a distinctive load signature) [27]. In the second case specific information about the operation of the devices that are on can be revealed as well (eg. the channel a TV is tuned on!) [28]. By repeatedly collecting such information an adversary could actually intrude in a customer's private life (Low Impact), knowing when he wakes up, when he goes to sleep, when he leaves for work, in what room he is at any given moment, when nobody is at home, even where the customer travels to (by collecting charging data from his PEV). This information could help an adversary plan more severe attacks against a customer (burglary, theft, kidnapping) (Moderate Impact). Presence information can also be inferred through traffic analysis attacks that do not reveal the data as such but their sending patterns (devices that are on send consumption messages more often) [22].

Other potential attacks could include message modification attacks or replay attacks. Under such attacks, the adversary could insert new or replay older consumption messages of an appliance to the EMS, so that the Smart Meter receives false consumption data, resulting in the financial burdening of a customer for energy he hasn't consumed [26] (Low Impact). EMS impersonation attacks are also a possibility under this scenario. Under such attacks, the adversary impersonates the EMS, so as to receive a device's consumption data, and then sends those messages either intact or modified to the Smart Meter and replies with acknowledgements back to the appliances.

2) SH_2 :Attacks aiming Energy Import/Export signals at the ESI/HAN

As we mentioned above, the Smart Grid gives the consumer the opportunity to become a producer of energy as well as a consumer. By installing distributed energy resources at his premises, a customer can generate energy which he can sell to the grid at times when the demand surpasses the supply. Furthermore, by using his plug in electrical vehicle as a battery, a customer not only can store but also import energy from the grid at urgent times. Thus protecting it from damages caused by overloading. Messages requesting the exporting of energy to the grid/or the importing of energy from the grid, arrive to the ESI/HAN from the Smart Grid. The ESI/HAN then processes those messages and forwards suitable commands to PEVs and DERs.

Possible threats under the aforementioned scenario are presented on Table I and might involve for example an ESI/HAN impersonation by an adversary. Under such a scenario the adversary impersonating the ESI/HAN, might receive the energy export/import signals from the grid and drop them so they never reach the PEVs or DERs. An attack, that could cause significant grid instabilities, should it reach massive proportions (Moderate Impact). Another possible threat with similar outcomes could occur if a message modification attack against the integrity of the export/import signals, occurred [22]. Altering the contents of messages, either by increasing the amount of energy to be discharged from houses to the grid, or by decreasing the amount of energy to be absorbed from the grid could, if massive, cause the grid to be unstable. In such a circumstance Demand Response or Load Shedding processes could be triggered even when they are truly unnecessary (Moderate Impact). Replay attacks requesting energy discharging at times of grid overloading and energy import at times of higher demand can cause analogous trouble (Moderate Impact). ***Repudiation*** is also an important threat under this scenario since we expect the customer to be collaborating with an ESP for the management of his DERs due to his lack of experience. In such a case the customer should not be able to suggest that his ESP did not react when it should have/ or reacted when it shouldn't have.

3) SH_3 : Physical meter tampering/ reversal or removal

Physical meter tampering incidents are common even in the era before Smart Grids [23][29]. With the meters becoming smarter we expect more incidents of physical meter tampering or fiddling with meter software to occur. Mischievous customers, trying to remove the meter, reverse the meter or alter its software, in an effort to relieve themselves from paying for their electrical bills, could become a common case in the Smart Grid future (Low Impact).

4) SH_4 : Attacks against remote home monitoring and control.

Potential threats under such a scenario as presented on Table I, could include client impersonations by an adversary, message modification attacks, replay attacks etc. In a client impersonation attack [30], for example, an adversary impersonating the client could send messages to the ESI/HAN, requesting that all devices within the premise get switched on (thereby financially burdening the legitimate client- Low Impact), or that all devices get switched off (a scenario that could get life threatening connotations if life support equipment is included in those devices – High Impact) . Replay attacks and message modification attacks could also have significant implications on the Smart Home. The replay of a signal that operates the washing machine could result in clothes being rewashed again and again (Low Impact). Furthermore, the modification of a message to set the sprinkler into operation for 3 hours instead of 30 minutes could also have significant implications (Moderate Impact). These however, are not the only possible threats. Other kinds of attacks can occur as well. A device impersonation attack, carried out by an adversary, is one such example. In such an attack, the customer believes he is remotely controlling one device when in reality he controls another (for example, instead of setting the oven to 120°C , one could set the sauna's temperature to 120°C – automatically risking the lives of anyone in it – High Impact). Non-repudiation is also of particular importance to this scenario where we need ensure that no customer will be able to prove not sending a remote control message when he has, or sending one when he hasn't.

5) SH_5 : Attacks aiming the requests for energy usage data.

The customer within the Smart Home, can request at any given time, to receive his detailed energy consumption profile. Consumption information are gradually collected by Smart Meters within the Smart Home, that are responsible to forward it to the MDMS system of the head end, which processes the metering data to apply billing information on them. The MDMS communicates with the CIS to store consumption information about each customer, which can be sent to him, upon request, along with feedback and suggestions [30]. Possible threats under such a scenario, are also presented on Table I and include customer impersonation attacks by adversaries wishing to gain an inside to the consumption of legitimate customers (for reasons mentioned above), eavesdropping attacks (during the forwarding of CIS/MDMS to the In Home Display of the consumer) and also message modification attacks (requesting more detailed information).

E. Smart Grid security issues

Having described possible security issues that could occur under the interaction of entities belonging to the Smart Home, we now move on to describing possible security issues that could affect Smart Grid entities with an impact on the Smart Grid as such. Below, we discuss potential threats and their possible outcomes, under some scenarios where Smart Grid entities could become attack targets. The scenarios are numbered following the symbolic notation SG_number, implying the scenario refers to an attack aiming at entities within the Smart Grid followed by the scenario's serial number. Table II provides a more concise view of the threats presented within each scenario described in this section, the security goals violated, and an impact evaluation.

We start by presenting three scenarios involving attacks against the Smart Grid's head end servers each of which aims to achieve a different blow to the head end [29].

TABLE I
SMART HOME SECURITY ISSUES

Scenario num:	Possible Threads	Security Goals Compromised	Degree of Impact
SH_1	Eavesdropping (N) Traffic Analysis (N) Message Modification (N) Replay Attack (N) EMS Impersonation (SH)	Confidentiality Integrity Authenticity	L-M
SH_2	Repudiation (N) Message Modification(N) Replay Attack (N)	Non repudiation Integrity Authentication	M
SH_3	Tampering/Reversal/ Removal of Meter (SH) Illegal Software Modification/Update(SH)	Authentication Integrity	L
SH_4	Customer Impersonation (N) Device Impersonation (SH) Message Modification(N) Replay attack(N) Repudiation(N)	Integrity Non repudiation Authentication	L-H
SH_5	Customer Impersonation(N) Eavesdropping/Message(N) Interception (N) Message Modification(N)	Confidentiality Integrity Authenticity	L-M

1) SG_1 : Attacks aiming to steal data from utility servers.
2) SG_2 : Attacks aiming to take control of utility servers.
3) SG_3 : Attacks aiming to take down utility servers.

All three scenarios described above, place Smart Grid's head end servers as their primary target, aiming to either *gain valuable information about the system* or *access into it*, in order to steal data from it, take control over it or take it down. Collecting valuable information about the system, enables the adversary to plan a targeted attack against it whilst gaining access into the system, gives the adversary the opportunity to interact with it in any way he wants.

One way of collecting valuable information about the system could be by exploiting publicly available information about the utility through the Internet [26]. Such information, if used in a smart way could give the adversary precious inside to help him plan an attack specifically targeting a weakness of the system. For example, Sean Gorman's thesis [31] is now considered a classified document of the U.S government. It presents the mapping of every company in America's industrial sector on the US's optical fiber network, a mapping purely carried out using publicly available information as found on the Internet! A similar mapping within the Smart Grid could result in a detailed Smart Grid blueprint for everyone wishing to attack such a complex system(Moderate to High Impact).

Alternative ways of gathering information about the system, could include port scanning or ping sweeps, using freely available software such as Nmap, to reveal information about active hosts, network services they are using, the operating systems they are running etc. Moreover, vulnerability scanners such as Nessus could also be used to

help the attacker gain knowledge regarding the system's weaknesses, exposing operating system vulnerabilities, bad network design that does not ensure proper isolation or poorly defined firewall rules that could be exploited for the purposes of an outside attack [32] (Moderate to High Impact).

Attacks against the Smart Grid though can also be perpetrated from the inside. Such attacks can be carried out by disgruntled employees who have both the knowledge and the motive to do harm to the Smart Grid's head end, or by any other adversary who manages to gain access to the Smart Grid's head end by exploiting social engineering attacks or weak platform configurations [26][33]. By weak platform configurations we refer to poorly defined policies resulting in superfluous access rights being given to users, unsuitable or non-existent authentication mechanisms, poorly defined password policies that could result in easy-to-break passwords, data (eg. passwords) being transferred unencrypted through the network raising the chances of leakage due to sniffing etc.

Having collected information about the target system or having ensured a way to gain access to it, is the first step of many possible attacks against the Smart Grid head end. Such attacks could include system infections by malicious software and denial of service attacks. In fact, incidents of SCADA system infections by malicious software have already been reported several times in the past few years [34-36] with Stuxnet, Flame and Duqu being infamous examples. The tremendous capabilities of this kind of software pose a major threat against any system within the Smart Grid. Such software can often modify or delete system files necessary for the system to operate, thus putting its availability at risk with severe consequences (High Impact). At the same time, non-system files such as log files, billing files, Load Shedding prioritization files could also serve as targets for modifications. By modifying a log file for example, an adversary could cover up his trace or frame an individual by implanting false evidence against him(Moderate Impact). By modifying load shedding prioritization files on the other hand, the implications could be even more severe. Fiddling with the degree of criticality of different areas could result in high-risk areas losing power supply in cases of emergency. A scenario, which could easily result in the loss of human life (High Impact). Of course, the capabilities of malicious software are not limited to those we just mentioned. Further features, such as key logging capabilities, conversation recording capabilities, come to add to this already powerful set of capabilities that can provoke irrevocable damage (High Impact).

Denial of Service attacks are also possible in such systems, and are considered to be amongst the most dangerous ones, since they could compromise network availability [26]. Such attacks could be the result of any effort to saturate the system's resources to an extend where it can no longer respond to its legitimate traffic due to heavy overloading, something that could have severe or catastrophic outcomes for the grid (High Impact).

4) SG_4 : Attacks against wide area measurement equipment.

Despite the fact that many attacks could affect the entities mentioned above, almost none of them can have comparable impact to a false data injection attack [37-38]. That is, an attack where adversaries manipulate measurements of field devices and metering devices in the Smart Grid network, introducing errors to those measurements destined for the head-end. False measurements going through the state estimation algorithm obviously result in a state estimation that has nothing to do with the actual state of the grid. As a result, the head-end, being ignorant to Smart Grid's actual state, reacts according to its perceived state, triggering Load Shedding or Demand Response programs at wrong times, wrongly estimating the demand of the next day thereby increasing the chances for instabilities or rolling blackouts etc. [33] (Moderate to High Impact).

TABLE II
SMART GRID SECURITY ISSUES

Scenario num:	Possible Threads	Security Goals Compromised	Degree of Impact
SG_1	Publicly available info Weak platform config. Software vulnerabilities Malware Insider attacks	Confidentiality Integrity Availability Authorization Authenticity	M-H
SG_2	Publicly available info Weak platform config. Software vulnerabilities Malware Passive Net Recon. Message Fabrication Replay attacks Fiddling with system/non system files	Confidentiality Integrity Availability Authorization Non repudiation Authenticity	M-H
SG_3	Eavesdropping Traffic Analysis Man-In-The-Middle Message Modification Replay Attack Device Impersonation Denial of Service Fiddling with system/non system files	Confidentiality Integrity Availability Authenticity Authorization	H
SG_4	False Data Injection Attacks Malware	Integrity Availability	M-H

F. Smart Home /Smart Grid Security Issues

Having acquired a more comprehensive view regarding threats to both the Smart Home and Smart Grid as individual elements, we can identify some of the main threats that aim at their interaction. This section is dedicated to threats initially affecting or taking control of entities within the Smart Home that end up affecting entities within the Smart Grid. The scenarios presented in this section are thus numbered following the symbolic notation SH-SG_number, standing for Smart Home initiated attacks affecting the Smart Grid followed by the scenario's serial number. Table III provides a more concise view of the threats presented within each scenario of this section, the security goals violated and an impact evaluation.

1) SH-SG_1: Attacks aiming the Demand Response signals at the ESI/HAN

Under such a scenario an adversary could choose to impersonate the ESI/HAN so as to intercept the Demand Response signals intended for it, in order to replace them with older ones (as part of a replay attack). An adversary can also modify signals received by the ESI/HAN (as part of a

message modification attack), before they are forwarded to the EMS or to the appliances/PEVs and DERs they are supposed to reach. These attacks could trick the ESI/HAN into issuing inappropriate signals towards the EMS or the appliances and could mislead the customer through false notifications via the In Home Display (regarding the tariffs or the urgency of DR signals received – Low Impact). As a result, appliances could be scheduled to operate at times when the Smart Grid is overloaded, thus further increasing the grid's load (Low to Moderate Impact) and also financially burdening the customer.

In addition to the aforementioned, another kind of attack aiming to disrupt the communication between the ESI/HAN and the appliances or the ESI/HAN and the EMS could occur under this scenario. This attack, known as jamming attack [13], is carried out by an adversary who introduces noise in the wireless medium connecting the ESI/HAN with the EMS or the appliances, aiming to reduce the strength of the carried signal (Signal to Noise Ratio – SNR). Should such an attack be successful the Demand Response server cannot communicate with its clients, thus the operation of devices cannot be rescheduled and people cannot receive proper feedback thus continue operating their devices regardless of the grid's state (Moderate).

Potential attacks under this scenario, can also be launched by the customer. More specifically, a mischievous customer who has agreed to participate in a Demand Response Program could decide to carry out a device impersonation attack so that he never has to postpone using his devices for later. By having for example his electric kettle impersonate his tumble dryer the signal received at the customer's premise for rescheduling the operation of large controllable loads (including the tumble dryer) will affect the electric kettle instead, without the utility realizing the difference. Such an attack "benefits" the customer who gets rewarded for his participation but can use his devices without any limitation. However this harms the Smart Grid, that expects to shave the peaks in demand but does not get the anticipated outcome (Low to Moderate Impact depending on scale).

Finally, repudiation incidents are also possible under this scenario. A client for example, could deny having received a Demand Response signal to explain the reasons he did not participate in the program and avoid the incurred penalties.

2) SH-SG_2 : Attacks threatening successful Outage Reporting.

Potential threats in this case could refer to meter impersonation attacks by an adversary, followed by a replay attack. In such a case, older messages (power outage reports) sent to OMS are replayed even when there is no interruption to service so that personnel is dispatched to specific areas when there is actually no need [30]. Such tasteless "jokes" are undoubtedly a hassle to the utility that makes every effort to ensure quality of service for its customers (Low Impact).

3) SH-SG_3 : Attacks threatening successful DER shutdown/isolation reporting

Meter impersonations, replay attacks and message modification attacks are only some of the possible attacks under this scenario. By impersonating the meter, the adversary can drop packets destined for it and replace them with older ones (he has intercepted and/or modified) or new ones (he has created), thus making the meters report a false/inaccurate outcome to the grid resulting in a distorted image of the grid's state being conveyed to its operators and thus to the personnel dispatched to handle the situation, with none of them knowing whether any errors occurred during shut down or islanding processes (Low to Moderate Impact depending on scale) .

4) SH_SG_4 : Attacks against the NAN aggregator.

Attacks under this scenario could involve either the passive interception of data to be transferred from the ESI/HAN to the Smart Meter (and from then on to the NAN aggregator), or an active modification of existing data/injection of new data in the grid. In the former case, we refer to an eavesdropping attack that invades customer privacy and exposes the kinds of communication protocols used, something that could help the adversary plan and carry out a meter impersonation attack injecting false traffic in the grid, with known consequences [39] (Low to Moderate Impact).

In the latter case, we refer to message modification attacks and false data injection attacks that could result in erroneous data being transferred to the head-end giving it an inaccurate view of the Grid's current state [40] (Moderate to High Impact). Man-In-the-Middle attacks, where the adversary impersonates the meter to the NAN aggregator and the NAN aggregator to the meter, are also likely to occur. Such attacks, give the adversary the complete control of all metering traffic flowing to the NAN aggregators (and thus to the grid) putting the Smart Grid at great risk (especially when being large-scale). Finally, Denial of Service attacks, aiming to overload the NAN aggregators until they can no longer receive their legitimate traffic, are also a possibility under this scenario (Moderate to High Impact).

TABLE III
SMART HOME TO SMART GRID SECURITY ISSUES

Scenario num:	Possible Threads	Security Goals Compromised	Degree of Impact
SH_SG1	ESI Impersonation Message Modification Replay Attacks Jamming Attacks Device Impersonation Repudiation	Integrity Availability Authenticity Non Repudiation	L-M
SH_SG2	Meter Impersonation and Replay attack	Integrity Availability Authenticity	L
SH_SG3	Meter Impersonation / Message Modification Replay attack	Integrity	L-M
SH_SG4	Eavesdropping Message Meditation ManInTheMiddle False Data Injection Denial of Service	Integrity Confidentiality Authenticity	L-H

G. Smart Grid to Smart Home security issues

The last category of threats we are going to present are the threats that start by affecting entities within the Smart Grid , and evolve in ways that affect the environment of the Smart Home. The scenarios presented in this section are numbered following the symbolic notation SG-SH_number, standing for Smart Grid initiated attacks affecting the Smart Home followed by the scenario's serial number. Table IV provides a more concise view of the threats presented in each scenario of this section, the security goals violated, and an impact evaluation.

1) SG-SH_1 : Attacks aiming Demand Response signals to the ESI/HAN

Possible attacks under this scenario, as illustrated in Table IV, could include the impersonation of the DRMS system by an adversary, who could then repeat older Demand Response messages as part of a replay attack. Such an attack could cause discomfort at the customer site and result in the financial burdening of the customer (Low Impact), primarily due to the fact that ESI/HAN and EMS systems responding to the Demand Response signals will schedule device operation at different times that are not necessarily the most profitable for the customer or the most beneficial for the Grid (Moderate Impact). Another possible attack under this scenario, could be a message modification attack. Under this kind of attack the adversary modifies the contents of messages created by the DRMS server (such as the pricing signal or the urgency) and forwards these messages to the customer site that reacts as described above(Low to Moderate depending on scale). False synchronization attacks are also probable under this scenario. This kind of attacks aim at fiddling with synchronization messages exchanged between DRMS and ESI/HAN and result in stringent timing requirements not being met by the system due to poor synchronization, with consequences affecting the entire Demand Response program(Moderate Impact).

2) SG-SH_2 : Attacks aiming Direct Load Shedding signals to the ESI/HAN

Sometimes, when the demand for electricity exceeds the available supply, planned supply interruptions in the form of load shedding, may have to be carried out in order to avoid instabilities in the grid that could damage its equipment. Such power supply interactions are triggered by an LMS server that is responsible for issuing and forwarding commands to premises at specific areas according to a predetermined schedule [25]. Denial of Service (DoS) attacks under such a scenario could prove to be particularly dangerous, since they can prevent these urgent signals from being delivered to destination on time, thus putting the grid's availability at risk (High Impact). DoS attacks could target either the LMS server or the physical medium connecting it to the ESI/HAN (if they take the form of jamming attacks)

A different kind of attack could involve the fiddling of an adversary with Load Shedding schedules which could result in critical areas losing their power supply, or the same non-critical areas being affected again and again. The consequences of such attacks could range from simple discomfort of customers (Low Impact) that have to lose their power supply over and over again, to the power loss in critical areas that could even put human life to risk (High Impact). Similar consequences could be observed under a replay attack, carried out by an adversary replaying older Load Shedding signals.

3) SG-SH_3: Attacks aiming Energy Import/Export signals to the ESI/HAN

DER encompasses both generation and storage. Generation coming from DER units such as photovoltaics, wind turbines, diesel generators and small hydro plants situated at the customer's premises are expected to be controlled by the utility or a third party ESP via the AMI system. Depending on the capabilities of the DER controller, schedules for net import/export levels can be predetermined so that units successfully discharge energy into the grid at times of increased demand or store energy from it in case load shifting from on-peak to off-peak hours needs to take place.

Replay attacks are amongst the attacks more likely to occur under such scenarios [30]. In this kind of attacks former messages for energy import/export are replayed, regardless of the needs of the grid, causing energy to be drawn from the grid at times of high demand, or energy being released to the grid at times when it is not necessary (Moderate to High Impact). Also likely to happen under this scenario, are message modifications attacks. These attacks are launched by an adversary that distorts messages containing the amounts of energy to be exported or imported causing the grid to behave in ways contrary to its true needs and creating the opportunity for brownouts and blackouts to occur (Moderate to High Impact). Similar outcomes could be observed by carrying out DoS attacks against the channel between the DRMS/LMS and the ESI/HAN, so as to render it incapable of forwarding its signals on time, to its legitimate receivers (Moderate to High Impact).

4) SG-SH_4 : Attacks aiming customer related data forwarded to a third trusted ESP

Highly probable attacks under such a scenario, could involve the impersonation by an adversary of the third party ESP or eavesdropping, in order for the adversary to receive the energy consumption and urgency messages destined to the third party ESP from the utility. Thus, violating customer privacy (Low to Moderate Impact according to what these data are used for) and potentially disrupting the communication of the utility with the third party ESP, preventing it from acting to the advantage of the customer.

TABLE IV
SMART GRID TO SMART HOME SECURITY ISSUES

Scenario num:	Possible Threads	Security Goals Compromised	Degree of Impact
SG_SH1	Message Modification Impersonation of DRMS/LMS Replay of Previous Messages False Synchronization Attack	Integrity Authenticity	L-M
SG_SH2	Denial of Service attacks Access the DRMs/LMS server False synchronization attack Replay attack	Availability Integrity Non repudiation Authenticity	L-H
SG_SH3	Replay attack Message Modification Attack Denial of Service attacks	Authentication Integrity Availability	M-H
SG_SH4	ESP Impersonation Eavesdropping	Integrity Authenticity Confidentiality	L-M

IV. SMARTHOME/SMART GRID SECURITY COUNTERMEASURES

In this section, we present several promising countermeasures suggested in literature which could be adopted against the different attacks identified in section III. As tabulated in Tables I to IV, several security goals are compromised. In the following section we see how each of

these goals may be fulfilled through a detailed survey of approaches and a comprehensive description of various techniques. A summarized view of the approaches presented in this section is provided in Table V.

A. Ensuring Confidentiality and Privacy

In section III we introduced Confidentiality as the security dimension concerned with preventing unauthorized access to specific information. Confidentiality might not be considered as the most critical dimension of Smart Grid Cyber Security; however it is one of the key concerns for the consumers as it is inextricably linked to their privacy. This section is devoted to presenting ways of ensuring confidentiality and privacy within the Smart Home/Smart Grid communication environment, as they are proposed in recent literature.

1) Ensuring Confidentiality

The most basic technique of achieving confidentiality nowadays is through cryptography. Modern cryptographic techniques available today, can be classified into two broad categories according to the type of key they use. The first category, includes symmetric key algorithms and it is also known as private-key cryptography, since both sender and receiver share a secret key for their communication. The second category includes asymmetric key algorithms and it is also known as public key cryptography since each of the communicating parties has its public key (known to all other parties) and its private key (which is kept secret)[41][42].

In an effort to ensure greater interoperability amongst security mechanisms within the grid the Cyber Security Work Group of the National Institute of Standards of the U.S evaluated (in 2010) the usability and expected lifespan of known symmetric and asymmetric algorithms [25]. Symmetric algorithms (such as the standards AES and TDES) are expected to be used for the purpose of data encryption within the Smart Grid. Asymmetric algorithms on the other hand, (such as the approved RSA, DSA, ECDSA etc.) are expected to be used for the purpose of digitally signing messages.

Of course cryptography is not only used for the purposes of ensuring confidentiality. Many works presented below, regarding ways of providing integrity, authenticity, non-repudiation and even authorization, exploit cryptography in one way or another.

2) Ensuring Privacy

Since their appearance, smart metering deployments have raised numerous concerns for being potentially privacy invasive. As we discuss in the previous section, the consumption data collected by smart meters can reveal a lot about the behavior, activities and habits of the residents within a premise, thus causing fear to customers. To date, various models have been proposed for ensuring the privacy of metering data within the Smart Home/Smart Grid environment. Our literature review regarding privacy enhancing technologies has revealed a variety of techniques that can be used alone or in combination to ensure privacy [43]. Some of these techniques are briefly introduced below.

Ensuring privacy can be achieved through:

- **Anonymization :** A process that removes the link between data and its origin in such a way, that the utility can receive the data it requires for carrying out its computations, but cannot attribute the received data to a specific meter.

- **Trusted Aggregators :** The meter or a third trusted party are considered to be trusted entities that can handle the aggregation of metering data and their forwarding to the utility. The utility in such a case can use only the aggregates of data without being able to have access to individual consumption information of participating meters.

- **Homomorphic Encryption:** A form of encryption that allows specific types of computations to be carried out on ciphertext and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext. The utility in such a case can decrypt the ciphertext of the aggregate of metering data but not the individual metering of the plaintext.

- **Perturbation models:** Models that introduce random noise from a known distribution to the privacy sensitive metering data, before they are transmitted to utility. The utility receiving the perturbed data reconstructs an approximation of the original data. A tradeoff between the level of privacy achieved and the loss of information exists.

- **Verifiable Computation models**: Models in which the aggregator provides a proof along with the aggregate of metering data, that the calculation has been performed as claimed. Such proof can be provided through a zero knowledge proof system, with the smart meter being the prover and the utility the verifier. In zero knowledge proof the verifier only confirms the prover has the knowledge he claims to have and nothing more than that.

- **Data obfuscation techniques:** Battery-based approaches that aim to conceal the amount of energy consumed by a premise by buffering or releasing their energy load.

We begin with work of Efthymiou et. al., [44], describing a method for securely anonymizing electric metering data. Their approach distinguishes amongst two types of traffic carried by a Smart Meter. Low frequency data i.e. data necessary for billing or account management purposes that need to be attributable and collected every day/week/month etc. and High frequency data, i.e. data needed for the efficient operation of the Smart Grid (Demand Response programs, demand estimation etc.), that should be collected every minute/five minutes but don't need to be attributable. The meters in this scheme have two IDs embedded within them, one for high and one for low frequency data.The low frequency ID (LFID) will be public, so that it can be used by the utility for billing a customer for his consumption. The high frequency ID (HFID) on the other hand has to remain hidden, so that no one will be able to identify the source of specific metering data. In order to maintain its secrecy, the high frequency ID should be hardcoded within the device whereas for the purposes of verifying an HFID is valid a

third party escrow service is introduced, knowing the relationship between a valid HFID and LFID.

A different protocol, combining anonymization techniques with verifiable computation without implying reliance on any gateway or Third Trusted Party is suggested by Jeske in [45]. His protocol essentially consists of two sub-protocols an Invoicing subprotocol, and a Load Reporting subprotocol. A smart meter uses the invoicing protocol to send the overall electric power consumption to the utility, encrypted and signed asymmetrically. During the invoicing process, the identities of both the customer and the meter are kept public. The Load Reporting Protocol, however exploits a different idea, namely group signature schemes. For the purposes of this protocol every smart meter is said to belong to a group (whose group manager is the energy provider). Whenever a meter wishes to report its consumption, it signs it using the name of the group. The energy provider can thus only verify the participation of a meter within a group, without being able to infer any further information about it specifically. The system utilized for group signatures is based on the model of Camenisch and Lysyanskaya [46]. In such a model once the meter has proven in a zero-knowledge manner that it holds a ticket signed by the provider and that the timestamp of the data it wishes to transfer is valid, it asks the provider to confirm its validity and sign the next ticket it will need.

An alternative approach is presented by Li et. al., in [47]. Their suggestion leverages a distributed incremental aggregation approach, where aggregation is performed on every meter in the route towards the utility. A carefully constructed aggregation tree efficiently connects all the nodes of an entire neighborhood to a collector device. Every node on this tree, which is essentially the spanning tree corresponding to the graph of the network of interconnected meters within a neighborhood, collects data from its children nodes, aggregates them and forwards them to its parent node, that repeats the process until the data reaches the root. At the root we find the collector, that handles the communication with the utility. To secure the data enroute, Paillier homomorphic encryption scheme is used, allowing for meters to participate in the aggregation process without being able to see any intermediate or final result.

Another idea is introduced by Acs et.al in [48], who propose their own privacy preserving scheme for smart metering data that uses homomorphic encryption and exploits the idea of perturbation. The encryption algorithm introduced by the authors is defined as the addition of the measurement with the encryption key, modulo a large number. Since this cryptosystem is homomorphic with respect to addition it follows that:

$$E(k_1, m_1) + E(k_2, m_2) = m_1 + k_1 + m_2 + k_2 \bmod n \quad (1)$$
$$= E\big((k_1 + k_2), (m_1 + m_2)\big)$$

Where k_1,k_2 are the keys, m_1 and m_2 are the measurements and n is the large number.

To make things quite simpler to understand, let's use an example. Let's suppose that Alice wants to communicate with Bob and Charli.e. Then both Alice and Bob have to feed a pseudorandom generator with their shared key, something that returns a random number $r_{1,2}$ that will be added to Alice's measurements and subtracted by Bob's measurements. The same process should then be repeated between Alice and Charlie resulting in $r_{1,3}$. After Alice has added $r_{1,3}$ to her results she will come to the sum presented below, which she will then send to the utility encrypted with their shared key.

$$E(K_{AliceUtility}, m_{1,t}) = m_{1,t} + r_{1,2} + r_{1,3} + K_{AliceUtility} \bmod n \quad (2)$$

Similarly Bob and Charlie will send their aggregates to the utility encrypted using the shared key each one maintains with the utility. The utility will then compute the aggregate and thus receive the sum of all the measurements that were sent to it.

$$\begin{aligned} Sum\ E(K_{AliceUtility}, m_{1,t}) + E(K_{BobUtility}, m_{2,t}) + E(K_{CharlieUtility}, m_{3,t}) \quad (3)\\ = (m_{1,t} + r_{1,2} + r_{1,3} + K_{AliceUtility} \bmod n\\ + m_{2,t} - r_{1,2} + r_{2,3} + K_{BobUtility} \bmod n\\ + m_{3,t} - r_{1,3} - r_{2,3} + K_{CharlieUtility} \bmod n)\\ = (m_{1,t} + m_{2,t} + m_{3,t} + K_{AliceUtility} + K_{BobUtility} + K_{CharlieUtility}) \bmod n \end{aligned}$$

The individual measurements are never revealed during this process. To maintain the privacy of the information the authors introduced Laplacian noise to the final aggregate before encrypting it. To succeed in doing so every meter that participated in the process introduced gamma noise on its measurement before encryption. Thus every $m_{i,t}$ presented above was actually the result of the addition of the actual measurement ($mo_{i,t}$) with two independent values randomly selected from the same gamma distribution :

$$m_{i,t} = mo_{i,t} + G_1(N, \lambda) - G_2(N, \lambda) \quad (4)$$

The final idea we present for the purposes of ensuring privacy, belongs to Varodayan et.al. [49], who propose the use of a rechargeable battery to partially protect the privacy of information derived from a premise's electrical load profile. This battery receives the aggregate load of all appliances within a household as an input, and outputs a load that is the result of the combination of the load of the battery and all the appliances. This is the load reported by the smart meter to the utility. At any given moment, the battery can either supply the energy it receives from the utility directly to the household's appliances, keep it for future use, or supply the appliances with its residue. Thus through this charging and discharging procedure the battery can obfuscate the exact load reported by appliances. The suggested model for charging and discharging the battery is stochastic, i.e. every decision for a state transition happens with a certain probability. A trellis algorithm is exploited to estimate the rate of information leakage.

B. Ensuring Integrity, Authenticity and Non Repudiation

Just as important as ensuring the confidentiality of personal data within the Smart Grid/Smart Home is to ensure data integrity and authenticity (regardless of their degree of privacy). This section is dedicated to presenting techniques of achieving these two key goals by reviewing related literature.

1) Ensuring Integrity

Inspired by traditional ways of ensuring integrity, cryptographic hashing techniques, designed for high integrity assurance in traditional networks could potentially be applied to the Smart Grid as well, provided they do not introduce

prohibitive delays. When using such techniques the sending side uses a hash function to compute the checksum of the message to be sent and attach it to the original message [41]. Upon receiving the message, the receiving side applies the same hash function to the message and compares resulting hash to the hash attached in the original message. Should the two hashes match, integrity is verified (i.e. it is proven that the message contents have not been altered in transit as a result of e.g. a message modification attack).

Attacks against integrity though are not only confined to message modifications. False data injection attacks, replay attacks, device impersonation attacks, and sparse attacks are also considered to be major threats against a system's integrity. Recent literature focusing on these attacks and their countermeasures may be limited; however it doesn't lack interesting ideas.

Bhattarai et.al in [50], present their own light weight digital watermarking technique as a simple, low-cost and efficient way to ensure defense against false data injection attacks. Digital watermarking is a technique of embedding digital data inside real time meter readings, with the watermark carrying unique information about the owner of the reading. The purpose of the watermark is to validate the integrity of data. Watermarked data, are sent from the meter to the utility through high speed unsecured networks that are prone to false data injection attacks. To ensure the successful detection of these attacks , the meters use low rate and secured channels to securely transmit the watermarks. The utility thus receives both the watermarks and the watermarked data, in order to correlate them and detect false data injection attacks.

Huang et.al. in [51], show that even without prior knowledge of the power grid's topology an adversary can still successfully launch stealthy bad data injection attacks. Specifically the authors prove that when the system dynamics are small and can be approximated linearly, an independent component analysis can be applied to calculate the Jacobian matrix that if multiplied by the eigenvectors of the covariance matrix of the state variables can expose information necessary to the adversary wishing to launch an unobservable false data injection attack. As a countermeasure, the authors introduce their adaptive cumulative sum algorithm, a recursive algorithm comprising of two interleaved stages. The first introduces the linear unknown parameter solver while the second applies the multi-threated CUSUM algorithm. The proposed defense mechanism aims at detecting attacks as quickly as possible with a minimum number of observations while maintaining a satisfactory level of accuracy.

Unobservable attacks involving the compromise of a modest number of power meter readings, specially designed and orchestrated to remain undetectable by bad data detection algorithms are the focus of Giani et.al in [52]. In their paper, the authors propose their own algorithm for detecting stealthy attacks and suggest the installation of known-secure phasor measurement units (PMUs) at specific buses, to thwart an arbitrary collection of attacks (not only sparse attacks). The minimum number of PMUs necessary to make the attacks observable is an NP-hard problem, thus the authors suggest an upper bound on the minimal number of PMUs required and present an algorithm to determine their placement. Their findings suggest p+1 PMUs are sufficient to disable p attacks.

As far as device impersonation attacks are concerned, Aravinthan et. al., suggest in [13], the use of load profiling algorithms as a countermeasure. In their suggested scheme, before an appliance can be put into operation, it seeks a permission from the AMI. The AMI either allows its operation or reschedules it for later according to the advertised class of the device and its current load. Every time a device is advertised to the AMI the AMI sends a previously formed load profile of that device to the outlet controlling the device so that a comparison can be made. If the loading pattern does not match the known profile then the outlet will not allow the device to operate.

When it comes to replay attacks, many different suggestions exist including the use of timestamps/ sequence numbers/ session keys, all suggested by Aravinthan et. al. in [13], or including the use of nonces (numbers used once) making each message unique, as suggested by Xiao et. al., in [53]. An interesting alternative to these approaches is the physical authentication methodology suggested by Mo et. al., in [54].

2) Ensuring Authenticity and Non repudiation

Ensuring authenticity and assuring that we can prove the truthfulness of any allegation regarding transactions within the Smart Grid, are also important for the overall Smart Grid security.

As we already mentioned above, cryptographic hash functions, are nowadays used for ensuring message integrity against deliberate alterations, the same way as checksums are used for detecting inadvertent ones. Similar to cryptographic hash functions, with the exception that they make use of a secret key, are message authentication codes such as HMAC which are amongst the most widely used approaches for achieving authenticity today [41]. Such schemes can also be used within the Smart Grid and so can digital signature schemes that ensure message authenticity via asymmetric encryption. These schemes operate on the premise that every communicating entity has its own public-private key pair. Before sending a message encrypted with the receiver's public key, the sender can hash the message and sign the hash with his private key. Upon receiving the message, the receiver uses his private key to decrypt it and evaluate its hash, and the public key of the sender to decrypt the original hash [41]. The two hashes are then compared, if they match the integrity of the message is proven and so is its authenticity (since no one, other than the sender, could have signed the message with the sender's private key). Meanwhile, non-repudiation can also be achieved if the sender demands a signed acknowledgement from the receiver, verifying he indeed received the message.

Alternative ways for achieving message authenticity and non-repudiation specifically designed for the Smart Grid have also been proposed in recent literature. Below, we present a number of interesting approaches.

Nabeel et.al. in [55], propose the use of Physically Unclonable Function (PUF) modules within meters for achieving strong hardware based authentication of smart meters and efficient key management. Key management guarantees the confidentiality and integrity of messages transmitted from smart meters to the utility and vice versa. PUFs are functions embodied in a physical structure inexpensive to manufacture but impossible to replicate even given the exact manufacturing process. Due to their

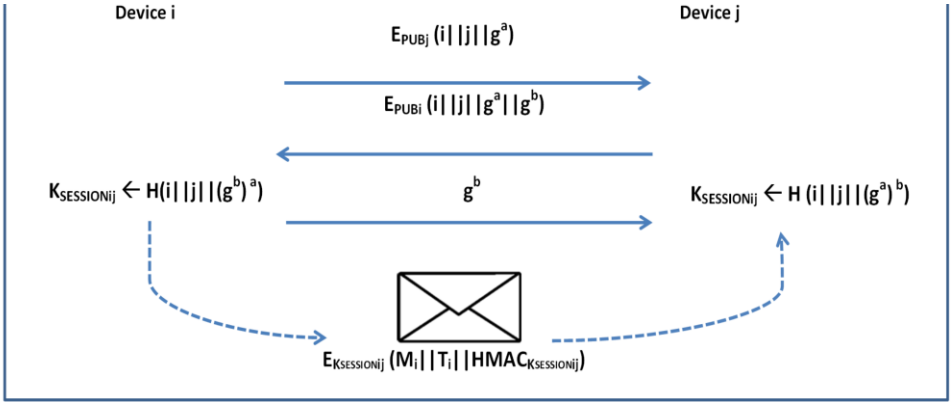


Fig.3 Lightweight message authentication by Fouda et.al. [56].

unclonability they can be described as the hardware analogs of one-way functions. PUFs implement challenge – response authentication, i.e. they receive a stimulus (challenge) that interacts with their physical microstructure (which is considered to be unique due to the intrinsic randomness in the fabrication process of integrated circuits) and react by providing an unpredictable yet repeatable response. PUFs map challenges to responses in a way that cannot be predicted or replicated. Their properties are exploited by the authors along with Pedersen commitment scheme and the Zero-Knowledge proof of knowledge protocol to ensure confidentiality, integrity and authenticity but also protect the secret keys used by Smart Meters.

A different approach towards message authentication, is proposed by Fouda et. al., in [56]. In their paper, the authors introduce a lightweight message authentication scheme as a crucial component of their envisioned framework for secure Smart Grid communications, in which smart meters are expected to be authenticated before they can communicate with other smart meters or smart grid gateways within the Grid. Their proposed scheme based on Diffie-Helman key establishment and hash-based authentication codes, can be simplistically described as follows. Suppose we have two devices i and j wanting to communicate with one another as shown on Figure 3. At the first step of this scheme, i will select a random number a, raise his g in the power of a, encrypt i||j||g^a using j's public key and send this message to j. At the second step j, who has followed the same procedure to produce his g^b, decrypts the message and sends his response i||j||g^a ||g^b back to i encrypted with i's public key. Following these two steps both parties can now evaluate g^{ab} and thus derive their shared session key as the hash H(i||j||g^{ab}) where H is a secure cryptographic hash function.

More recently Lu et. al., in [57], presented an experimental approach on a small scale substation automation prototype aiming to determine whether current security solutions can be applied directly to substation automation systems (SAS) without implications. Commonly used mechanisms and algorithms ensuring authentication and integrity such as RSA, Message Authentication Codes and One-Time Signatures were all evaluated for their ability to ensure message authenticity and integrity while not violating the stringent timing requirements introduced by certain message categories and despite being run on devices with limited processing power. Their results suggest that RSA can be deployed for the protection of messages transmitted across substations, but is not suitable for the transmission of delay-sensitive messages within the substations, whereas MAC-attached and HORS-signed messages demonstrate better delay performance for delay sensitive communications within the substation. Their paper concludes by stressing the need for better suited security solutions for substation automation system communications.

Turning our attention to non-repudiation now, we introduce the work of Xiao et. al. [53], who present a mutual inspection strategy aiming to ensure non-repudiation of smart meter readings within the neighborhood area networks of the Smart Grid. Their strategy involves the installation of two smart meters with one electric wire connecting the sending side with the receiving side. The meter on one side represents the subscriber's reading whilst the meter on the other end represents the provider's reading. These two readings are not always expected to be the same even under normal circumstances due to power losses during energy transfer, synchronization issues and other delays. However, sometimes their inconsistency could suggest meter compromise, jamming or any other sort of attack. In such cases, the readings of the two ends are exchanged and the inconsistency is checked against an acceptable threshold. Should the reading be proved to be the result of compromise, further investigation will begin. The authors compliment their approach with a security analysis and an evaluation that shows the mutual inspection technique can achieve satisfactory performance when combined with an optimized time window method.

Alternatively, Aravinthan et. al., [13] suggest that both the customers and the AMI use unique keys for encryption (once they have authenticated one another using their preassigned public-private key pairs). In addition to that, they suggest that the AMI keeps a log of all transactions for a predefined number of days, so that disagreements can be resolved, though tracing back the events.

C. Ensuring Availability

Usually, when presenting security requirements for a system using the basic CIA triad (Confidentiality, Integrity, Availability) the ordering does not have any specific meaning. However, when it comes to the Smart Grid/Smart Home, some stakeholders suggest that the triad should be prioritized as Availability Integrity Confidentiality (AIC) so that the ordering reflects that availability is the most important goal, followed by integrity and then confidentiality [58].

Potential attacks against the availability of the Smart Grid, were introduced in section III under the general name "Denial of Service attacks" defining attacks aiming to saturate the Grid's resources in order to prevent it from being accessible to its legitimate users. A number of attacks we

introduced were attacks in the physical layer. Such physical layer attacks were the False Data Injection Attacks (countermeasures for which were presented in the section for Ensuring Integrity) and jamming attacks for which countermeasures will be introduced below.

Aravinthan et. al., in [13] suggest that the best way to defend against intentional jamming is to use multiple alternate frequency channels when interference is detected in the current channel. According to them, the AMI and all nodes within it, could be programmed to move though a common, predefined sequence of channels, hardcoded into them, if the default channel suffers from packet losses that are above an acceptable threshold, for a specified period. Every node that gets introduced into the AMI network and authenticated to it, receives this predefined channel-hopping sequence encrypted with the customer's public key. The node then retrieves the sequence by decrypting with the customer's private key and begins communicating in the current channel used. According to the authors, due to the pseudo randomness of the channel-hopping sequence it is considered difficult for the jammer to predict what channel is to be used next, and thus to perform a jamming attack against it.

A similar opinion, seems to be shared by Lee et.al in [59]. In their work, they propose a random spread-spectrum-based wireless communication scheme that prevents eavesdropping and active attacks, while also ensuring protection against jamming. Their proposed scheme, called Frequency Quorum Rendezvous (FQR), introduces the novelty of coordinating two random hopping sequences using a quorum system, a property that guarantees the sender and the receiver will rendezvous within a bounded time. A quorum system is a collection of subsets (or quorums) of a universal set. Each subset of this set has at least one common element with every other subset in it. The suggested model makes use of a Quorum system to construct the hopping sequences, so nodes are bound to meet with one another.

Equally capable to compromise Smart Grid availability are Denial of Service attacks occurring at layers higher than the physical layer. The common practice against those attacks is the deployment of Intrusion Detection Systems (IDS).

Intrusion Detection Systems can be classified into three broad categories [60]: signature-based, specification-based and anomaly-based. A signature-based IDS recognizes intrusions using a black-list of known attack patterns. Whereas a specification based IDS detects attacks using a set of constraints (rules) defining the correct operation of a program or protocol. An anomaly-based IDS, finally, recognizes deviations from what is considered to be normal, by building a model of normal system behavior where any deviation from normal is identified as an intrusion.

According to the authors of [60], signature based IDSs are not suitable for the Smart Grid, due to the fact that they cannot be expected to keep up with the ever increasing number of new attacks that so often manifest themselves within it. On the other hand specification-based and anomaly-based IDSs seem to be quite promising for the Smart Home/Smart Grid environment. An example for each of the two models is presented below.

Faisal et.al. in [60], propose the exploitation of an architecture of anomaly-based IDSs as a second line solution after firewalls, cryptography and authorization techniques, to detect intrusions. Their proposed architecture, involves the placement of three IDSs, in smart meters, data concentrators and the AMI head-end and is used in combination with stream mining techniques to detect anomaly. Specifically, the authors suggest the integration, within or outside each smart meter, of an entity namely a 'security box'. This security box serves as the IDS within the smart meter. IDSs of similar configuration to this one will be installed in the data concentrator and the central system. A serial process describes the operation of this IDS. The data that arrive in the Smart meter, are inserted in the IDS's acceptor module. The acceptor module then forwards them towards a pre-processing unit responsible to generate new data according to some predefined attributes. These new data are then input in the stream mining module algorithm whose outcome goes through the decision maker unit which decides whether an alarm should be triggered or not.

As an alternative to this approach, we present the one proposed by Berthier et.al. in [61]. In their work, they suggest the installation, in key points within the network, of sensors characterized by specification-based intrusion detection mechanisms suitable for detecting intrusions at the application, transport and network layers. The authors detect the expected behavior of meters at the network layer based on the specification of protocols used by these meters. This behavior is then modeled in a simple state diagram representing all possible meter states and transitions from one to the other. A similar state machine for the application layer is presented as well. Each state of these state machines defines a different set of rights and functionalities. Any operation of the meter that does behave in the expected manner and does not abide by the expected set of rules is considered suspicious. This work is complemented by a proof of correctness and a prototype.

D. Ensuring Authorization

The last security goal we focus on, is authorization, i.e. the attestation that no entity within the Smart Home/Smart Grid environment can have access to information or services beyond its authority [22]. Despite, its importance for Smart Home/Smart Grid security the literature on authorization is still limited. Nevertheless, some interesting works have been proposed.

To begin with, we introduce the work of Ruj et. al. in [62]. Their work is based on an architecture consisted of HAN, BAN and NAN gateways in one side and RTUs on the other. Each of the HAN, BAN and NAN gateways in that architecture is responsible to create an aggregate of its received data, encrypt that aggregate using the Paillier encryption scheme and forward it further (HAN to BAN, BAN to NAN and NAN to RTU). Access control in Ruj et.al. scheme is introduced with the use of an attribute-based encryption variant specifically modified by the authors, according to the needs of the Smart Grid. In their paradigm, the RTU collecting data from different units, encrypts those data under a set of attributes before sending them to the data repository they should be kept in. These attributes could be any information related to that data like the source of energy (e.g. solar, wind, fossil fuel), the type of consumer (e.g. individual, company, vehicle), the type of equipment (e.g. dryer, heater), the time of use (e.g. peak, off-peak) etc. In this way, the RTU creates an access policy for the data it places into the data repository. Thus, users wanting to have access to them should first acquire secret keys,

corresponding to the attributes of their interest, from a KDC (key distribution center). In this way, users can only decrypt those data for which they have matching attributes, hence access control is achieved.

Vaidya et.al. in [63] suggest a somewhat different approach for authentication and attribute-based authorization, specific to Substation Automation Systems. Their approach exploits the idea of public key certificates and zero knowledge systems for the purposes of authentication and the idea of attribute certificates (ACs) for authorization. An attribute certificate can be regarded as complimentary to a public key certificate. A public key certificate (PKC) is issued by a certification authority (CA) and is used to verify the identity of its owner, just like a passport. An attribute certificate, on the other hand, is issued by an attribute authority (AA) and is used to characterize or entitle its holder just like a visa gives a person the permission to live/work at a specific place for a particular amount of time. Whenever a user requests access to an IED of a substation, both the user and the IED are authenticated. Following their authentication the substation controller provides the user with his attribute certificate (defining his permissions), signed by the controller using an elliptic curve algorithm. From that moment on every time a user wishes to have access to the IED he sends his signed request, his PKC and his AC that will be used for ensuring authenticity and authorization.

In an alternative approach, Jung et.al. in [64] propose their own model for securing access control within the Smart Grid. Their model leverages XACML (eXtensible Access Control Markup Language) and SAML (Security Assertion Markup Language). The XACML standard defines a declarative language for describing access policies and a processing model describing how to evaluate requests for authorization according to the rules defined in policies. XACML can be characterized as an Attribute Based Access Control system, where the various attributes associated with a user are given as input to the function that determines whether a user can access a particular resource in a particular way. XACML policies are defined according to a set of rules. The process followed to achieve authorization when using XACML could be described as follows: Initially a user (called subject in XACML terminology) requests access to data / services (called resources) from a particular entity within the Smart Grid. The request is routed to an entity known as a Policy Enforcement Point (PEP) which uses XACML language to create a request based on the attributes of the subject, the resource it wants to access and other relevant information. Once the request is created, it is forwarded to a Policy Decision Point (PDP), which communicates with a Policy Store to retrieve any applicable policies. When the potential policies are retrieved, the PDP compares the request them and determines whether access should be granted or not.

Table V provides a summarized view of the approaches presented in this section. For each security goal a number of promising approaches are listed. Different subnetworks within the Smart Home/Smart Grid environment, may exploit different combinations of such approaches towards the fulfillment of each security goal. Table V, is not exhaustive, however it is indicative of the many directions in research when it comes to security solutions for such complex environments as the Smart Home/Smart Grid.

TABLE V
REVIEW OF SECURITY COUNTERMEASURES BY GOAL

Confidentiality and Privacy
▪ Symmetric/Asymmetric Encryption Algorithms (eg. AES/RSA/ECC) ▪ Anonymization ▪ Trusted Aggregators ▪ Homomorphic Encryption ▪ Perturbation Models ▪ Verifiable Computation Models – Zero Knowledge Proof Systems ▪ Data obfuscation
Integrity
▪ Cryptographic Hashing Techniques (eg. SHA-3) ▪ Digital Watermarking ▪ Adaptive Cumulative Sum Algorithm ▪ Installation of known secure PMUs in network ▪ Load Profiling ▪ Timestamps ▪ Sequence Numbers ▪ Session Keys ▪ Nonces
Authenticity
▪ Keyed cryptographic hash functions (eg. HMAC) ▪ Physically Unclonable Functions ▪ Hash based authentication codes ▪ MAC-attached and HORS-signed messages
Non Repudiation
▪ Mutual Inspection with Smart Meters ▪ Unique keys for customer-AMI communication ▪ AMI transaction logging
Availability
▪ Alternate Frequency Channels according to hardcoded sequence ▪ Frequency Quorum Rendezvous ▪ Anomaly Based IDSs ▪ Specification Based IDSs
Authorization
▪ Attribute Based Encryption ▪ Attribute Certificates ▪ Attribute Based Access Control System based on XACML

V. Ongoing Activities In Industry

At present, numerous standards, guidelines and recommendations underpinning Smart Grid Cyber-Security are being developed by international standardisation bodies and industry fora. Major economies across the globe strongly support the efforts for international standards upon which national standards can be built. Their aim is to enhance the prospects for international harmonization of Smart Grid standards, despite the diversity of infrastructure requirements around the world. This section provides a brief overview of prominent contributions of both national and international standardisation bodies and institutions with respect to Smart Grid cyber-security.

A. International level - International Electrotechnical Commission (IEC)

Being the leading international standardisation organisation for the electrical industry, IEC has already defined a series of well-focused ICT standards for the electrical grid, all based on IEC's Service Oriented Architecture for management and automation of energy transmission and distribution systems (IEC 62357). Amongst these, one can find standards for substation automation (IEC 61850), distribution management (IEC 61968), information models and APIs for Transmission Network management (IEC 61970) and standards for information security for power system control operations (IEC 62351 1-8) [65].

For the purposes of promoting the development of Smart Grids, IEC created the Smart Grid Strategy Working Group (IEC SG3) in 2008. IEC SG3, works in collaboration with many ongoing Smart Grid projects and is responsible for the research and creation of standards regarding different aspects of Smart Grids. The five standards we mentioned above, were identified as the core standards of the Smart Grid standards-system by IEC SG3 [66]. These standards seem to be gaining wide acceptance across the globe, leading us to believe that despite regional differences in subjects like Metering, Smart Homes and Buildings, Demand Response plans, EVs and the security and privacy thereof, the world is more or less reaching a consensus on subjects like Smart Grid Architecture, Communication and Communication Security, Common Data Models and Distributed Energy Resources manipulation [67].

B. US - Smart Grid Interoperability Panel (SGIP)

Established by the U.S National Institute of Standards (NIST) in 2009, the Smart Grid Interoperability Panel is a public-private partnership aiming to facilitate the participation of electricity industry stakeholders from 22 industry segments in the Smart Grid standardisation efforts lead by NIST. The primary contributions of the SGIP in the development of standards, are in the area of identifying certification requirements, reviewing use cases, actively educating Smart Grid industry stakeholders on interoperability, overseeing standardisation efforts but also conducting serious efforts for the global interoperability alignment[68].

SGIP is organized in several committees, working groups and task forces. Of specific interest to us, is the Cyber Security Working Group (CSWG), whose goal is to develop an overall cyber security strategy for the Smart Grid [65]. In September 2010, SGIP-CSWG published a three volume report known as "Guidelines for Smart Grid Cyber Security". Volume one, focuses on the description of the high level architecture of the Smart Grid, the categorisation of different interfaces and the identification of cyber security requirements for these interface categories. Volume two, focuses on customer privacy issues. Volume three, provides additional material regarding vulnerabilities within the Smart Grid. At the moment of writing this paper, NIST is seeking public comments for its first revision of the above-mentioned guidelines, with the 24th of December 2013 being the last date for comment submission [69].

C. European Union –Smart Grid Coordination Group (SG-CG)

The European Smart Grid Coordination Group was formed by CEN-CENELEC and ETSI in response to the EU Commission mandate M/490, in order to provide a comprehensive framework on Smart Grids. As part of this framework several reports were released by the end of 2012. Of particular interest to us, are those reports on or relevant to Smart Grid Cyber Security. Such reports are presented below.

- The "First Set of Standards" report [70] provides a list of consistent standards regarding information exchange within the Smart Grid, including an overview of current cyber-security standards like IEC's 62351 parts 1 to 8, IEC 61850-90-5, several IETF RFCs and several ETSI standards.
- The "Smart Grid Reference Architecture" report [71] defines a three dimensional reference architecture of the Smart Grid upon which the analysis of information security use cases identified by the Smart Grid Information Security Working Group of the SG-CG, is based.
- The "Sustainable Processes" report [72] creates a list of use cases describing the functionality of the Smart Grid. These use cases are used by the Smart Grid Information Security Working Group for the purposes of risk and threat analysis but also for the assessment of proposed methods for ensuring Cyber Security within the Smart Grid.
- Finally, the "Smart Grid Information Security" report [58], provides a high level guidance on how different standards apply to Smart Grid information security, data protection and privacy by defining five security levels aiming to bridge electrical grid operations and information security, and two data protection levels for the classification of information.

D. China

For the purposes of efficiently setting up the national Smart Grid standards-system a steering group of members of the China Electricity Council (CEC), Standardisation Administration China (SAC), Energy Bureau and State Grid Corporation China (the largest state-owned electric utility in the world) was established in 2010. By the end of that year, two important reports : the "Smart Grid technical standard plan" and "Smart Grid key equipment R&D plan" were formally released, however these reports are not available to the public [65]. What is publicly available, is the "Framework and Roadmap for Strong & Smart Grid Standards" report, released in 2010 by State Grid Corporation. Within this report a list of core standards is presented, and a standards gap analysis is performed. The list of standards, also known as First Batch of SGCC Smart Grid Standards [66], strongly refers to international standards (especially IEC standards such as those we have already mentioned, including IEC 62351 for security), but also includes national standards and guidelines defined by the corporation itself. China's heavy interest on Smart Grid cyber security, is expected to reflect on its cyber security market which is estimated to reach USD 50 billion by 2020 [74].

E. Japan

In order to promote the development of Smart Grid standardisation, the Ministry of Economy, Trade and Industry in Japan, formed a strategic working group, the Smart Grid Standardisation Study Group, in August 2009. By January 2010, this group issued a report outlining its principal initiatives. These initiatives included among others the implementation of IEC's roadmap of standards (including cyber-security standards), close collaboration with NIST, CENELEC and other standardisation bodies and promotion of related policy studies [66]. Japan, also commissioned four large scale pilot projects - Kyoto Keihanna district,

Yokohoma city, Toyota city and Kitakyushu city - to study different aspects of the Smart Grid.

F. Australia

In June 2011, the Australian Department of Resources, Energy and Tourism commissioned Standards Australia and Rare Consulting to identify deficiencies in the Australian set of Smart Grid standards. This effort resulted in the "Australian Smart Grid Standards RoadMap" [75] published in June 2012. Within this Standards RoadMap a collection of foundation (national and international) standards can be found. Of specific interest to us are those regarding Smart Grid Cyber Security. For Smart Grid Cyber Security, Standards Australia, suggested the adaptation of existing international standards such as IEC/TS 62351 parts 1-8, ISO/IEC 27001, ANSI/ISA-99 and ITU-T in a way that best meets the requirements of the Australian electricity industry. The report suggests NIST's completed work as a good primary source for security guidelines while underlying the importance of conformity of potential cyber security standards with the Australian Privacy legislation.

VI. Further Challenges And Future Directions

Thus far, we have identified illustrative scenarios of interaction amongst entities of the Smart Home and the Smart Grid. We have analyzed potential cyber and physical security threats, studied them in terms of the security goals they violate and evaluated their impact on the grid. Likewise, we have also reviewed the existing literature suggesting promising solutions and proposing countermeasures to help us achieve the security goals we set for our system.

To complete our overview of Smart Home/Smart Grid security, open challenges and directions for future research are described below and are summarized in Table VI.

- Establishing a universal standardisation framework for secure communication within the Smart Home and the Smart Grid.

As we have mentioned in section II, the Smart Grid is a complex, heterogeneous network of networks whose success largely depends on the continuous communication of its entities. With each sub network in the Smart Grid, having its own equipment, its own requirements and its own capabilities, ensuring the interoperable and uninterrupted communication between Smart Grid entities becomes a rather intimidating task. Hence, a universal standardization framework developing guidelines and including protocols and model standards for the secure communication between the entities belonging to different sub networks within the Smart Grid/Smart Home environment, is considered essential. In establishing this universal standardization framework, Smart Home/Smart Grid communicating entities should be regarded both as stand-alone but also as part of the entire Grid. Such an approach could contribute to the successful meeting of the unique requirements posed by specific Smart Grid subsystems.

- Establishing authorities to evaluate the conformance of Smart Home/Smart Grid industry to the different voluntary standards.

Most standards created for the Smart Grid, are voluntary, i.e. they have not been mandated by governments or business contracts. However, this cannot justify the lack of a coordinated approach for monitoring the extend at which the industry has adopted those standards. Having authorities responsible to evaluate the level of conformance of the industry to those voluntary standards could prove to be particularly valuable in helping regulators decide if a standard is effective or if any changes are needed for its improvement.

- Establishing new/altering old protocols with respect to the Smart Grids unique requirements.

The stringent requirements of some of the Smart Grids sub networks are part of the reason why the Smart Grid demands the redesigning of existing protocols, or the creation of new ones. Smart Home/Smart Grid standards, should be characterized by the flexibility needed for successfully meeting their functional requirements. Let's consider IEC61850 standard for substation communication. This standard, in order to be able to ensure that critical messages for a substation (such as an islanding command for fault isolation) will not experience delays of more than 3ms, thus putting the entire substation equipment at risk, defines three deferent protocol stacks (TCP/IP , UDP/IP and Application to MAC layer). In fact, any protocol used in the Smart Grid, for authentication, secure communication, data aggregation or even routing of data, should be designed to meet the Smart Grid's unique requirements.

- Establishing new metrics for the evaluation of the cyber security mechanisms and solutions suggested.

In order for Smart Grid authorities to be able to evaluate the extent to which a proposed security mechanism meets the security goals set, well defined metrics have to be agreed upon by the electricity industry. Such a development will enable authorities to compare amongst suggested solutions on a common basis, thus making the best decisions when it comes to which mechanisms or solutions should be standardized, or used in combination to one another. Such metrics could also allow for a better evaluation of the expected outcomes of an investment on a particular security mechanism.

- Evaluating the security implications arising from the introduction of PHEVs/PEVs and Distributed Energy Resources as part of the Smart Grid and the Smart Home.

As our grid becomes smarter, new entities are expected to be incorporated in it. Plug in electric vehicles (hybrid or not) and distributed energy resources (in Smart Homes or as part of the Smart Grid) are two categories of entities of particular interest that have received very limited attention up to now [64]. We believe that additional research studies should be carried out on the security implications raised by their incorporation. Furthermore, new methods of guaranteeing their operation could be closely observed so that any abnormalities will be detected and addressed before they become large-scale problems.

- Establishing a legal framework specific to Smart Grid privacy.

For the purposes of ensuring privacy within the Smart Grid, a legal framework specific to privacy in the Smart Grid has to be implemented. Such a framework is expected to define accurately: how sensitive data should be collected; who is supposed to collect them; for how long and where can they be stored; under what circumstances is the owner expected to provide his consent before his data can be disclosed etc….

- Establishing new aggregation schemes that do not involve a trusted aggregator.

Relative to the above challenge, another challenge that has to do with privacy is establishing new schemes for aggregating data without involving a trusted aggregator. Such schemes are expected be able to produce a summary of a given input, without being able to understand that input and without introducing further delays in the entire process that could actually threaten the grid's stability.

- Establishing new techniques for facing jamming attacks.

As our literature review revealed, spread spectrum techniques are prominent when it comes to facing jamming attacks against resource availability. Despite their effectiveness however these techniques introduce an overhead in the network which could potentially affect the timely delivery of critical messages in the Smart Grid, resulting in instabilities. We thus need new systems securing us from jamming attacks without burdening the network with extra overhead.

- Establishing Intrusion Detection, Intrusion Prevention and Intrusion Recovery Systems specifically for the Smart Grid.

Denial of Service Attacks and Distributed Denial of Service Attacks are amongst the most dangerous attacks against the Smart Grid. If such attacks, threatening the Smart Grid's availability, are not detected and quarantined early enough, we could risk losing the functionality of our most critical infrastructure. Early detection and prevention of attacks, specifically tailored for the Smart Grid, is therefore another challenge. New methods for risk assessment not based on prior knowledge and not introducing further delays into the overall system operation are exactly what we need. Also, in the case an attack is not detected and prevented, appropriate Intrusion Recovery techniques must be in place to ensure graceful degradation.

- Designing systems that can support the logging of information for the purposes of audit controls and forensics analysis.

For the Smart Home/Smart Grid environment, to ensure accountability and non-repudiation, it is imperative that it has the ability to provide undeniable evidence proving the existence and details of any transaction. Such information should be kept in logs situated all across the Smart Grid. The data collected in such logs is to be used for the purposes of forensic analysis as well as for resolving legal disputes. Every modification on this data has to be carried out by an authenticated entity and it will be logged into the system. Special care should be given in the designing process, so as to avoid the introduction of too much overhead into this logging process.

- Establish more key management techniques specifically for the AMI and the Wide Area Measurements Network.

As AMI, we define the architecture that enables two way communication between the Smart Meters and the utility. The AMI enables the utility to receive near-real time information regarding the energy consumption of premises; and the consumer to receive near-real time pricing signals and feedback regarding his energy consumption. The messages sent by the utility to Smart meters are critical since they define how the operation of appliances within premises is scheduled. The messages sent by the Smart meter to the utility are also considered to be critical, since they are used by the utility for demand prediction and demand-supply management.

Critical messages are also exchanged within another type of network in the Smart Grid, the Wide Area Measurement Network. Such a network consists of many sub-networks equipped with advanced metering technology (such as PMUs). Their purpose is to enhance the operator's real-time situational awareness through regular reports of the grid's current state. The measurements collected from different phasor-measurement sites reveal abnormalities and trigger immediate action to protect the grid's equipment in cases of emergency thus maintaining their integrity is of primary importance for the overall functioning of the grid.

Despite the significance of these messages however, to date, the majority of key management schemes proposed for securing communications within the Smart Grid, address the establishment of keys for the communicating entities within the SCADA systems only. In fact, few research studies have been carried out on key management schemes for the AMI entities and the Wide Area Measurement Network entities. For this reason, we believe additional research should be focused on the creation of key establishment schemes specifically designed for the AMI and the Wide Area Measurement Networks.

TABLE VI
FUTURE CHALLENGES AND OPEN DIRECTIONS

CHALLENGES OF REGULATORY NATURE
▪ Standardisation framework for secure communication within the SH/SG environment. ▪ Authorities and criteria to evaluate conformance to standards. ▪ New metrics for evaluation of cyber-security mechanisms ▪ Adaptation of old/Creation of new protocols to meet SG constraints and requirements. ▪ Legal Framework on SG privacy.
TECHNICAL CHALLENGES
▪ Evaluation of security implications of PEV/DER integration within SH/SG. ▪ New aggregation schemes without trusted aggregators. ▪ New techniques against jamming attacks with less overhead than spread spectrum. ▪ New IDSs specifically for SH/SG environments. ▪ Support of logging functionality for user-involving transactions. ▪ New key management schemes for AMI and WAMS.

VII. Concluding Remarks

Sooner than later, the traditional grids of today will evolve into the electrical grids of tomorrow. An evolution, that holds the promise of a robust, effective and efficient energy infrastructure for the future, is known as the Smart Grid. Little by little every entity within today's grid, even our home, will undergo its own transformation towards the smartening of our electrical grid with the benefits of this evolution being indisputable for both the utilities and the consumers. As an indispensable part of this evolution, we recognize the transformation of our homes into the Energy Aware Smart Homes of the future. Homes, that will be in constant interaction with the utilities in an effort for better energy management. Of vital importance, during this redesigning of our homes and grid, is ensuring security and privacy. A task that becomes more intimidating, as new technologies get incorporated into these already complex infrastructures.

In this paper we presented dangers looming under some of the most illustrative scenarios of interaction amongst entities of the Smart Home/Smart Grid environments, evaluating their impact on the entire grid. In addition to that, we conducted a review of recent literature on potential solutions and countermeasures, aiming to identify approaches for prevention or defense against attacks that could help us achieve the security objectives we set for both the Smart Home and the Smart Grid. Smart Grid cyber security standardisation efforts across the globe were also outlined, whereas a section devoted to open challenges and future directions for research served as the conclusion of our paper. Through that section, we suggested several topics that need to be further investigated.

The heterogeneity of the Smart Home/Smart Grid environment does not leave room for "one-size-fits-all" security solutions making Smart Home/Smart Grid security a challenging yet promising research field for the future.

References

[1] Yih-Fang Huang; S. Werner, Jing Huang; N. Kashyap, V. Gupta , "State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid," *Signal Processing Magazine, IEEE* , vol.29, no.5, Sept. 2012, pp.33-43

[2] CEN/CENELEC/ETSI Joint Working Group, "Final report on Standards for Smart Grids", [Online] Available : http://www.etsi.org/WebSite/document/Report_CENCLCETSI_Standards_Smart%20Grids.pdf

[3] U.S. Department of Commerce, National Institute of Standards and Technology (2010,January) NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 [Online] Available : http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

[4] Shui Bin; Li Jun, (2012,July),Research Report E129, Building Energy Efficiency Policies in China: Status Report [Online]Available : http://www.aceee.org/research-report/e129

[5] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A Review of Smart Homes—Past, Present, and Future," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, Nov. 2012, pp. 1190–1203

[6] W. Wang and Z. Lu, (2013) , "Cyber security in the smart grid: survey and challenges," Computer Networks, Computer Networks, vol. 57, issue 5, 7 April 2013, pp. 1344-1371

[7] Xu Li; Xiaohui Liang; Rongxing Lu; Xuemin Shen; Xiaodong Lin; Haojin Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *Communications Magazine, IEEE* , vol.50, no.8, August 2012,pp.38-45

[8] Young-Jin Kim; M. Thottan, V. Kolesnikov, L. Wonsuck, "A secure decentralized data-centric information infrastructure for smart grid," *Communications Magazine, IEEE* , vol.48, no.11, November 2010, pp.58-65

[9] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, Dec. 2011,pp. 796–808,.

[10] ENISA (2012, June) Annex I. General Concepts and Dependencies with ICT of ENISA study 'Smart Grid Security: Recommendations for Europe and Member States [Online] Available : http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ict-inderdependencies-of-the-smart-grid/

[11] IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads," *IEEE Std 2030-2011* , pp.1-126, Sept. 10, 2011

[12] OpenHAN Task Force of the Utility AMI Working Group, (2008,August), Utility AMI 2008 Home Area Network System Requirements Specification,Version 1.0 [Online] Available : http://osgug.ucaiug.org/sgstore/Shared%20Documents/UtilityAMI%20HAN%20SRS%20-%20v1.04%20-%20080819-1.pdf

[13] V. Aravinthan, V. Namboodiri, S. Sunku, W. Jewell, "Wireless AMI application and security for controlled home area networks," *Power and Energy Society General Meeting, 2011 IEEE* , pp.1-8, 24-29 July 2011

[14] E Source Companies LLC, (2003) ,Demand Response 101 : The Basics of Utility Load Management Programs, [Online] Available : http://www.mlgw.com/images/content/files/pdf/peakalertsDemandResponse101.pdf

[15] K. Kok, , S. Karnouskos, D. Nestle, A. Dimeas, A. Weidlich, C. Warmer, P. Strauss, B. Buchholz, S. Drenkard, N. Hatziargyriou, V. Lioliou (2009):Smart Houses for a Smart Grid, *20th International Conference on Electricity Distribution CIRED*, Prague, June 2009.

[16] CITIPOWER, Powercor (2013), Load Shedding, [Online] Available : http://www.citipower.com.au/Electricity_Networks/Power_Outages_Explained/Load_Shedding/

[17] Darby, Sarah.(2006). "The effectiveness of feedback on energy consumption." *A Review for DEFRA of the Literature on Metering, Billing and direct Displays* 486 .

[18] W. Kempton, L. Layne, 'The consumer's energy analysis environment', Energy Policy, vol. 22, no. 10, 1994,pp. 857-866.

[19] A. Kamilaris, A. Pitsillides, M. Yiallouros, Building Energy-aware Smart Homes using Web Technologies, Journal of Ambient Intelligence and Smart Environments (JAISE), (DOI 10.3233/AIS-130201, IOS Press), 2013, pp.161–186.

[20] BSOL Batteriesysteme GmbH , Smart Grid Solutions, [Online] Available : http://www.bsol.de/files/TechNotes/Smart%20Grid%20-%20A3.pdf

[21] A. Kamilaris, Y. Tofis, C. Bekara, A. Pitsillides, and E. Kyriakides, "Integrating Web-Enabled Energy-Aware Smart Homes to the Smart Grid," *International Journal On Advances in Intelligent Systems*, vol. 5, 2012, pp. 15–31.

[22] G. Mantas, D. Lymberopoulos, N.Komninos, "Security in Smart Home Environment", in A. Lazakidou, K. Siassiakos, & K. Ioannou (Eds.), *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications, Hershey, PA: Medical Information Science*, 2010, ch.10, pp.170-191.

[23] F.M. Cleveland, , "Cyber security issues for Advanced Metering Infrasttructure (AMI)," *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE* , pp.1,5, 20-24 July 2008

[24] Computer Security Division Information Technology Laboratory National Institute of Standards and Technology (2004, February), Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, [Online] Available : http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[25] The Smart Grid Interoperability Panel – Cyber Security Working Group, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security - All Volumes, September. 2010.

[26] I. Ghansah , (2009). Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risks California Energy Commission, PIER Energy-Related Environmental Research Program.CEC-500-2012-047.

[27]S. Saponara and T. Bacchillone, "Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid," *Journal of Computer Networks and Communications*, pp. 1–19, 2012.

[28] U.Greveler, , B. Justus, and D. Loehr. "Multimedia content identification through smart meter power usage profiles." *Computers, Privacy and Data Protection* ,2012.

[29] J. Liu, Y. Xiao, S. Member, S. Li, W. Liang, and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," vol. 14, no. 4, 2012, pp. 981–997.

[30] Xantus Consulting International, (2009), White Paper for NIST CSWG: Cyber Security Requirements for Business Processes Involving Home Area Networks (HAN), [Online] Available : http://xanthus-consulting.com/Publications/documents/HAN_Business_Processes_Cyber_Security_Requirements.pdf

[31] Blumenfield L, (July, 2003), "Dissertation Could Be Security Threat: Student's Maps Illustrate Concerns About Public Information", Washington Post [Online] Available : http://seclists.org/isn/2003/Jul/28

[32] F.Tony, and J. Morehouse. "Securing the smart grid: next generation power grid security". Elsevier, 2010.

[33] Cyber-Physical Systems Security for Smart Grid Future Grid Initiative White Paper (2012,February), PSERC, [Online] Available : http://www.pserc.wisc.edu/documents/publications/papers/fgwhitepapers/Govindarasu_Future_Grid_White_Paper_CPS_Feb2012.pdf

[34] B. Bencsáth, G. Pék, L. Buttyán, M. Felegyhazi, sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks, CrySyS Lab Technical Report, No. CTR-2012-05-31, 2012.

[35] Duqu Trojan Questions and Answers (2011, October) SecureWorks Counter Threat Unit Research Team, DELL,[Online]. Available : http://www.secureworks.com/cyber-threat-intelligence/threats/duqu/

[36] R. Langner (2011, March) , Cracking Stuxnet, a 21st century cyber weapon, TED Talks, [Online],Available : http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html

[37] M. A. Rahman and H. Mohsenian-Rad, "False Data Injection Attacks with Incomplete Information Against Smart Power Grids," *in Proc. of IEEE Conference on Global Communications* (GLOBECOM'12), Anaheim, CA, December 2012.

[38] Y. Liu, P. Ning, and M.l K. Reiter. False data injection attacks against state estimation in electric power grids, *in Proc. of the 16th ACM conference on Computer and communications security*. ACM, New York, NY, USA, pp.21-32, 2009.

[39] D. Grochocki, , J.H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cárdenas, , & J. G. Jetcheva, (2012, November). AMI Threats, Intrusion Detection Requirements and Deployment Recommendations. In Proceedings of the 3rd IEEE International Conference on Smart Grid Communications (SmartGridComm), Tainan City, Taiwan.

[40] F. Skopik., Z. Ma, T. Bleier, & H.Grüneis. A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures. *International Journal of Smart Grid and Clean Energy*, no.1, 2012, pp. 22-28.

[41] J. Benoit, "An Introduction to Cryptography as Applied to the Smart Grid," Cooper Power Systems, February 2011.

[41] "Cryptographic Key Management for the Advanced Metering Infrastructure." [Online].Available http://www.smartenergyuniverse.com/spotlight/13389-cryptographic-key-management-for-the-advanced-metering-infrastructure
[43] M. Jawurek, F. Kerschbaum, and G. Danezis, "SoK : Privacy Technologies for Smart Grids – A Survey of Options ."

[44] C. Efthymiou, G. Kalogridis, , "Smart Grid Privacy via Anonymization of Smart Metering Data," *Smart Grid Communications (SmartGridComm),* pp.238,243, 4-6 Oct. 2010

[45] T. Jeske, "Privacy-preserving Smart Metering without a Trusted-third-party", in Proc. SECRYPT 2011, Seville, Spain, 18 - 21 July, 2011, pp.114-123.

[46] J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In S. Cimato, C. Galdi, and G. Persiano, editors, SCN, volume 2576 of Lecture Notes in Computer Science, pages 268–289. Springer, 2002.

[47] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," International Journal of Security and Networks, vol. 6, no. 1, 2011,pp. 28-39.

[48] G.Acs, , & C. Castelluccia, (2012). Dream: Differentially private smart metering. arXiv preprint arXiv:1201.2531.

[49] D.Varodayan, , & A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage". *in* IEEE *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2011, pp. 1932-1935.

[50]S. Bhattarai, G. Linqiang, and Y. Wei, "A novel architecture against false data injection attacks in smart grid," in *2012 IEEE International Conference on Communications (ICC)* ,10-15 June 2012 , pp. 907 – 911.

[51] Y. Huang, H. Li, K. A. Campbell, and H. Z, "Defending false data injection attack on smart grid network using adaptive CUSUM test," *45th Annual Conference on Information Sciences and Systems*. IEEE, 23-25 March 2011, pp. 1–6.

[52] Giani, A.; Bitar, E.; Garcia, M.; McQueen, M.; Khargonekar, P.; Poolla, K., "Smart grid data integrity attacks: characterizations and countermeasuresπ," 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm),17-20 Oct. 2011, pp.232-237

[53]Z. Xiao, Y. Xiao, and D. H.-C. Du, "Non-repudiation in neighborhood area networks for smart grid*," Communications Magazine, IEEE*, vol. 51, no. 1, pp. 18 – 26, 2013

[54] Yilin Mo; T.H-H Kim; K.Brancik,; D.Dickinson,; L. Heejo; A.Perrig,; B.Sinopoli, "Cyber–Physical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE* , vol.100, no.1, Jan. 2012, pp.195-209.

[55]M. Nabeel, S. Kerr, and E. Bertino, "Authentication and key management for Advanced Metering Infrastructures utilizing physically unclonable functions," *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, November 2012, pp. 324–329

[56] M.M.Fouda,; Z.M Fadlullah,.; N. Kato; Lu Rongxing; Shen Xuemin, "A Lightweight Message Authentication Scheme for Smart Grid Communications," *IEEE Transactions on Smart Grid* , vol.2, no.4, pp.675-685, Dec. 2011

[57]X. Lu, W. Wang, and J. Ma, (2012) "Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems," *International Journal of Distributed Sensor Networks*, pp. 1–13, 2012

[58] CEN/CENELEC/ETSI Joint Working Group, "Smart Grid Information Security", [Online] Available : http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_security.pdf, 2012

[59] E.-K. Lee, S. Y. Oh, and M. Gerla, (2011,February) "Frequency quorum rendezvous for fast and resilient key establishment under jamming attack," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 14, no. 4, February 2011,pp. 1-3.

[60] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Using Intrusion Detection System with Data Stream Mining" in *Intelligence and Security Informatics Pacific Asia Workshop, PAISI 2012, Kuala Lumpur, Malaysia, May 29, 2012, ProceedingsSeries: Lecture Notes in Computer Science*,vol.7299, pp. 96–111

[61] R. Berthier and W. H. Sandersm, "Specification-Based Intrusion Detection for Advanced Metering Infrastructures," *2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing*, December 2011, pp. 184–193

[62] S. Ruj, , A. Nayak, , & I. Stojmenovic, "A security architecture for data aggregation and access control in smart grids", arXiv preprint arXiv:1111.2619, 2011

[63] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for Smart Energy Home Area Networks," *2011 IEEE International Conference on Consumer Electronics (ICCE)*, no. 1, pp. 787–788, Jan. 2011.

[64] M.Jung; G.Kienesberger; W.Granzer; M. Unger; W.Kastner, "Privacy enabled web service access control using SAML and XACML for home automation gateways", *2011 International Conference for InternetTechnology and Secured Transactions (ICITST),* pp.584-591, 11-14 Dec. 2011

[65] SGEM, "Smart Grid Standardization Analysis", [Online] Available : https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDAQFjAA&url=http%3A%2F%2Fwww.cleen.fi%2Fen%2FSitePages%2Fpublicdeliverables.aspx%3FfileId%3D1031%26webpartid%3Dg_1449a1fa_9f05_4750_900e_6294262dcbd4&ei=Plm3Uun-AoKctQbcwYD4CA&usg=AFQjCNEmCprqOVuKDXPGsu4L6hQbgrxKQA&sig2=NMExM9fG7NeZqboPhlcucA

[66] State Grid Corporation of China, "SGCC Framework and Roadmap for Strong and Smart Grid Standards", [Online] Available : http://esci-ksp.org/?publication=sgcc-framework-and-roadmap-for-strong-smart-grid-standards

[67] A. Rolf, Presentation "International Smart Grid Standardization Hype, Competition of Standards or useful cooperation?" (2011), [Online] Available:http://www.epcc-workshop.net/archive/2011/Presentations/TI%202%20Apel%20(p).pdf

[68] Smart Grid Interoperability Panel Official Website, [Online] Available, http://www.sgip.org/about_us/#SGIP-mission-vision

[69] "NIST Requests Public Comments on Revised Guidelines for Smart Grid Cybersecurity" (2012), [Online] Available : http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=3773.

[70] CEN/CENELEC/ETSI, "First Set of Standards" [Online] Available : http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_first_set_of_standards.pdf

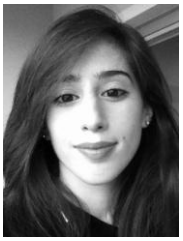
[71] CEN/CENELEC/ETSI, "Smart Grid Reference Architecture", [Online] Available : http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf

[72] CEN/CENELEC/ETSI, "Sustainable Processes" [Online] Available : http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_sustainable_processes.pdf

[73] IEEE Standards Association, Smart Grid Research: Cyber Security, [Online] Available : http://www.techstreet.com/ieee/products/1864660

[74] J. Lazar , M. McKenzie,"Australian Standards for Smart Grids – Standards Roadmap" (2012), [Online] Available : http://www.standards.org.au/Documents/120904%20Smart%20Grids%20Standards%20Road%20Map%20Report.pdf

Dr. Nikos Komninos received his Ph.D. in Information and Network Security in 2003 from Lancaster University (UK). He is currently a Lecturer (Assistant Professor) in Cyber Security at the Department of Computer Science, City University London. Prior to his current post, he has held teaching and research positions in the University of Cyprus, Carnegie Mellon University in Athens (Athens Information Technology), University of Piraeus, University of Aegean, and University of Lancaster. Between 2003 and 2007, he was honorary research fellow with the Department of Communication Systems at the University of Lancaster. He was also a visiting faculty at the University of Cyprus and faculty member at Carnegie Mellon University in Athens (Athens Information Technology), between 2005 and 2011. Part of his research has been patented and used in mobile phones by Telecommunication companies; in crypto-devices by Defense companies; and in healthcare applications by National Health Systems. Since 2000, he has participated in a large number of European and National R&D projects, as a researcher or principal investigator in the area of information security, system and network security. He has authored or co-authored more than fifty journal publications, book chapters and conference proceedings publications in his areas of interest. He has been invited to give talks in conferences and Governmental Departments, as well as to train employees in Greece and UK businesses.



Eleni Philippou received her Bachelor degree in Computer Science from the University of Cyprus in 2013, ranking 3rd overall in her class. As of September Eleni is currently pursuing an MSc in Information Security at the University College London. Her research interests include Cyber Security of Critical Infrastructures, Smart Grids and Smart Homes.

Dr. Andreas Pitsillides (M'90, SM'05) received the B.Sc. degree (Hns) in Electrical Engineering from the University of Manchester Institute of Science and Technology, UMIST (Manchester, U.K.) and the PhD in Broadband Networks at the Swinburne University of Technology (Melbourne, Australia) in 1980 and 1993 respectively. He is a Professor in the Department of Computer Science, University of Cyprus, and heads NetRL, the Networks Research Laboratory. His research interests include communication networks (fixed and mobile/wireless), the Internet- and Web- of Things, the Smart Grid, and Internet technologies and their application in Mobile e-Services, especially e-health, and security. He has a particular interest in adapting tools from various fields of applied mathematics such as adaptive control theory, nature inspired techniques, and computational intelligence to solve problems in communication networks. Published over 230 referred journal papers in flagship journals (e.g. IEEE, Elsevier, IFAC, Springer), international conferences and book chapters, and 2 books (one edited), participated in over 30 European Commission and locally funded research projects as principal or co-principal investigator, presented keynotes, invited lectures at major research organisations, short courses at international conferences and consulting and short courses to industry, and serves/served on several journal and conference executive committees. (http://www.NetRL.ucy.ac.cy).